Unit 42 Attack Surface Threat Report

LESSONS IN ATTACK SURFACE RISK

paloalto NETWORKS | CORTEX XPANSE

paloalto NETWORKS | CORTEX XPANSE®

TABLE OF CONTENTS

paloalto NETWORKS | CORTEX XPANSE

01 EXECUTIVE SUMMARY

Key Findings

Attack surface change inevitably leads to exposures.

Across industries, attack surfaces are always in a state of flux. Our research indicates that, on average, an organization's attack surface has over 300 new services every month. These additions account for nearly 32% of new high or critical cloud exposures for organizations.

Opportunities for lateral movement and data exfiltration are abundant.

Just three categories of exposures—IT and Networking Infrastructure, Business Operations Applications, and Remote Access Services—account for 73% of high-risk exposures across the organizations we studied and can be exploited for lateral movement and data exfiltration.

Critical IT and security services are dangerously exposed to the internet.

Over 23% of exposures involve critical IT and security infrastructure, opening doors to opportunistic attacks. These include vulnerabilities in application-layer protocols like SNMP, NetBIOS, PPTP, and internet-accessible administrative login pages of routers, firewalls, VPNs, and other core networking and security appliances.

Organizations are accelerating the modernization of their network architectures, driven by the adoption of new security models, cloud computing, SaaS, and the need to support distributed workforces. This rapid evolution has introduced complexity into security efforts that were already stretched thin by significantly expanding known and unknown IT infrastructure. Assets made public-facing, intentionally or not, stand out to malicious actors like prey in the open desert.

A critical challenge remains: keeping track of and protecting all assets, as many companies and government agencies struggle to inventory their holdings and identify the most vulnerable services. According to the 2024 Unit 42 Incident Response Report, in the past year, attackers' initial access most often started with a software vulnerability. The largest attack campaigns began with the successful exploitation of internet-facing systems. So, to better understand these challenges, Unit 42® conducted a comprehensive analysis of public internet data, leveraging Palo Alto Networks Cortex Xpanse®. This report distills insights from several petabytes of data collected in 2023 to provide security leaders with a clear picture of the evolving global attack surface and what risks to look for in their environment.

Recommendations

While this exposure data may seem overwhelming, it shouldn't instill panic or fear. Fear is the mind-killer. Face these risks head-on.

Maintain persistent, comprehensive visibility

The key to being able to discern and respond to attack surface risks (such as new, high-profile vulnerabilities) begins with having comprehensive attribution of your organization's attack surface. This can be accomplished with continuous scanning of both standard and nonstandard ports, as well as accurate fingerprints of services and devices in your environment and assessments of risks. Your organization can use our Cortex Xpanse platform to proactively find and fix exposures on your internet-connected assets before attackers can exploit them.

Monitor for unsanctioned services or shadow IT

Checking known perimeter resources can help you distinguish between expected assets and unknown or out-of-scope ones. No matter the industry you're protecting, it's important to use common configuration baselines for security. Deviations from these baselines or policies are usually the most vulnerable to compromise.

paloalto NETWORKS | CORTEX XPANSE

Focus on high-priority vulnerabilities

Concentrate remediation efforts on the most critical security issues, particularly those that are internet-exposed, which would lead to high severity and likelihood scores. Consider leveraging external expertise to identify the most impactful starting points for improvement.

Remediate critical exposure risks in real time

Detecting internet-exposed risks, whether due to misconfigurations or vulnerabilities, is only half the battle. Organizations should have processes and, ideally, technology to aid security operation teams in identifying service owners, communicating risk details, and tracking remediation.

Seek expert guidance

If your organization is new to attack surface management or looking to enhance existing practices, consider a Unit 42 Attack Surface Assessment.

Strengthen remote access security

Implement robust authentication protocols, such as multifactor authentication, for all remote access services. Establish monitoring systems to detect and respond to potential unauthorized access attempts or brute-force attacks.

