thalesesecurity.com

THALES

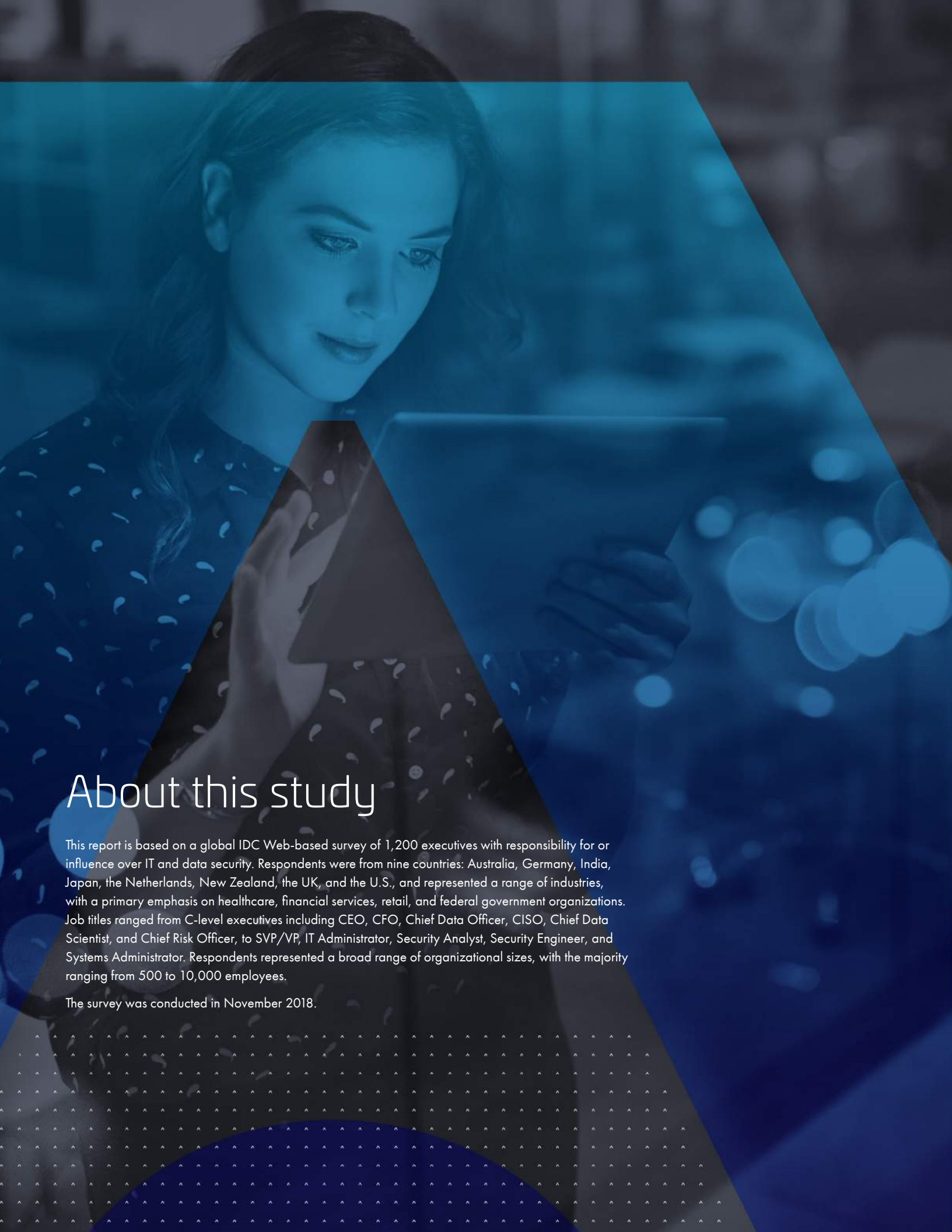
The Changing Face of Data Security
2019 Thales Data Threat Report

Global Edition

#2019DataThreat

RESEARCH AND ANALYSIS FROM:

IDC ANALYZE THE FUTURE



About this study

This report is based on a global IDC Web-based survey of 1,200 executives with responsibility for or influence over IT and data security. Respondents were from nine countries: Australia, Germany, India, Japan, the Netherlands, New Zealand, the UK, and the U.S., and represented a range of industries, with a primary emphasis on healthcare, financial services, retail, and federal government organizations. Job titles ranged from C-level executives including CEO, CFO, Chief Data Officer, CISO, Chief Data Scientist, and Chief Risk Officer, to SVP/VP, IT Administrator, Security Analyst, Security Engineer, and Systems Administrator. Respondents represented a broad range of organizational sizes, with the majority ranging from 500 to 10,000 employees.

The survey was conducted in November 2018.

Contents

Our Sponsors:

Executive Summary

Digital transformation (DX) is changing the way we live and work

Companies are fundamentally reimagining their businesses and taking advantage of digital technologies like cloud, mobile, social, and the Internet of Things to transform the experience their customers receive, create innovative new business models, and find ways to create new efficiencies and reduce their operating costs. Our results showed that DX is well underway, with 39% of companies in our study saying they are either aggressively disrupting the markets they participate in or embedding digital capabilities that enable greater enterprise agility.

39%

of companies in our study saying they are either aggressively disrupting the markets they participate in or embedding digital capabilities that enable greater enterprise agility.

The information security professional is being stretched

While DX is providing tremendous benefits to the enterprise and its customers and constituents alike, it is complicating the lives of information security professionals. In fact, security professionals could be forgiven for feeling they are caught in a vice. Not only must they deal with a very real threat environment, in which 60% of organizations report that they have been breached (30% in the past year alone) and with threats now emerging from a wide variety of external as well as internal sources – but they must also deal with a fundamental change in the nature of what they need to protect.

In today's information-oriented economy, the crown jewels of an organization are its data. Sensitive customer, financial, and other proprietary data is the most important thing an organization can protect. And yet an integral part of many companies' digital transformation journey consists of migrating data away from "locked vaults" in the organization's data center out to the cloud and edge technologies like mobile devices and the Internet of Things. No longer can the organization simply set up a secure perimeter and feel good about its stance.

No organization is safe from data security risks

One of the big messages coming from this year's data threat report is that no one is safe. Even the most sophisticated companies are getting breached, and our study shows that the greater the level of sophistication, the more likely respondents are to say that they have been breached.

64% of those who spend more than 10% of their IT budget on security say they have experienced at least one breach and, of those, 34% say that they have experienced a breach in the past year. Compare this to organizations that spend 10% of less of their IT budget on security. 47% of those say that they have experienced at least one breach in the company's history, while 17% say that they experienced a breach in the last year.

It may be that organizations that spend more than 10% of their IT budget on security are larger, more technology focused and therefore have a greater attack surface contributing to an increased risk of being breached. In may be that organizations that spend 10% or less of their over IT budget on security are less mature and may be unaware of past breaches or have yet to discover ongoing ones. At the very least, the finding demonstrates that no matter the spend, no company can rest easy.

64%

of those who spend more than 10% of their IT budget on security say they have experienced at least one breach.

A multi-layered approach is the "new normal"

Organizations need to take a multi-layered approach to security, and we see evidence of this in our survey. Respondents are placing a roughly equal amount of focus on network, application, and data security with 36% of their focus on network, 34% on data, and 30% on application security. However, implementing a multi-layered security approach is hard to do. Respondents have long "to do" lists with plans to implement a wide variety of technologies over the next 12 months.

But budgets are not growing at the rates they have been in years past, and increasingly stringent regulatory and compliance environments are forcing security professionals to make critical tradeoffs and consider how to do more with less.

Tools are needed to assist enterprise

Organizations need to put tools in place that will let them manage complexity. These tools should span both legacy on-premises needs as well as modern, cloud-based, edge technology-oriented technologies with solutions like encryption and tokenization that provide some of the best protection in today's threat environment.

01 Key Findings

Innovating toward mediocre security

Digital transformation (DX) is well underway. 39% of the respondents in our survey believe they are in one of the two most advanced DX categories, characterized by aggressively disrupting their markets or embedding digital capabilities into the enterprise tightly linked to an agile management vision. Only 22% say they have no DX stance or are applying it in an ad-hoc manner (Figure 1).

