Market Report

2016 Next-gen Infrastructure Security Report

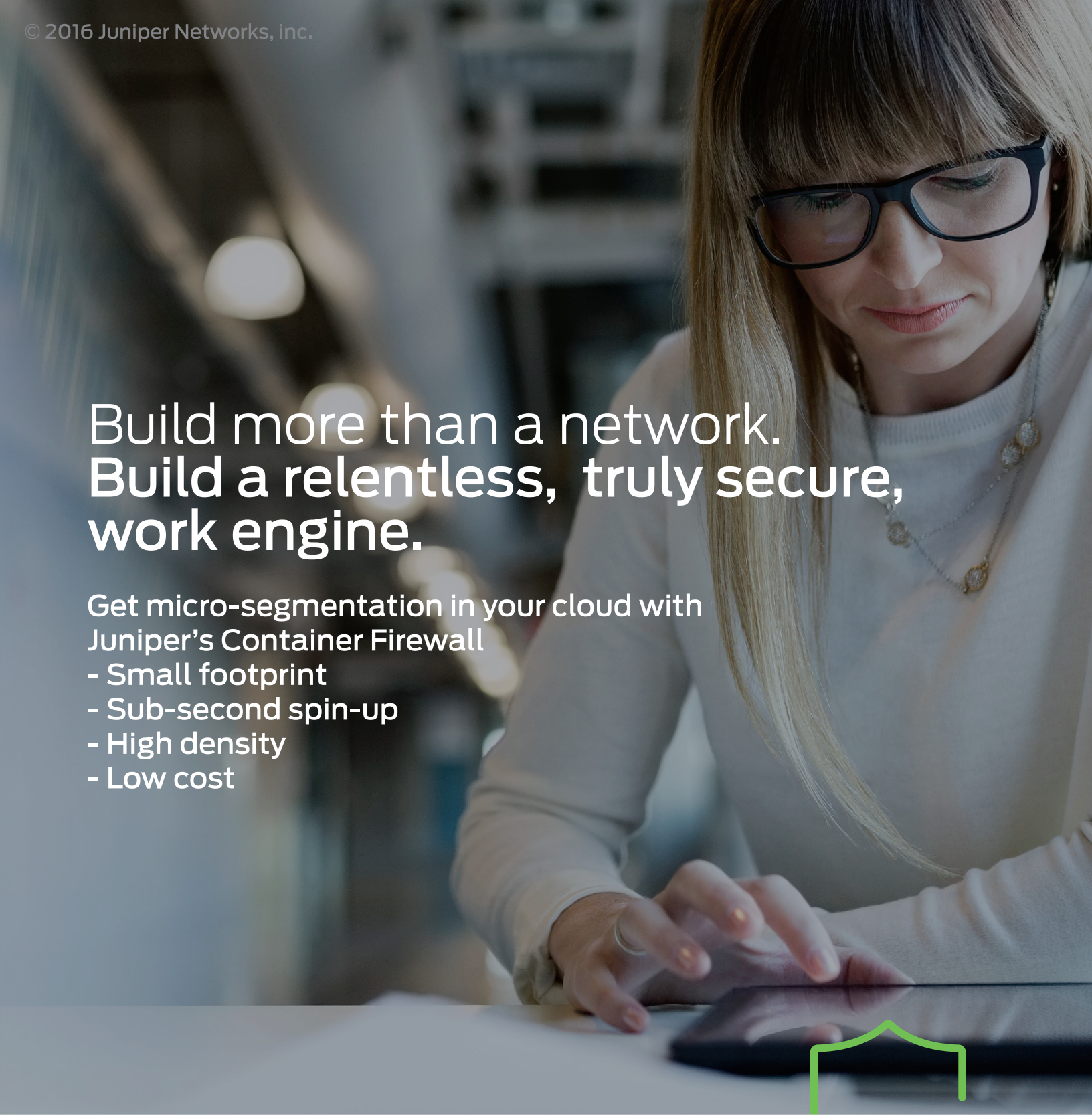
The Trusted News and Resource Site for SDx, SDN, NFV, Cloud and Virtualization Infrastructure

Table of Contents

market summary

See Software Defined Networking Security out front
www.nuagenetworks.net/security-out-front

nuagenetworks
From Nokia



Build more than a network. **Build a relentless, truly secure, work engine.**

Get micro-segmentation in your cloud with Juniper's Container Firewall

- Small footprint
- Sub-second spin-up
- High density
- Low cost

JUNIPER NETWORKS

SECURITY

Intro: Trends in Next-gen Cloud Infrastructure Security

The cloud model of delivering IT services and infrastructure, coupled with extensive connectivity to the Internet, has brought an unprecedented level of security challenges. This means the cybersecurity and security solutions landscape is in constant flux and that a wide range of next-gen infrastructure security technology is needed.

Over the past year, we have seen threat factors, motivated by financial gain, competitive advantage, political aspirations, etc., continue to escalate the scale and sophistication of their attacks. They are exploiting old and new attack vectors created by all the people, services and Internet of things (IoT) that are now connected and communicating with one another. They are also taking advantage of the highly dynamic environments of today's networks, which contain a mix of encrypted traffic (SSL/TLC), virtualized services and apps, and cloud platforms, to hide and propagate undetected.

On the flip side, we have seen progressively intelligent counter measures introduced to try to beat the attackers at their own game. Today's security paradigm assumes attackers are in (or going to get into) the network (the defensible perimeter has long been dead). New approaches are taking the fight to them (in the wild, on the darknet, etc.) and making it harder to get anything of value, by trusting nothing, locking resources down, and obviating critical information.

There are many different types of infrastructure security solutions available – figuring out the right ones is no easy task. Our 2016 Next-gen Infrastructure Security Report is designed to provide an overview of technology focusing on cloud and infrastructure security. This report aims to give readers visibility into some of the security challenges and opportunities emerging within the SDx infrastructure and provide information on a sampling of the advancements being made by cybersecurity technologies and solutions on the market.

This report covers:

- Cybersecurity landscape – a look at trends in the marketplace
- Drivers for change – why SDx security is increasing in importance
- An introduction to SDx infrastructure security
- Capabilities to look for in next-gen cloud and SDx infrastructure security solutions
- Challenges in deploying and executing infrastructure security solutions
- Benefits of security technology
- Examples of early innovations and use cases for SDx security technologies and products

In analyzing the market, we include the results[1] from research the SDxCentral team conducted within the SDx community. The report also includes detailed technology solution profiles based on submissions by key vendors in this space. Thank you for downloading the report. We hope you find it a useful resource, as you look to understand and adopt SDx infrastructure security technologies.

Cloud Security Threats and Drivers

Cybersecurity has been in the news a lot lately, as threats grow and data breaches occur on a regular basis. There is also a global debate on what cybersecurity really means to us and our civil liberties. How far are we willing to go to stay safe? What are we willing to sacrifice? What is paramount to protect?

Recently, we have seen companies push back on government requirements, particularly in the United States, as companies question the implications of some of the government's 'asks' under the guise of national security (e.g. **Apple refused to write code to unlock its phones**; **Microsoft sued the Justice Department over requests for customer data**).

1 Survey ran on SDxCentral in the month of April 2016. There were 97 respondents – 27% enterprises, 21% service providers, 40% technology vendors, and 12% other.

market summary

The bottom line is that security has never been higher on everybody's minds and priority list.

Let's delve deeper into some of the major drivers for security technology.

Regulatory Landscape Impact

Beyond wanting to protect oneself from the disruption and costs (both hard and soft) of cyberattacks, organizations are driven by compliance requirements. Last year, European courts invalidated Safe Harbor after revelations that U.S. agencies (primarily the NSA) were collecting information on all sorts of individuals (a.k.a. the Snowden Effect), which called into question the integrity and privacy of the personal information handled and stored by companies outside Europe. This matters, because an inability to adhere to relevant rules and regulations can greatly impact the bottom line. The Information Technology and Innovation Foundation estimates that U.S.-based cloud providers may lose as much as $35 billion over the next three years due to fears they cannot maintain the security of their information. According to a survey by the **Cloud Security Alliance**, 10% of non-U.S. companies have already canceled contracts with American cloud providers, after the court ruling on Safe Harbor.

There are a host of industry and country/regional regulations designed to assist organizations in mitigating their exposure to risk. Most have provisions in them designed to ensure organizations are implementing measures to protect sensitive data and personally identifiable information (PII); many can inflict penalties or fines when organizations are found to be lacking appropriate protective measures; some mandate the reporting incidents/breaches. (Note: IDC found that 52% of corporate information that requires protection [e.g., corporate financial data, PII] is not currently protected.) It is important to note that many of these regulations are not clear cut, providing general guidelines that can be up to interpretation by an organization.

The backdrop of regulatory requirements and ongoing cyber threats is driving the cybersecurity market, which is estimated,

Sampling of the Complex Regulatory Landscape

- **Health Insurance Portability and Accountability Act (HIPAA)** - contains Privacy and Security Rules designed to protect the integrity, privacy and availability of personal health information (PHI). Fines, into the six figures, can be imposed for violations to the Rules.
- **Payment Card Industry Data Security Standards (PCI DSS)** – offers guidance to maintain payment security (applies to anyone/company that processes payment transactions).
- **Manufacturing's International Traffic in Arms Regulations (ITAR)** – has provisions to protect the electronic transfer of controlled technology, technical data and software. In 2015, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) published amendments to the Export Administration Regulations (EAR) (a complementary regulation) to implement controls on cybersecurity related items.
- **The Gramm-Leach Bliley Act (GLBA)** – covers information sharing for financial institutions, requiring institutions to implement "administrative, technical and physical safeguards" for customer records and information.
- **The Sarbanes-Oxley Act** – requires companies to put internal controls in place to ensure financial reports are accurate and complete (cybersecurity isn't explicitly required, but rather implied).
- **Family Educational Rights and Privacy Act (FERPA)** – protects access to U.S. citizens' educational information and records.
- **Cybersecurity Information Sharing Act** – a U.S. federal law, signed in December 2015, that allows technology and manufacturing companies to share Internet traffic information with the government around cyber threats (some fear it may weaken privacy protections).
- **Personal Information Protection and Electronic Documents Act (PIPEDA)** – Canada's data privacy law governing how organizations can collect, use and disclose personal information during the course of their business.
- **Freedom of Information Act (FOIA)** – found in many countries – U.S., U.K., Australia – defines the access rights of the public around certain types of information/documents.
- **CaliforniaSB 1386** - breach notification act for companies operating in California, U.S.
- **European Union's General Data Protection Regulations (GDPR)** - looks like it will come into effect in 2018, filling the gap created last year with the invalidation of the Safe Harbor agreement. GDPR tries to harmonize laws across Europe and impose strict requirements to protect a citizen's privacy rights. It includes mandatory data breach notifications, as well as fines of 4% or €20 million for serious breaches.

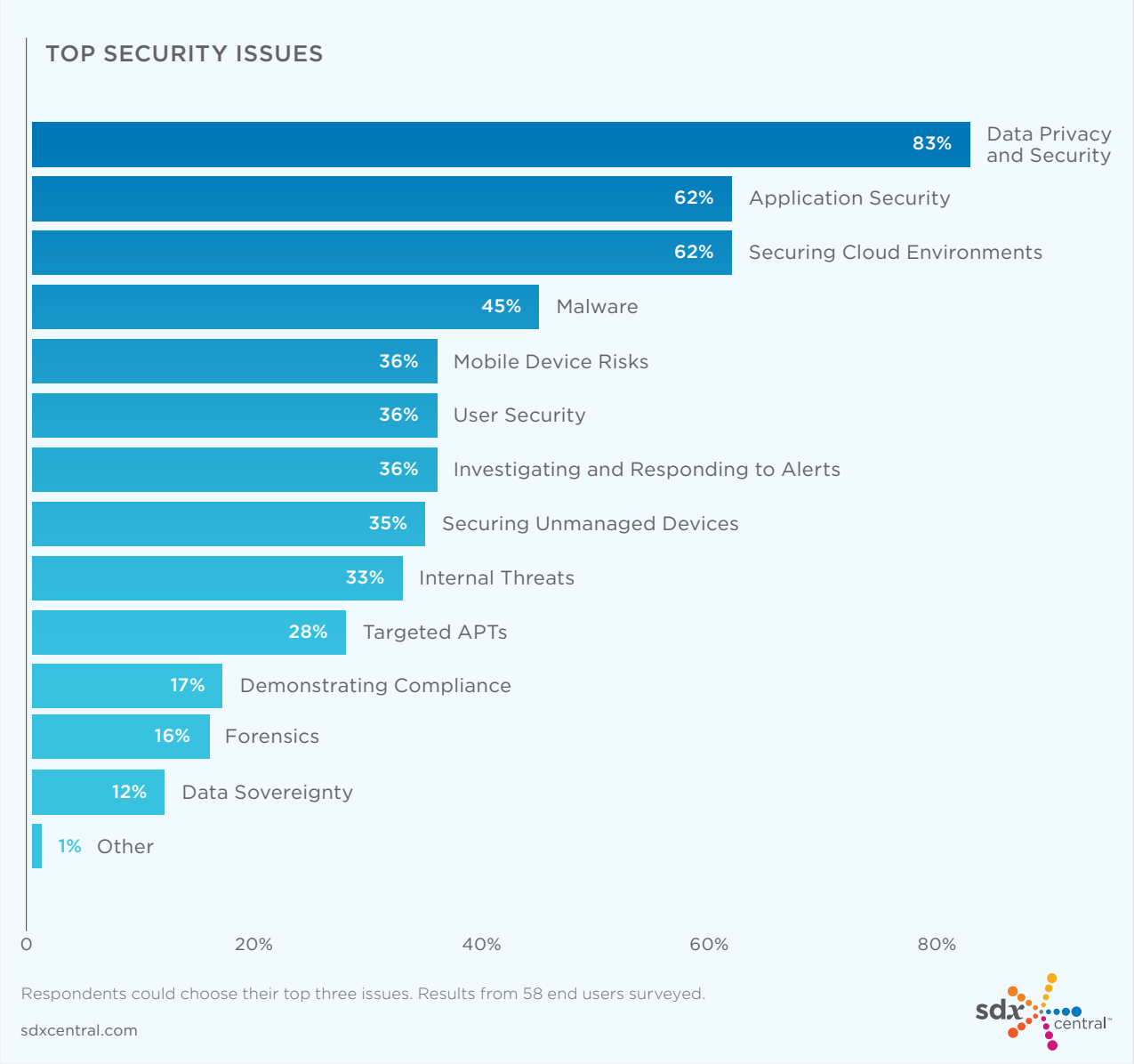
depending on how you define it, to be between $75 to $100 billion, according to several technology market research firms.

Types of Security Threats Evolve

Cyberattacks continue to evolve, in terms of frequency and sophistication, and they show no signs of slowing, making cybersecurity a particularly relevant market, across industries, across the globe. According to **a survey conducted by the ISACA and RSA Conference**, almost 75% of respondents worldwide expect to fall prey to a cyberattack in 2016.

These attacks cost organizations dearly, in terms of lost productivity, lost revenue, and reputational damage. The **cost of global cyber espionage** is approximately $500 billion annually, hitting $1 trillion, if you include the

Top Security Issues: Respondents to the SDxCentral survey indicated that "Data privacy and security" was their top concern (83%), followed by "Application security" and "Securing cloud environments."



market summary

costs associated with stolen intellectual property. According to the **2015 Cost of Data Breach Study** by IBM and the Ponemon Institute, the average total cost of a data breach increased from $3.52 million, in 2014, to $3.79 million last year. The costs, both direct and indirect (reputational, future revenue) have gotten the attention of boards everywhere – the ISACA survey found that 82% of boards are concerned (46%) or very concerned (36%) about cybersecurity.

And no industry is immune. **The Identify Theft Resource Center (ITRC)** reported that, in 2015, nearly 40% of attacks hit the business sector, with the health/medical sector targeted by 35.5% of the attacks, followed by the banking/credit/financial sector at 9.1%, government/military at 8.1%, and education at 7.4%. Verizon's annual report, **2016 Data Breach Investigations Report**, collected data on breaches that ranged across all geographies and industries, finding the mix hasn't changed much from past years. In the World Economic Forum (WEF)'s Global Risks Report 2016, they posited most cyber incidents actually go unreported, with a significant percentage going undetected.

A quick review of the landscape during the first few months of 2016, confirms the prevalence of widespread threats and activity in all industries:

- **Financial:** The **ThreatMetrix Cybercrime Report** predicted major financial institutions are likely to be hit by a significant cyberattack in 2016. Attackers successfully installed malware in computer systems within **Bangladesh's central bank**, using it to get credentials that allowed them to steal over $80 million from the institute's Federal Reserve bank account. HSBC had their personal banking website and mobile application shut down by a denial of service (DoS) attack. **The Ponemon Institute** found that, on average, 83% of financial companies suffer over 50 attacks per month.

  On the plus side, seven **Iranian hackers were indicted**, in March, for the coordinated attacks they carried out on dozens of U.S. banks (and a New York dam) from 2011 to 2013. This is the first time the U.S. government has charged individuals connected with a nation-state, which could indicate a potential shift in policy by the government to more openly address cyberattacks on critical resources. (This comes on the heels of the first piece of U.S. cybersecurity legislation – the Cybersecurity Act of 2015 – which was signed into law at the end of 2015).
- **Healthcare:** **Ponemon Institute** found that on average healthcare organizations are hit by an attack once a month, with almost half of survey respondents indicating they experienced an incident that involved the loss or exposure of patient data (26% of respondents were unsure). Early this year, **21st Century Oncology** had 2.2 million patient and employee records compromised. MedStar Health fell victim to a ransomware attack that held the files of their 10 hospitals hostage. This attack came just weeks after attacks on the Methodist Hospital in Henderson, Kentucky, which ended without payment, and the Hollywood Presbyterian Medical Center, in California, which was resolved with a $17,000 ransom payment for data that had been held hostage for 10 days.
- **Law Firms:** **Panamanian law firm Mossack Fonesca** was infiltrated by 'hackavists' who gave journalists access to almost every file the firm had collected over the past 40 years - 11.5 million files, totaling 2.6 terabytes of data – the volume of which is being dubbed the Panama Papers. The FBI, U.S. Secret Service and other law enforcement agencies have long been warning companies privy to potential corporate mergers, patents, financials, trade secrets, and more, they will likely be the target of attacks from sophisticated cyber-criminal rings and nation-states. According to Daniel Garrie, founding editor of the **Journal of Law & Cyber Warfare** there is a thriving black market for the type of corporate information in the possession of law firms.
- **Retail:** Retailers are challenged to stop attacks targeting their online and mobile apps, without creating friction in the customer's online shopping experience. **Research conducted by UpGuard** found U.K. retailers, such as Matalan, Waitrose, Tesco, Debenhams and TopShop, are at risk for cyberattacks on their web sites and warned consumers to think twice before transacting online. In the last three months of 2015, the **ThreatMetrix Digital Identity Network** detected and stopped approximately 58 million attacks on e-commerce merchants, many of which were bot attacks trying to compromise user credentials. The Ponemon Institute found that, on average, 44% of retail firms suffer over 50 attacks per month.

market summary

- **Critical Infrastructure:** The IRS Commissioner was required to answer questions from the U.S. Senate Finance Committee on their plans to implement the **94 recommendations made by the Government Accountability Office** to improve their ability to maintain the confidentiality, integrity and availability of taxpayer data. A breach last year, thought to be conducted by Russian hackers, compromised the information of more than 700,000 taxpayers. The agency also confirmed that in January there were unauthorized attempts to access more than 450,000 social security numbers. Overall, the U.S. Federal Government has budgeted $14 billion for cybersecurity initiatives in 2016.