Optimize cloud configurations

Establish a regular schedule for reviewing and updating cloud settings to align with industry best practices and mitigate potential security risks. Foster collaboration between security and development teams to promote secure cloud-native application development.

Enforce secure data handling practices

Implement and maintain stringent access controls and secure file-sharing protocols for all databases and shared resources to prevent unauthorized access and data breaches and ensure regulatory compliance.

Stay informed about emerging threats

Develop a system for keeping abreast of new vulnerabilities, exploits, and threat actors. Regularly reassess your organization's attack surface in light of this evolving threat landscape. Follow the Unit 42 blog for our insights, and if you'd like a consulting relationship, consider a services retainer for threat landscape briefings and Incident Response services.

02

THE SHIFTING SANDS OF ATTACK SURFACES

The days of imagining your attack surface as static and easily tracked are gone. The state of your attack surface changes in sometimes imperceptible ways. Every configuration change, new cloud instance, and vulnerability disclosure creates an opening for attackers. Security teams are asked to manage this constant flux in addition to all the other demands placed on their time, which is a challenging task.

At the same time, we've seen how attackers speed up their activity both before launching an attack and after successfully infiltrating a target network. According to prior research from the Xpanse team, attackers can scan the entire IPv4 address space, all 4.3 billion IPv4 addresses in minutes, looking for opportunities. Additionally, once attackers are in, they move faster to steal data, according to Unit 42 research, sometimes getting in and out in less than one day.

It's no secret that organizations have consistently been moving to the cloud as part of IT modernization efforts, so that's where we focused our analysis in this report.

We found that the very qualities that make cloud environments so powerful—their flexibility, scalability, and ease of deployment—also introduce an element of complexity and unpredictability to the attack surface. Our research showed that a typical organization adds or updates over 300 services every month, and these new and updated services are responsible for nearly 32% of organizations' new high or critical cloud exposures.