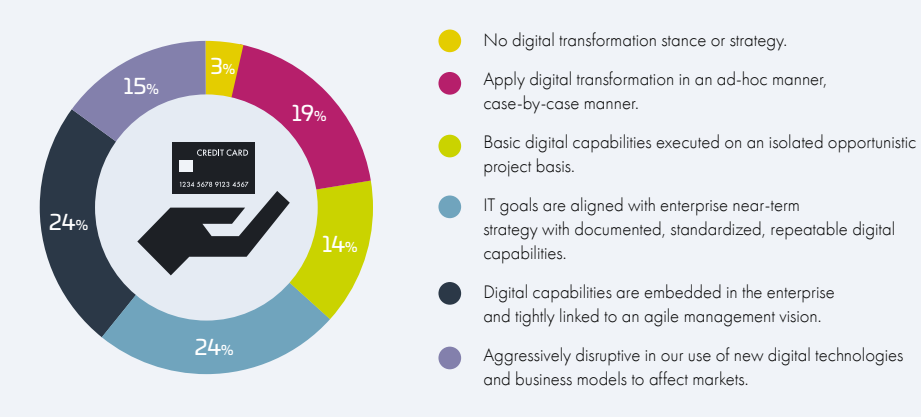


Figure 1 – Digital Transformation Stance

Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

While digital transformation is providing benefits to companies and their customers alike, it is also introducing a digital divide between the DX "haves", those that are aggressively implementing modern IT architectures, and DX "have-nots", those that still have a significant amount of infrastructure tied up in traditional, on-premises equipment. Most pundits will tell you that enterprises that win the race to digitally transform their organizations are well on their way to leading in their respective markets. Strictly speaking, that makes perfect sense, but it also does not fully capture the security challenges that DX presents.

As it relates to security, the DX "haves" may quickly find that they are the organizations struggling to apply consistent security across architectures and throughout transformed business processes. Companies are continuing to prop up old infrastructures while simultaneously rolling out new cloud-based, digitally transformative technologies. However, with finite budgets and labor pools, companies may not have the ability to secure data across all their environments. Ironically, the "haves" may actually be worse off from a security perspective because they have less budget to secure their infrastructure, and yet they have more to secure.

"A budget that is stretched thinly across so many environments, and so many potential landing spots for data, will require organizations to find **better value** in solutions."

Reaching a security spend ceiling

This year, only 50% of companies told IDC that they expect an increase in their security budget. That is down compared to last year's Data Threat Report in which 79% of organizations reported an expected increase in their security budget (Figure 2). Does this mean that we're reaching a security spending ceiling? If it does indicate the beginning to a hard-line cap on security budget against IT budget, it doesn't bode well for point security solutions. A budget that is stretched thinly across so many environments, and so many potential landing spots for data, will require organizations to find better value in solutions. That's good news for platform-based security solutions with options for on-premises, cloud, and hybrid protections.

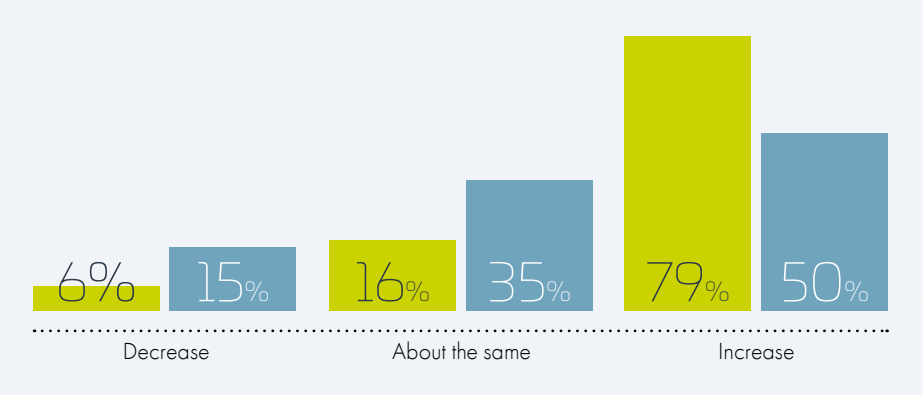


Figure 2 – IT Security Spend

Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

> "...the amount of spending on data security is very low for a great many organizations. Half of the organizations surveyed say they are spending only **6% to 15%** of their security budget on data security - a figure that amounts to **0.6% to 3%** of their overall IT budget."

Furthermore, the amount of spending on data security is very low for a great many organizations. Half of the organizations surveyed say they are spending only 6% to 15% of their security budget on data security – a figure that amounts to 0.6% to 3% of their overall IT budget. These results are in part a reflection of the current security market: network security, which relies on hardware and devices, is generally more expensive than data security.

The spending ceiling may be one reason why sensitive data in new initiatives isn't receiving the attention it should. As a case in point, while 97% of respondents will use sensitive data on digitally transformative technologies, fewer than 30% of respondents are using encryption within these environments. One potentially troubling explanation for the relatively low adoption of data protection mechanisms for new technology is that businesses are making risk management decisions to continue transformation even if it outpaces security architecture. Some companies are making the decision to drive business first, and worry about security later.

It appears that the security investment is being stretched, somewhat unsuccessfully, to meet the growing demands of more complex environments (Figure 3).

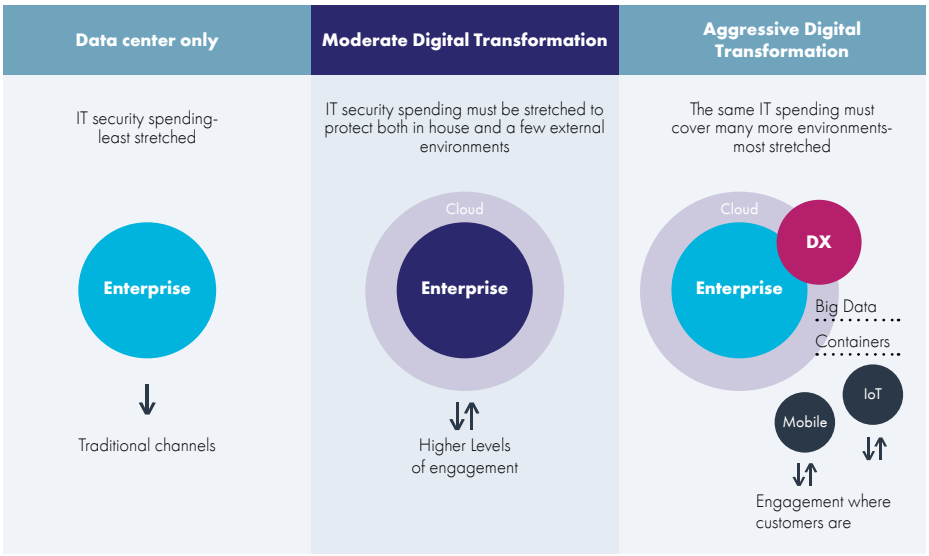


Figure 3 – Security Investments Are Being Stretched to Cover Additional Needs and Technologies

Source: IDC, January 2019

Security pros are aiming at the wrong target. They think they are secure as they roll out new technologies, but they aren't able to put as much budget against it as they should. Moreover, as more data moves to new DX efforts supported by cloud, the monetary value decreases. Organizations require smarter, better ways to approach security, and to implement security tools and platforms designed for modern, hybrid and multi-cloud architectures, not jerry-rigged from legacy technologies.

Threat vectors are shifting to external actors

Our research this year found that a significant number of respondents report having experienced a breach. Globally, 60% say they have been breached at some point in their history, with 30% experiencing a breach within the past year alone. In the U.S. the numbers are even higher, with 65% ever experiencing a breach, and 36% within the past year (Figure 4). And respondents acknowledge they are vulnerable – 86% of all respondents acknowledge they are vulnerable to data security threats, with 34% globally calling themselves "very" or "extremely" vulnerable (Figure 5).

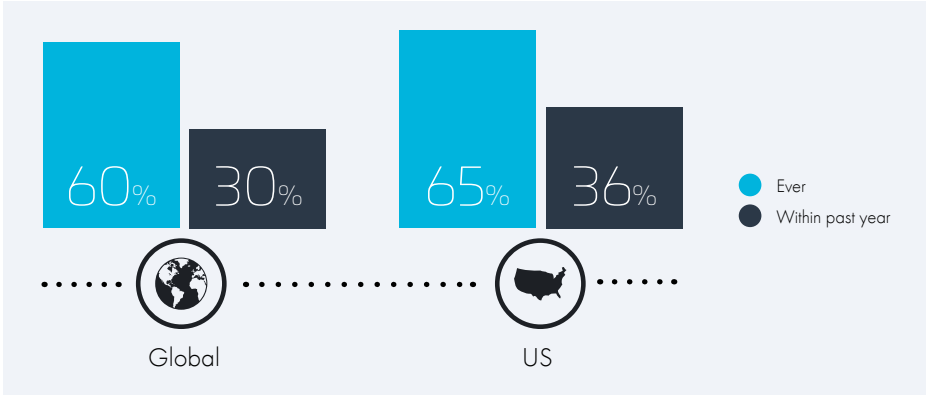


Figure 4 – Breach Incident Rates

Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

"Globally, **60%** say they have been breached at some point in their history, with 30% experiencing a breach within the past year alone. In the U.S. the numbers are even higher, with 65% ever experiencing a breach, and 36% within the past year."