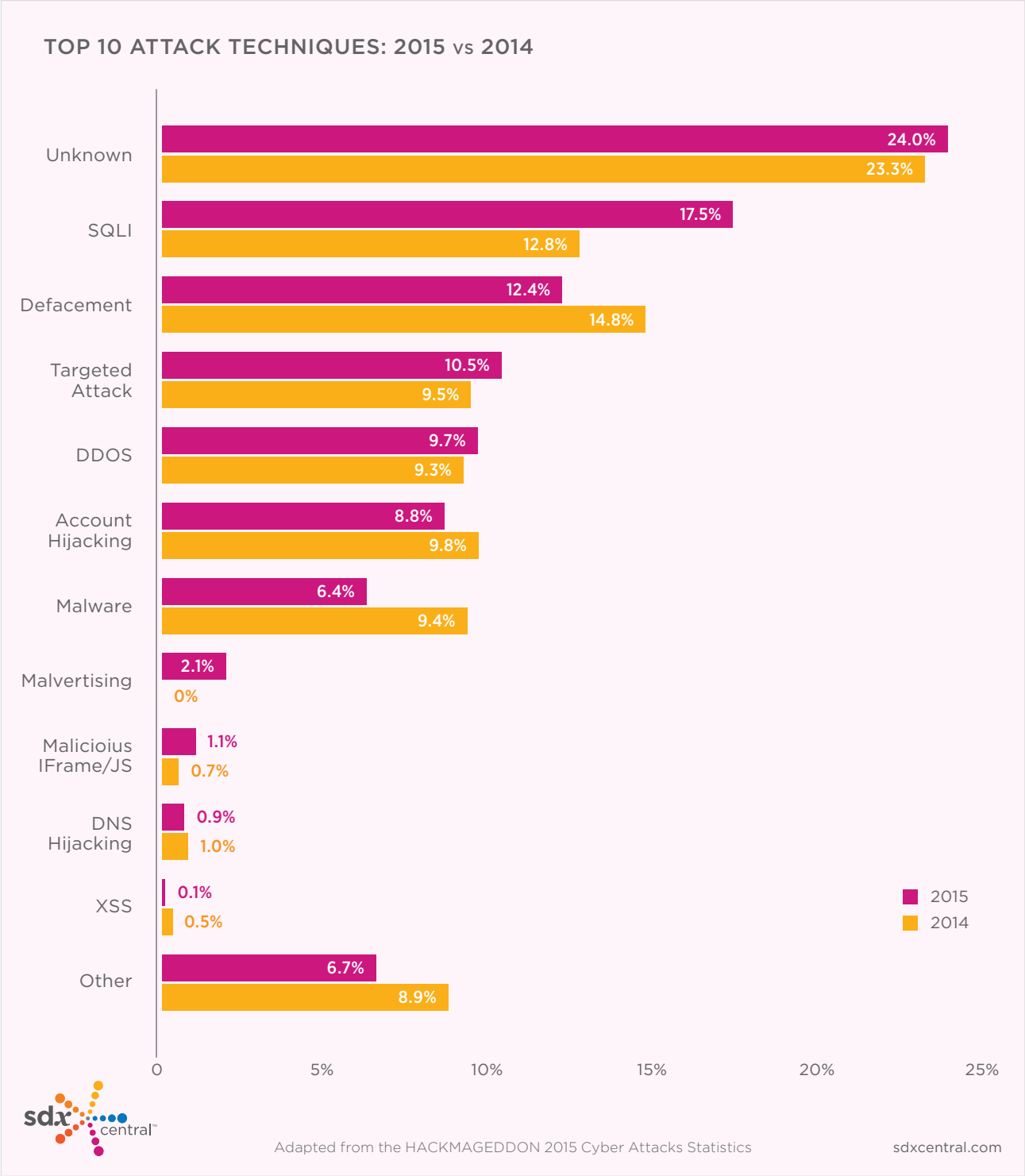
  An attack targeting the industrial control systems of **Ukraine's power grid**, in December 2015, knocked out the power of 225,000 citizens; officials worldwide warn (**including the U.S.**) this kind of attack could happen in their countries. In response, the **U.S. Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI)** launched a nationwide campaign to educate electrical power infrastructure companies on the very real risks to the electrical grid. A **survey by Tripwire, Inc.** of the energy, utilities, oil and gas industry revealed that in the past 12 months, 78% of respondents had experienced an attack from an external source, while 30% reported being attacked by an inside employee. A follow up survey of attendees to this year's RSA Conference found that 83% believe a cyberattack would cause physical damage to critical infrastructure in 2016. This is in line with a survey of IT professionals done by **Statista** that found that 38% believe an attack on critical infrastructure is highly likely in 2016, with 46% indicating the risk was of a medium level.

Analyzing Attack Types

Attackers have all types of motivations, from financial gain to political activism. **2015 saw an uptick in organized crime**, which will likely continue through 2016. This means organizations can expect well-coordinated, targeted attacks on their networked resources. It also means we may see more integrity attacks, which manipulate data to drive decisions or actions that benefit the attacker (e.g. make a payment to the wrong account), as well as ransomware (the **FBI investigated 2453 complaints** of ransomware attacks in 2015 that cost $24.1 million).

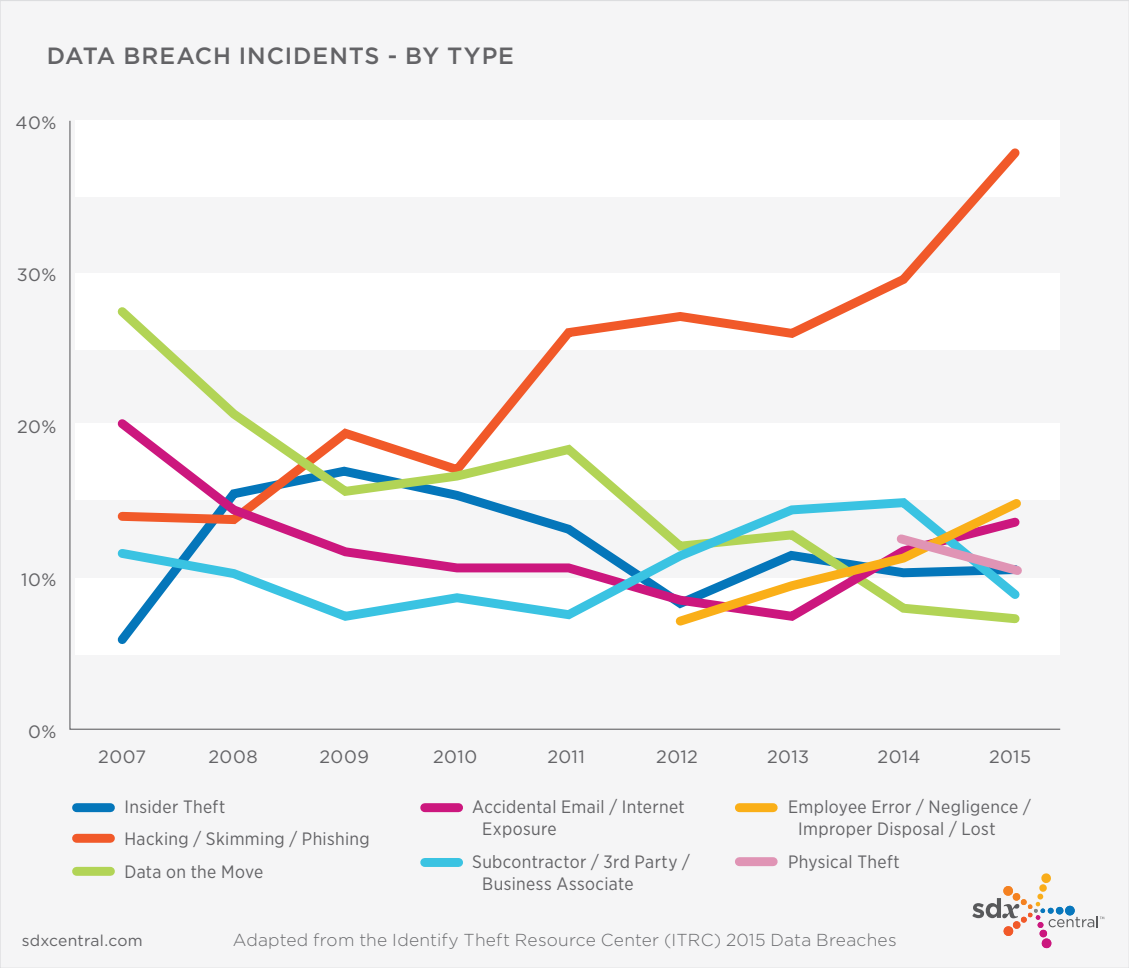
Industry watcher **Hackmageddon** broke down the top attack techniques used in 2015 (see below). Many are the usual tactics we have seen in years past, but almost a quarter are unknown, which makes them harder to identify and defend against.

market summary



Verizon identified point-of-sale (POS) and phishing attacks as the "rock stars" of threats in their 2016 report. The **Identify Theft Resource Center (ITRC)** looked at the publicly available information on attack types in the U.S. and found that hacking, skimming and phishing are by far the most popular tactics used by attackers.

market summary



One thing is certain – cyberattacks are just a part of doing business. **Ponemon Institute** reports 45% of senior executives say their company experiences cyberattacks hourly or daily; **according to the ISACA**, phishing is a daily occurrence for 30% of organizations; and good old denial of service (DoS) attacks occur on a weekly basis for the majority (53%) of organizations.

Cybersecurity Disconnect

While attackers are able to compromise organizations in minutes (**60% of attacks according to Verizon**), organizations are often not able to identify them as quickly. There is a serious lag time between compromise and detection; a report by **Mandiant Consulting**, an incident response consulting service of FireEye, found the average time it takes a company to detect a breach was 205 days.

Once detected, the **Ponemon Institute reported**, it takes organizations an average of 32 days to resolve a cyberattack; for insider attacks, the average time for containment goes up to 65 days. This is in alignment with the struggle organizations have dealing with the known vulnerabilities in their organization. According to a survey by **Kenna**, a risk and vulnerability platform, which analyzed 50,000 organizations, 250 million vulnerabilities and over 1 billion breach events, most companies take 100–120 days to fix known vulnerabilities – the likelihood that a vulnerability will be exploited hits 90% between 40–60 days after discovery.

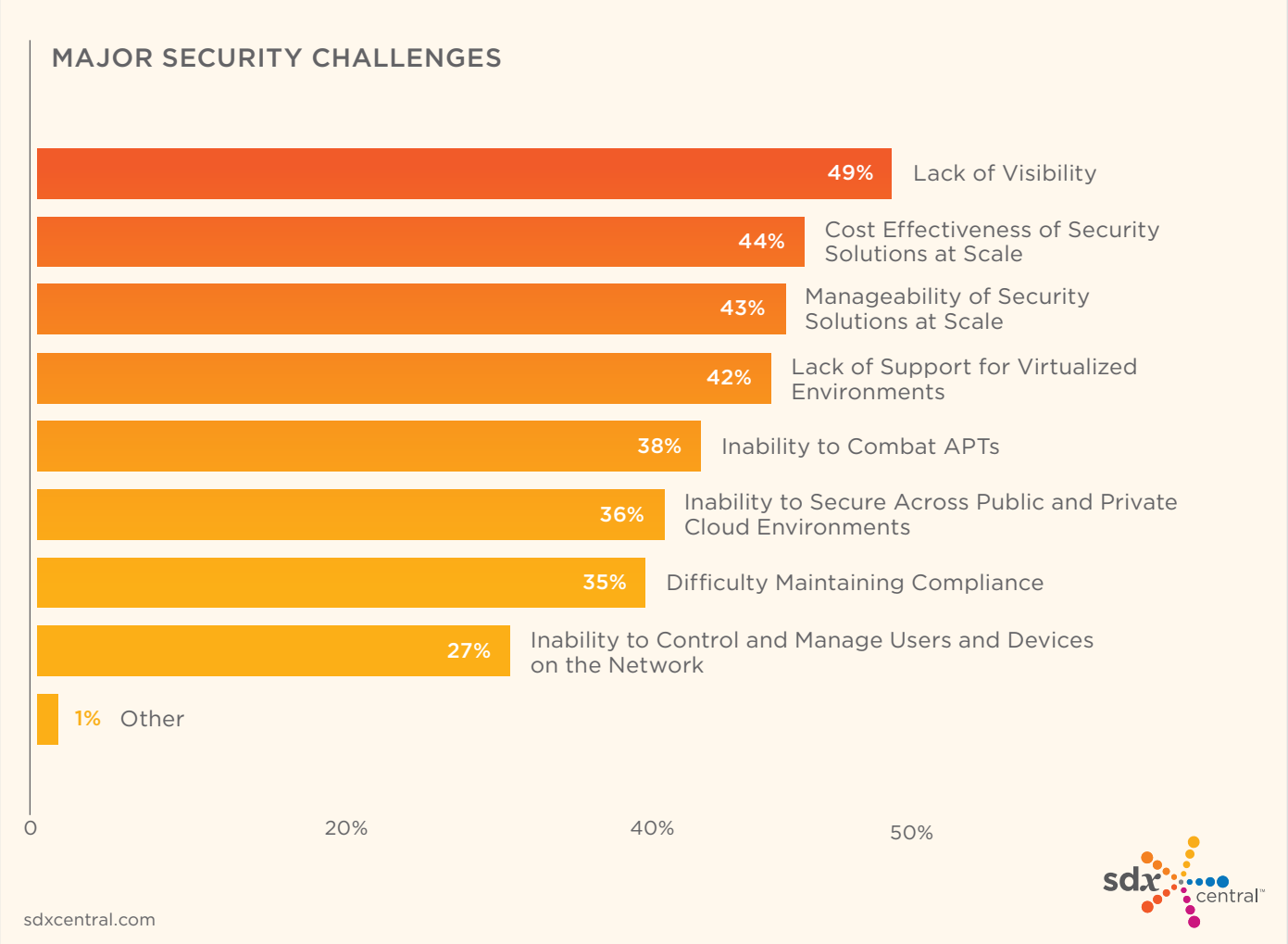
All of these factors explain why most organizations (61% according to **Ponemon**) are not confident they would be able to detect an attack when it occurs. The reasons they give for their deficiencies are: the cybersecurity

market summary

technologies they have are either too hard to deploy (59 %), too slow to produce intelligence (55 %), or not well integrated with their other security solutions (53%). It could also be influenced by constrained resources available within most organizations.

There is a well-documented shortage of cybersecurity professionals with the skills and experience to implement cybersecurity measures and respond to incidents. In private sector, according to the **2015 State of Cybersecurity Survey**, it takes organizations an average of three (26%) to six (28%) months to fill an open information security position; 9% report they cannot fill the open positions they have. In terms of the capabilities of the applicants out there, 65% of all entry-level cybersecurity applications lack the requisite skills needed to perform the tasks related to the jobs they were seeking; most (61%) don't have the technical skills or communication abilities they need, while 75% don't understand the business. The public sector, which often has limited funds to entice personnel, is having a lot of trouble recruiting (**DHS can't fill open slots**). Symantec's CEO, Michael Brown, estimates the worldwide demand for the cybersecurity workforce will rise to 6 million by 2019, with a projected shortfall of 1.5 million.

SDxCentral Survey – Security Challenges: When asked to indicate all their major security challenges, there was no single overwhelming problem identified by respondents to the SDxCentral survey; 49% said "Lack of visibility" was an issue, followed by the "Cost effectiveness of security solutions at scale," at 44%."



Cybersecurity Expert Shortage Drives Managed Services

A shortage of expertise is bad for enterprises and governments, but good for consultants and managed service providers. It is fueling the global managed security services market, as organizations look to augment their capabilities.

In 2014, research firm **Infonetics reported** cloud-based managed security services grew to $7.2 billion, up 13.5% from the year before. **Technavio**, a research firm, predicts the global managed security services market will grow at a CAGR of nearly 12% until 2020, driven by increasing demand by small and medium businesses (SMB) looking to protect sensitive and confidential information and improve their ability to respond to incidents. They estimate the cloud-based managed security services segment will account for more than 56% of the total market by 2020.

Allied Market Research is a little more aggressive, expecting the global managed security services market to reach $29.9 billion by 2020, with a CAGR of 15.8%. They agree that growth will be fastest in the cloud-based managed security services segment and will be driven by SMB demand.

This is one reason **FireEye** continues to invest in the Mandiant Consulting Services it acquired back in 2014, introducing new offerings (Mandiant Red Team Operations and Penetration Testing) in March of this year designed to conduct "no-holds-barred attacks on organizations to highlight weakness in systems or procedures and to enhance detection and response capabilities," and assess an organization's exposure to risks in potentially vulnerable areas, such as Industrial Control Systems (ICS), Internet of Things (IoT) devices, and Mobile Applications and Devices. In fact, just recently, former Mandiant CEO Kevin Mandia **took over as FireEye's CEO**, as the company redirects more resources towards security software and subscription models.

SDx Security Requirements

The persistence of successful attacks, combined with a lack of resources that can be applied to the problem, means the industry is going to have to come up with new, disruptive ways to address the cybersecurity problems we are facing.

This is where taking a software-defined anything (SDx) approach to security solutions come into play. SDx infrastructure security is uniquely positioned to address the security challenges presented by today's environments.

Impact of Virtualization on Cybersecurity

The move to virtualize computing resources and adopt cloud technologies has impacted an organization's ability to maintain visibility and control over their information and protect their resources. Virtualized resources are quick and easy to deploy, move and scale to meet varying demands. This fluidity has many business benefits (speed, agility, performance, productivity, etc.), but it has radically altered an organization's threat profile, opening up additional attack vectors as information flows in, between, and amongst these virtualized resources.

In addition, as organizations adopt cloud services (e.g. Salesforce, Egnyte, WebEx, Concur, Workday, ADP, etc.) and leverage cloud platforms (e.g. IaaS offerings, such as Amazon AWS, Windows Azure, Google Compute Engine, Rackspace Open Cloud, IBM SmartCloud Enterprise, Hewlett-Packard Enterprise (HPE) Converged Infrastructure, etc.) to house their apps and workloads, it can be difficult for an organization to maintain visibility and consistently enforce policies. In many ways organizations have to relinquish some measure of control to the provider of that cloud offering, relying on the security inherent in that service/platform. This can be problematic, particularly when the information is regulated or business critical.

A **report** from Intel Security found that only 34% of IT pros feel senior management fully understand the security implications of the cloud. **Alert Logic's 2015 Cloud Security Report** found security incidents were much more likely to occur in the cloud than on-premises. Of the 842,711 incidents they tracked within the environments of their 3026 customers, in 16 different countries, 78% of them were in the cloud.

Issues are compounded with the use of a mix of private, public and hybrid clouds resources. An organization may be relying on multiple providers, platforms and services to run their business, creating a complex environment that can span multiple geographies and make it difficult to track activity and consistently enforce policies. Today's security solutions need to keep up with today's highly virtualized, dynamic environment.

Delivering Security with Software

Security that relies on the deployment of proprietary, purpose-built hardware simply can't meet the demands of today's dynamic environments. Today's solutions must mirror the networks in which they need to be deployed; they must be able to effectively secure all the highly virtualized, hybrid networks, new services and applications (Day One, Quartz, Uber, Vevo, Spark, etc.) and managed/mobile/IoT devices that make up the SDx Infrastructure.

Almost every security function can be delivered in software, such as firewalling, unified threat management (UTM), identity access management (IAM), encryption, data loss prevention (DLP), risk and compliance management, deep packet inspection (DPI), network and host intrusion detection and prevention (IDS/IPS), anti-virus (AV), anti-malware, security information and event management (SIEM), incident response and forensics, disaster recovery (DR), denial of service (DoS) mitigation, distributed denial of service (DDoS) mitigation, web filtering, and many other security services.

When security functionality is delivered via software, it can be quickly moved or adapted to address changing needs. It can provide comprehensive coverage, as security services can be more easily applied to workloads and apps when they are spun up or down, as well as across environments, including on-premises deployments and private, public and hybrid clouds.

To ensure traffic is appropriately inspected and protected, individual cybersecurity services can be delivered as virtual network functions (VNFs) and then chained together (service chaining). For example, email traffic may be routed to virus, spam and phishing services; web traffic to virus, URL filtering, DLP and DPI services; while internal traffic may pass through internal gateways, honeypots, etc.

These security services can be hosted on the same appliance deployed at various ingress/egress points in the network, either stand-alone or as modules/blades within the packet transport systems (routers/switches). They are available from vendors, service providers (as a value-added offering) and cloud/data center operators (as a cloud-based service).

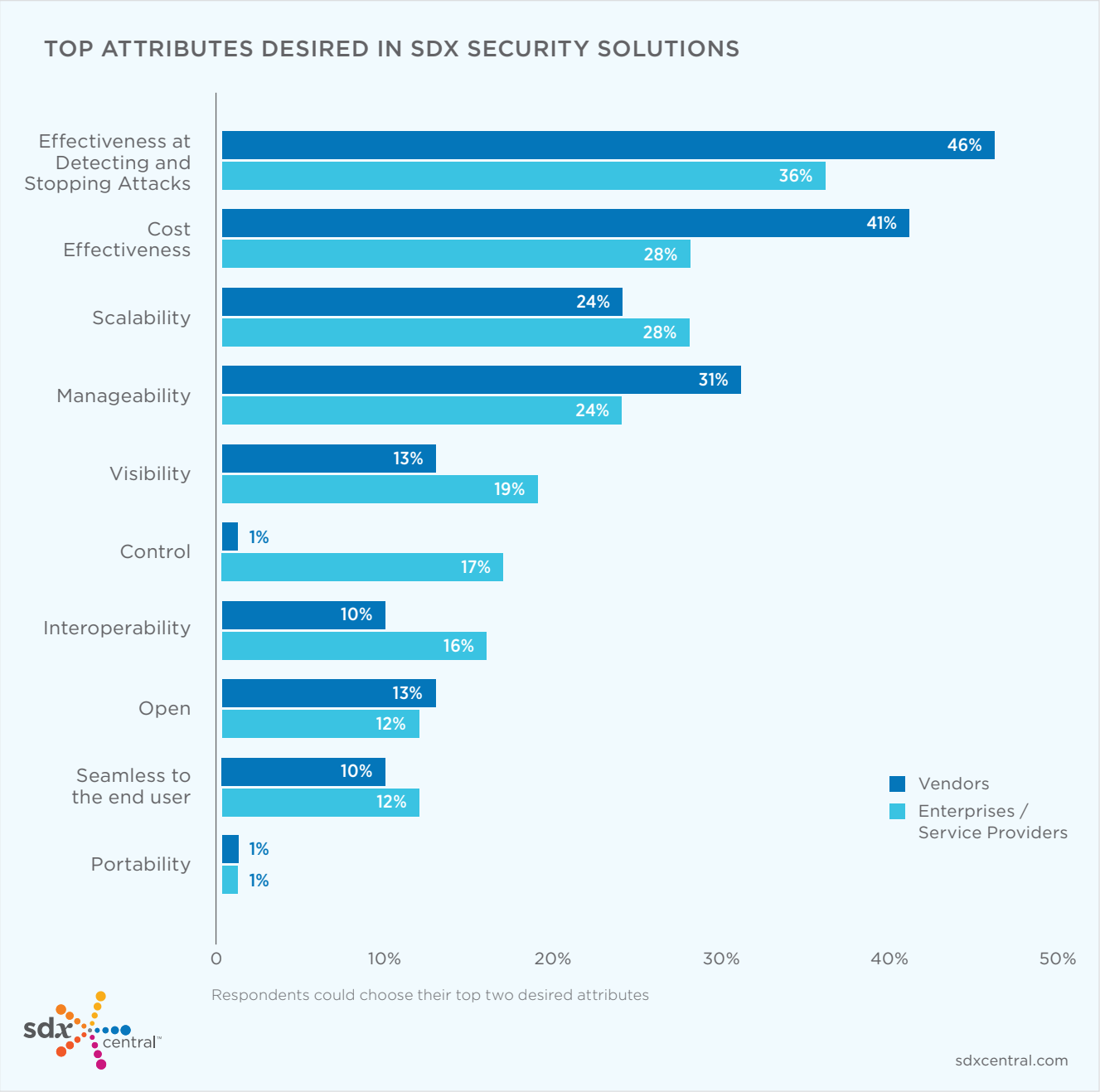
Characteristics of SDx Security

SDx security that mirrors the SDx Infrastructure can both protect and enable greater agility, scalability, personalization, and automation.

