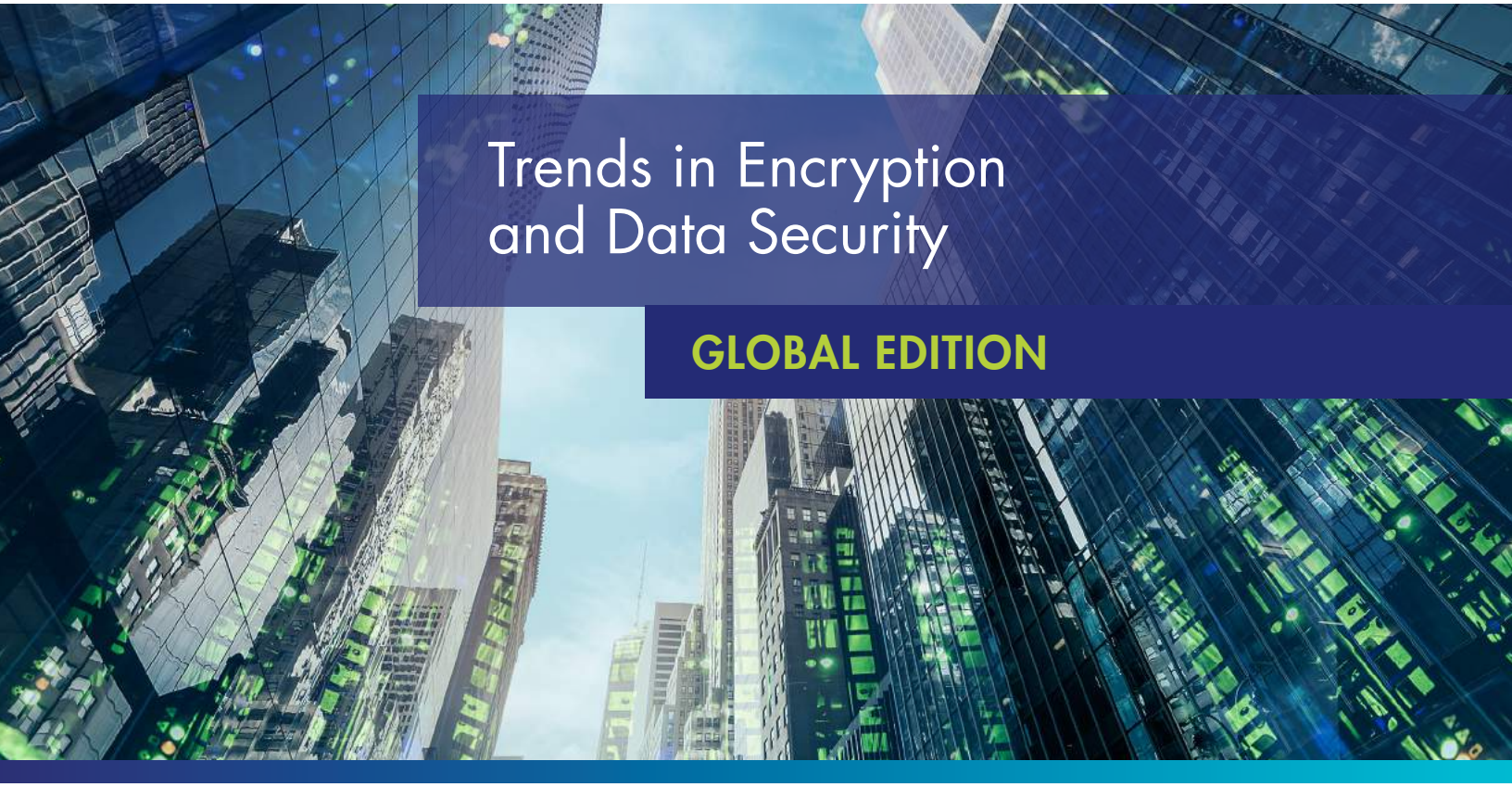
THALES

451 Research®

2018 THALES DATA THREAT REPORT



Trends in Encryption and Data Security

GLOBAL EDITION

#2018DataThreat

TABLE OF CONTENTS

INTRODUCTION 3

EXECUTIVE SUMMARY 6

To the least effective go the spoils 7

KEY FINDINGS 8

BODY OF REPORT 13

Contradictions, conundrums and enigmas 13

The security spending paradox 13

Spending up significantly, but… 13

…So are data breaches 14

Who are the risky threat actors? 14

Compliance and security – two sides of the same coin, or distant cousins? 15

Protecting data-at-rest gets its due – sort of… 17

BARRIERS TO SECURITY 18

Encryption as antidote for proliferating data sovereignty mandates 18

Encryption and tokenization top the list of data security projects 19

STRATEGIES FOR A MULTI-CLOUD WORLD 19

New security challenges from emerging technologies 21

Encryption with key management an essential cloud security control 22

BIG DATA, BIG QUESTIONS 23

IoT RISING, BUT SO ARE IoT SECURITY CONCERNS 25

DOCKER/CONTAINERS 27

AI/MACHINE LEARNING 27

MOBILE PAYMENTS 28

BLOCKCHAIN TRENDS 29

RECOMMENDATIONS 30

OUR SPONSORS

GEOBRIDGE CRITICALSTART CSA cloud security alliance℠ OASIS

INTRODUCTION

The harsh realities of the current state of cybersecurity are made starkly apparent by the seemingly endless reports of major data breaches, which continue unabated despite consistent increases in IT security spending. This ongoing game of cat-and-mouse suggests that the tactics, sophistication and motivation are helping global attackers stay at least one step ahead of their often overwhelmed and beleaguered defenders. The obvious – or what should be obvious – question is whether the cyber defenses that are being deployed today need to be re-examined for overall effectiveness and recalibrated.

"Clearly, doing what we have been doing for decades is no longer working. The more relevant question on the minds of IT and business leaders, then, is more direct: "What will it take to stop the breaches?"

A generation ago, IT security was fairly straight-forward. Most data was contained within the proverbial 'four walls' of the organization behind corporate firewalls and Intrusion Prevention System (IPS) devices. Access to that data and applications was via terminals, desktops, laptops and consoles for the most part. And the worst threat actors hacked as much for fun and notoriety as anything else.

By sharp contrast, today's computing environments are increasingly driven by the desire for digital transformation, resulting in highly distributed implementations – data is increasingly held beyond the corporate boundaries, in complex hybrid cloud and mobile environments. Hackers are now motivated by everything from nationalism to anarchy to the promise of instant riches. Clearly, doing what we have been doing for decades is no longer working. The more relevant question on the minds of IT and business leaders, then, is more direct: "What will it take to stop the breaches?"