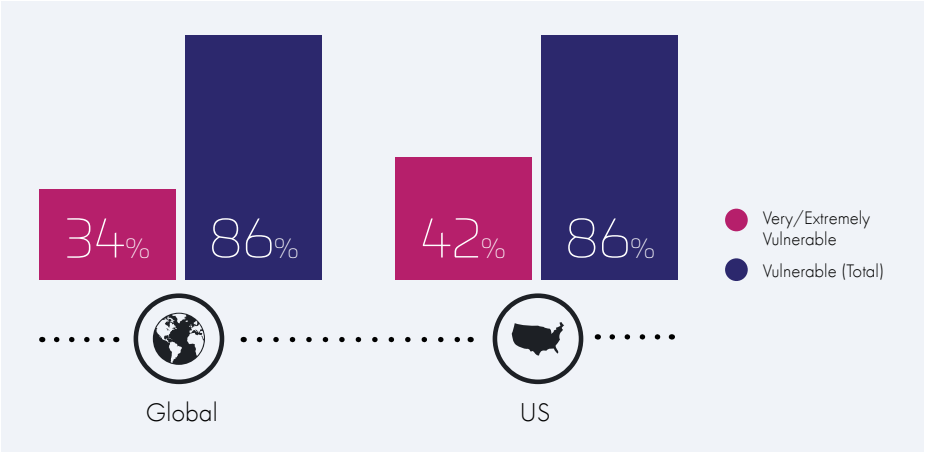


Figure 5 – Vulnerability to Data Security Threats

Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Only a few years ago, the general consensus was that internal actors were the greatest threat, whether from malicious privileged users or carelessness among non-privileged employees or contractors. Privileged users have a unique level of access that must be carefully managed and have barriers that protect against external actors purposefully stripped away to allow employees and contractors to perform their job functions. This year's study, however, shows an incredible respect for the types of harm that external actors are capable of inflicting (Figure 6). Respondents ranked external threat actors 1, 2, and 3 when asked to identify current data security threats with cyber-criminals finishing first.

*Note: IDC understands the complex definitional issue associated with cyberterrorism in that many definitions exist.**

> "Respondents ranked external threat actors 1, 2, and 3 when asked to identify current **data security threats** with cyber-criminals finishing first."

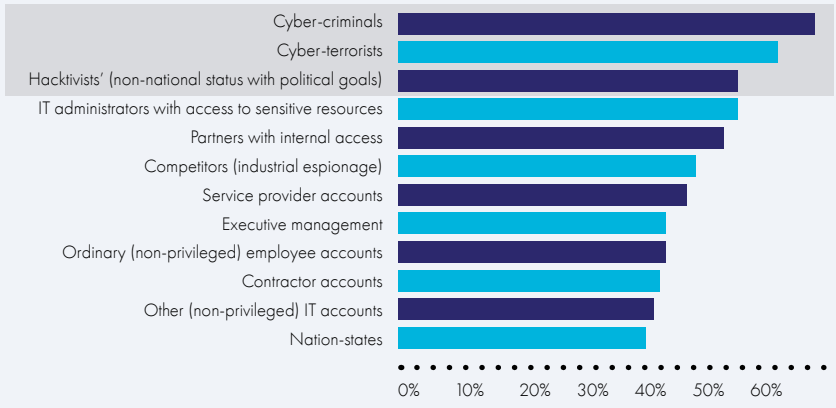


Figure 6 – Greatest Data Security Threats

Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

**In some cases, individuals use the terms cyberterrorism in concert or interchangeably with state sponsored attacks, hacktivism, etc. In the interest of balance, IDC chose not to attempt to redefine a term where respondents may already feel they possess a concrete understanding. IDC would tend to define the term in a way similar to physical terror attacks, meaning clandestine and with intent to cause real world harm recognizing that this definition would generally encompass a narrow group of attacks.*

No One Is Immune

Another key finding from our research is that no organization is immune from data security threats, and in fact, we found that the most sophisticated organizations are ***more likely*** to indicate that they have experienced a data security breach. This trend is consistent no matter how we define the sophistication of the audience: those who are spending more on IT security (Figure 7), those for whom data security is a larger portion of their security budget or those who are further along in their digital transformation journey. There could be multiple factors at work here. It could be that companies with greater brand recognition, because of their industry or market profile, are greater targets and are therefore forced to spend more on security. It could be that their greater level of sophistication makes them more aware of breaches, i.e., less sophisticated companies are also getting breached but are unaware of them. Alternatively, it could be that in their race to implement digital transformation, leading-edge companies are trading off security for time to market, which is the most troubling possible interpretation.

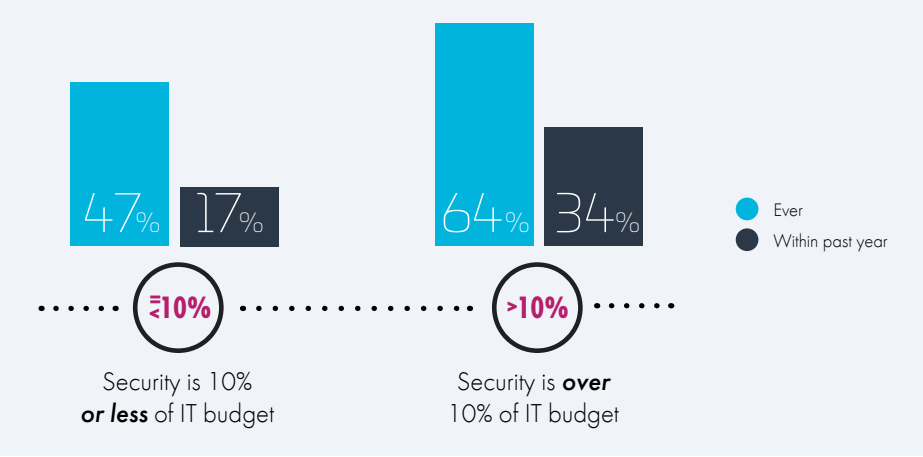


Figure 7 – Breach Incident Rates by Level of IT Spend

Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

> "Another key finding from our research is that **no organization is immune from data security threats**, and in fact, we found that the most sophisticated organizations are *more likely* to indicate that they have experienced a data security breach."

Seemingly paradoxically, breach prevention is a relatively low priority. Responding to a breach that occurred in the past was one of the least-important factors impacting organizations' IT security spending (only "executive directive" ranked lower). This seems to speak to a significant blind spot when it comes to data security. Organizations generally believe they have adequate security and may be lulled into a false sense of complacency. 66% of organizations rate the security they provide for new technology deployments as "very" or "extremely" secure, compared to only 12% who believe they don't have adequate security (Figure 8). In particular, less sophisticated organizations appear to be most at risk of complacency and need to improve their security measures.

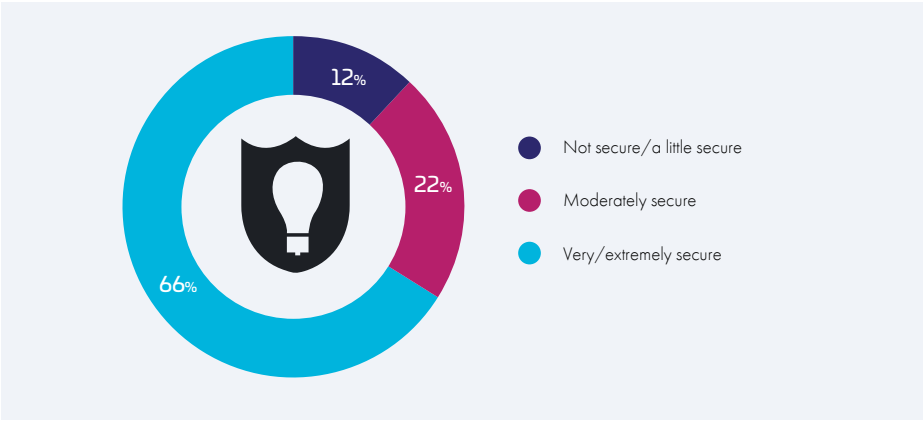


Figure 8 – Security Level of New Technology Deployments
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Complex Data Environments Are a Top Barrier to Data Security

Data environments are increasingly complex. Workloads that used to be handled by a single on-premises environment are now being augmented with multiple IaaS and PaaS environments, as well as tens and even hundreds of SaaS applications (Figure 9). Moreover, even as they shift new workloads to the cloud, companies must still maintain mission-critical applications that run onon-premises environments.