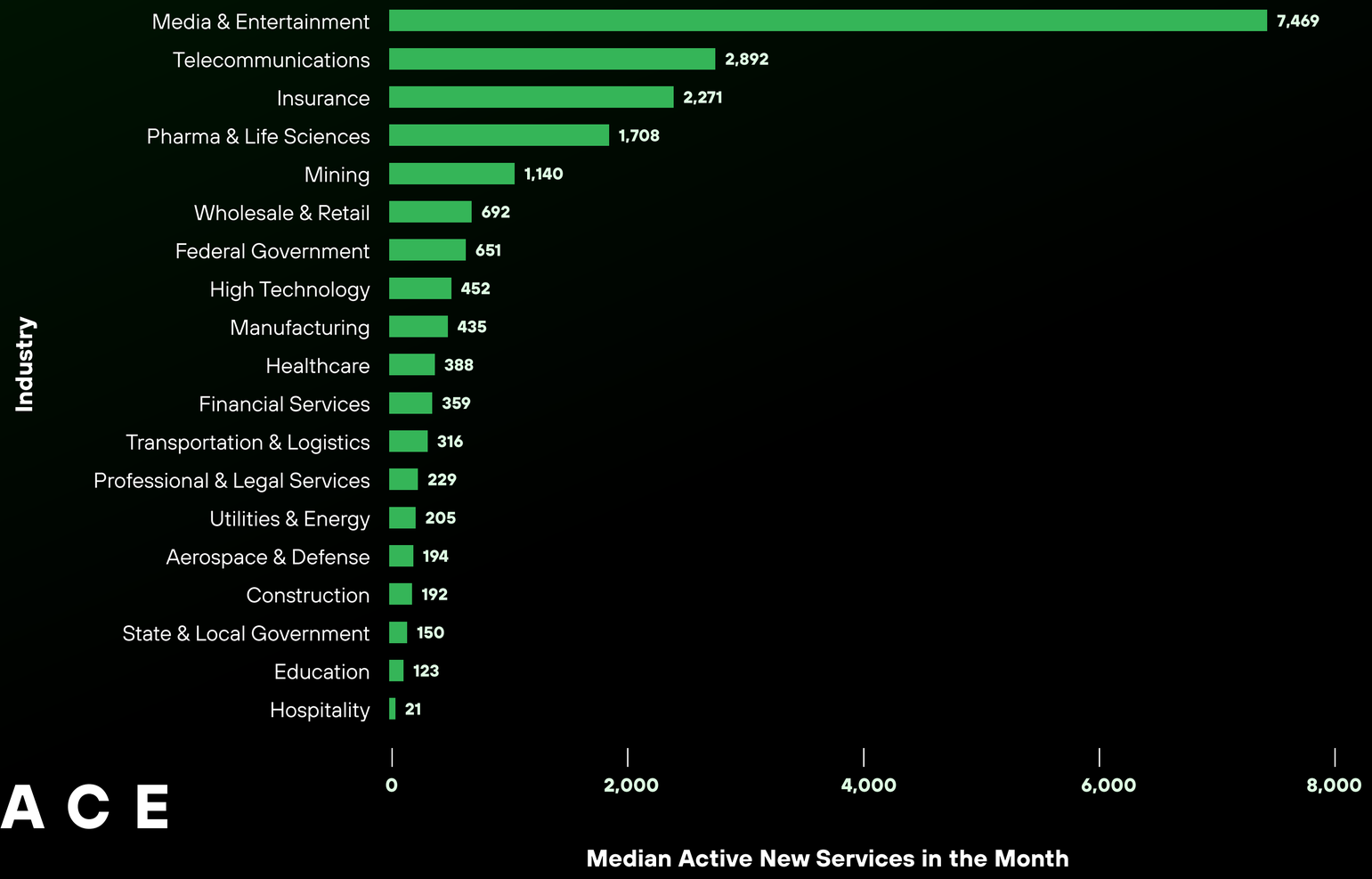
This rapid growth of new services without central oversight inevitably leads to misconfigurations and exposures, and those risks mean a higher chance of a breach. It's challenging to strengthen your defenses appropriately without complete knowledge of your entire attack. The 2024 Unit 42 Incident Response analysis revealed that organizations with partial or incomplete deployment of security controls, particularly endpoint detection and response tools, enabled attackers to operate unhindered in undefended network areas.

03

INDUSTRY ATTACK SURFACE OUTLOOK

To delve deeper into the dynamic nature of modern IT environments, Unit 42 studied new services over 12 months. The analysis revealed that almost every organization studied introduced a significant number of new services each month. This constant flux, illustrated in figure 1, underscores the critical need for continuous visibility. Without it, organizations risk losing track of accidental misconfigurations and the spread of shadow IT, leading to increased risks in their environment.

FIGURE 1: MEDIAN COUNT OF NEW SERVICES INTRODUCED BY A TYPICAL COMPANY IN EACH INDUSTRY DURING A GIVEN MONTH



Our analysis revealed that the media and entertainment industry experienced the highest rate of new services added, exceeding 7,000 per month. The telecommunications, insurance, pharma, and life sciences sectors also faced substantial increases, with over 1,000 new services added to each of their attack surfaces. Critical industries such as financial services, healthcare, and manufacturing saw their attack surfaces add over 200 new services every month in each of those industries.