In the SDxCentral security survey, when asked to pick the top two attributes most desired in an SDx Security solution, it's not surprising respondents said that "Effectiveness at detecting and stopping attacks" was top of the list.

When we looked at disconnects between what customers (enterprises and service providers) are looking for and what vendors think is most important to deliver, we found that "Control," while important to customers (17%), wasn't even on the radar of vendors (1%). "Visibility" and "Interoperability" were also deemed less important than what was indicated by customers, at 19% and 16% respectively. From last year's results, the biggest shift was seen around "Scalability" – in 2015, scalability was the top attribute, chosen by 55% of respondents; this year, only 28% picked it.

market summary



To recap, some of the characteristics to look for in an SDx security solution include:

- Software-centric – to meet the agility, portability, scalability and efficiency requirements of SDx networks, applications, services, devices, etc. The software should be easily deployed on anything – a virtual server/blade, endpoint, or as a stand-alone solution. For stand-alone solutions, commercial, off-the-shelf (COTS) hardware platforms should be capable of delivering adequate compute and data handling capabilities.
- Highly Virtualized – across compute, networking and storage elements. The type of virtualization may vary from hypervisor- and container-based, to API-based. Ideally the functionality can be managed and orchestrated by resource management systems to link the security to the services, apps and workloads to protect to ensure they are protected as they are deployed, moved, and scaled.

- Central management – for visibility, orchestration, and control. For those solutions that rely on endpoint agents, they need to be easy to update and manage. For example, Cylance
- Policy and intent-driven – capable of continually monitoring the infrastructure for events and changes and reacting to them automatically. It should provide sufficient embedded intelligence that can automatically translate intent into actual commands on infrastructure elements, without requiring DevOps teams to create complex automation scripts. It should support of template-driven deployments, snapshotting, and rollbacks.
- Context-driven – with the ability to understand the appropriate context of users, applications, devices and locations related to the creation of a virtual machine, container, data flow or set of network attributes, such as source/destination addresses and tags.
- Modular architecture – ensures the solution is adaptable and extensible. SDx Infrastructure consists of a larger number of small agile components, sometimes geographically disparate, so the ability to quickly make adjustments to reflect the changing needs of the changing infrastructure is critical.
- Open – to seamlessly work within the environment in which it is being deployed. It is important to enable organizations to pick and choose the solutions that meet their unique needs to keep up with the accelerated pace of change within the market. Support of open standards (e.g. OpenFlow, ONUS, etc.), in this emerging market, is key for ongoing relevance and frictionless deployments.
- End-User extensibility – to support the constant state of flux. To maintain their competitive edge, businesses often need to quickly add new features and capabilities to applications, which may require new functionality at the infrastructure level. The solution should offer APIs that allow it to be adapted for the unique environment in which it is deployed.
- Seamless to end-user – so it doesn't require a lot of effort on their part to be secure. Ideally, end-users won't even know it is there, unless something bad is happening; basically, the onus of SD security solutions should be on them, not the user to protect the environment.

Benefits of SDx Security

SDx Security solutions can provide greater visibility, scalability and flexibility, as well as improved functionality through the use of innovative software approaches. The benefits of an effective SDx infrastructure security solution are wide ranging and include many new features not present in legacy, hardware-driven security products.

Here is a look at some of the major benefits of SDx security:

Enhanced Security: Comprehensive security, covering both applications and data across enterprise networks and Data Centers, public, private and hybrid clouds, as well as protecting the virtualized infrastructure itself. Other requirements:

- Protection of employees and enterprise devices (laptops and mobile), regardless of whether they are in or outside the corporate network.
- Sophisticated algorithms that use machine learning and new techniques to detect threats throughout the SDx Infrastructure.
- Improved analytics and orchestration to provide global control and visibility across all elements of the SDx Infrastructure.

Reduced Capital Expenditures: The use of commodity servers reduces hardware costs; by delivering security services in software, organizations are no longer forced to rely on specialized, proprietary hardware.

Reduced Operational Expenditures: Software enables organizations to quickly and easily move and scale functionality to address the changing needs of SDx applications.

Flexibility and Agility: Overall, virtualized functions provide greater flexibility and less complexity in

management; organizations can quickly deploy with templates to make it simple to move or redeploy functionality across the organization.

Accelerated Roll Out: SDX-based security can be easily installed and provisioned to enable an organization to quickly deploy security when, and where it is needed. The ability to run virtual security services on top of physical infrastructure means organizations do not need to incur the time or costs of having to forklift upgrade their existing systems to add new services.

Challenges with SDx Security

SDx security can create new challenges within the infrastructure. While visibility may improve at the app and user level, with the ability to more easily track and control transactions and activity across public/private/hybrid environments, visibility into the underlying mechanics of the network and all the details of what is happening may be abstracted. This can be problematic when dealing with attacks exploiting vulnerabilities in that infrastructure.

SDx security can also blur the lines, which can add confusion and complexity – what once was a clear network security problem, may now actually be a software as a service (SaaS) issue. This means as roles and responsibilities of both technology/solutions and people become even more fluid, there will need to be insights and security controls embedded/available at all levels (Layer 1-7), to ensure consistent, comprehensive coverage can be applied (to try to eliminate any weak links).

It also means cybersecurity solutions are going to need to be simple and intuitive for anyone to use, since it is reasonable to assume everyone (network, application, database, storage, system and cloud admins) will be taking some share of responsibility for the security posture of the organization. The centralized management offered by software-defined network (SDN) controllers actually lends itself to a more distributed model, as long as it is user-friendly for the wide swath of people that may need to start to use it.

The deployment of security capabilities may be subsumed, to a certain extent, by software and DevOps teams, who can automate the roll out and improve consistency at a macro level. We may find the adoption of SDx security drives new DevOps use cases and tools. At this moment, however, **DevOps often breaks security**. Typically, the needs of DevOps, which looks to create a state of continuous software development, is in contrast with that of security, which is tasked with maintaining a steady, secure state.

There is speculation that the disconnect could be bridged if every machine was given an identity and then mapped to an appropriate policy, but this could create more management headaches than it solves. It is certain the general management of security is going to need to become a lot simpler, as it is embedded everywhere, to ensure consistent, effective policy enforcement that protects an organization from attack.

SDx Security Market Landscape

There are a thousand different ways the cybersecurity market can be sliced and diced. You can look at solutions based on the types of threats they combat (e.g. mobile, advanced persistent threats, viruses, web, data, identity); where they are deployed (e.g. data center, endpoint, cloud, SOC/CIRT, etc.); what stage of the attack lifecycle they address (e.g. intelligence, detection, response, etc.).

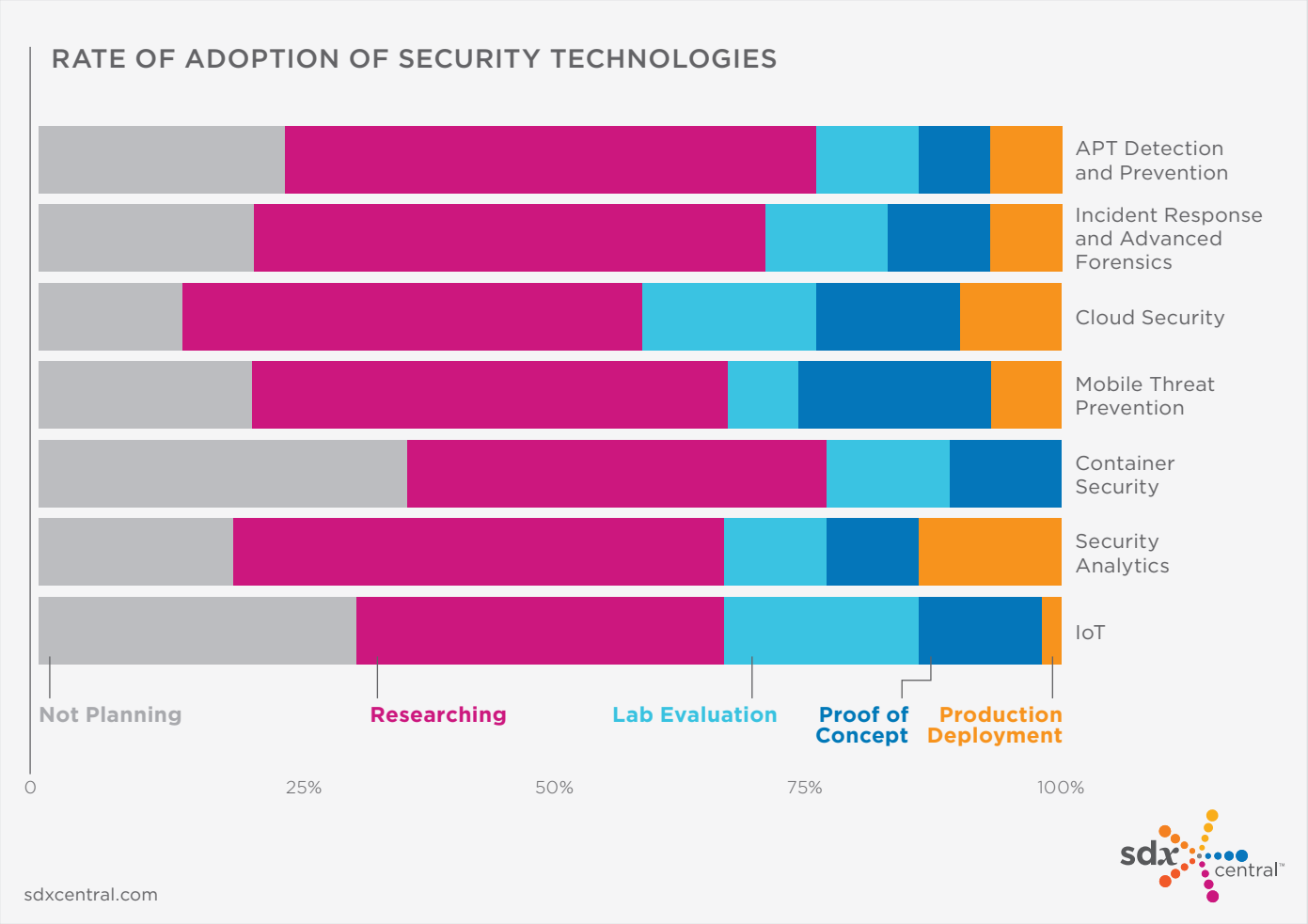
At SDxCentral, we looked at the market under the lens of solutions designed for the SDx Infrastructure. To that end, there are several interesting areas where we are seeing a lot of innovation:

- Data Centers
- Cloud
- Identity
- IoT

market summary

- Content
- Endpoint
- Incident Management

According to the respondents of the SDxCentral security survey, most enterprise and service provider customers are in the research phase. This is similar to the results from last year's survey. Security analytics had the most production deployments at 14%.



Let's dive a little deeper into each group of solutions.

Data Center Security

Traditionally, organizations sequentially placed security solutions/tools (e.g. firewall, intrusion prevention, AV, etc.) at key ingress and egress points to protect the data center (or in the DMZ). Recognizing that today's data center networks are permeable, not trusted, organizations have been re-evaluating how they think about and design their data center security; it's no longer just about ingress/egress traffic, but also lateral (east-west) traffic that needs to be inspected.

Once an attacker is in the network, they can often move about freely to carry out their attack objectives. This issue can be amplified in a virtualized environment that is very fluid. As a result, organizations are looking to

deploy controls that enable consistent policy enforcement across their physical and virtual infrastructures. Virtualized security functions are better able to provide ubiquitous deployments, which is required in today's data centers (and clouds).

Virtualized security functions enable security to be embedded (as an application on a bare metal hypervisor or as a hosted service on a virtual machine (VM)) throughout the data center's infrastructure to protect all the traffic flowing through it. As a result, organizations can quickly deploy security controls throughout the data center (and across cloud environments) to combat an attack's lateral movement and minimize the impact of incidents.

SDx security can make it easier to segment the network at a micro-level to apply controls within the virtual fabric to protect applications and even individual workloads. With micro-segmentation, organizations can enforce granular policies to identify, contain, and prevent attacks from propagating.

For example, **vArmour** enables application-aware micro-segmentation that can protect workloads across an organization's data center and cloud environments. Being able to partition workloads and apply controls (and prevent them from interacting with one another) enables organizations to strengthen the security of high-value assets/data and better support regulatory requirements.

Application-aware micro-segmentation is complimentary to the network-level segmentation offered by virtualized platforms, offering defense-in-depth that can strengthen the overall security of the organization. We've seen players combine to offer more complete solutions, such as vArmour and **Cisco**, which announced a partnership (March 2016) that enables organizations to 'wrap' every workload across Cisco's Application Centric Infrastructure (ACI) fabric to minimize the attack surface and provide visibility and control over those applications. (This followed an announcement they made late last year about their relationship with AWS, which extended their ability to provide workload-level visibility, policy enforcement and network controls into AWS environments).

VMware says NSX's micro-segmentation capabilities, with the option to distribute enforcement to every hypervisor, has driven more than half of NSX's sales. Cisco touts their micro-segmentation support for VMware VDS, Microsoft Hyper-V virtual switch, and bare-metal applications as one of the key capabilities that has helped drive more than 1000 customers to adopt the ACI infrastructure.

We have also started seeing traditional 'perimeter' devices, such as firewalls, virtualize their functionality to extend their capabilities into the fabric of the data center. For example, **Palo Alto Networks** has virtualized their next-generation firewall, their VM-Series, which has flavors for AWS, Citrix, KVM and OpenStack, VMware NSX, and VMware ESXi/vCloud Air, that can be used to enforce application policies within data center and cloud environments. **Fortinet** has also introduced virtual firewall appliances to protect east-west traffic, with out-of-the-box integration with VMware NSX and Cisco ACI. (Interestingly, not all big players have made this move – **Check Point** continues to focus on its appliances).

Also within the data center we are seeing honeynet capabilities deployed to try to lure attackers into revealing themselves. The concept of a honeynet/honeypot is far from new, but traditional deployments were either ineffective, because they weren't believe-able, or too costly and unwieldy, because they required the organization to buy, build and maintain a network that could lure an attacker to interact with it (with desktops, servers, storage, etc.).

Now, with the ability to virtualize all the components that make up a network, it is much easier and cost-effective to create a believable environment that can deceive an attacker and trick them into interacting with it instead of real, high value assets. The technology has adopted a new moniker – deception tools/networks – and is being heralded as a 'game-changing' solution that will enable organizations to uncover advanced persistent threats that tend to allude most other measures. Gartner predicts that by 2018 more than 10% of enterprises will be using deception tools.

Security for the Cloud

As we've already mentioned, when organizations adopt cloud services and platforms they relinquish a level of control. The cloud provider must be accountable for the security of their service/platform, but the organization must also take measures to ensure their cloud usage doesn't become the weak link in their overall security posture.

There can be an overlap in responsibilities, which creates a defense-in-depth strategy that minimizes the organizations risk profile. It comes down to visibility and control; organizations need to be able to see what is happening, Layers 1-7, and then make decisions and enforce policies around acceptable use that adheres to compliance and security requirements. This can be tricky, particularly as users, apps and workloads hop between public, private and hybrid cloud environments, but increasingly vital as those cloud environments are an extension of (and sometimes even a replacement for) an on-premises data center.

Over the past few years, a new category of security solution provider has started to ramp up, with the emergence of the cloud access security broker (CASB) in 2012. CASBs are software services that can be deployed on-premises or in the cloud to enable organizations to set policies, monitor user behavior and activity, identify threats (including shadow IT) and manage risks for all the cloud services an organization uses. Market leaders often offer granular policy development, robust investigation consoles, tokenization, threat analysis engines/sandboxes (or relationships with third-parties), and threat intelligence feeds (with their own research team/labs) to enable organizations to detect, manage and respond to the changing risks/threats within their cloud environment.

Gartner predicts CASBs will be an essential component of software and service deployments by 2017, and that by 2020, 85% of large enterprises will use them to protect their cloud services. Vendors in the space to check out include **NetSkope**, **CipherCloud**, and **Skyhigh**, as well as **IBM Cloud Security Enforcer**, **Zscaler**, etc.

Identity Management

Understanding who is doing what can be one of the biggest challenges faced by organizations that have heterogeneous environments. To combat, organizations need to think of how they define a user's digital identity and take measures to mitigate risks that can consistently protect assets across digital channels. No longer is it okay to rely on credentials; organizations must ensure they take a holistic view of that user, that takes into account usage, device, location, anonymized personal/behavioral information, etc.

The question of identity, which covers the ability to not only verify an individual, but also ensure that individual is only able to access what they should, has given rise to a new group of identity and access management solutions, from the likes of **Centrify**. This is not an extension of traditional physical access solutions, they have been purpose-built for the modern, fluid multi-channel networks of today.

In addition, we are starting to see software solutions that can provide organizations visibility into what their own teams are doing in the cloud (administrative access). For example, **HyTrust** Cloud Control can be deployed on the management plane, as a transparent proxy, to monitor, log and provide policy-based authorization of all administrative activity. This gives organizations, such as McKesson, visibility into administrator activity that was previously untraceable, enabling them to better manage access (with granular, role-based controls) that reduce risks and support compliance requirements.

IoT Security

Everyday objects are becoming smarter and more connected, from homes and cars to cameras and clothes. By the end of this year, **Gartner** predicts 6.4 billion "things" will be connected, reaching 20.8 billion by 2020.

This has enormous security implications. For example, smart home automation systems can be exploited to unlock doors for burglars; security cameras can be hacked to allow attackers to watch video of homeowners;

even **coffeemakers** can be used as a way into a homeowner's WiFi network, giving an attacker access to all the home's networked resources (computers, TVs, etc.).

In healthcare, the IoT is being used to increase access to diagnostic testing, ongoing monitoring, and treatments and telemedicine initiatives that can help improve care and patient outcomes. A 2015 **MarketResearch.com** Report predicts the healthcare segment of IoT will grow to $117 billion by 2020. Goldman Sachs estimates IoT can save patients, healthcare providers and insurance companies billions in asthma care alone. For all the good that IoT can do for the healthcare industry, it also significantly expands the attack surface of healthcare organizations.

A cyberattacker can hack into an unmanned medical device (e.g. heart monitor, MRI machine, sensors, etc.) and use it to get access to an organization's entire network and all its connected resources. According to Aberdeen Group, medical health records sell for up to $500 on the black market. Of course, there are also the nefarious consequences possible if an attacker compromises a device that is managing a patient's health and interferes or tampers with its operations.

In the automotive industry, the U.S. Assistant Attorney General for National Security **raised the profile of these potential dangers**, issuing a warning that connected cars can be attacked – **Telefonica** estimates by 2020, 90% of cars will be connected. **White hat hackers** validated the real risk by targeting the connected cars on the road today. They were able to take complete control over the vehicles – doing everything from turning on the windshield wipers to killing the engine on the freeway.

Security vendors are stepping in to fill the gaps, and a whole new category of IoT products is being created. For example, there's **Bayshore Networks** (securing operational technology (OT) environments), **Mocana** (protects cross-industry devices), SecuriThings (platform for IoT service providers), **Karamba Security** (securing connected cars), **Bastille Networks** (software and sensor technology to protect against airborne threats), **Gemalto** (protecting digital services), **ZingBox** (enterprise IoT), etc.

Data Security & Analytics

Organizations need to understand what types of data (regulated, business critical/intellectual property, etc.) they have, on-premises and across their public, private and hybrid cloud environments, and then take appropriate actions to mitigate risks. (A **survey commissioned by Veritas** found that 54% of company data across Europe is 'Dark Data', where the value of the information hasn't been identified yet.) This also means organizations need to understand not only how information is being used (accessed, shared, modified, etc.), but also who is accessing it.