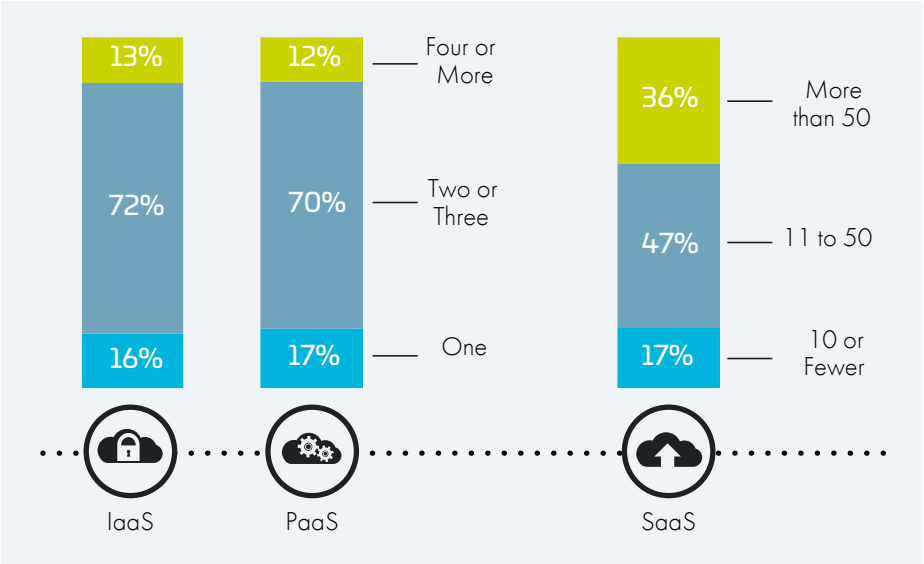


Figure 9 – Number of Cloud Environments
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Managing all these cloud instances brings new layers of complexity to IT departments. It is challenging enough managing encryption, tokenization, and providing visibility and access to sensitive data within a single environment, let alone three or five or fifty. In fact, respondents rated complexity as their number one perceived barrier to implementing data security, higher than staff, budget, and organizational buy-in (Figure 10). And with the amount of DX activity only increasing, the complexity that organizations are concerned about regarding their data security is sure to grow.

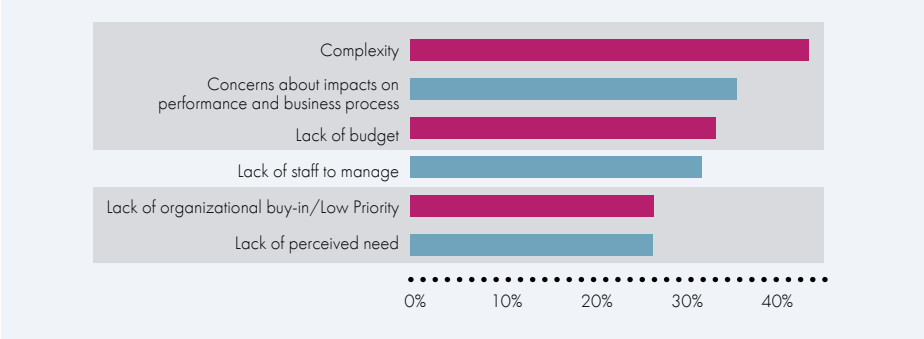


Figure 10 – Perceived Barriers to Implementing Data Security

Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Notably, complexity, impacts on performance and business processes, and budget are the top data security concerns, compared to lack of importance and organizational buy-in, which came at the bottom of the list. It's not that organizations don't recognize the importance of data security; they clearly do. However, they realize that implementing data security is challenging and they need better, simpler solutions that allow them to address these challenges. IDC is particularly struck by the fact that lack of budget is less of a barrier than complexity and ensuring performance/business processes. This is a powerful message. Organizations are looking to get data security right and are willing to spend the budget (and have the organizational backing) to do so.

"It's not that organizations don't recognize the importance of data security; they clearly do. However, they realize that implementing data security is challenging and they need **better, simpler solutions** that allow them to address these challenges."

"In today's information-oriented economy, the crown jewels of an organization are its data. Sensitive customer, financial, and other proprietary data is the most important thing an organization can protect. "

Clouds Have Established Themselves as Leading Technology Environments

Not only are companies deploying a large number of cloud environments, but clouds have emerged as a leading repository for sensitive data. When asked where they store sensitive data, over 40% of respondents say they use each of the three flavors of cloud – SaaS, PaaS, and IaaS (Figure 11).

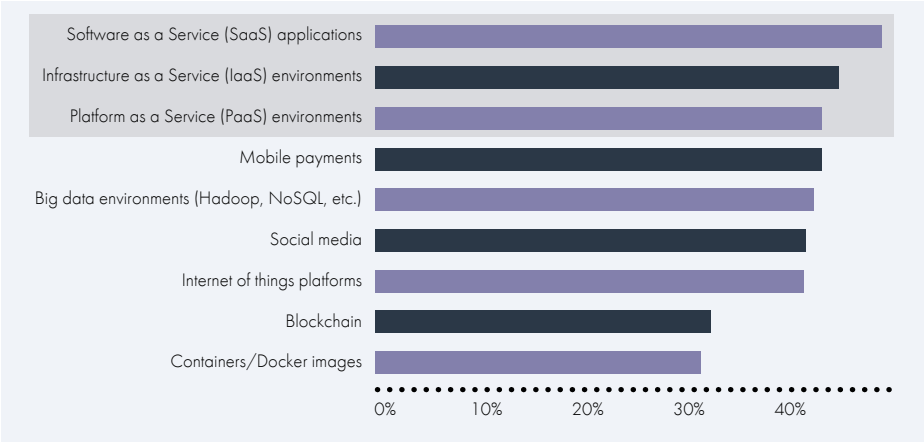


Figure 11 – Environments Used to Store Sensitive/Regulated Data

Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

> "the use of clouds to store sensitive data does not mean you can simply abdicate security responsibility to your cloud provider. Cloud security must be seen as **a shared security model** between the enterprise customer and the **PaaS, IaaS, or SaaS** provider."

However, the use of clouds to store sensitive data does not mean you can simply abdicate security responsibility to your cloud provider. Cloud security must be seen as a shared security model between the enterprise customer and the PaaS, IaaS, or SaaS provider. While the underlying or supportive infrastructure must be secured by the PaaS or IaaS provider, and the software platform by the SaaS provider, ensuring that customer-owned software and data is well-protected is where organizations must continue to be hyper-vigilant. In many cases, this means enterprises must take on responsibility for ensuring data protections like encryption, tokenization, and masking within their environments or ensuring its protection when the data moves between SaaS applications or migrates to another application.

As we have seen, organizations already appear to be confident in placing sensitive data in the cloud. This creates an environment in which sensitive data is moving further away from the traditional enterprise data controls in which organizations have already invested. Data must be protected where it sits, in the data center, in the cloud, or at its termination point. If that termination point happens to be another cloud service, a B2B provider, or the workstation of a remote worker, the data must be protected. For many organizations, this mesh of complex data traffic creates a challenge.

Companies Are Taking a Multi-Layered Approach to Security

In the past, when the majority of enterprises' data was located on premises, organizations placed a great amount of security focus on network and device security. The idea was that having a hard outer perimeter, backed up by device-level defenses within the firewall, was the best approach to securing sensitive data. There used to be a "two for one" spending effect in that the money spent on network security also protected the organization's data.

As companies pursue digital transformation and change their IT landscape, so too the emphasis on different types of security is shifting. In this year's study we found that respondents are putting only slightly less emphasis on data security (with issues such as data loss prevention, digital rights management, encryption, and PKI) as they are on network security (including endpoints, firewalls, UTM), and slightly more than they are on application security (software development security, DevSecOps, vulnerability scanning) (Figure 12). With more environments to protect, organizations need different ways to protect their data, and to put greater focus on data security. Put another way, data security is not a poor stepchild any more.