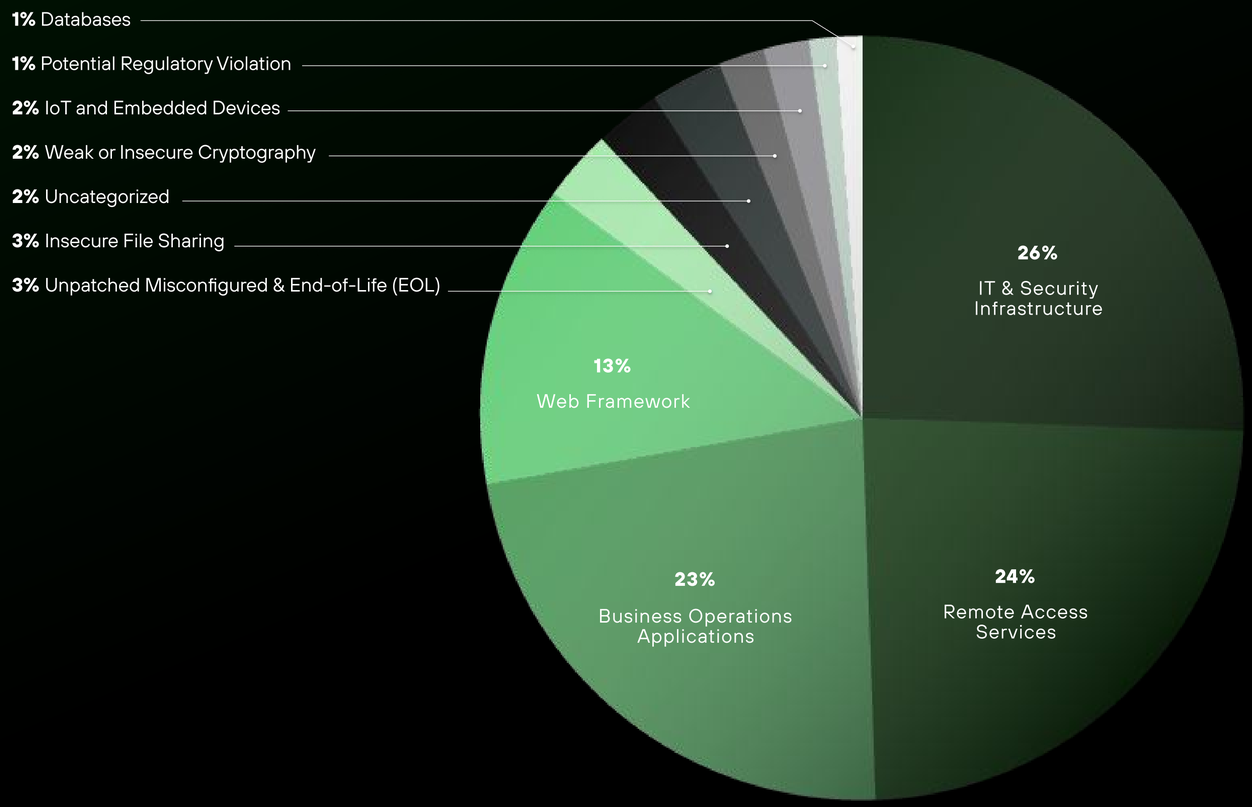
For the past three years, Unit 42 analysis has consistently identified professional services, healthcare, high technology, finance, manufacturing, wholesale, and retail as the top six industries to which we've provided Incident Response services. While that statistic shows which industries ask us for expert Incident Response help, it doesn't mean the others aren't at risk, either.

The *Unit 42 Incident Response Report* is a valuable resource for seeing how attackers are successfully exploiting exposures for access, but Cortex Xpanse data shows every organization has risks and must maintain readiness to respond effectively. The basis of any sound response strategy begins with the current, complete, and accurate visibility of the entire attack surface.

In general, when a device is compromised on the attack surface, it can fall into two categories of risk for the organization:

- **Immediate threat risks:** Examples of this include exfiltration of sensitive documents and ransomware attacks.
- **Exploited access risks:** Examples of this include lateral movement within networks and infrastructure compromise for later exploitation.

FIGURE 2: DISTRIBUTION OF EXPOSURE CATEGORIES OBSERVED ACROSS THE 265 ORGANIZATIONS IN THE LAST 12 MONTHS



04

TOP ATTACK SURFACE EXPOSURES

paloalto NETWORKS | CORTEX XPANSE®

Total Attack Surface Risk

The total risk an organization faces from its attack surface can be conceptualized as the product of two key factors: the potential cost of a security breach and the probability of such a breach occurring. This framework provides a more nuanced understanding of the evolving risk landscape in our increasingly digitized world.