Instead of trying to distinguish between what is good and bad or implementing policies around what is allowed and disallowed, there are a host of new cloud-based services and software-based solutions focused on 'keeping content clean' to eliminate the threat of malware and exploits. There is:

- An isolation approach – prevents potential attacks from ever reaching their destination by executing the code/file/etc. in a contained space. This is the approach that **Menlo Security** has taken with their Isolation Platform (MSIP), which executes and contains all user web sessions and content within the platform, delivering only safe information to the endpoint.

  It is also the approach that containers take – isolating applications by limiting their view and access to the operating system, so they remain private and secure. Container solutions include the **Docker** (open source project), **Twistlock**, **ClusterHQ**, **CoreOS**, **Kismatic**, **PortWorx**, **Rancher Labs**, **Shippable**, **Sysdig**, **Tatum**, **Weaveworks**, etc. For more information on the Linux container and container security market, it was profiled in our **Inside the Linux Container Ecosystem Report**.
- A reconstruction approach – cleans (rebuilds) data before it is sent on to the user/endpoint.
- A tracking approach – protects information across environments. This encrypts and tracks critical information, with the ability to revoke access and audit activity.

- A 'gold master' approach – disallowing any foreign code or anything that attempts to run that doesn't match expectations. It doesn't matter what the code is attempting to do, if it is introduced in way that violates processes/protocols/etc., it is automatically stopped.

The beauty of these solutions is they don't rely on signatures or known attack behaviors, which means they can work against zero-day attacks and don't generate false alarms. (Organizations indicate that only 19% of malware alerts received from existing solutions are reliable.) Often these solutions are offered as cloud-based services or virtual instances/appliances that can be integrated along with/within an organization's existing infrastructure (firewall, gateway, mail servers, etc.).

Endpoint Security

When it comes to endpoints, the advantage is clearly in the attacker's court – organizations need to protect all the endpoints that come in and out of their environment, while attackers only need to compromise one. Anti-virus, while a good first step, is simply not enough to protect against today's advanced threats.

As a result, we have seen a host of endpoint security solutions crop up that attempt to give organizations visibility and control over endpoints (even those they don't own/control) to protect them from exploit. These solutions tend to integrate with orchestration platforms (or mobile device management (MDM) solutions for mobile endpoints) to minimize management headaches associated with deploying endpoint clients on devices.

These solutions will use a variety of methods to identify threats and then either block or isolate them (so the organization can remediate them) to prevent propagation and mitigate attack damage. There seem to be as many endpoint security solutions out there as there are endpoints. Each is a little different – for example, **FireEye** touts the visibility and extensive threat knowledge their HX Series delivers, while **Cylance** plays up their use of artificial intelligence to proactively prevent persistent threats and malware.

There is also a subset of endpoint security solutions that focus on the threats posed by mobile devices (smartphones and tablets). Mobile presents a variety of attack vectors that can be exploited and used to gain entry to corporate networks. If an attacker compromises a mobile device, they can get access to all the data accessed by that device (corporate, contact lists, calendar info, etc.), as well as use features, such as cameras and microphones to eavesdrop and spy on the individual anywhere they go.

82% of global IT leaders who participated in an IDG Research Services reported the majority of their corporate data is accessible via mobile devices. 74% confirmed they had experienced a data breach as a result of a mobile issue, which is why 90% are making it a priority to increase investments in mobile security. (**Mobile transaction volume was up 200% in the fourth quarter of 2015 versus the previous year**.)

Security Information and Event Management (SIEM)

Organizations are struggling to manage all the information and alerts they receive from all the solutions in their security infrastructure, known as the SIEM space. As we have already noted, it can take weeks or months, for a detected attack to be remediated – that's time in the network the attacker is free to snoop, steal, disrupt and alter critical information.

The problem is information overload. The Security Operations Center (SOC) may receive hundreds/thousands of alerts on a daily/weekly basis. Each alert requires investigation – it requires an admin to gather and make sense of all the information generated by all relevant devices (some of which may not be security – e.g. DNS logs, active directory, etc.), so they understand exactly what is going on in the network/device/app/etc.

Initially, security management platforms focused on bringing the data together (correlating it) and presenting it to the admin for them to explore. Now, with SIEM tools, we are seeing these platforms and new services start to apply intelligence and analytics to help the admin understand what they are looking at, and get at the information they need, easier and faster.

Some companies in the SIEM space include **AlienVault**, **Splunk**, **Intel Security**, **IBM Security**, and **RSA**.

SDx Security Infrastructure Vendor Profiles

The following sections of this report profile some of the vendors focused on delivering SDx solutions that tackling some of the toughest security problems. It by no means represents an exhaustive list, rather if focuses on a select number of products and vendors that have established an early position within the SDx security infrastructure space for data center & cloud security, Iot security, and endpoint security.

These vendors were selected via surveys and polls by SDx readers; they were also identified during discussions the SDxCentral research team had with enterprise and service provider users. The following are the vendors covered in the report:

Akamai Technologies, Allot Communications Ltd, Arkin, Bayshore Networks, Inc., Bromium, Carbon Black, Catbird Security, Centrify Corporation, CipherCloud, Checkpoint, Cisco Systems, Inc., Citrix, CloudPassage, CrowdStrike, Cybera, CyberArk, Cylance, Endgame, FireEye, Fortinet, Huawei, GuardiCore, HyTrust, IBM Security, Kaspersky Labs, Illumio, Imperva, Infoblox, Intel Security, Juniper Networks, Inc., KEMP Technologies, Lastline, LightCyber, M2Mi, Menlo Security, Mocana Corporation, NetNumber, Inc., NetSkope, Nuage Networks, Palo Alto Networks, Proofpoint, Qualys, QOSMOS, RSA Security, Shape Security, Skyhigh Networks, Skyport Systems, Soha Systems, Splunk, Symantec, Tanium, Telco Systems, Trend Micro, Twistlock, vArmour, Vectra Networks, Versa Networks, VMware, Inc., Wedge Networks, Zscaler.

While every attempt has been made to validate the capabilities listed in the profiles, SDxCentral advises end users to verify the veracity of each claim for themselves in their actual deployment environments. SDxCentral cannot be held liable for unexpected operations, damages or incorrect operation due to any inaccuracies listed here.

SDxCentral welcomes feedback and additional information from end users based on their real-world experiences with the products and technologies listed. The SDxCentral Research Team can be reached at **research@sdxcentral.com**.

Juniper Networks, Inc. PUBLIC

(Click for Online Version)

www.juniper.net

1133 Innovation Way
Sunnyvale, CA 94089 USA
srx-info@juniper.net
888.JUNIPER (888.586.4737)

Description of Company: Juniper Networks strives for solutions that give it's customers true advantage over their competition, whether that's bringing new, revenue-generating services to market in minutes versus months; or reducing network costs; enabling smarter, more efficient business processes; providing security and protection for their most valuable assets; or delivering a richer end-user experience. Whatever the challenge, every day our customers set out to build the best possible networks for their businesses. And they look to Juniper Networks to help them do that.

▸ **Juniper Networks, Inc. in SDxCentral Company Directory**

Description of Security Product(s):

vSRX Virtual Firewall: The vSRX delivers core firewall, networking, advanced security, and automated lifecycle management for enterprises and service providers. The industry's fastest virtual security platform, vSRX offers firewall speeds up to 17 Gbps using only two vCPUs, scaling to 100Gbps with 12 vCPUs to provide scalable, secure protection across private, public, and hybrid clouds.

Speed and performance enhancements for the existing vSRX, enabling the industry's first 100G Firewall

▸ **Juniper vSRX Integrated Virtual Firewall in SDxCentral Product Directory**

cSRX Container Firewall: cSRX provides advanced security services, including content security, AppSecure, and unified threat management in a container form-factor. With its small footprint and Docker as a container management system, cSRX enables agile, high-density security service deployment.

A Docker-based, compact SRX (cSRX) in a container form-factor, providing advanced L4-L7 services (Content Security, AppSecure, UTM)

▸ **Juniper cSRX Container Firewall in SDxCentral Product Directory**

SRX Series Services Gateways URL: www.juniper.net/us/en/products-services/security/srx-series

Unique Value Proposition
Software-defined infrastructure is being deployed in data centers globally, delivering significant increases in service agility and cost optimization. Within these virtualized, highly dynamic environments, security must be pervasive. The cSRX and 100G vSRX are key additions to our security portfolio and will further our Software-Defined Secure Networks vision.
Solution Demand
Cloud Service Providers, Financials
Product Areas/Functions
Antivirus & malware protection, Cloud security, Data center security, Container security, Network security/ firewall
Licensing/Pricing
The vSRX provides a base package and optional advanced security services via perpetual, subscription or utility based models.

Company Size
5,001–10,000
Customers
• CloudSeeds: www.juniper.net/us/en/company/case-studies/service-provider/cloudseeds • Expedient: www.juniper.net/us/en/company/case-studies/service-provider/expedient • Orange Business Services: www.juniper.net/us/en/company/case-studies/service-provider/orange-business-services • UniMAP: www.juniper.net/us/en/company/case-studies/public-sector/unimap • Virtual1: www.juniper.net/us/en/company/case-studies/service-provider/virtual1 • VirtualArmor: www.juniper.net/us/en/company/case-studies/service-provider/virtualarmor

Nuage Networks PRIVATE

(Click for Online Version)

www.nuagenetworks.net

755 Ravendale Drive
Mountain View, CA 94043
www.nuagenetworks.net/about-our-company/contact-us
650.623.3300

Description of Company: Nuage Networks brings a unique combination of groundbreaking technologies and unmatched networking expertise. This enables us to create solutions that do more than provide incremental improvement. It allows us to introduce radically new thinking and pick up where the others have left off, delivering a massively scalable SDN solution that makes the datacenter network instantaneous and boundary-less. In a field rife with upstart vendors offering the SDN flavor of the month, Nuage Networks has the pedigree to serve the needs of the world's biggest clouds.

The cloud has made us all promises. Our mission is to help you keep them.

▸ Nuage Networks in SDxCentral Company Directory

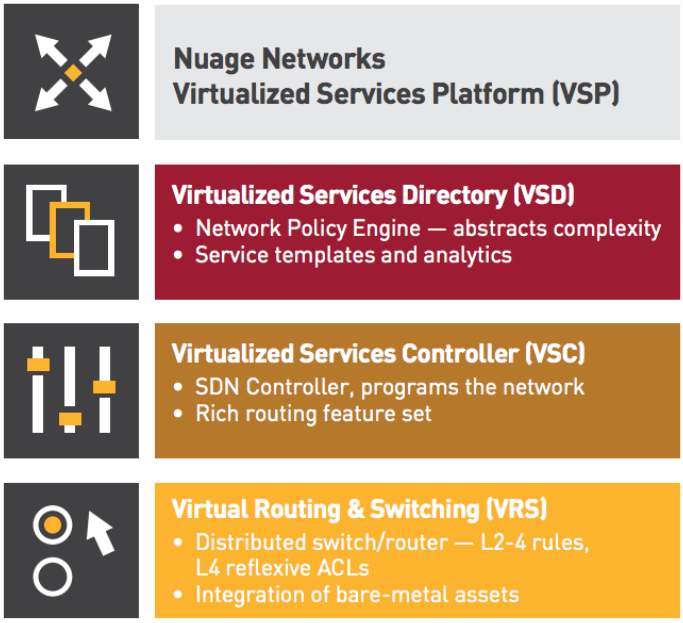
Description of Security Product(s): Nuage Networks Virtual Services Platform (VSP) delivers and manages SDN orchestration and overlay networks on shared datacenter infrastructures, managing connectivity between both physical and virtual workloads, across the data center and WAN. By including virtual and physical security devices in these application networks, Nuage Networks VSP is able to enforce a zero-trust model, where security policies are potentially enforced between every tenant, zone, application, and individual workload.

▸ Nuage Networks Virtualized Services Platform (VSP) in SDxCentral Product Directory

Unique Value Proposition
Microsegmentation and a zero-trust model can halt the lateral spread of malware in contrast to traditional perimeter security approaches. Nuage Networks has been proven in large-scale networks such as cellular providers with billions of end-points. VSP enables detection of malicious end-points with contextual visibility and analytics to quarantine of infected workloads. Users can integrate best-of-breed security analytics and enforcement to meet the most stringent security requirements.
Solution Demand
Cloud Service Providers, Financials, Telecom
Product Areas/Functions
Compliance, Cloud security, Data center security, Container security, IoT security, Network security/ firewall
Company Size
501–1000
Number of customers as of March 2016
50+
Number of active POCs as of March 2016
125+

Customers
Betfair, Banco Santander/Produban, MyRepublic (Singapore), China Mobile, University Pittsburgh Medical Center

FIGURE 1. Nuage Networks VSP is an SDN cloud networking platform that includes the SDN controller and virtual networking infrastructure.



Akamai Technologies PUBLIC

(Click for online version) SDxCentral Directory Listing

www.akamai.com

Description of Security Product(s):
Kona Site Defender provides Integrated website protection against DDoS and web application attacks. Kona Site Defender combines automated DDoS mitigation with a scalable WAF to protect websites from a wide range of online threats, including network and application-layer DDoS, SQL injection and XSS attacks. Kona Site Defender can stop the largest attacks and leverages Akamai's visibility into global web traffic.

Unique Value Proposition	Solution Demand
Akamai has delivered web traffic reaching more than 40 Tbps. On the Akamai network, attacks measured in hundreds of Gbps are absorbed. Kona Site Defender defends against all types of DDoS, web application, and direct-to-origin attacks and optional Akamai FastDNS solution also mitigates attacks on DNS infrastructure. Kona Site Defender is deployed across the Akamai Intelligent Platform, which consists of over 200,000 servers deployed across more than 1,400 networks in over 110 countries.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Advanced threat protection, Compliance, Data center security, Network security/firewall, Web and application security
	Customers
	Ad4Game, Adobe, AirBnB, Afla Laval, American Idol.com

Allot Communications Ltd PUBLIC

(Click for online version) SDxCentral Directory Listing

www.allot.com

Description of Security Product(s):
Allot Web Security solutions empower operators to offer Security-as-a-Service to consumers, SMBs and enterprises. Through full integration with Allot Service Gateway, service providers can rapidly roll out network-based managed security services, including, anti-malware, and parental controls that increase customer loyalty and generate incremental revenue.

Unique Value Proposition	Solution Demand
Allot Communications is a leading provider of security and monetization solutions that enable service providers to protect and personalize the digital experience. Allot leverages the intelligence in data networks, enabling service providers to get closer to their customers; safeguard network assets and users; and accelerate time-to-revenue for value-added services.	Cloud Service Providers, Telecom
	Product Areas/Functions
	Antivirus & malware protection, Cloud security, IoT security, Network security/firewall, Web and application security
	Customers
	Allot solutions are currently deployed at 5 of the top 10 global mobile operators and in thousands of CSP and enterprise networks worldwide with customers such as Vodafone Germany, Swisscom and Datafort among others. The Telecommunications and Information Technology Center of the Generalitat de Catalunya (CTTI) also selected Allot to protect Catalonia's September 2015 elections from Distributed Denial of Service (DDoS) cyber-attacks.

Arkin PRIVATE

(Click for online version) SDxCentral Directory Listing

www.arkin.net

Description of Security Product(s):
Arkin is transforming security and operations for the Software Defined Data Center (SDDC). Several F500/G2000 organizations have deployed the Arkin solution to get deep visibility across virtual and physical, to implement newer security models such as micro-segmentation, and to establish zero-trust security in their data center.

Unique Value Proposition	Solution Demand
Arkin is uniquely positioned as visibility and security platform for the new wave of "software-defined" data centers (SDDCs). Arkin enables modeling and deployment of micro-segmentation security models. Arkin bridges visibility gaps between virtual and physical, and truly connects overlay to underlay. Arkin provides converged operations for the entire datacenter via Google-like search.	Cloud Service Providers, Healthcare, Financials, Government & Education, Retail
	Product Areas/Functions
	Advanced threat protection, Compliance, Cloud security, Data center security, Network security/firewall, Microsegmentation and zero-trust model
	Customers
	California Department of Water Resources (CDWR)

Catbird Security PRIVATE

(Click for online version) SDxCentral Directory Listing

www.catbird.com

Description of Security Product(s):
Catbird provides solutions for software defined segmentation and security for the hybrid IT infrastructure. Catbird's software suite consists of Catbird Insight, which automatically discovers all assets in the virtual fabric and groups them into Catbird TrustZones. Catbird Secure enables automated enforcement of flexible security policies across Catbird TrustZones and detects potential security incidents, initiates corrective enforcement actions and provides instant compliance reporting.

Unique Value Proposition	Solution Demand
Organizations still need to enforce security, compliance, and governance policies as virtualization adoption expands to the network layer and challenges the traditional perimeter model. Perimeter controls also sit outside the virtual fabric, which prevents them from visualizing and securing traffic between virtual machines (east-west traffic). Catbird TrustZones and Secure visualize asset relationships and the east-west traffic flows between them for improved security and analytics.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom
	Product Areas/Functions
	Advanced threat protection, Compliance, Cloud security, Data center security, Visualizing East-West Traffic, Micro-segmentation, Protection against Lateral Spread Attacks, Application-centric Security, Securing VDI Implementations, Continuous Monitoring
	Customers
	www.catbird.com/resources/case-studies

Centrify Corporation PRIVATE

(Click for online version) SDxCentral Directory Listing

www.centrify.com

Description of Security Product(s):
Centrify Identity Service, Centrify Privilege Service and Centrify Server Suite are all part of the Centrify Identity Platform, which secures access to apps and infrastructure from any device, for all users. Solutions include multi-factor authentication, cloud & on-premises apps, privileged access security, big data security, compliance and Mac and mobile management.

Unique Value Proposition	Solution Demand
Centrify uniquely protects enterprise internal and external users as well as privileged accounts to stop the threats at multiple points in the cyberattack chain.	Healthcare, Financials, Government & Education, Telecom, Retail, High tech
	Product Areas/Functions
	Compliance, Cloud security, Data center security, Identity management
	Customers
	National Weather Service, Interval International, HSBC, Citi, GE Capital

Check Point Software Technologies Ltd. PUBLIC

(Click for online version) SDxCentral Directory Listing

www.checkpoint.com

Description of Security Product(s):
Check Point delivers a multi-layered line of defense to help address increasing threats and close security gaps. Consolidation and integration of multiple security appliances using a Next Generation Threat Prevention methodology with common policy management and monitoring results in greater efficiency. Check Point's solution includes "SandBlast" zero-day protection, threat prevention appliances and software, threat intelligence, web security. and DDoS solutions.

Unique Value Proposition	Solution Demand
Check Point Software Technologies Ltd., the largest pure-play security vendor globally protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks including mobile devices, with with enterprise class security management. Check Point promotes academic information and computing security research through the Check Point Institute for Information Security (CPIIS).	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail, Enterprise
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Cloud security, Data center security, Encryption, Identity management, IoT security, Network security/firewall, SIEM, Web and application security, DDoS, Mobile
	Customers
	Check Point customers can be found at www.checkpoint.com/testimonials and include name such as Samsung, SF Police Credit Union, Independence Care System, Optix, Courtagen Life Sciences and more.

CipherCloud PRIVATE

(Click for online version) SDxCentral Directory Listing

www.ciphercloud.com

Description of Security Product(s):
CipherCloud delivers a cloud access security broker (CASB) solution. The CipherCloud Trust Platform integrates two models including the the Cloud Security Broker which provides visibility, control, and data protection through friction-less API integration with multiple clouds, and the Cloud Security Gateway which provides inline protection, enabling you to encrypt or tokenize specific data fields while maintaining exclusive control over the encryption keys.

Unique Value Proposition	Solution Demand
CipherCloud is unique in providing extensive integration capabilities with on-premises and cloud ecosystems. The platform integrates with enterprise DLP, SSO, directories, databases, custom apps, SIEM, and more. CipherCloud also provides broad ecosystem support for key cloud applications. The CipherCloud product portfolio protects popular cloud applications out-of-the-box such as Salesforce, Force.com, Chatter, Box, Google Gmail, Microsoft Office 365, and Amazon Web Services.	Cloud Service Providers, Healthcare, Financials, Government & Education, Enterprise
	Product Areas/Functions
	Antivirus & malware protection, Compliance, Cloud security, Encryption, Network security/firewall, Web and application security, Tokenization, Enterprise Key Management, Cloud Discovery, Activity Monitoring and Anomaly Detection
	Customers
	https://www.ciphercloud.com/customers

Cisco Systems, Inc. PUBLIC

(Click for online version) SDxCentral Directory Listing

www.cisco.com

Description of Security Product(s):
Cisco Advanced Malware Protection provides global threat intelligence via various context sensitive agents such as email, web, and files to provide advanced threat analysis and containment. AMP works both in real-time and retrospectively.

Unique Value Proposition	Solution Demand
• Contextual and correlated global Threat Intelligence • File analysis and threat sandboxing • Realtime malware detection and blocking • Continuous analysis and retrospective security	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Cloud security, Data center security
	Customers
	www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html#Case%20Studies

Citrix PUBLIC

(Click for online version) SDxCentral Directory Listing

www.citrix.com

Description of Security Product(s):
NetScaler AppFirewall is an integral part of Citrix NetScaler, an industry-leading Application Delivery Controller (ADC) that provides secure remote access and application delivery. Chosen by large enterprises, clouds, e-commerce and telcos, NetScaler delivers full instance isolation across physical, virtual, cloud and Container form factors with advanced defenses for packet, network and application attacks. NetScaler is PCI and HIPAA-ready.