It is with this question foremost in our minds that we have designed the 2018 version of the *Thales Global Data Threat Report*. This year's report is based on a global survey conducted by 451 Research during October and November of 2017.

"By sharp contrast, today's computing environments are increasingly driven by the desire for digital transformation, resulting in highly distributed implementations — data is increasingly held beyond the corporate boundaries, in complex hybrid cloud and mobile environments."

In contrast to last year's report, we surveyed 1,200+ senior security executives from across the globe (up from 1,100), including respondents from key regional markets in the U.S., U.K., Germany, Japan, Sweden, the Netherlands, Korea and India. We also surveyed key segments within those countries including federal government, retail, finance and healthcare. While all 1,200 respondents have at least some degree of influence in data security decision-making, more than one-third (34%) have 'major' influences on these decisions and nearly half (46%) have sole decision-making authority.

The results are sobering: while planned spending on IT security is up globally over the previous year, so too are data breaches, with evidence mounting that hackers are indeed hitting the bottom line. At the same time, data privacy regulations are looming, with the potential to substantially impact organizations of all stripes, the most potent of which is the General Data Protection Regulation (GDPR). GDPR takes full effect in May 2018 and ushers in sweeping changes in the way organizations must deal with any data related to the European Union's 740 million residents.

Also from the EU comes the Revised Payment Service Directive (PSD2), which takes effect in 2018 and in essence ends retail banks' monopoly on their customer's account information and payment services. PSD2 enables bank customers, both consumers and businesses, to use third-party providers to manage their finances, with banks obligated to provide those providers with access to customers' accounts through open APIs. Furthermore, Japan's Act on the Protection of Personal Information (APPI), which dates back to 2003 and is one of Asia's oldest and most potent data protection statutes, underwent significant revisions in mid-2017.

Combined with Japan's new Personal Information Protection Commission (PPC), APPI is having a profound impact on the international community's cross-border data transfers with Japan.

Year to year comparisons made in this year's report reflect all 1,200 responses, including approximately 400 gathered from respondents in India, Korea, Sweden and Netherlands. Respondents from these countries in our 2018 report replaced respondents from Australia, Brazil and Mexico in last year's report. We will take care to note when changes in this year's data appear to be due primarily to changes in the sample. It's also worth noting that response data from 800 respondents in four countries – U.S., Germany, UK and Japan – have been included in each of our two prior reports.