1. **Cost of a security breach:** The potential cost of a security incident has been steadily rising as more business-critical systems are modernized and more data is collected. This trend means that a successful attack can now impact core business operations, leading to:
   - Direct financial losses
   - Operational disruptions
   - Reputational damage
   - Regulatory penalties
   - Loss of intellectual property

2. **Probability of a security breach:** The likelihood of a successful attack is significantly influenced by the presence and duration of vulnerabilities in internet-exposed assets. Each vulnerable, internet-facing asset represents a potential entry point for attackers, and the severity of each vulnerability also increases the risk. The longer these vulnerabilities remain unaddressed, the higher the chance that they'll be discovered and exploited by malicious actors. This is particularly critical given that sophisticated attackers are constantly scanning for new opportunities and can often weaponize new vulnerabilities within hours or days of their discovery.

Multiplying these two factors—the increasing cost of potential breaches and the rising probability of successful attacks due to expanded attack surfaces—allows us to see the total risk growing at an alarming rate for many organizations.

This perspective underscores the critical importance of:

1. Rapidly identifying and addressing vulnerabilities in internet-exposed assets
2. Minimizing the attack surface by carefully managing which systems are exposed to the internet
3. Implementing robust security measures for business-critical digital systems
4. Continuously monitoring and updating security protocols to keep pace with the evolving threat landscape

By focusing on these areas, organizations can work to reduce both the potential impact and likelihood of security breaches, managing their overall attack surface risk in an increasingly digitized business environment.

Attack Surface Exposures by Device Function

Unit 42 examined global attack surface exposures and classified them by device business function, aligning with the risk implications for organizations. The findings from the analysis follow.

IT and networking infrastructure exposures constitute over 25% of the exposures observed by Unit 42. These include vulnerabilities in application-layer protocols like SNMP, NetBIOS, PPTP, and internet-accessible administrative login pages of routers, firewalls, VPNs, and other core networking and security appliances. Compromising these assets can severely impact organizations by exploiting core business functions, applications, and the sensitive data they hold.

Remote access services exposures constitute a significant portion, comprising almost 24% of observed exposures. These services, such as Remote Desktop Protocol (RDP), Secure Shell (SSH), and Virtual Network Computing (VNC), are critical for enabling remote connectivity to organizational networks and systems. However, when left exposed or improperly configured, they present substantial security risks. For instance, attackers running brute-force exploitation against these services can gain unauthorized access to sensitive data or critical infrastructure. In addition, RDP has been shown to be a leading vector for business interruption via ransomware.

Business operations application exposures account for 23% of attack surface exposures. Compromising these systems can lead to severe operational disruptions, including halted projects and broken communication. Sensitive data exposure, particularly in sectors handling personally identifiable information (PII) and protected health information (PHI), poses significant risks to confidentiality and safety. Financial losses arise from both direct impacts, like recovery costs, and indirect effects, such as lost business opportunities. Regulatory penalties may result from noncompliance with privacy laws and can include hefty fines and mandatory breach notifications.The most common exposures under this category included popular collaboration tools, project management tools, IT service management tools, and even customer relationship management tools.

Web framework takeover exposures are a significant concern for organizations due to their potential to cause widespread security breaches. As illustrated in figure 2, these exposures constitute almost 13% of all security vulnerabilities observed across the surveyed organizations. Attackers often prioritize these targets due to their ubiquity and the potential for exploitation. This underscores the critical risk posed by outdated or insecure web frameworks. The most common exposure types were insecure versions of Apache web servers, PHP, and jQuery.