Unique Value Proposition	Solution Demand
The software-first design architecture of NetScaler enables customers to run workloads on any standard Intel server. The unique differentiator of NetScaler is the common code base across all form factors, which helps customers by delivering a common operations API and strong investment protection. NetScaler provides the highest level of scalable protection with its Citrix TriScale technology. NetScaler delivers full instance isolation across physical, virtual, cloud and Container form factors.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Compliance, Cloud security, Data center security, Container security, Encryption, Identity management, IoT security, Network security/firewall, Web and application security
	Customers
	Not Provided

CloudPassage PRIVATE

(Click for online version) SDxCentral Directory Listing

www.cloudpassage.com

Description of Security Product(s):
Halo is a security and compliance automation platform purpose-built to deliver a broad range of controls in any application hosting environment, at any scale, on demand. Delivered as a service, Halo provides instant visibility and continuous protection for servers in any combination of data centers, private and public clouds.

Unique Value Proposition	Solution Demand
Using Halo, security teams instantly gain full visibility into their entire infrastructure. Halo bakes security into the deployment process, allowing businesses to securely embrace continuous development methods like DevOps. Halo enables micro-segmentation (reducing risk from lateral movement of threats), and automates manual compliance processes (saving money and improving efficiency).	Cloud Service Providers, Healthcare, Financials, Government & Education
	Product Areas/Functions
	Compliance, Cloud security, Data center security, Container security
	Customers
	eBay, Salesforce, Sony Music, Citrix, Adobe

CrowdStrike PRIVATE

(Click for online version) SDxCentral Directory Listing

www.crowdstrike.com

Description of Security Product(s):
CrowdStrike Falcon Platform is delivered via a Software as a service (SaaS) model combines analytics with threat intelligence to deliver the CrowdStrike Falcon product portfolio: Falcon Host, Falcon Intelligence, and Falcon DNS. The Falcon Platform protects the end point and also monitors 70+ adversarial organizations globally to predict attacks. Additionally, Falcon DNS protects access to a critical component of your network based on that intelligence: your DNS systems.

Unique Value Proposition	Solution Demand
Falcon applies a different strategy: The indicator of attack approach to security. By focusing on more than malware, which only accounts for 40% of all attacks, Falcon identifies Indicators of Attack (IOAs), not just IOCs that malware-based solutions rely on. The architecture employs Falcon Advanced Threat Intelligence Cloud and Threat Graph Data Model, which provide real-time detection and prevention of attacks 24X7.	Healthcare, Financials, Government & Education, Retail, Enterprise
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Web and application security
	Customers
	Not Provided

Cybera PRIVATE

(Click for online version) SDxCentral Directory Listing

www.cybera.com

Description of Security Product(s):
Cybera One is an SDN/NFV based virtual application networking solution and is a fully managed SDN-based security and networking platform for distributed enterprises with extended sites, systems and devices. Cybera One is designed to reduce the inherent complexity of networks by providing a solution that includes hyper-convergence-based security appliances and a Software Defined networking (SDN)/Network Function Virtualization (NFV) based cloud, combined into a single managed platform.

Unique Value Proposition	Solution Demand
With Cybera's virtual application network (VAN) solution, Cybera One, businesses are no longer subject to the pitfalls of connecting multiple applications securely through traditional site-to-site networking models. VANs enable enterprises to deploy multiple applications without security and performance policy conflicts, mitigate the cascading of security threats between applications and network segments, and deploy new applications faster by alleviating bandwidth limits.	Cloud Service Providers, Healthcare, Financials, Government & Education, Retail, Industrial, Enterprise
	Product Areas/Functions
	Antivirus & malware protection, Other end-point threats, Compliance, Cloud security, Data center security, Network security/firewall, Virtual Application Networking (VAN), Universal Policy Controller (UPC)
	Customers
	Verizon, Kahala Brands, Rocky Mountain Chocolate Factory Franchisees, and Shell Stores & Oil

CyberArk PUBLIC

(Click for online version) SDxCentral Directory Listing

www.cyberark.com

Description of Security Product(s):
The CyberArk Privileged Account Security Solution is a centralized policy manager for user management.

The consolidated platform delivers a single management interface, centralized policy creation and management, a discovery engine for provisioning new accounts, enterprise-class scalability and reliability, and a secure digital vault. The CyberArk platform supports LDAP directories, ticketing and workflow systems and supports SIEM integrations, SNMP traps, and email notifications

Unique Value Proposition	Solution Demand
According to CyberArk, privileged accounts represent the largest security vulnerability an organization faces today. CyberArk has developed the broadest suite of offerings for privileged account security management that includes their components of an Enterprise Password Vault, SSH Key Manager, Privileged Session Manager, Privileged Threat Analytics, Application Identity Manager, CyberArk Viewfinity, On-Demand Privileges Manager.	Financials, Government & Education, Enterprise, Industrial
	Product Areas/Functions
	Advanced threat protection, Cloud security, Identity management, Network security/firewall, SIEM, Centralized User Policy Management, Remove vendor access
	Customers
	CyberArk's customers can be found at www.cyberark.com/company/customers and include names Astra-Zeneca, Time, Deloitte, Rockwell Automation, Revlon and more.

FireEye, Inc PUBLIC

(Click for online version) SDxCentral Directory Listing

www.fireeye.com

Description of Security Product(s):
The Fireeye Central Management System consolidates the monitor and administration of the multiple Fireeye products and allows for realtime intelligence on threats.

Unique Value Proposition	Solution Demand
• Realtime threat intelligence • Centralized and correlated analysis of targeted attacks • Dashboard • Central configuration • Centralized reporting	Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Cloud security, Data center security
	Customers
	https://www.fireeye.com/customers.html

Fortinet PUBLIC

(Click for online version) SDxCentral Directory Listing

www.fortinet.com

Description of Security Product(s):
Fortinet's broad security portfolio helps small business, enterprise, industrial, and services providers with the solution called "Fortinet Security Fabric". Fortinet's flagship FortiGate security appliances deliver ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line of complementary solutions goes beyond UTM to help secure the extended enterprise – from endpoints, to the perimeter and the core, including databases and applications.

Unique Value Proposition	Solution Demand
Fortinet's flagship enterprise firewall platform, FortiGate, is available in a wide range of sizes and form factors, and provides a broad array of next generation security and networking functions. Complementary products can be deployed with a FortiGate to enable a simplified, end-to-end security infrastructure covering network security, data center security (physical and virtual), cloud security, secure (wired and wireless) access, infrastructure (switching and routing) security.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Cloud security, Data center security, Container security, IoT security, Network security/firewall, SIEM, Web and application security, SCADA / Industrial
	Customers
	Fortinet's reference-able customers can be found at https://www.fortinet.com/customers.html

GuardiCore Ltd. PRIVATE

(Click for online version) SDxCentral Directory Listing

www.guardicore.com

Description of Security Product(s):
The GuardiCore Centra Security Platform helps address this interior data center security challenge by providing a unique combination of process-level visibility, threat deception, semantics-based analysis and automated response to detect, investigate and mitigate data center threats in real-time. Distributed per hypervisor or server, the Centra Platform offers full coverage of all traffic inside data centers and scales to large network sizes and traffic rates with low performance impact.

Unique Value Proposition	Solution Demand
GuardiCore is the only platform that covers all of these five critical areas for securing east-west traffic in the data center in a single platform: Visibility, Micro-Segmentation, Breach Detection, Automatic Analysis, Response. GuardiCore deception technology employs real machines, services and IP addresses rather than far less effective emulation techniques. This ensures a high-interactive, believable deception environment that is more effective at engaging confirmed attackers.	Cloud Service Providers, Healthcare, Financials
	Product Areas/Functions
	Advanced threat protection, Cloud security, Data center security, Container security
	Customers
	As a private company we do not disclose this information.

Huawei PUBLIC

(Click for online version) SDxCentral Directory Listing

www.huawei.com

Description of Security Product(s):
The Huawei Cloud Data Center Security Solution provides cost-effective, end-to-end security protection for data centers. It meets the basic requirements for data center development, capacity expansion, and service deployment. The solution is built from a variety of Huawei's products including the CloudEngine Data Center Switches, USG-Series Firewalls, and Huawei's Anti-DDoS Solution.

Unique Value Proposition	Solution Demand
Huawei's solution offers on-demand flexibility that allows services to be deployed within minutes. It offers Layer-4 to Layer-7 security as a service to support multi-tennant environments, and also features security virtualization which allows randomly combined software and hardware devices to be deployed into physical and virtual resource pools.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Cloud security, Data center security, Network security/firewall, Web and application security
	Customers
	Alibaba, National Supercomputing Center in ShenZhen, Peking University, TenCent Inc,

Hytrust PRIVATE

(Click for online version) SDxCentral Directory Listing

www.hytrust.com

Description of Security Product(s):
The integrated HyTrust platform includes:

CloudControl – enabling fine grained policy control over administrators and their actions, enabling automated compliance and more.

DataControl – cloud/virtualization encryption and key management - encryption stays with the VM regardless of migration, zero downtime encryption and rekey for painless ongoing compliance;.

BoundaryControl – data sovereignty solution leverages Intel TXT to so VMs can only run on authorized hardware – enabling geofencing.

Unique Value Proposition	Solution Demand
HyTrust enables organizations including enterprise, government, and military to securely move to more virtualization and cloud. It uses military grade encryption featuring zero downtime encryption and rekey. It also includes additional policy enforcement that allows virtual administrators to do what they need to be able to do and nothing more, minimizing risk of error and insider threats. Hytrust also provides data sovereignty solutions that prevent VMs from running on unauthorized hardware.	Cloud Service Providers, Financials, Government & Education
	Product Areas/Functions
	Compliance, Cloud security, Data center security, Container security, Cloud/Virtualization Policy, Data Sovereignty
	Customers
	Visa, Intel, Zurich, Experian

IBM PUBLIC

(Click for online version) SDxCentral Directory Listing

www.ibm.com

Description of Security Product(s):
IBM Dynamic Cloud Security is designed to be flexible and help protect workloads in the cloud, be it Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS). IBM Dynamic Cloud Security creates an integrated system that includes traditional IT, private, public and hybrid cloud models. In addition, IBM Cloud Security Enforcer provide secure access to public cloud services. IBM helps you monitor the cloud for security breaches and compliance violations.

Unique Value Proposition	Solution Demand
IBM Security is a complete solution and a large services organization that can help enterprises manage and protect against risks associated with all models of cloud computing. Services are available to help build and deploy secure apps, better manage and monitor access to business critical applications and more support for cloud security services.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail, Enterprise
	Product Areas/Functions
	Other end-point threats, Compliance, Cloud security, Data center security, Container security, Encryption, Identity management, Network security/firewall, SIEM, Web and application security
	Customers
	Not Provided

Illumio PRIVATE

(Click for online version) SDxCentral Directory Listing

www.illumio.com

Description of Security Product(s):
Illumio ASP is a distributed software platform designed to continuously protect communications within and across tiers of applications. It creates secure segmentation to compartmentalize workloads and applications, reducing the attack surface exposed to cyber vulnerabilities.

Illumio ASP is decoupled from the infrastructure. It supports all server computing formats (Windows/Linux, virtual machines, containers) and all computing environments (data center, private and public cloud).

Unique Value Proposition	Solution Demand
The Illumio ASP attaches adaptive segmentation and enforcement to workloads, allowing the enterprise to secure individual applications and processes without changing subnets, firewalls rules, zones, VLANs, or any existing infrastructure. Illumio delivers adaptive security that works across legacy data centers and modern cloud computing environments providing live visibility, adaptive traffic segmentation, and instant encryption through a centrally managed solution.	Cloud Service Providers, Financials, Enterprise, Software
	Product Areas/Functions
	Compliance, Cloud security, Data center security, Container security, Encryption, Network security/firewall, Web and application security, Key management
	Customers
	https://www.illumio.com/customers

Imperva PUBLIC

(Click for online version) SDxCentral Directory Listing

www.imperva.com

Description of Security Product(s):
Imperva's cyber security platform can be deployed in the cloud or on-premises to protect a single application or tens of thousands of servers. Imperva SecureSphere delivers that data center security, with robust hardware and virtual appliances that provide high performance, resilient components for an exceedingly long product life, and fail-open interfaces for high availability and flexible deployment on VMware ESX and Amazon Web Services (AWS), and SecureSphere virtual appliances.

Unique Value Proposition	Solution Demand
Imperva SecureSphere is a comprehensive, cyber security platform that includes web, database and file security. It scales to meet the security demands of even the largest organizations and is backed by the Imperva Defense Center, a world-class security research organization that maintains the product's cutting-edge protection against evolving threats.	Cloud Service Providers, Healthcare, Financials, Government & Education, Retail, Enterprise
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Cloud security, Data center security, Network security/firewall, SIEM, Web and application security, DDOS
	Customers
	www.imperva.com/Resources/CaseStudies

Infoblox PUBLIC

(Click for online version) SDxCentral Directory Listing

www.infoblox.com

Description of Security Product(s):
Infoblox DNS Firewall is the leading DNS-based network security solution which contains and controls malware that uses DNS to communicate with C&Cs and botnets. It works by employing DNS Response Policy Zones (RPZs), automated threat intelligence, and optional Infoblox Threat Insight to prevent data exfiltration. Infoblox External DNS Security provides defense against the widest range of DNS-based attacks such as DNS DDoS, exploits, NXDOMAIN, and DNS hijacking attacks.

Unique Value Proposition	Solution Demand
It's critical that the technology you deploy for network control provide maximum protection and offer minimum attack surface. Infoblox is clearly differentiated from other vendors with regards to security as the industry's first DDI vendor to seamlessly integrate with leading security solutions to enable contextual sharing of threat intelligence and automation of response workflows, providing better protection against evolving threats.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Antivirus & malware protection, Compliance, Data center security, IoT security, Network security/firewall
	Customers
	Adobe Systems, Geisinger Health System, Council Rock School District, Clark County School District, Everi Holdings, Inc.

Intel Security PUBLIC

(Click for online version) SDxCentral Directory Listing

www.intelsecurity.com

Description of Security Product(s):
McAfee Virtual Network Security Platform from Intel Security provides next-generation IPS protection that segments and secures traffic between virtual machines and virtualized workloads in private and hybrid cloud environments. Enterprise SDDC operators and multi-tenant service providers will benefit from strong micro-segmentation along with rapid discovery and blocking of advanced threats.

Unique Value Proposition	Solution Demand
McAfee Virtual Network Security Platform can be deployed as a VNF for fully automated security within VMware NSX and other virtualized environments. Centralized management simplifies and unifies policy deployment and administration, while integration with McAfee sandboxing, SIEM, endpoint, and server security solutions enables complete ownership of the threat defense lifecycle.	Healthcare, Financials, Government & Education
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Cloud security, Data center security, Network security/firewall
	Customers
	Not Provided

KEMP Technologies PRIVATE

(Click for online version) SDxCentral Directory Listing

http://kemptechnologies.com

Description of Security Product(s):
KEMP's Application Firewall Pack (AFP) combines Layer 7 Web Application Firewall protection with other application delivery services including intelligent load balancing, intrusion detection, intrusion prevention, edge security, and authentication. Kemp AFP utilizes an open source web application firewall engine, ModSecurity, and augments threat intelligence and research from Trustwave to provide ongoing protection against known and evolving vulnerabilities.

Unique Value Proposition	Solution Demand
KEMP AFP along with KEMP LoadMaster provides integrated security capabilities including Web Application Firewall protection (WAF), edge security, L7 IPS/IDS, DDos Mitigation, application publishing and authentication services as standard features on all platforms including select hardware appliances. KEMP also provides PCI-DSS Compliance protecting web applications focusing on those which process payments reducing the need for extensive code reviews with regularly updated rule sets.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Enterprise.
	Product Areas/Functions
	Advanced threat protection, Cloud security, Identity management, Network security/firewall, Layer 7 web application firewall, intelligent load balancing, intrusion detection, intrusion prevention as well as edge security.
	Customers
	KEMP's broad market focus includes small-to-medium sized businesses, Fortune 1000 enterprises, remote enterprise branch offices, managed service providers and public sector clients, who view end-user satisfaction and IT web and application infrastructure reliability and optimization as mission-critical to their long-term success.

Lastline PRIVATE

(Click for online version) SDxCentral Directory Listing

www.lastline.com

Description of Security Product(s):
The Lastline Breach Detection Platform is comprised of four core components: Sensor, Engine, Manager and Advanced Threat Intelligence. The four components work together to continuously monitor all datastreams, expose IOCs related to active data breaches, and prioritize incidence response.

Unique Value Proposition	Solution Demand
Lastline provides comprehensive detection of advanced and evasive threats across the entire enterprise and operating systems (Windows, Mac OS X, and Android), physical and virtual hosts, services, users, network infrastructure and Web, email, file, and mobile applications. Lastline's flexible software-base platform allows organizations to scale their breach defenses on a predictable basis, from a single location to any number of remote, branch, and mobile offices. Licensing is done by user.	Cloud Service Providers, Financials, Government & Education, Enterprise
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Cloud security, Data center security, Container security, Encryption, Identity management, Network security/ firewall, SIEM, Web and application security
	Customers
	https://www.lastline.com/customers/success

LightCyber PRIVATE

(Click for online version) SDxCentral Directory Listing

http://lightcyber.com

Description of Security Product(s):
LightCyber solves the data breach crisis with Behavioral Attack Detection to provide accurate and efficient security visibility into attackers that have slipped through the cracks of traditional security controls. The LightCyber Magna platform pinpoints network intruders & malicious insiders by detecting their operational activities. Today, most enterprises and organizations lack the ability to find an active attacker on their network. The industry average is five months to discover an intruder.

Unique Value Proposition	Solution Demand
Using machine learning, LightCyber Magna profiles all users and devices to learn good behavior on a network and discern malicious anomalies. It is the first security product to integrated user, network and endpoint context to provide security visibility into a range of attack activity, including targeted external attacks, internal threats, risky behavior and opportunistic malware. Magna uses machine learning, full network DPI and agentless, on-demand client technology to produce few alerts.	Healthcare, Financials, Government & Education, Telecom, Retail, Legal, Energy, Manufacturing
	Product Areas/Functions
	Behavioral Attack Detection
	Customers
	Not Provided

NetNumber, Inc. PRIVATE

(Click for online version) SDxCentral Directory Listing

http://netnumber.com

Description of Security Product(s):
The NetNumber Multi-Protocol Signaling Firewall solution provides network-wide ability to mitigate security threats such as ID spoofing, information threats and DoS attacks at the signaling layer. Automatically blocks unwanted signaling traffic that can accumulate rapidly and impact network stability and availability; shapes inbound and outbound traffic to manage traffic bursts from IoT devices; and provides operational consistency across all signaling firewalls for SS7, Diameter, SIP, etc.

Unique Value Proposition	Solution Demand
NetNumber offers the industry's most comprehensive multi-protocol signaling firewall on its TITAN platform, providing firewall capabilities for all signaling protocols including SS7, Diameter, SIP, HTTP and DNS/ENUM. As these firewall applications can be combined seamlessly with other NetNumber applications such as an STP, DSC, HSS or HLR on the same TITAN platform, operators have an unprecedented level of multi-protocol signaling protection, flexibility, and operational uniformity.	Telecom
	Product Areas/Functions
	IoT security, Network security/firewall
	Customers
	Not Provided

Netskope PRIVATE

(Click for online version) SDxCentral Directory Listing

www.netskope.com

Description of Security Product(s):
The Netskope Active Platform gives IT the ability to find, understand, and secure cloud apps. Netskope empowers organizations to gain surgical visibility and control, protect sensitive data using "noise-cancelling" data loss prevention (DLP), and ensure compliance in real-time, on any device, for any cloud application. There are three primary phases of safe cloud enablement that Netskope provides: find, understand, and secure. Netskope also provides reporting on those cloud analytics.

Unique Value Proposition	Solution Demand
The Netskope Active Platform combines four key areas that are required by cloud access security brokers to be considered enterprise class solutions that include advanced enterprise DLP, granular policies for all applications, a solution that is architected for any use case, and providing active threat protection. Most CASBs provide a subset of the solutions required to address all business problems.	Cloud Service Providers, Healthcare, Financials
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Cloud security, Encryption, IoT security, DLP, Shadow IT, Vendor Assurance
	Customers
	Netskope customers can be found at https://www.netskope.com/customers and include Amgen, Netapp, Starbucks, Nvida, New York Life and more.

Palo Alto Networks PUBLIC

(Click for online version) SDxCentral Directory Listing

www.paloaltonetworks.com

Description of Security Product(s):
Palo Alto Networks has long secured networks with rich security devices. Today, Palo Alto's Aperture extends the visibility and granular control traditional network security into cloud / SaaS applications themselves. Because SaaS can be invisible to traditional IT, Aperture integrates into SaaS applications directly, providing full visibility into the day-to-day activities of users and data. Granular controls ensure policy is maintained to eliminate data exposure and threat risks.