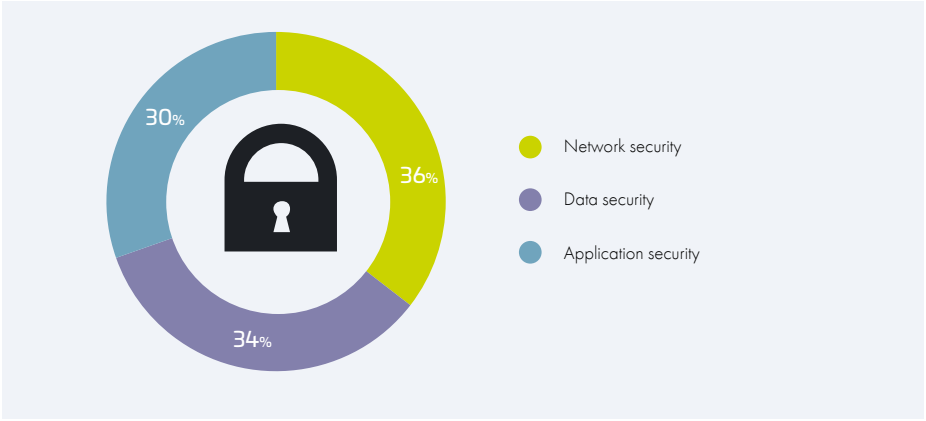


Figure 12 – Proportion of Security Focus

Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

"As companies pursue digital transformation and change their IT landscape, so too the emphasis on **different types of security** is shifting."

Aspirational Desires Disconnect with Budget Realities

Organizations interviewed for this study have high aspirations. While adoption levels for foundational technologies such as cloud, social media, mobile, and Internet of Things generally averaged over half of respondents, the majority of those who do not have those technologies implemented said they are planning to do so over the next 12 months (Figure 13).

> "compliance requirements are clearly driving a significant portion of organizations' data security efforts."

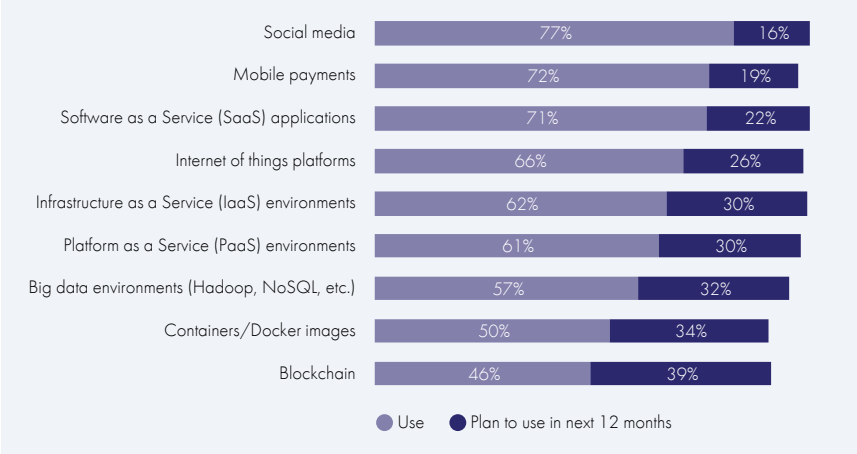


Figure 13 – Technology Adoption Levels
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Security professionals in our survey also have big plans when it comes to adopting data security technologies. Roughly half of the organizations surveyed currently support technologies like file encryption, database encryption, IAM, MFA, and HSMs. But of those who don't, the vast majority say they plan to implement these technologies in the next 12 months (Figure 14).

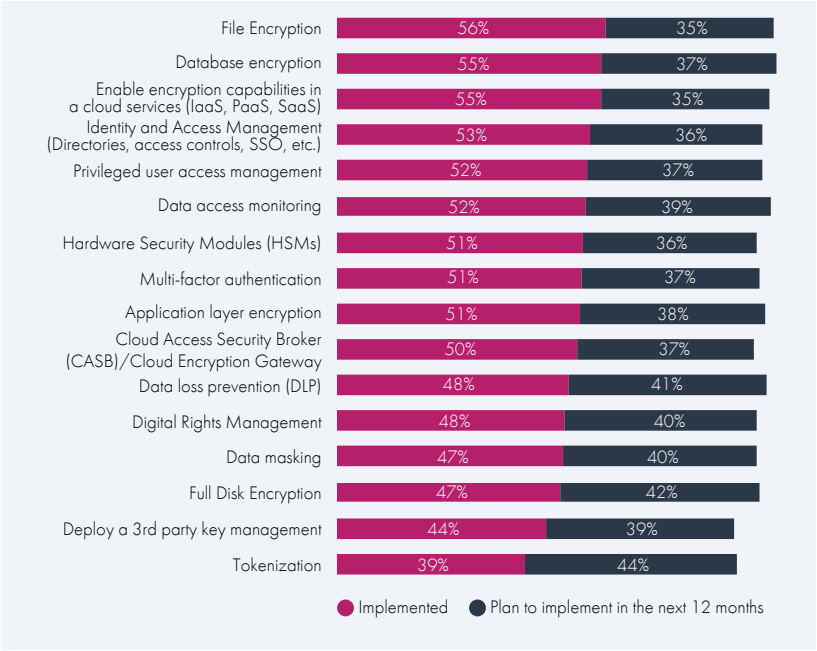


Figure 14 – Data Security Technology Adoption Levels
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

IDC cautions the reader to keep in mind that these are aspirational plans and that they likely speak to adoption but not penetration. DRM, full disk encryption, and tokenization don't have 50% TAM penetration today and won't be over 75% a year from now. It's likely that these penetration percentages speak to individual pockets of the organization, such as isolated DevOps teams, and not to full enterprise-wide deployments.

Nevertheless, these are ambitious adoption plans, the extent of which becomes even more evident when considering that the rate of security spending growth is declining, as discussed previously. The implication is that C-suite patience and support of continuously growing security budgets is waning. Security professionals are going to need to be smarter in their spending moving forward; they will need to prioritize and to figure out how to do more with less.

> "Despite the recognition of the importance of protecting sensitive data, encryption rates throughout the enterprise are surprisingly low. Fewer than **30% of enterprises** say they use encryption for the vast majority of use cases studied."

Regulatory and Compliance Changes Introduce New Challenges

Data privacy and sovereignty have become leading drivers in adopting data security controls. There are now more than 100 privacy laws and privacy initiatives promoted by governments around the world, ranging from the EU's GDPR regulations, which went into full effect in 2018, Germany's BDSG, and new California and New York standards on data privacy. This is on top of other industry-level regulations such as PCI DSS and Sarbanes Oxley in financial services, HIPAA HITECH in healthcare, and FedRAMP, NIST, fisma, and FIPS in the Federal Government. Just to name a few.

These compliance requirements are clearly driving a significant portion of organizations' data security efforts. When asked how they are addressing data privacy and sovereignty issues, encryption and tokenization emerged as the leading method of addressing them, with 44% of respondents saying they encrypt personal data subject to privacy/sovereignty regulations, and another 19% using tokenization (Figure 15).

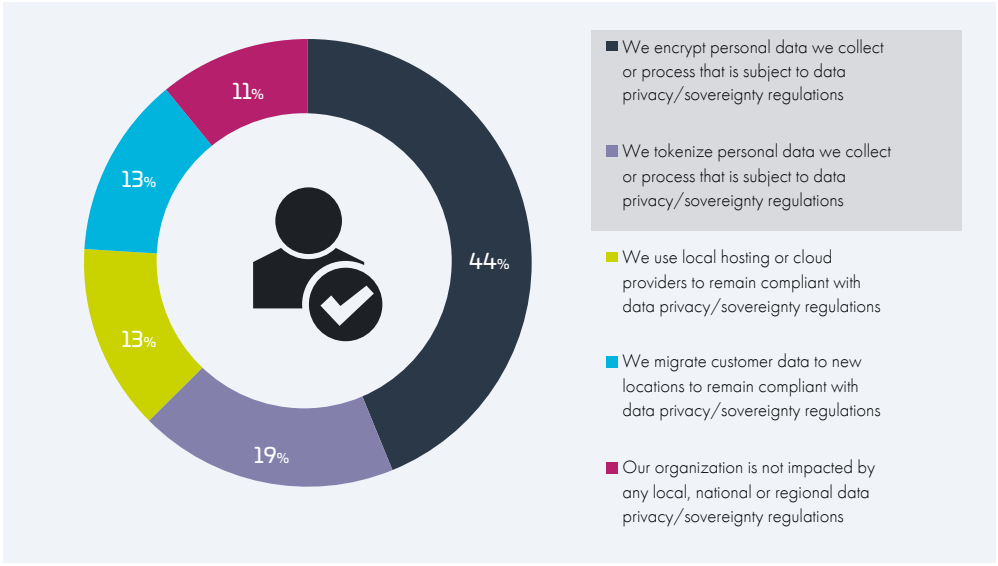


Figure 15 – Data Privacy/Sovereignty Stance
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Encryption Rates Are Low

Despite the recognition of the importance of protecting sensitive data, encryption rates throughout the enterprise are surprisingly low. Fewer than 30% of enterprises say they use encryption for the vast majority of use cases studied, including disk encryption within datacenters, from cloud providers, in big data environments, in databases, within mobile devices, and in IoT environments. Encryption for PC data at rest topped the list at 31% of companies using it (Figure 16). Given the high usage of sensitive data, these low rates of encryption pose a risk to the enterprise.