Insecure file-sharing exposures account for 3% of all security exposures in organizations and pose significant risks, including data breaches. Common examples include publicly accessible file-sharing services, traditional FTP servers, and misconfigured cloud storage. These exposures allow attackers to trivially access the current data stored on the systems. The impacts include financial loss, reputational damage, and legal liabilities.

paloalto NETWORKS | CORTEX XPANSE

Other Attack Surface Exposures Observed

Unit 42 also observed other types of exposures, including those that follow.

Unpatched, misconfigured, and end-of-life (EoL) systems leave open vulnerabilities that attackers exploit to gain unauthorized access or disrupt operations. For example, an attacker could exploit an unpatched critical router to intercept or modify network traffic, compromising data integrity or confidentiality. Misconfigured firewalls might inadvertently allow unauthorized access to internal networks, facilitating data exfiltration or malware propagation.

Weak or insecure cryptography exposes sensitive communications and data to interception or decryption by malicious actors. This could result in unauthorized access to confidential information or intellectual property theft, impacting competitive advantage and regulatory compliance. These risks may also feature heavily in third-party security ratings, which can impact cyber insurance premiums and business opportunities.

Operational Technologies (OT), embedded devices, and the Internet of Things (IoT) often operate with limited security controls, making them vulnerable to exploitation. A malicious actor could use a compromised IoT device, such as a smart camera or sensor, as a foothold for attacking internal networks or as part of a botnet for launching distributed denial-of-service (DDoS) attacks. Further, compromised OT devices can have immediate and severe impacts on business operations and even physical safety.

Unencrypted logins and text-based protocols expose credentials transmitted in plaintext that attackers can intercept and use for unauthorized access to critical systems or sensitive data. Similarly, protocols like Telnet or FTP transmit data in cleartext, making it susceptible to eavesdropping and manipulation.

Development infrastructure, including repositories and build servers, is also a prime target for attackers. Compromising these environments can lead to the theft of source code, intellectual property, or injection of malicious code into software builds. This could potentially impact software integrity and user trust.

05

CONCLUSION

Organizations across various sectors are experiencing constant changes in their attack surfaces. Without continuous visibility and discovery, these changes will inevitably lead to accidental exposures that attackers are quick to exploit. The *Unit 42 Incident Response Report* indicates that the surge in software vulnerability exploitation may be linked to widespread automated intrusion campaigns in 2023.

Attackers are automating exploits to target exposed vulnerabilities opportunistically. Organizations need to take a proactive approach to effectively manage and secure their attack surfaces. This includes maintaining continuous visibility and prioritizing remediation efforts to retain control over their internet-facing infrastructure.

Implementing the recommendations outlined in this report is crucial for organizations aiming to reduce and secure their dynamically shifting attack surfaces.

paloalto NETWORKS | CORTEX XPANSE

06

RECOMMENDATIONS TO SECURE YOUR ATTACK SURFACE

Continuously scanning all internet-exposed services for vulnerabilities

An accurate view of your attack surface and its vulnerabilities is a necessity and no longer a "nice-to-have," especially when new services can be provisioned without the IT team's purview. Your organization can use our Cortex Xpanse platform to proactively find and fix exposures on your internet-connected assets before attackers can exploit them.

Finding and prioritizing exposures and vulnerabilities

Once you have a continuously updated inventory of internet-connected assets, the next step is to ensure all exposures and vulnerabilities are identified and routed to the appropriate stakeholders for swift remediation. Focus on addressing the most critical vulnerabilities and exposures, such as those with a high Common Vulnerability Scoring System (CVSS), which indicates severity, and Exploit Prediction Scoring System (EPSS), which indicates the likelihood of exploitation, to reduce the risk of successful cyberattacks. Cortex Xpanse includes this calculation, and a Unit 42 Attack Surface Assessment can help you determine the most effective starting points.

Leveraging external expertise

Attack surface management (ASM) offers a proactive approach to securing your systems, unlike the reactive measures common to most security teams. Consult external experts to build your ASM program if your team lacks in-house expertise. Unit 42's Attack Surface Assessment can help you begin with guidance from a cybersecurity expert.