Unique Value Proposition	Solution Demand
Palo Alto Networks has combined network, cloud, and endpoint security into a tightly integrated platform that delivers automated prevention against cyberattacks including known and unknown. Palo Alto's security platform, based on PAN OS 7.1, is focused eliminating threats by integrating Next-Generation Firewall, Advanced Endpoint Protection, and Threat Intelligence Cloud suites into a single solution supporting all clouds with highly automated preventative measures against cyberthreats.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail, Electric Utilities, ICS & SCADA, Oil & Gas
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Cloud security, Data center security, Network security/firewall, SIEM, IPS, URL filtering, threat intelligence
	Customers
	Palo Alto Networks customers can be found at https://www.paloaltonetworks.com/customers and include University South Hampton, University of Colorado, Ausram, Mercy Medical Center, and more.

Qosmos PRIVATE

(Click for online version) SDxCentral Directory Listing

www.qosmos.com

Description of Security Product(s):
Qosmos ixEngine is a Software Development Kit (SDK) composed of software libraries and tools that are easily integrated into new or existing solutions. Developers benefit from market-leading IP flow parsing technology to accelerate the delivery of application aware solutions. Qosmos ixEngine can be used in all environments: physical, virtualized and in SDN architectures.

Unique Value Proposition	Solution Demand
Qosmos provides the richest view into network traffic on the market today, with thousands of protocols classified and metadata attributes extracted. Security vendors embedded our software into their solutions for a wide array of software form factors and security use cases, including for virtualized environments and container-based architectures.	Cloud Service Providers, Telecom
	Product Areas/Functions
	Advanced threat protection, Cloud security, Data center security, Container security, Network security/firewall, SIEM
	Customers
	HPE, Clavister, F5 Networks

Qualys PUBLIC

(Click for online version) SDxCentral Directory Listing

www.qualys.com

Description of Security Product(s):
Qualys' flagship product, QualysGuard Cloud Platform and its integrated suite of security and compliance applications provides organizations with a global view of their security and compliance solutions. The QualysGuard solutions include vulnerability management, policy compliance, web application scanning, malware detection and Qualys SECURE Seal for security testing of web sites.

Unique Value Proposition	Solution Demand
Qualys sensors, a core service of the Qualys Cloud Plaform, extends security throughout global enterprises. These sensors, which can be in the form of appliances or lightweight agents, are remotely deployable, centrally managed and self updating. Qualys sensors collect threat data automatically and it is used as critical data by the Qualys Cloud Platform, which continuously analyzes and correlate the information to identify threats and eliminate vulnerabilities.	Healthcare, Financials, Government & Education, Telecom, Retail, Insurance, & Media
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Network security/firewall, Web and application security, Security assessment questionnaire, and secure seal for security testing of websites
	Customers
	Qualys customers can be found at https://www.qualys.com/customers and include Oracle, Cisco, T-Mobile, Facebook, HPE, and more.

Shape Security PRIVATE

(Click for online version) SDxCentral Directory Listing

www.shapesecurity.com

Description of Security Product(s):
Shape Security Application Defense is delivered as a service via cloud or enhanced control integrated into physical or virtual infrastructure focusing on security, fraud, network operations, application development, prevention, detection and response, machine learning systems and network data. Any combination of these is also supported, and no changes to your website or mobile API servers are required.

Unique Value Proposition	Solution Demand
Shape Security offers clients a a full platform, with continuous improvement, with unique application defense functions in each stage of Gartner's Adaptive Protection Architecture. Shape enhances every team that helps defend your applications, including your NOC, SOC, fraud team, and application security team, helping each of them with their most difficult attacks and deliver this as a service, without requiring functionality changes, complex integrations, or requiring headcount.	Healthcare, Financials, Government & Education, Retail
	Product Areas/Functions
	Advanced threat protection, Other end-point threats, Compliance, Cloud security, Network security/firewall, Web and application security, Mobile application attacks, like credential stuffing, content scraping, and application DDoS.
	Customers
	Shape Security does not provide a customer list, but does have a list of industry case studies available at https://www.shapesecurity.com/case-studies

Skyhigh Networks PRIVATE

(Click for online version) SDxCentral Directory Listing

www.skyhighnetworks.com

Description of Security Product(s):
Skyhigh is a cloud access security broker (CASB). With Skyhigh, organizations leverage a single cross-cloud platform to gain visibility into cloud usage and risks, meet compliance requirements, enforce security policies, and detect and respond to potential threats.

Unique Value Proposition	Solution Demand
Skyhigh discovers all cloud services in use and provides a 1-10 CloudTrust Rating of enterprise readiness for each service, reveals gaps in cloud policy enforcement, and enables real-time coaching and policy enforcement to guide users to corporate-sanctioned services. Skyhigh leverages machine learning to accurately detect insider threats, compromised accounts, privileged user threats, and attacks using the cloud as a data exfiltration vector.	Cloud Service Providers, Healthcare, Financials, Government & Education, Enterprise, Manufacturing
	Product Areas/Functions
	Compliance, Cloud security, Data center security, Identity management, Network security/firewall, SIEM, Web and application security
	Customers
	Skyhigh network custoers can be found at https://www.skyhighnetworks.com/customers and include Adventist Health System, Western Union, DirecTV, Equinix, and Perrigo.

Skyport Systems PRIVATE

(Click for online version) SDxCentral Directory Listing

www.skyportsystems.net

Description of Security Product(s):
Skyport provides turnkey, secure infrastructure as a service. The SkySecure Platform is designed to host critical and exposed application workloads simply and securely. Each application is provided its own secure enclave on the user's premises, with security and infrastructure services as well as auditing managed centrally. SkySecure protects against data and credential theft, lateral attacks and unpatched vulnerabilities.

Unique Value Proposition	Solution Demand
SkySecure integrates 12 always-on security functions with hardened infrastructure, which simplifies operations while simultaneously providing more effective security. The unified policy model and integrated workflow for infrastructure and security configuration and management supports collaboration across disciplines.	Healthcare, Financials, Media
	Product Areas/Functions
	Compliance, Data center security, Identity management, Network security/firewall, Web and application security, Infrastructure security
	Customers
	Not Provided

Soha Systems PRIVATE

(Click for online version) SDxCentral Directory Listing

http://soha.io

Description of Security Product(s):
Soha Systems brings a radically new approach for employee and third-party access to applications hosted in data centers and hybrid cloud environments. Our service, Soha Cloud, provides a unique alternative to traditional remote access technologies. With Soha Cloud, no one can get to applications directly because they are hidden from the Internet and public exposure.

Unique Value Proposition	Solution Demand
Soha Cloud's unique dual-cloud architecture closes all inbound firewall ports while providing authenticated end users access to only their specific applications. Soha Cloud integrates data path protection, identity access, application security and management visibility and control into a single service. Soha Cloud can be deployed in minutes, through a unified portal, with a single point of control, in any network environment, and at a fraction of the cost of traditional solutions.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Other end-point threats, Compliance, Cloud security, Data center security, Identity management, IoT security, Network security/firewall, Web and application security
	Customers
	Not Provided

Symantec Corporation PUBLIC

(Click for online version) SDxCentral Directory Listing

www.symantec.com

Description of Security Product(s):
Symantec offers a complete suite of products that include security management, threat protection, threat detection, identity management, and endpoint protection. In addition to security products, Symantec also offers cyber security services. Customers can take advantage of Symantec's experts, global threat intelligence, advanced monitoring, incident response, and cyber readiness services.

Unique Value Proposition	Solution Demand
Only Symantec offers the following advantages: 1) Better security with real-time reputation and behavioural monitoring technology 2) Enhanced performance – 70 percent lower scan overheads and number one in performance vs. Kaspersky, Trend Micro, Sophos, Microsoft, and McAfee 3) Tested and optimised for today's virtual environments. 4) Faster, flexible management for simple upgrading and configuration 5) Smart scheduling technology intelligently scans during idle periods	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Advanced threat protection, Other end-point threats, Cloud security, Data center security, Encryption, Identity management, Network security/firewall, Web and application security
	Customers
	Asia Pacific Telecom, The State of Oklahoma, Hillsborough County Public Schools, Mary Washington Healthcare and others can be seen at www.symantec.com/resources/customer_success

Telco Systems PRIVATE

(Click for online version) SDxCentral Directory Listing

www.telco.com

Description of Security Product(s):
NFV CyberGuard is a virtualized cybersecurity solution for protecting SDN and NFV infrastructures. The solution consists of advanced networking probes, NFVI agents, and a big data analytics engine. It provides complete visibility of the entire network, real-time analysis of network threats and the ability to apply cybersecurity policies to the entire infrastructure.

Unique Value Proposition	Solution Demand
1) NFV CyberGuard is designed specifically to protect SDN and NFV networks. 2) NFV CyberGuard is deployed as a NFV at the network edge at the closest point to all endpoints, providing real-time monitoring and analysis of network threats, complete visibility of the entire network and the ability to apply cybersecurity policies and efforts to the entire infrastructure. 3) NFV CyberGuard includes an open API for integration of external systems and third-party applications and algorithms.	Telecom
	Product Areas/Functions
	Advanced threat protection, Compliance, Cloud security, Data center security, Container security, NFVi and SDN specific cybersecurity threats
	Customers
	Not Provided

Trend Micro PUBLIC

(Click for online version) SDxCentral Directory Listing

www.trendmicro.com

Description of Security Product(s):
Trend Micro offers a complete range of security products for home, small business, and medium-sized enterprises. It consists of a combination of cloud-based security services, virus protection, web security, advanced threat protection, endpoint security, mobile security, and centralized security management.

Unique Value Proposition	Solution Demand
The Trend Micro Smart Protection Network mines data around the clock and across the globe to ensure that you are always protected. We use our up-to-the-second threat intelligence to immediately stamp out attacks before they can harm you. And the same accelerated cloud security powers all of our products and services, protecting millions of businesses and users around the globe. Since 2009, IDC has ranked Trend Micro as the global market leader in server security.	Retail, SMB
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Cloud security, Web and application security
	Customers
	AlliedTelesyn, A&W, Mazda, McGill University, the United Way and other success stories can be seen at http://cloudsecurity.trendmicro.com/us/technology-innovation/customers-partners/index.html

Twistlock PRIVATE

(Click for online version) SDxCentral Directory Listing

www.twistlock.com

Description of Security Product(s):
Twistlock provides an enterprise suite for container security. We address risks on the host and within the containerized applications, enabling organizations to enforce consistent security policies from development to production. Our innovative technologies monitor container activities, manage vulnerabilities, detect and isolate threats targeting production containers. Twistlock's mission is to provide an end-to-end, enterprise-grade security stack for the container environment.

Unique Value Proposition	Solution Demand
Twistlock's Container Security Suite allows organizations to a) detect and manage security vulnerabilities within containerized applications, b) enforce security best practices across the container lifecycle, and c) detect and isolate advanced threats targeting containers in production. We do all this without changing your hosts, your containers or your applications. We also provide extensive integration with existing ecosystem tools to maximize your current investments.	Financials, Government & Education
	Product Areas/Functions
	Advanced threat protection, Container security
	Customers
	AppsFlyer, Wix. One of the largest medical research centers in the US, a fortune 50 insurer, two intelligence community US government agencies, and one of the largest digital media service providers.

vArmour PRIVATE

(Click for online version) SDxCentral Directory Listing

www.varmour.com

Description of Security Product(s):
vArmour is the industry's first distributed security system for application-aware micro-segmentation with advanced security analytics. With its patented software, vArmour DSS moves security next to each asset, wrapping fine-grained protection around each workload, regardless of location. Monitoring of network, applications, and users combined with control of 100% data center and cloud traffic helps organizations prevent, detect, and respond to security events from a single, integrated system.

Unique Value Proposition	Solution Demand
vArmour DSS is built to protect data centers and clouds at scale. 1. Broad: Protects across multi-clouds, with centralized policy & 10X* throughput 2. Deep: Contextual visibility & control of users and Layer 2-7 traffic 3. Independent: Policy abstraction from workloads maintains state & integrity 4. Integrated: Built-in analytics with inline policy for 1-click threat detection-to-quarantine 5. Simple: Deploy micro-segmentation in minutes, not months, in 3 steps (*compared to alternatives).	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Advanced threat protection, Cloud security, Data center security, Network security/firewall
	Customers
	John Muir Health, Booz Allen Hamilton, Education Networks of America, Equens

Vectra Networks PRIVATE

(Click for online version) SDxCentral Directory Listing

www.vectranetworks.com

Description of Security Product(s):
The Vectra Networks X-series platform continuously monitors network traffic, detects active cyber attacks as they progress inside the network, and prioritizes the highest-risk threats based on certainty and severity scores – automatically and in real time.

The Vectra Networks S-series sensors are easy to deploy at remote sites or with access switches on internal network segments to extend the reach of the Vectra X-series platform.

Unique Value Proposition	Solution Demand
Vectra Networks closes the dangerous security gap between perimeter defenses and post-breach analysis by detecting the actions and behaviors of cyber attackers who spy, spread and steal inside networks. Automatically and in real time, Vectra detects attacks in progress and prioritizes the highest-risk threats so you can quickly mitigate and prevent data loss.	Healthcare, Financials, Government & Education, Telecom, Retail, Energy, Gaming and Hospitality, Manufacturing, Media, Professional Services, Technology
	Product Areas/Functions
	Advanced threat protection
	Customers
	Not Provided

Versa Networks PRIVATE

(Click for online version) SDxCentral Directory Listing

www.versa-networks.com

Description of Security Product(s):
Versa enables providers to deliver more agile and cost-efficient managed security by migrating from hardware-based services to software that leverages virtualized network and security functions (VNFs). Versa provides a broad set of security VNFs, including NG firewall, malware protection, URL and content filtering, IPS and anti-virus, DDOS and VPN/NG VPN.

All of these VNFs run on commodity hardware in both the head-end and branch office, and are service-chained and fully multi-tenant.

Unique Value Proposition	Solution Demand
Versa managed security solutions have built-in multi-tenancy, service chaining, elasticity, and zero-touch provisioning, enabling providers to deliver security services much more rapidly, with far lower capital and operating costs than proprietary CPE-based managed services, resulting in faster time-to-service, higher revenue and profitability.	Financials, Telecom
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Cloud security, Encryption, Network security/ firewall, Web and application security
	Customers
	Orange, Colt, RCN

VMware, Inc. PUBLIC

(Click for online version) SDxCentral Directory Listing

http://www.vmware.com

Description of Security Product(s):
The VMware NSX embeds networking and security functionality that is typically handled in hardware directly into the hypervisor. It delivers the operational model of a virtual machine for networking and security. It reproduces in software the entire networking environment, including L2, L3 and L4–L7 network services within each virtual network. It delivers micro-segmentation and granular security to the individual workload, enabling a fundamentally more secure data center.

Unique Value Proposition	Solution Demand
VMware NSX enables organizations to divide the data center into distinct security segments logically, down to the level of the individual workload – irrespective of the workload's network subnet or VLAN. It reduces network provisioning time from days to seconds and improves operational efficiency through automation. It also offers enhanced security and advanced networking services through an ecosystem of leading third-party vendors.	Financials, Government & Education, Retail, Enterprise
	Product Areas/Functions
	Data center security, Network security/firewall
	Customers
	Tribune Media, IBM, Armor, University of New Mexico, Exostar and others can be seen at www.vmware.com/products/nsx/customerstories.html

Wedge Networks PRIVATE

(Click for online version) SDxCentral Directory Listing

http://wedgenetworks.com

Description of Security Product(s):
Wedge Networks' Cloud Network Defense is an orchestrated threat management platform designed to enforce security at the cloud-layer of the network to combat the shifting threat landscape associated with cloud, mobility, bring your own device, Internet of Things and consumerization of IT.

Unique Value Proposition	Solution Demand
With Cloud Network Defence, by applying security policies at the cloud-layer, enterprises and network operators offering security-as-a-service can achieve more effective security, using best-in-class, continuously updated multi-vendor technologies for EverGreen Security, with greater efficiency and scale.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Cloud security, Data center security, IoT security, Network security/firewall, SIEM, Web and application security
	Customers
	Not Provided

Zscaler PRIVATE

(Click for online version) SDxCentral Directory Listing

www.zscaler.com

Description of Security Product(s):
Zscaler's secure web gateway architecture was created as a pure cloud product. It delivers a multi-tenant scalable platform by distributing components of a standard proxy to create a network that acts as a single virtual proxy. Users access any / nearest gateway for policy-based secure Internet access. Zscaler infrastructure comprises three key components: Zscaler Enforcement Nodes (ZENs), Central Authority (CA), and Nanolog Servers.

Unique Value Proposition	Solution Demand
Zscaler benefits from fifty newly patented technologies including a distributed, multi-tenant architecture, that supports 10 Gbps throughput based on a next-gen TCP stack and single scan multiple action technology that enables inspection of every byte of traffic by every service. Other components of the Zscaler solution include ByteScan, which provides ultrafast content scanning, Page Risk Index, which analyzes real-time web activities, and Nanolog, which encrypts web-logs.	Cloud Service Providers, Healthcare, Financials, Government & Education, Retail, Enterprise, Manufacturing, Consumer Goods, SMB
	Product Areas/Functions
	Advanced threat protection, Other end-point threats, Cloud security, Identity management, Network security/ firewall, Web and application security, Data Loss Prevention, SSL Inspection, Guest Wifi, Internet Security
	Customers
	Zscaler customers can be found at https://www.zscaler.com/customers and include Jabil, Johnston Controls, Lazy Boy, United Airlines, Avaya and more.

Allot Communications Ltd PUBLIC

(Click for online version) SDxCentral Directory Listing

www.allot.com

Description of Security Product(s):
Allot Web Security solutions empower operators to offer Security-as-a-Service to consumers, SMBs and enterprises. Through full integration with Allot Service Gateway, service providers can rapidly roll out network-based managed security services, including, anti-malware, and parental controls that increase customer loyalty and generate incremental revenue.

Unique Value Proposition	Solution Demand
Allot Communications is a leading provider of security and monetization solutions that enable service providers to protect and personalize the digital experience. Allot leverages the intelligence in data networks, enabling service providers to get closer to their customers; safeguard network assets and users; and accelerate time-to-revenue for value-added services.	Cloud Service Providers, Telecom
	Product Areas/Functions
	Antivirus & malware protection, Cloud security, IoT security, Network security/firewall, Web and application security
	Customers
	Allot solutions are currently deployed at 5 of the top 10 global mobile operators and in thousands of CSP and enterprise networks worldwide with customers such as Vodafone Germany, Swisscom and Datafort among others. The Telecommunications and Information Technology Center of the Generalitat de Catalunya (CTTI) also selected Allot to protect Catalonia's September 2015 elections from Distributed Denial of Service (DDoS) cyber-attacks.

Bayshore Networks PRIVATE

(Click for online version) SDxCentral Directory Listing

www.bayshorenetworks.com

Description of Security Product(s):
The Bayshore IT/OT Gateway is a content-aware cybersecurity platform for industrial enterprises. The platform secures data and transactions for industrial IoT operations and Machine-to-Machine (M2M) communications. It inspects, dissects and filters industrial application data streaming through the network using deep inspection at t he content level where it can secure, segment, filter and isolate machine application data not just machines or endpoints.

Unique Value Proposition	Solution Demand
The platform deploys as a cloud-based service, a virtual machine, or a bump-in-the-wire hardware appliance and is distinguished by granular inspection and filtering of network flows, policy building and enforcement, and its ability to detect, parse and segment industrial protocols. Bayshore IT/OT Gateway is designed for industrial environments and can feed machine telemetry to analytics engines such as SAP, Splunk and GE Predix.	Industrial Enterprise
	Product Areas/Functions
	Advanced threat protection, Compliance, Network security/firewall, Predictive Maintenance, Plant Safety, Industrial Controls, L7 Network Segmentation
	Customers
	Bayshore has strategic partnerships with leading technology companies including Cisco Systems and BAE Systems.

Check Point Software Technologies Ltd. PUBLIC

(Click for online version) SDxCentral Directory Listing

www.checkpoint.com

Description of Security Product(s):
Check Point delivers a multi-layered line of defense to help address increasing threats and close security gaps. Consolidation and integration of multiple security appliances using a Next Generation Threat Prevention methodology with common policy management and monitoring results in greater efficiency. Check Point's solution includes "SandBlast" zero-day protection, threat prevention appliances and software, threat intelligence, web security. and DDoS solutions.

Unique Value Proposition	Solution Demand
Check Point Software Technologies Ltd., the largest pure-play security vendor globally protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks including mobile devices, with with enterprise class security management. Check Point promotes academic information and computing security research through the Check Point Institute for Information Security (CPIIS).	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail, Enterprise
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Cloud security, Data center security, Encryption, Identity management, IoT security, Network security/firewall, SIEM, Web and application security, DDoS, Mobile
	Customers
	Check Point customers can be found at www.checkpoint.com/testimonials and include name such as Samsung, SF Police Credit Union, Independence Care System, Optix, Courtagen Life Sciences and more.

Cisco Systems, Inc. PUBLIC

(Click for online version) SDxCentral Directory Listing

www.cisco.com

Description of Security Product(s):
Cisco Advanced Malware Protection provides global threat intelligence via various context sensitive agents such as email, web, and files to provide advanced threat analysis and containment. AMP works both in real-time and retrospectively.