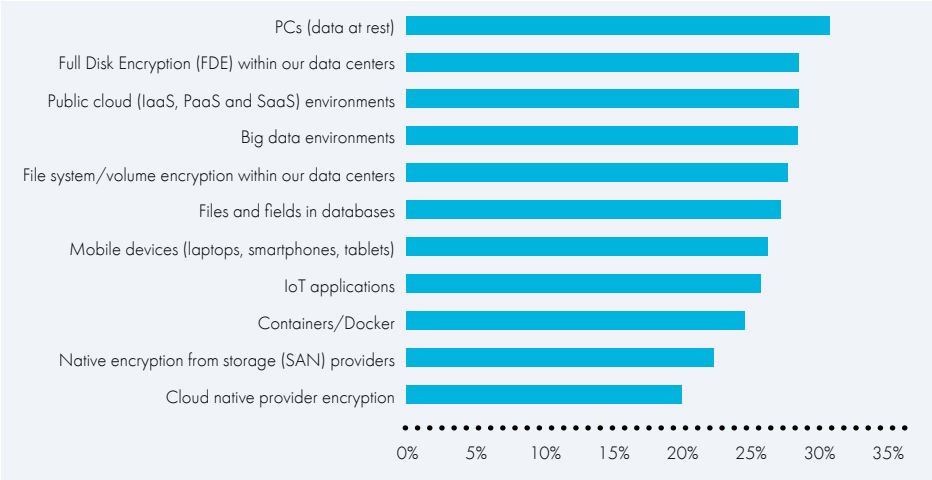


Figure 16 – Encryption Use Rates
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

02 Cloud

Overall Cloud Security Concerns

With cloud emerging as a critical environment for data security, we asked about respondents' concerns when it comes to cloud data security, both overall and for each type of cloud. Overall, respondents' concerns cover a wide range of issues, with the business stability of the provider, breaches at the provider, and lack of data privacy policies topping the list (Figure 17).

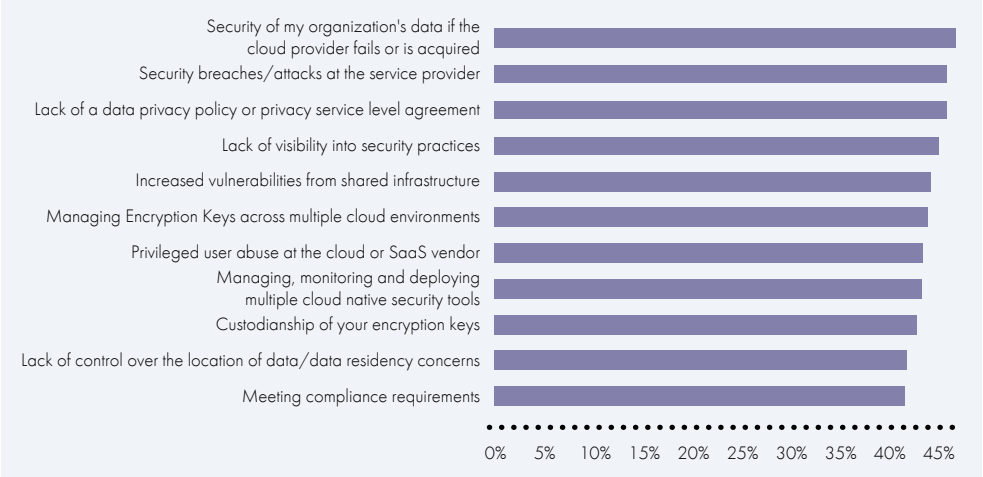


Figure 17 – Overall Cloud Data Security Concerns
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Software as a Service

Looking specifically at software as a service (SaaS), respondents had a similarly broad set of concerns, with their top concerns being encryption of data within the service provider's infrastructure, encryption with the ability to store and manage keys locally, and support for HSMs (Figure 18).

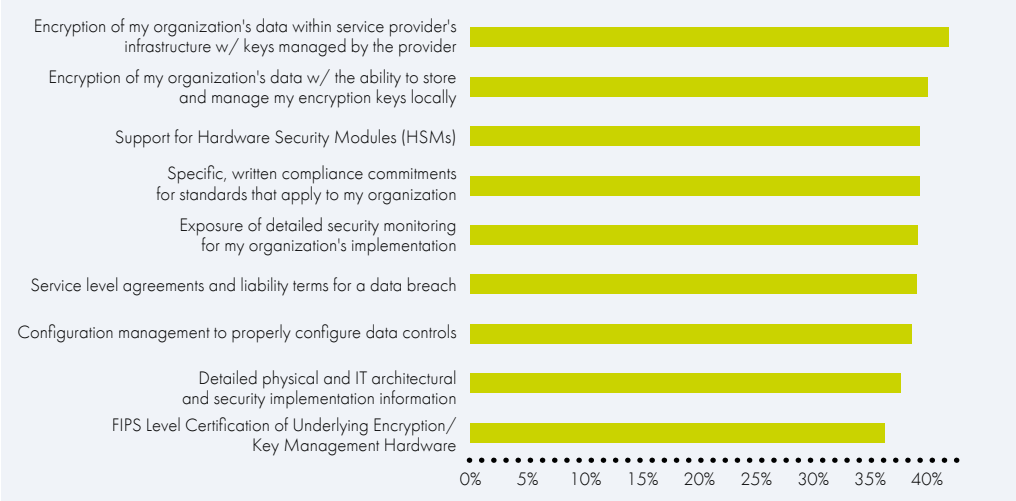


Figure 18 – SaaS Data Security Concerns
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Infrastructure as a Service

In terms of infrastructure as a service, respondents' top concerns included understanding their providers' physical/IT architectural security implementations, support for hardware security modules (HSMs), and SLAs surrounding a security breach (Figure 19).

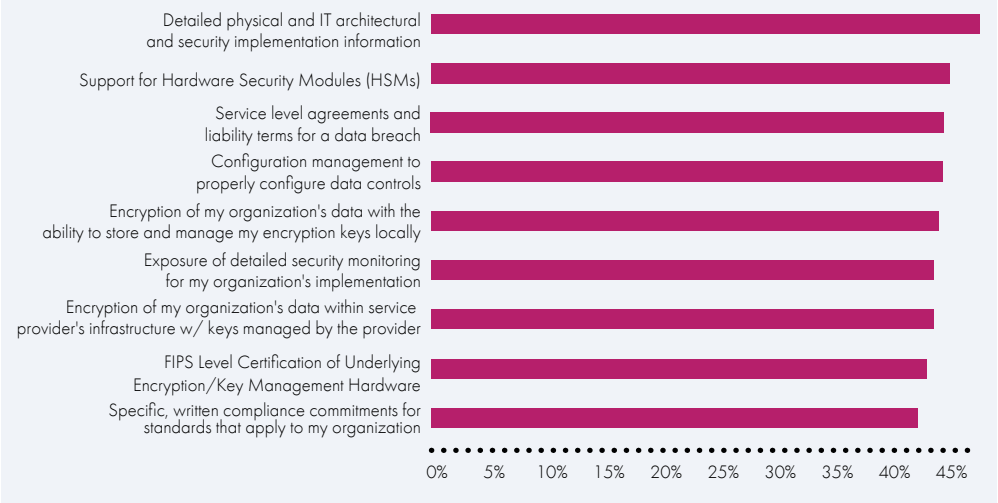


Figure 19 – IaaS Data Security Concerns
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Platform as a Service

Finally, the leading data security concerns around platform as a service include exposure of the organization's security monitoring, support for HSMs, and encryption within the service provider's infrastructure (Figure 20).