Centrally monitoring and enforcing policies

The ability to fine-tune policies for detecting internet-exposed vulnerabilities, misconfigurations, and inventory hygiene issues puts defenders in control of how they want to be notified of actionable findings on their attack surfaces. Cortex Xpanse can identify over 60,000 different applications and offers over 800 different rules, which allow for customization to match your organization's policies and initiatives.

Leveraging automation for prioritization

Triaging and remediating findings is oftentimes a very manual process for defenders. In large organizations, seemingly simple tasks like finding an owner can take days or weeks. Automation from Cortex Xpanse's Active Response Module is tailored to answer questions like "Who owns this service?" or "What is the business context of this application?" This saves analysts time and reduces exposure windows.

07

METHODOLOGY

In 2023, Unit 42 and Cortex Xpanse collected petabytes of information on internet-accessible exposures across 265 organizations. Unit 42 used this data to analyze issues associated with these exposures. Over the entire year, the research team studied the changes in cloud services and the associated risks they create in a typical organization across various industries. The 12-month period provided sufficient data for thorough computation and analysis.

For each industry category, the research team included data from at least five large organizations. Cortex Xpanse classified systems as either on-premises or cloud-hosted based on various factors. To ensure speed, precision, and scale in their work, the research team leveraged a machine-learning model for accurate asset attribution to different organizations. This model was supervised by a team of attack surface analysts supporting Cortex Xpanse.

On-premises assets of an organization are publicly accessible systems and services owned by the organization with statically assigned IP addresses. In contrast, cloud assets are publicly accessible systems and services leased by the organization in dynamic IP space, excluding multitenant, SaaS-delivered services.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyber threats so organizations can embrace technology with confidence. We provide next-generation cybersecurity to thousands of customers globally, across all sectors.

Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

For more information, visit www.paloaltonetworks.com.

About Cortex Xpanse

Cortex Xpanse® is an active attack surface management solution that helps your organization actively discover, learn about, and respond to unknown risks in all connected systems and internet-accessible services.

Cortex Xpanse protects the U.S. Department of Defense, all six branches of the U.S. military, several federal agencies, and over 200 large enterprises.

For more information, visit www.paloaltonetworks.com/cortex/cortex-xpanse.

About Unit 42

Palo Alto Networks Unit 42® brings together world-renowned threat researchers, elite incident responders, and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against real-world threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time so that you get back to business faster.

Visit paloaltonetworks.com/unit42.

About the ASM Module for XSIAM

Cortex XSIAM® extended security intelligence and automation management is the AI-driven security operations platform for the modern security operations center (SOC) harnessing the power of artificial intelligence to improve security outcomes and transform security operations radically. By adding the Attack Surface Management (ASM) Module to your XSIAM deployment, you can gain comprehensive visibility across your attack surface, get immediate zero-day visibility, and automate the remediation of exposures.

Read the ASM Module for XSIAM Solution Brief to learn more.

About the Unit 42 Attack Surface Assessment

The Unit 42 Attack Surface Assessment helps you identify and manage exposure, mitigate risk, and bolster your security posture now and in the future. This assessment provides an expert view of your internet-connected assets with prioritized recommendations to improve your defenses so you can remediate issues before attackers can exploit them.

With our security expertise and Cortex Xpanse data, you'll find previously unknown assets, including shadow IT infrastructure, to identify vulnerabilities and security gaps. You get recommendations tailored to your specific business and security concerns.

Identifying and remediating issues in your attack surface can reduce insurance premiums and show measurable progress to regulators, board members, and other stakeholders. If your organization needs help with starting or advancing your attack surface management program, the Unit 42 Attack Surface Assessment can help. [1]

1 *"Unit 42 Attack Surface Assessment" datasheet, Palo Alto Networks, January 31, 2023.*