Unique Value Proposition	Solution Demand
• Contextual and correlated global Threat Intelligence • File analysis and threat sandboxing • Realtime malware detection and blocking • Continuous analysis and retrospective security	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Cloud security, Data center security
	Customers
	www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html#Case%20Studies

Kaspersky Lab PRIVATE

(Click for online version) SDxCentral Directory Listing

http://usa.kaspersky.com

Description of Security Product(s):
Kaspersky Endpoint Security for Enterprise provides security teams with full visibility and control over every endpoint, static or mobile, under your jurisdiction, wherever it sits and whatever it's doing. A scalable solution provides access to inventories, licensing, remote trouble-shooting and network controls, all accessible from one console, the Kaspersky Security Center. Security solutions range from encryption, application controls and whitelisting to web controls.

Unique Value Proposition	Solution Demand
Kaspersky provides a next-generation endpoint security platform, powered by a global intelligence network (Kaspersky Security Network), which provides a higher level of business processes and data protection together with a wide range of security capabilities to fight advanced threats (detecting suspicious activities and protecting against zero-day attacks). Kaspersky protects all endpoints including desktops, servers, mobile devices, and virtual machines.	Healthcare, Financials, Government & Education, Home, Small Business, Enterprise, Industrial
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Cloud security, Data center security, Encryption, IoT security, Network security/firewall, SIEM, Web and application security, DDoS, Indudstrial, Mobile Security, Virtualization Security
	Customers
	A list of Kaspersky customers can be found at http://usa.kaspersky.com/about-us/why-kaspersky/success-stories and include, Nedis, Univesity of Chile, Swiss Exhibition, The Minol Group, Grupa Remontowa SA, and more.

Machine-to-Machine Intelligence (M2Mi) PRIVATE

(Click for online version) SDxCentral Directory Listing

www.m2mi.com

Description of Security Product(s):
M2Mi's patented Lockbox Security module, part of the M2Mi platform, addresses the scale and unique architectural requirements of the diverse M2M & IoT ecosystem. M2Mi ensures that access to a resource meets Lockbox security policies. M2Mi protects each and every asset, device and transaction within the connected ecosystem. M2Mi Security provides key management across to provide secure connectivity from devices to and through the entire enterprise, industrial operation, and data center.

Unique Value Proposition	Solution Demand
The M2M Intelligence M2M and IoT platform provides three groups of modules including infrastructure, insight, and monetization. Security is a key component of all as the M2M and IoT environment is ever changing. Lockbox security policies are dynamic and based on the current context and state of the environment. For example, it can allow message transfer only if the connection is within a certain geography or using SSL. Security policies can also be customized based on company requirements.	Software, Enterprise, Industrial, IoT, Oil, Automobile, Agribusiness
	Product Areas/Functions
	Cloud security, Data center security, Encryption, Identity management, IoT security, Network security/firewall, Cyber security, Machine-To-Machine
	Customers
	M2Mi customers can be found at www.m2mi.com/industry/customers and include IBM, Oracle, Intel, Siemens, and more.

Mocana PRIVATE

(Click for online version) SDxCentral Directory Listing

www.mocana.com

Description of Security Product(s):
Mocana corporation's IoT security platform is designed for any device that is networked connected. Mocana's Security of Things Platform is a collection of security software that addresses various security issues in industrial automation, federal organizations, automotive, and healthcare. All Mocana IOT security software components are OS/ Microcontroller independent, and this architecture allows customers to easily implement in their existing infrastructure across multiple projects.

Unique Value Proposition	Solution Demand
Mocana's highly certified solution addresses IoT vulnerabilities in various industries. Mocana's byte-efficient code provides solid security for devices in every industry, from automotive to government. Mocana's cryptographic library is FIPS 140-2 Level 1 certified with strong cryptography tested in real time. Mocana's solution addresses unique threat areas from authorization to secure boot to firmware validation to preventing data leakage in cloud connectivity in a single platform.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail, Auto, SmartCity, Oil and Gas, Agribusiness, IoT
	Product Areas/Functions
	Advanced threat protection, Other end-point threats, Compliance, Cloud security, Data center security, Encryption, Identity management, IoT security, Network security/firewall, SIEM
	Customers
	Not Provided

Netskope PRIVATE

(Click for online version) SDxCentral Directory Listing

www.netskope.com

Description of Security Product(s):
The Netskope Active Platform gives IT the ability to find, understand, and secure cloud apps. Netskope empowers organizations to gain surgical visibility and control, protect sensitive data using "noise-cancelling" data loss prevention (DLP), and ensure compliance in real-time, on any device, for any cloud application. There are three primary phases of safe cloud enablement that Netskope provides: find, understand, and secure. Netskope also provides reporting on those cloud analytics.

Unique Value Proposition	Solution Demand
The Netskope Active Platform combines four key areas that are required by cloud access security brokers to be considered enterprise class solutions that include advanced enterprise DLP, granular policies for all applications, a solution that is architected for any use case, and providing active threat protection. Most CASBs provide a subset of the solutions required to address all business problems.	Cloud Service Providers, Healthcare, Financials
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Cloud security, Encryption, IoT security, DLP, Shadow IT, Vendor Assurance
	Customers
	Netskope customers can be found at https://www.netskope.com/customers and include Amgen, Netapp, Starbucks, Nvida, New York Life and more.

Splunk PUBLIC

(Click for online version) SDxCentral Directory Listing

www.splunk.com

Description of Security Product(s):
Splunk provides a software platform for machine data that enables customers to gain real-time Operational Intelligence (OI). Splunk can actively indexes machine data in real time from applications, web servers, databases, networks, virtual machines, mobile devices, IoT sensors, mainframes and much more. Splunk can combine and enrich machine data with Hadoop-based data, as well as traditional data from relational databases and data warehouses.

Unique Value Proposition	Solution Demand
Splunk provides a scalable and complete enterprise class solution that integrates OT and and IT with services ranging from advanced searching to reporting. Splunk Enterprise Security (ES) is a premium security solution that provides insight into machine data generated from security technologies such as network, endpoint, access, malware, vulnerability and identity information. It enables security teams to quickly detect and respond to internal and external attacks to simplify threat management.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail, Utilities, AreoSpace and Defense
	Product Areas/Functions
	Other end-point threats, Cloud security, IoT security, IT Operations, Industrial Operations
	Customers
	Splunk customers can be found at www.splunk.com/en_us/customers.html and include AAA, 7-Eleven, Academy Sport, Alcatel-Lucent, Adobe and more.

Tanium PRIVATE

(Click for online version) SDxCentral Directory Listing

www.tanium.com

Description of Security Product(s):
Tanium's Endpoint Security Platform provides 15-second visibility and control across network and can scale to millions of endpoints without requiring ongoing infrastructure additions. Tanium scans for threats by examining for complex Indicators of Compromise (IOC) connects to any number of external threat intelligence feeds and supports open standards like OpenIOC, Yara, STIX and TAXII.

Unique Value Proposition	Solution Demand
The patented linear-chaining Tanium End Point Architecture and solution decentralizes management intelligence directly onto individual endpoints through a single, lightweight agent. Each managed endpoint maintains an awareness of nearby machines on the network by contacting the Tanium Server periodically to get a concise update on the current state of its neighbors. Tanium uses Kerberos-based authentication leveraging Active Directory infrastructure, credentialing and security policies.	Healthcare, Financials, Government & Education, Telecom, Retail, Enterprise
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Identity management, IoT security, SIEM, Web and application security, real-time security visibility
	Customers
	Tanium customers can be found at https://www.tanium.com/customers and include names such as JPMorgan Chase, Voya, GoDaddy, Verizon, Best Buy and more.

Allot Communications Ltd PUBLIC

(Click for online version) SDxCentral Directory Listing

www.allot.com

Description of Security Product(s):
Allot Web Security solutions empower operators to offer Security-as-a-Service to consumers, SMBs and enterprises. Through full integration with Allot Service Gateway, service providers can rapidly roll out network-based managed security services, including, anti-malware, and parental controls that increase customer loyalty and generate incremental revenue.

Unique Value Proposition	Solution Demand
Allot Communications is a leading provider of security and monetization solutions that enable service providers to protect and personalize the digital experience. Allot leverages the intelligence in data networks, enabling service providers to get closer to their customers; safeguard network assets and users; and accelerate time-to-revenue for value-added services.	Cloud Service Providers, Telecom
	Product Areas/Functions
	Antivirus & malware protection, Cloud security, IoT security, Network security/firewall, Web and application security
	Customers
	Allot solutions are currently deployed at 5 of the top 10 global mobile operators and in thousands of CSP and enterprise networks worldwide with customers such as Vodafone Germany, Swisscom and Datafort among others. The Telecommunications and Information Technology Center of the Generalitat de Catalunya (CTTI) also selected Allot to protect Catalonia's September 2015 elections from Distributed Denial of Service (DDoS) cyber-attacks.

Bromium PRIVATE

(Click for online version) SDxCentral Directory Listing

www.bromium.com

Description of Security Product(s):
Bromium protects an enterprise while enabling users to click on anything without risk of breach. Unlike traditional endpoint security which is ineffective against modern attacks, Bromium's solution integrates CPU-enforced threat isolation, threat analytics and continuous host monitoring to enable organizations to protect, detect and respond to zero-day threats and attempted breaches in real time.

Unique Value Proposition	Solution Demand
Bromium's unique value is micro-virtualization, which fundamentally stops all malware without requiring prior knowledge of the attack. Far superior to detection-based approaches or porous virtual containers, Bromium's CPU-enforced task isolation vastly reduces the attack surface, protecting against known and unknown attacks for users on and off the corporate network.	Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Advanced threat protection, Other end-point threats
	Customers
	Not Provided

Carbon Black PRIVATE

(Click for online version) SDxCentral Directory Listing

www.carbonblack.com

Description of Security Product(s):
Carbon Black produces an endpoint security solution runs across Windows, Mac and Linux machines to keep all endpoints and servers secure, whether on or off network, and reduces organization attack's surface focusing on file integrity monitoring and control capabilities. Carbon Black enables organizations to exceed PCI-DSS, HIPAA/HITECH, SOX, NERC CIP, NIST 800-53, and other regulatory frameworks.

Unique Value Proposition	Solution Demand
Bit9 and Carbon Black provide solutions against advanced threats that target organizations' endpoints and servers enabling users to immediately stop threats. Carbon Black serves organizations by combining continuous, real-time visibility into what's happening on every computer; real-time signature-less threat detection; incident response that combines a recorded history with live remediation; and prevention that is proactive and customizable.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail, Enterprise, Oil and Gas, Utilities
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Data center security, Identity management, Network security/ firewall, SIEM
	Customers
	Carbon Black customers can be found at https://www.carbonblack.com/company/customers and include names such as Adobe, Bed Batch and Beyond, America Eagle Outfitters, BJ's, Amica and more.

Centrify Corporation PRIVATE

(Click for online version) SDxCentral Directory Listing

www.centrify.com

Description of Security Product(s):
Centrify Identity Service, Centrify Privilege Service and Centrify Server Suite are all part of the Centrify Identity Platform, which secures access to apps and infrastructure from any device, for all users. Solutions include multi-factor authentication, cloud & on-premises apps, privileged access security, big data security, compliance and Mac and mobile management.

Unique Value Proposition	Solution Demand
Centrify uniquely protects enterprise internal and external users as well as privileged accounts to stop the threats at multiple points in the cyberattack chain.	Healthcare, Financials, Government & Education, Telecom, Retail, High tech
	Product Areas/Functions
	Compliance, Cloud security, Data center security, Identity management
	Customers
	National Weather Service, Interval International, HSBC, Citi, GE Capital

Check Point Software Technologies Ltd. PUBLIC

(Click for online version) SDxCentral Directory Listing

www.checkpoint.com

Description of Security Product(s):
Check Point delivers a multi-layered line of defense to help address increasing threats and close security gaps. Consolidation and integration of multiple security appliances using a Next Generation Threat Prevention methodology with common policy management and monitoring results in greater efficiency. Check Point's solution includes "SandBlast" zero-day protection, threat prevention appliances and software, threat intelligence, web security. and DDoS solutions.

Unique Value Proposition	Solution Demand
Check Point Software Technologies Ltd., the largest pure-play security vendor globally protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks including mobile devices, with with enterprise class security management. Check Point promotes academic information and computing security research through the Check Point Institute for Information Security (CPIIS).	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail, Enterprise
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Cloud security, Data center security, Encryption, Identity management, IoT security, Network security/firewall, SIEM, Web and application security, DDoS, Mobile
	Customers
	Check Point customers can be found at www.checkpoint.com/testimonials and include name such as Samsung, SF Police Credit Union, Independence Care System, Optix, Courtagen Life Sciences and more.

Cisco Systems, Inc. PUBLIC

(Click for online version) SDxCentral Directory Listing

www.cisco.com

Description of Security Product(s):
Cisco Advanced Malware Protection provides global threat intelligence via various context sensitive agents such as email, web, and files to provide advanced threat analysis and containment. AMP works both in real-time and retrospectively.

Unique Value Proposition	Solution Demand
• Contextual and correlated global Threat Intelligence • File analysis and threat sandboxing • Realtime malware detection and blocking • Continuous analysis and retrospective security	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Cloud security, Data center security
	Customers
	www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html#Case%20Studies

category: ■ Endpoint and Identity

CrowdStrike PRIVATE

(Click for online version) SDxCentral Directory Listing

www.crowdstrike.com

Description of Security Product(s):
CrowdStrike Falcon Platform is delivered via a Software as a service (SaaS) model combines analytics with threat intelligence to deliver the CrowdStrike Falcon product portfolio: Falcon Host, Falcon Intelligence, and Falcon DNS. The Falcon Platform protects the end point and also monitors 70+ adversarial organizations globally to predict attacks. Additionally, Falcon DNS protects access to a critical component of your network based on that intelligence: your DNS systems.

Unique Value Proposition	Solution Demand
Falcon applies a different strategy: The indicator of attack approach to security. By focusing on more than malware, which only accounts for 40% of all attacks, Falcon identifies Indicators of Attack (IOAs), not just IOCs that malware-based solutions rely on. The architecture employs Falcon Advanced Threat Intelligence Cloud and Threat Graph Data Model, which provide real-time detection and prevention of attacks 24X7.	Healthcare, Financials, Government & Education, Retail, Enterprise
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Web and application security
	Customers
	Not Provided

Cybera PRIVATE

(Click for online version) SDxCentral Directory Listing

www.cybera.com

Description of Security Product(s):
Cybera One is an SDN/NFV based virtual application networking solution and is a fully managed SDN-based security and networking platform for distributed enterprises with extended sites, systems and devices. Cybera One is designed to reduce the inherent complexity of networks by providing a solution that includes hyper-convergence-based security appliances and a Software Defined networking (SDN)/Network Function Virtualization (NFV) based cloud, combined into a single managed platform.

Unique Value Proposition	Solution Demand
With Cybera's virtual application network (VAN) solution, Cybera One, businesses are no longer subject to the pitfalls of connecting multiple applications securely through traditional site-to-site networking models. VANs enable enterprises to deploy multiple applications without security and performance policy conflicts, mitigate the cascading of security threats between applications and network segments, and deploy new applications faster by alleviating bandwidth limits.	Cloud Service Providers, Healthcare, Financials, Government & Education, Retail, Industrial, Enterprise
	Product Areas/Functions
	Antivirus & malware protection, Other end-point threats, Compliance, Cloud security, Data center security, Network security/firewall, Virtual Application Networking (VAN), Universal Policy Controller (UPC)
	Customers
	Verizon, Kahala Brands, Rocky Mountain Chocolate Factory Franchisees, and Shell Stores & Oil

CyberArk PUBLIC

(Click for online version) SDxCentral Directory Listing

www.cyberark.com

Description of Security Product(s):
The CyberArk Privileged Account Security Solution is a centralized policy manager for user management.

The consolidated platform delivers a single management interface, centralized policy creation and management, a discovery engine for provisioning new accounts, enterprise-class scalability and reliability, and a secure digital vault. The CyberArk platform supports LDAP directories, ticketing and workflow systems and supports SIEM integrations, SNMP traps, and email notifications

Unique Value Proposition	Solution Demand
According to CyberArk, privileged accounts represent the largest security vulnerability an organization faces today. CyberArk has developed the broadest suite of offerings for privileged account security management that includes their components of an Enterprise Password Vault, SSH Key Manager, Privileged Session Manager, Privileged Threat Analytics, Application Identity Manager, CyberArk Viewfinity, On-Demand Privileges Manager.	Financials, Government & Education, Enterprise, Industrial
	Product Areas/Functions
	Advanced threat protection, Cloud security, Identity management, Network security/firewall, SIEM, Centralized User Policy Management, Remove vendor access
	Customers
	CyberArk's customers can be found at www.cyberark.com/company/customers and include names Astra-Zeneca, Time, Deloitte, Rockwell Automation, Revlon and more.

Cylance PRIVATE

(Click for online version) SDxCentral Directory Listing

www.cylance.com

Description of Security Product(s):
Cylance PROTECT is an antivirus (AV) solution that leverages artificial intelligence to detect AND prevent malware from executing on your endpoints in real time. Cylance PROTECT utilizes a mathematical approach to malware identification utilizing patent-pending, machine learning techniques instead of reactive signatures and sandboxes, and can render new malware, viruses, bots and unknown future variants useless.

Unique Value Proposition	Solution Demand
At the core of Cylance's malware identification capability is a revolutionary machine learning research platform that harnesses the power of algorithmic science and artificial intelligence. It analyzes and classifies hundreds of thousands of characteristics per file, breaking them down to an atomic level evel to discern whether an object is "good" or "bad" in real time. Cylance consists of a small agent that integrates with existing software management systems or Cylance's cloud console.	Healthcare, Financials, Government & Education, Retail, Energy
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats
	Customers
	Not Provided

Endgame PRIVATE

(Click for online version) SDxCentral Directory Listing

www.endgame.com

Description of Security Product(s):
Endgame integrates data science capabilities with domain expertise to provide detection and prevention capabilities at each stage of what it calls “the kill chain”. Endgame employs a multi-stage approach that targets classes of tactics, techniques, and procedures to counter three key phases in the "Hunt cycle" including exploit-techniques, identifying adversarial-behavior, and a malware solution that includes functionality such as process anomalies, and domain reputation file reputation.

Unique Value Proposition	Solution Demand
Endgame has pioneered an offensive security strategy called the Endgame Hunt Cycle and aims to deliver the next generation of Security Intelligence & Analytics (SIA) solutions based on core capabilities that utilize data science. Endgame provides an ecosystem of applications that benefit from deep data science-based insights that address a wide array of security problems an was pioneered by the U.S. DoD.	Financials, Government & Education, Enterprise, Commercial
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats
	Customers
	Not Provided.

Fortinet PUBLIC

(Click for online version) SDxCentral Directory Listing

www.fortinet.com

Description of Security Product(s):
Fortinet's broad security portfolio helps small business, enterprise, industrial, and services providers with the solution called “Fortinet Security Fabric”. Fortinet’s flagship FortiGate security appliances deliver ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet’s broad product line of complementary solutions goes beyond UTM to help secure the extended enterprise – from endpoints, to the perimeter and the core, including databases and applications.

Unique Value Proposition	Solution Demand
Fortinet's flagship enterprise firewall platform, FortiGate, is available in a wide range of sizes and form factors, and provides a broad array of next generation security and networking functions. Complementary products can be deployed with a FortiGate to enable a simplified, end-to-end security infrastructure covering network security, data center security (physical and virtual), cloud security, secure (wired and wireless) access, infrastructure (switching and routing) security.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Cloud security, Data center security, Container security, IoT security, Network security/firewall, SIEM, Web and application security, SCADA / Industrial
	Customers
	Fortinet's reference-able customers can be found at https://www.fortinet.com/customers.html

IBM PUBLIC

(Click for online version) SDxCentral Directory Listing

www.ibm.com

Description of Security Product(s):
IBM Dynamic Cloud Security is designed to be flexible and help protect workloads in the cloud, be it Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS). IBM Dynamic Cloud Security creates an integrated system that includes traditional IT, private, public and hybrid cloud models. In addition, IBM Cloud Security Enforcer provide secure access to public cloud services. IBM helps you monitor the cloud for security breaches and compliance violations.

Unique Value Proposition	Solution Demand
IBM Security is a complete solution and a large services organization that can help enterprises manage and protect against risks associated with all models of cloud computing. Services are available to help build and deploy secure apps, better manage and monitor access to business critical applications and more support for cloud security services.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail, Enterprise
	Product Areas/Functions
	Other end-point threats, Compliance, Cloud security, Data center security, Container security, Encryption, Identity management, Network security/firewall, SIEM, Web and application security
	Customers
	Not Provided

Infoblox PUBLIC

(Click for online version) SDxCentral Directory Listing

www.infoblox.com

Description of Security Product(s):
Infoblox DNS Firewall is the leading DNS-based network security solution which contains and controls malware that uses DNS to communicate with C&Cs and botnets. It works by employing DNS Response Policy Zones (RPZs), automated threat intelligence, and optional Infoblox Threat Insight to prevent data exfiltration. Infoblox External DNS Security provides defense against the widest range of DNS-based attacks such as DNS DDoS, exploits, NXDOMAIN, and DNS hijacking attacks.