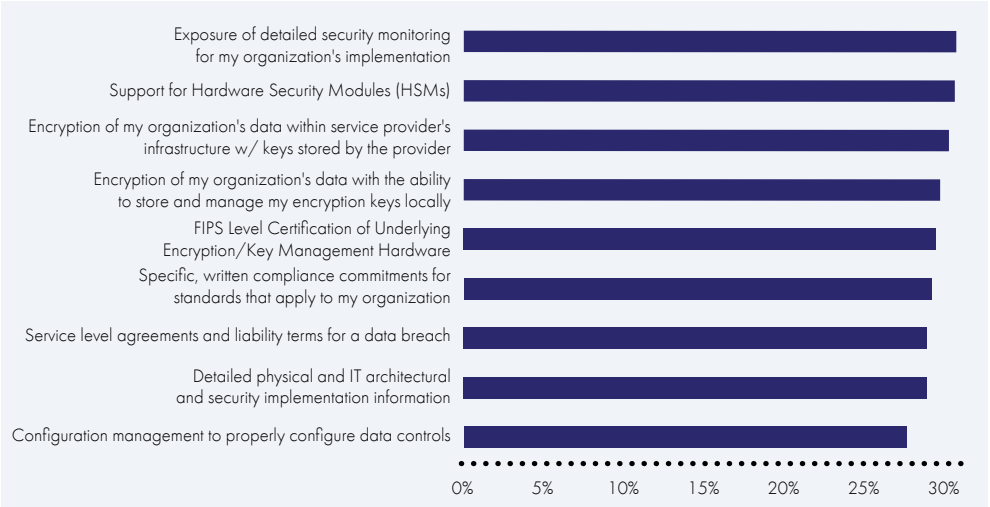


Figure 20 – PaaS Data Security Concerns
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Security Concerns and Methods of Alleviation by Data Technology Environment

A critical component of digital transformation is the edge. DX creates opportunities for new technologies that engage businesses and consumers where they are, but it introduces new complexities as companies push an increasing amount of data and computing power to the edge. An increase in edge technologies demands that security spend shifts away from traditional enterprise security and even away from cloud. Mobile and IoT are specific examples of this, but big data, containers, and blockchain are also enabling technologies that help expand and customize edge computing.

Mobile Payments

Respondents have a wide range of data security concerns regarding mobile payment technologies. Fraudsters hold a slight lead in the list of concerns and are joined by exposure of PII, weak authentication protocols, and potential exposure of payment card information (Figure 21). Leading methods to address mobile payment concerns include the use of strong encryption (cited by 31% of respondents), multi-factor authentication (MFA) (30%), and strict password compliance (30%).

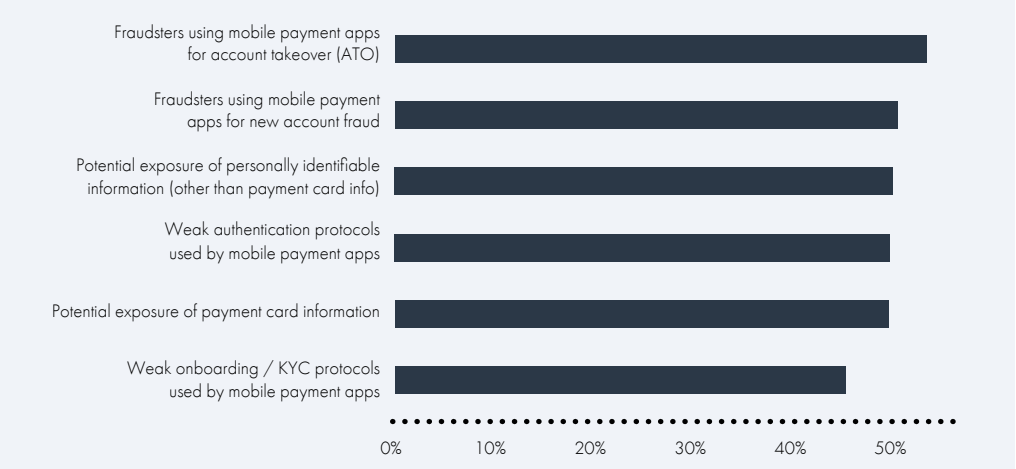


Figure 21 – Mobile Payment Data Security Concerns
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Internet of Things

The main data security concerns around IoT include attacks on IoT devices, lack of frameworks and controls, and protecting sensitive data through encryption and tokenization (Figure 22). The main ways they look to alleviate IoT security concerns include encryption/tokenization (cited by 42% of respondents), authentication/digital identification of IoT devices (41%), and anti-malware (40%). IDC notes that there is relatively little anti-malware available for the vast majority of IoT devices on the market today. This finding could point to respondents' desire to see more of it become commercially available.

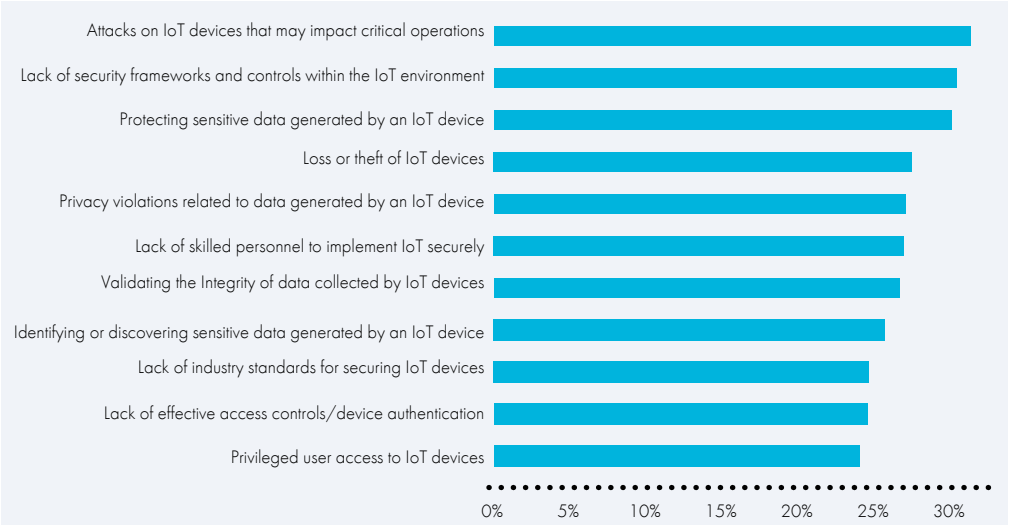


Figure 22 – IoT Data Security Concerns
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

"The main **data security concerns** around IoT include attacks on IoT devices, lack of frameworks and controls, and protecting sensitive data through encryption and tokenization."

Big Data

Leading data security concerns regarding big data include sensitive data residing throughout the environment, data quality concerns, and privacy violations from internationally-originated data (Figure 23). The top methods of alleviating big data security concerns are stronger authentication (48%), system-level encryption and access controls (45%), and sensitive data discovery/classification (45%).

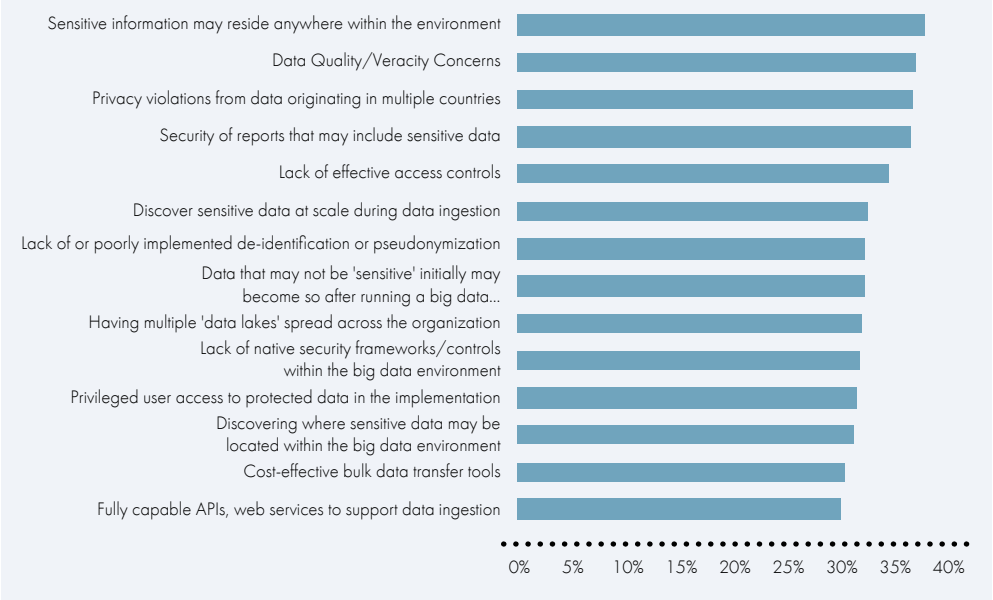


Figure 23 –Big Data Security Concerns
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Containers/Docker

When it comes to containers/Docker, the leading security concern was the security of data stored in containers, followed by unauthorized access to containers and spread of malware among containers (Figure 24). The main ways respondents looked to alleviate containers/Docker data security concerns include encryption (47%), anti-malware (43%), and vulnerability scanning (38%).