Unique Value Proposition	Solution Demand
It's critical that the technology you deploy for network control provide maximum protection and offer minimum attack surface. Infoblox is clearly differentiated from other vendors with regards to security as the industry's first DDI vendor to seamlessly integrate with leading security solutions to enable contextual sharing of threat intelligence and automation of response workflows, providing better protection against evolving threats.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Antivirus & malware protection, Compliance, Data center security, IoT security, Network security/firewall
	Customers
	Adobe Systems, Geisinger Health System, Council Rock School District, Clark County School District, Everi Holdings, Inc.

Intel Security PUBLIC

(Click for online version) SDxCentral Directory Listing

www.intelsecurity.com

Description of Security Product(s):
McAfee Virtual Network Security Platform from Intel Security provides next-generation IPS protection that segments and secures traffic between virtual machines and virtualized workloads in private and hybrid cloud environments. Enterprise SDDC operators and multi-tenant service providers will benefit from strong micro-segmentation along with rapid discovery and blocking of advanced threats.

Unique Value Proposition	Solution Demand
McAfee Virtual Network Security Platform can be deployed as a VNF for fully automated security within VMware NSX and other virtualized environments. Centralized management simplifies and unifies policy deployment and administration, while integration with McAfee sandboxing, SIEM, endpoint, and server security solutions enables complete ownership of the threat defense lifecycle.	Healthcare, Financials, Government & Education
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Cloud security, Data center security, Network security/firewall
	Customers
	Not Provided

Kaspersky Lab PRIVATE

(Click for online version) SDxCentral Directory Listing

http://usa.kaspersky.com

Description of Security Product(s):
Kaspersky Endpoint Security for Enterprise provides security teams with full visibility and control over every endpoint, static or mobile, under your jurisdiction, wherever it sits and whatever it's doing. A scalable solution provides access to inventories, licensing, remote trouble-shooting and network controls, all accessible from one console, the Kaspersky Security Center. Security solutions range from encryption, application controls and whitelisting to web controls.

Unique Value Proposition	Solution Demand
Kaspersky provides a next-generation endpoint security platform, powered by a global intelligence network (Kaspersky Security Network), which provides a higher level of business processes and data protection together with a wide range of security capabilities to fight advanced threats (detecting suspicious activities and protecting against zero-day attacks). Kaspersky protects all endpoints including desktops, servers, mobile devices, and virtual machines.	Healthcare, Financials, Government & Education, Home, Small Business, Enterprise, Industrial
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Cloud security, Data center security, Encryption, IoT security, Network security/firewall, SIEM, Web and application security, DDoS, Indudstrial, Mobile Security, Virtualization Security
	Customers
	A list of Kaspersky customers can be found at http://usa.kaspersky.com/about-us/why-kaspersky/success-stories and include, Nedis, Univesity of Chile, Swiss Exhibition, The Minol Group, Grupa Remontowa SA, and more.

KEMP Technologies PRIVATE

(Click for online version) SDxCentral Directory Listing

http://kemptechnologies.com

Description of Security Product(s):
KEMP's Application Firewall Pack (AFP) combines Layer 7 Web Application Firewall protection with other application delivery services including intelligent load balancing, intrusion detection, intrusion prevention, edge security, and authentication. Kemp AFP utilizes an open source web application firewall engine, ModSecurity, and augments threat intelligence and research from Trustwave to provide ongoing protection against known and evolving vulnerabilities.

Unique Value Proposition	Solution Demand
KEMP AFP along with KEMP LoadMaster provides integrated security capabilities including Web Application Firewall protection (WAF), edge security, L7 IPS/IDS, DDos Mitigation, application publishing and authentication services as standard features on all platforms including select hardware appliances. KEMP also provides PCI-DSS Compliance protecting web applications focusing on those which process payments reducing the need for extensive code reviews with regularly updated rule sets.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Enterprise.
	Product Areas/Functions
	Advanced threat protection, Cloud security, Identity management, Network security/firewall, Layer 7 web application firewall, intelligent load balancing, intrusion detection, intrusion prevention as well as edge security.
	Customers
	KEMP's broad market focus includes small-to-medium sized businesses, Fortune 1000 enterprises, remote enterprise branch offices, managed service providers and public sector clients, who view end-user satisfaction and IT web and application infrastructure reliability and optimization as mission-critical to their long-term success.

Lastline PRIVATE

(Click for online version) SDxCentral Directory Listing

www.lastline.com

Description of Security Product(s):
The Lastline Breach Detection Platform is comprised of four core components: Sensor, Engine, Manager and Advanced Threat Intelligence. The four components work together to continuously monitor all datastreams, expose IOCs related to active data breaches, and prioritize incidence response.

Unique Value Proposition	Solution Demand
Lastline provides comprehensive detection of advanced and evasive threats across the entire enterprise and operating systems (Windows, Mac OS X, and Android), physical and virtual hosts, services, users, network infrastructure and Web, email, file, and mobile applications. Lastline's flexible software-base platform allows organizations to scale their breach defenses on a predictable basis, from a single location to any number of remote, branch, and mobile offices. Licensing is done by user.	Cloud Service Providers, Financials, Government & Education, Enterprise
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Cloud security, Data center security, Container security, Encryption, Identity management, Network security/ firewall, SIEM, Web and application security
	Customers
	https://www.lastline.com/customers/success

LightCyber PRIVATE

(Click for online version) SDxCentral Directory Listing

http://lightcyber.com

Description of Security Product(s):
LightCyber solves the data breach crisis with Behavioral Attack Detection to provide accurate and efficient security visibility into attackers that have slipped through the cracks of traditional security controls. The LightCyber Magna platform pinpoints network intruders & malicious insiders by detecting their operational activities. Today, most enterprises and organizations lack the ability to find an active attacker on their network. The industry average is five months to discover an intruder.

Unique Value Proposition	Solution Demand
Using machine learning, LightCyber Magna profiles all users and devices to learn good behavior on a network and discern malicious anomalies. It is the first security product to integrated user, network and endpoint context to provide security visibility into a range of attack activity, including targeted external attacks, internal threats, risky behavior and opportunistic malware. Magna uses machine learning, full network DPI and agentless, on-demand client technology to produce few alerts.	Healthcare, Financials, Government & Education, Telecom, Retail, Legal, Energy, Manufacturing
	Product Areas/Functions
	Behavioral Attack Detection
	Customers
	Not Provided

Menlo Security PRIVATE

(Click for online version) SDxCentral Directory Listing

www.menlosecurity.com

Description of Security Product(s):
The Menlo Security Isolation Platform (MSIP) is the foundation for all Menlo Security services, including web isolation, document isolation and email isolation. The MSIP is available as a public cloud service and can also be delivered as a virtual appliance for deployment in an organization's data center. User sessions and all active content (e.g., Java, Flash, etc.), whether good or bad, are fully executed and contained in the isolation platform.

Unique Value Proposition	Solution Demand
The Menlo Security Isolation Platform (MSIP) uses Adaptive Clientless Rendering (ACR) technology that allows only safe, malware-free rendering information is delivered to the user's endpoint. No active content including any potential malware ever leaves the platform. Services supported by the MSIP enable administrators to open up more of the Internet to their users while simultaneously eliminating the risk of attacks.	Financials, Enterprises
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Data center security, Identity management, Network security/firewall, Web and application security
	Customers
	Not Provided

Netskope PRIVATE

(Click for online version) SDxCentral Directory Listing

www.netskope.com

Description of Security Product(s):
The Netskope Active Platform gives IT the ability to find, understand, and secure cloud apps. Netskope empowers organizations to gain surgical visibility and control, protect sensitive data using "noise-cancelling" data loss prevention (DLP), and ensure compliance in real-time, on any device, for any cloud application. There are three primary phases of safe cloud enablement that Netskope provides: find, understand, and secure. Netskope also provides reporting on those cloud analytics.

Unique Value Proposition	Solution Demand
The Netskope Active Platform combines four key areas that are required by cloud access security brokers to be considered enterprise class solutions that include advanced enterprise DLP, granular policies for all applications, a solution that is architected for any use case, and providing active threat protection. Most CASBs provide a subset of the solutions required to address all business problems.	Cloud Service Providers, Healthcare, Financials
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Cloud security, Encryption, IoT security, DLP, Shadow IT, Vendor Assurance
	Customers
	Netskope customers can be found at https://www.netskope.com/customers and include Amgen, Netapp, Starbucks, Nvida, New York Life and more.

Palo Alto Networks PUBLIC

(Click for online version) SDxCentral Directory Listing

www.paloaltonetworks.com

Description of Security Product(s):
Palo Alto Networks has long secured networks with rich security devices. Today, Palo Alto's Aperture extends the visibility and granular control traditional network security into cloud / SaaS applications themselves. Because SaaS can be invisible to traditional IT, Aperture integrates into SaaS applications directly, providing full visibility into the day-to-day activities of users and data. Granular controls ensure policy is maintained to eliminate data exposure and threat risks.

Unique Value Proposition	Solution Demand
Palo Alto Networks has combined network, cloud, and endpoint security into a tightly integrated platform that delivers automated prevention against cyberattacks including known and unknown. Palo Alto's security platform, based on PAN OS 7.1, is focused eliminating threats by integrating Next-Generation Firewall, Advanced Endpoint Protection, and Threat Intelligence Cloud suites into a single solution supporting all clouds with highly automated preventative measures against cyberthreats.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail, Electric Utilities, ICS & SCADA, Oil & Gas
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Cloud security, Data center security, Network security/firewall, SIEM, IPS, URL filtering, threat intelligence
	Customers
	Palo Alto Networks customers can be found at https://www.paloaltonetworks.com/customers and include University South Hampton, University of Colorado, Ausram, Mercy Medical Center, and more.

Proofpoint, Inc PUBLIC

(Click for online version) SDxCentral Directory Listing

www.proofpoint.com

Description of Security Product(s):
Proofpoint Email Protection secures and controls inbound and outbound email through a cloud-based solution and protects data from threats such as impostor email, phishing, malware, spam, and bulk mail. Email Protection uses multiple layers of technology to detect threats, including malicious content and malware and supports cloud, hybrid and on-premises installations with virtual or physical appliances.

Unique Value Proposition	Solution Demand
Proofpoint can be deployed in the cloud and offers 99.999% service availability with 99% blocked or redirected spam, 100% virus protection, and adds less than 1 minute email latency. Proofpoint Email utilizes a dynamic classification and control system of email across spam, phishing, impostor, bulk, adult and malware. Via its multi-layered threat protection schema Proofpoint supports flexible policy creation, detailed reporting and can scale to support even the largest organizations.	Healthcare, Financials, Government & Education, Retail, Enterprise, pharmaceutical
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Network security/firewall, SIEM, Advanced email security
	Customers
	Proofpoint clients can be found at http://proofpoint.com/us/customer-stories and include Envoy Mortgage / Mountain Regional, US Physical Therapy, Inc., Wiregrass Georgia Technical College, EMC National Life Insurance, the Golden State Warriors and more.

Qualys PUBLIC

(Click for online version) SDxCentral Directory Listing

www.qualys.com

Description of Security Product(s):
Qualys' flagship product, QualysGuard Cloud Platform and its integrated suite of security and compliance applications provides organizations with a global view of their security and compliance solutions. The QualysGuard solutions include vulnerability management, policy compliance, web application scanning, malware detection and Qualys SECURE Seal for security testing of web sites.

Unique Value Proposition	Solution Demand
Qualys sensors, a core service of the Qualys Cloud Plaform, extends security throughout global enterprises. These sensors, which can be in the form of appliances or lightweight agents, are remotely deployable, centrally managed and self updating. Qualys sensors collect threat data automatically and it is used as critical data by the Qualys Cloud Platform, which continuously analyzes and correlate the information to identify threats and eliminate vulnerabilities.	Healthcare, Financials, Government & Education, Telecom, Retail, Insurance, & Media
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Network security/firewall, Web and application security, Security assessment questionnaire, and secure seal for security testing of websites
	Customers
	Qualys customers can be found at https://www.qualys.com/customers and include Oracle, Cisco, T-Mobile, Facebook, HPE, and more.

RSA Security PUBLIC

(Click for online version) SDxCentral Directory Listing

www.rsa.com

Description of Security Product(s):
RSA offers a suite of products and services for security management, analytics, and forensics. In addition, with RSA Via, organizations can provide comprehensive identity management that includes 1) secure access to cloud and mobile applications 2) the ability to deliver a streamlined request, approval, and fulfillment process with embedded policy controls and 3) the ability to automate the monitoring, certification, reporting and remediation of entitlements to ensure appropriate access.

Unique Value Proposition	Solution Demand
The modular architecture of RSA Security solutions allows organizations to improve their ability to detect and respond to security incidents without having to rip and replace existing solutions. The RSA tools can integrate and expand upon existing environments, allowing organizations to grow when they need. It provides a single monitoring platform to gain the visibility organizations need, combining logs, network, and endpoint visibility to see what is happening acroos an enterprise.	Enterprise
	Product Areas/Functions
	Advanced threat protection, Other end-point threats, Compliance, Identity management
	Customers
	ADP, Banco Popular, St. Luke's Health System, State of Texas Department of Information Resources, Berkshire Bank and others can be seen at https://www.rsa.com/en-us/company/why-rsa

Shape Security PRIVATE

(Click for online version) SDxCentral Directory Listing

www.shapesecurity.com

Description of Security Product(s):
Shape Security Application Defense is delivered as a service via cloud or enhanced control integrated into physical or virtual infrastructure focusing on security, fraud, network operations, application development, prevention, detection and response, machine learning systems and network data. Any combination of these is also supported, and no changes to your website or mobile API servers are required.

Unique Value Proposition	Solution Demand
Shape Security offers clients a a full platform, with continuous improvement, with unique application defense functions in each stage of Gartner's Adaptive Protection Architecture. Shape enhances every team that helps defend your applications, including your NOC, SOC, fraud team, and application security team, helping each of them with their most difficult attacks and deliver this as a service, without requiring functionality changes, complex integrations, or requiring headcount.	Healthcare, Financials, Government & Education, Retail
	Product Areas/Functions
	Advanced threat protection, Other end-point threats, Compliance, Cloud security, Network security/firewall, Web and application security, Mobile application attacks, like credential stuffing, content scraping, and application DDoS.
	Customers
	Shape Security does not provide a customer list, but does have a list of industry case studies available at https://www.shapesecurity.com/case-studies

Skyhigh Networks PRIVATE

(Click for online version) SDxCentral Directory Listing

www.skyhighnetworks.com

Description of Security Product(s):
Skyhigh is a cloud access security broker (CASB). With Skyhigh, organizations leverage a single cross-cloud platform to gain visibility into cloud usage and risks, meet compliance requirements, enforce security policies, and detect and respond to potential threats.

Unique Value Proposition	Solution Demand
Skyhigh discovers all cloud services in use and provides a 1-10 CloudTrust Rating of enterprise readiness for each service, reveals gaps in cloud policy enforcement, and enables real-time coaching and policy enforcement to guide users to corporate-sanctioned services. Skyhigh leverages machine learning to accurately detect insider threats, compromised accounts, privileged user threats, and attacks using the cloud as a data exfiltration vector.	Cloud Service Providers, Healthcare, Financials, Government & Education, Enterprise, Manufacturing
	Product Areas/Functions
	Compliance, Cloud security, Data center security, Identity management, Network security/firewall, SIEM, Web and application security
	Customers
	Skyhigh network custoers can be found at https://www.skyhighnetworks.com/customers and include Adventist Health System, Western Union, DirecTV, Equinix, and Perrigo.

Symantec Corporation PUBLIC

(Click for online version) SDxCentral Directory Listing

www.symantec.com

Description of Security Product(s):
Symantec offers a complete suite of products that include security management, threat protection, threat detection, identity management, and endpoint protection. In addition to security products, Symantec also offers cyber security services. Customers can take advantage of Symantec's experts, global threat intelligence, advanced monitoring, incident response, and cyber readiness services.

Unique Value Proposition	Solution Demand
Only Symantec offers the following advantages: 1) Better security with real-time reputation and behavioural monitoring technology 2) Enhanced performance – 70 percent lower scan overheads and number one in performance vs. Kaspersky, Trend Micro, Sophos, Microsoft, and McAfee 3) Tested and optimised for today's virtual environments. 4) Faster, flexible management for simple upgrading and configuration 5) Smart scheduling technology intelligently scans during idle periods	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Advanced threat protection, Other end-point threats, Cloud security, Data center security, Encryption, Identity management, Network security/firewall, Web and application security
	Customers
	Asia Pacific Telecom, The State of Oklahoma, Hillsborough County Public Schools, Mary Washington Healthcare and others can be seen at www.symantec.com/resources/customer_success

Tanium PRIVATE

(Click for online version) SDxCentral Directory Listing

www.tanium.com

Description of Security Product(s):
Tanium's Endpoint Security Platform provides 15-second visibility and control across network and can scale to millions of endpoints without requiring ongoing infrastructure additions. Tanium scans for threats by examining for complex Indicators of Compromise (IOC) connects to any number of external threat intelligence feeds and supports open standards like OpenIOC, Yara, STIX and TAXII.

Unique Value Proposition	Solution Demand
The patented linear-chaining Tanium End Point Architecture and solution decentralizes management intelligence directly onto individual endpoints through a single, lightweight agent. Each managed endpoint maintains an awareness of nearby machines on the network by contacting the Tanium Server periodically to get a concise update on the current state of its neighbors. Tanium uses Kerberos-based authentication leveraging Active Directory infrastructure, credentialing and security policies.	Healthcare, Financials, Government & Education, Telecom, Retail, Enterprise
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Identity management, IoT security, SIEM, Web and application security, real-time security visibility
	Customers
	Tanium customers can be found at https://www.tanium.com/customers and include names such as JPMorgan Chase, Voya, GoDaddy, Verizon, Best Buy and more.

Trend Micro PUBLIC

(Click for online version) SDxCentral Directory Listing

www.trendmicro.com

Description of Security Product(s):
Trend Micro offers a complete range of security products for home, small business, and medium-sized enterprises. It consists of a combination of cloud-based security services, virus protection, web security, advanced threat protection, endpoint security, mobile security, and centralized security management.

Unique Value Proposition	Solution Demand
The Trend Micro Smart Protection Network mines data around the clock and across the globe to ensure that you are always protected. We use our up-to-the-second threat intelligence to immediately stamp out attacks before they can harm you. And the same accelerated cloud security powers all of our products and services, protecting millions of businesses and users around the globe. Since 2009, IDC has ranked Trend Micro as the global market leader in server security.	Retail, SMB
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Cloud security, Web and application security
	Customers
	AlliedTelesyn, A&W, Mazda, McGill University, the United Way and other success stories can be seen at http://cloudsecurity.trendmicro.com/us/technology-innovation/customers-partners/index.html

Wedge Networks PRIVATE

(Click for online version) SDxCentral Directory Listing

http://wedgenetworks.com

Description of Security Product(s):
Wedge Networks' Cloud Network Defense is an orchestrated threat management platform designed to enforce security at the cloud-layer of the network to combat the shifting threat landscape associated with cloud, mobility, bring your own device, Internet of Things and consumerization of IT.

Unique Value Proposition	Solution Demand
With Cloud Network Defence, by applying security policies at the cloud-layer, enterprises and network operators offering security-as-a-service can achieve more effective security, using best-in-class, continuously updated multi-vendor technologies for EverGreen Security, with greater efficiency and scale.	Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail
	Product Areas/Functions
	Antivirus & malware protection, Advanced threat protection, Other end-point threats, Compliance, Cloud security, Data center security, IoT security, Network security/firewall, SIEM, Web and application security
	Customers
	Not Provided

Zscaler PRIVATE

(Click for online version) SDxCentral Directory Listing

www.zscaler.com

Description of Security Product(s):
Zscaler's secure web gateway architecture was created as a pure cloud product. It delivers a multi-tenant scalable platform by distributing components of a standard proxy to create a network that acts as a single virtual proxy. Users access any / nearest gateway for policy-based secure Internet access. Zscaler infrastructure comprises three key components: Zscaler Enforcement Nodes (ZENs), Central Authority (CA), and Nanolog Servers.

Unique Value Proposition	Solution Demand
Zscaler benefits from fifty newly patented technologies including a distributed, multi-tenant architecture, that supports 10 Gbps throughput based on a next-gen TCP stack and single scan multiple action technology that enables inspection of every byte of traffic by every service. Other components of the Zscaler solution include ByteScan, which provides ultrafast content scanning, Page Risk Index, which analyzes real-time web activities, and Nanolog, which encrypts web-logs.	Cloud Service Providers, Healthcare, Financials, Government & Education, Retail, Enterprise, Manufacturing, Consumer Goods, SMB
	Product Areas/Functions
	Advanced threat protection, Other end-point threats, Cloud security, Identity management, Network security/firewall, Web and application security, Data Loss Prevention, SSL Inspection, Guest Wifi, Internet Security
	Customers
	Zscaler customers can be found at https://www.zscaler.com/customers and include Jabil, Johnston Controls, Lazy Boy, United Airlines, Avaya and more.

SDNCentral, LLC
955 Benecia Avenue
Sunnyvale, CA 94085 USA
www.sdxcentral.com

The Trusted News and Resource Site for SDx, SDN, NFV, Cloud and Virtualization Infrastructure

Rev B