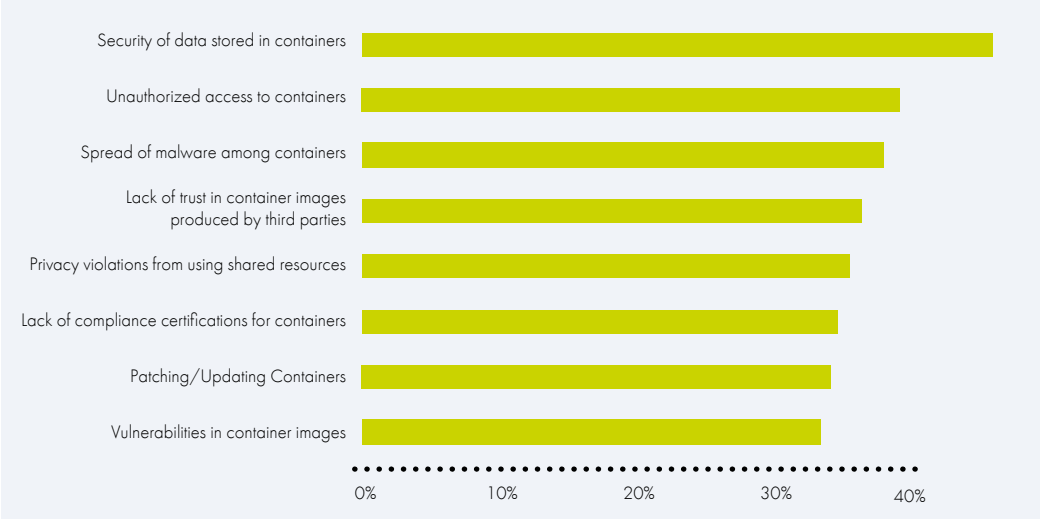


Figure 24 – Containers/Docker Data Security Concerns
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

"When it comes to containers/Docker, the leading security concern was the **security of data** stored in containers."

Blockchain

Blockchain data security concerns were also very broadly spread. The leading concern by a slight margin was threat of cryptojacking, followed by exposure of private data from improper public ledgers (Figure 25). The leading methods to alleviate blockchain data security concerns are continuous authentication, identity proofing, and strong entitlements. IDC notes that Blockchain is still a relatively new technology and respondents are probably not as familiar with it and its security issues as they are with other technologies in this study.

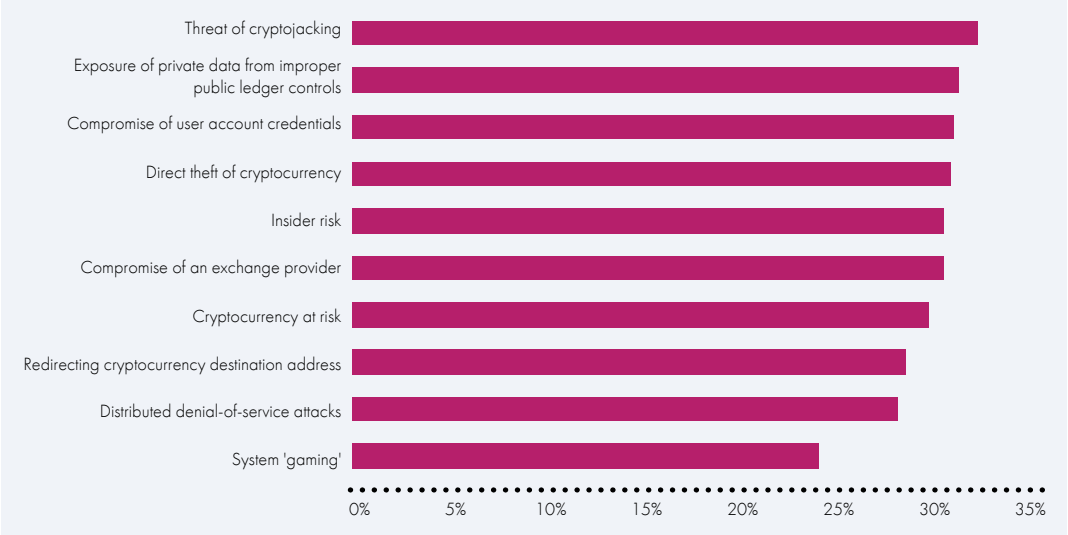


Figure 25 – Blockchain Data Security Concerns
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

"The leading concern by a slight margin was **threat of cryptojacking**, followed by exposure of private data from improper public ledgers."

"Digital transformation (DX) is **changing the way we live and work**. Companies are fundamentally reimagining their businesses and taking advantage of digital technologies like cloud, mobile, social, and the Internet of Things..."

IDC Guidance/Key Takeaways

Data security is hard. But it's vitally important. As DX drives increasing complexity into IT environments and changes the nature of how sensitive data is stored, organizations need to take a fresh look at how they provide data security. Against this backdrop, IDC recommends security professionals consider the following guidelines:

> "You need new data security methods to protect today's IT landscape, and this **starts with encryption**."

- **Focus on all threat vectors**. We live in an era in which threats are coming from all over, both external to and from within the organization. Bad actors are changing their methods daily, and enterprises need to continually evolve to match them. Don't be complacent and don't assume that the technology and processes you currently have in place are sufficient for your needs today or in the future.

- **Invest in modern, hybrid and multi-cloud-based data security tools and measures that scale to modern architectures**. Yesterday's perimeter-security defenses are no longer sufficient to protect against the myriad of data threats facing your organization. Organizations should focus on solutions that can simplify the data security landscape and reduce complexity, and that span legacy concerns as well as modern, cloud-based digital transformation technologies.

- **Look for solutions that let you do more with less**. Even as C-level executives understand the mandate for enterprise security, free-spending days marked by ever-increasing security budgets as companies "throw money at the problem" are on the decline. CFOs are questioning the ROI of security spending, and security professionals are going to need to identify solutions and platforms that let them address multiple layers of security concerns in a cost-effective manner, and that also reduces the burden on operating staff.

- **Prioritize compliance and sovereignty issues**. With the overarching impact of GDPR and strengthening of other global data compliance requirements, 2018 could be considered "the year of data protection." But the impact of data use compliance and sovereignty is likely still on the rise, and regulations are likely to become more rigid, and not less. Already, countries are following Europe's lead to further protect citizen data. Global corporations need to become intimately familiar with the regulatory environments in which they operate and prioritize them appropriately when developing their security stance.

- **Data security, starting with encryption, is an important part of the mix**. As data migrates away from the enterprise premises and to the cloud, network security is no longer sufficient to protect your data. Regulatory compliance and sovereignty issues are forcing companies to rethink their security stance. You need new data security methods to protect today's IT landscape, and this starts with encryption.

Principal analyst profiles

Sean Pike

Sean Pike is program Vice President for IDC's Security Products group. In this role, Sean leads IDC's Security Products, Data Security, Information Governance & eDiscovery, and Identity & Access Management research programs.

Sean provides competitive intelligence, strategic advisory, and thought leadership for security, data protection, governance, risk, compliance, and legal discovery technology and solutions. He examines the implications of emerging technology, legal and regulatory developments, and the threat landscape on organizations' risk and compliance programs, information governance and data privacy initiatives, and legal discovery efforts. He also tracks the convergence of information management, storage, security, and IT operations technologies and the impact on various governance and discovery use cases.

Frank Dickson

Frank Dickson is a Research Vice President within IDC's Security Products research practice. In this role, Frank provides thought leadership and guidance for clients on a wide range of security products including endpoint security, identity and access management, authentication, threat analytics, and emerging products designed to protect transforming architectures and business models

About International Data Corporation (IDC)

IDC Is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,100 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries.

IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG), the world's leading media, data and marketing services company that activates and engages the most influential technology buyers.

About Thales eSecurity

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing amount of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

2860 Junction Ave, San Jose, CA 95134, USA

+1 888 267 3732
+1 408 433 6000

> thalesesecurity.com <

thalesesecurity.com/DTR

#2019DataThreat