As we did with prior reports, the 2018 version retains most of the base questions from the previous year, but adds several new questions around the new technologies that firms are adopting to drive their digital transformation. Specifically, this year we added five new questions addressing the prevalence of multi-cloud adoption, securing Big Data environments, the security impact of machine learning and AI, mobile payments and blockchain. We also combined two questions regarding external and internal threats in order to get a sense of the relative importance of each, rather than treating them as separate threats. In sum, we have attempted to maintain comparative consistency from year to year, while at the same time permitting the report to evolve, reflecting changes in the threat landscape as well as emerging technologies and the new vulnerabilities and attack vectors they may introduce, along with new techniques to secure them.

We have also incorporated analysis of the emerging technologies used for digital transformation – previously a separate stand-alone report – within the narrative of the overall global report. As will be discussed in more detail later in the report, organizations continue to deal with the security ramifications of emerging technologies that now are firmly rooted within most organizations' overall IT strategy.

"This year we added five new questions addressing multi-cloud adoption, securing Big Data, and the security impacts of machine learning and AI, mobile payments and blockchain."

"A bright spot in the cloud-enabling technology area, 451 Research predicts that containers will have a compounded annual growth rate of 40%, reaching $2.7 billion by 2020."

These include:

- **Big Data**, which continues to flood and even overwhelm organizations struggling to figure out how to leverage Big Data – 99% of respondents plan to use Big Data this year – while also keeping it secure.

- **The Internet of Things (IoT)** which, as we saw last year, has become a prime target of hackers as well as a jumping off point for launching large-scale attacks such as the Mirai botnet attacks. Data from 451 Research found that nearly three quarters (71%) of enterprises are already gathering data for IoT initiatives, while security remains a major concern and impediment to IoT deployments.

- **SaaS** which continues to spawn concerns over sensitive data stored outside the firewalls of the organization and is the 'new' technology most likely to house sensitive data (45% globally).

- **Containers**, which continue their impressive growth and acceptance by development staff despite nascent efforts to secure containers and the sensitive data within them – nearly one-quarter (24%) are using containers in production environments. A bright spot in the cloud-enabling technology area, 451 Research predicts that containers will have a compounded annual growth rate of 40%, reaching $2.7 billion by 2020.

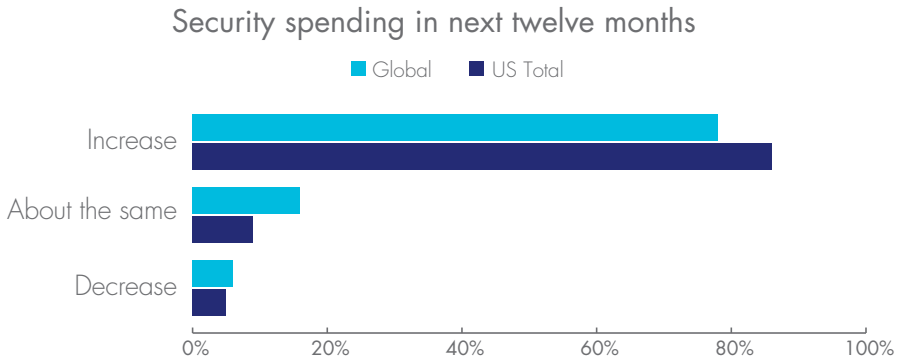
- **Blockchain**, which is becoming more widely used for commercial transactions outside the highly established payment settlement systems. 451 Research believes blockchain, which drives the execution and integrity of digital currency, can potentially disrupt virtually all business models and industries globally, as well as security markets such as Public Key Infrastructure (PKI), information rights management and identity management.

"Data from 451 Research found that nearly three quarters (71%) of enterprises are already gathering data for IoT initiatives, while security remains a major concern and impediment to IoT deployments."

EXECUTIVE SUMMARY

As with past reports, this year's *Thales Global Data Threat Report* showcases a mix of good and bad news. From the glass-half-full perspective, most respondents plan to increase their spending on security, for the fourth consecutive year: 78% of the 1,200 organizations polled plan in increasing IT security spending in 2018, including nearly 86% of U.S. organizations, up from 73% globally, in 2017.

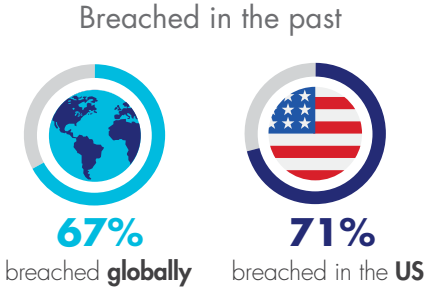
"78% of the 1,200 organizations polled plan in increasing IT security spending in 2018, including nearly 86% of U.S. organizations, up from 73% globally, in 2017."

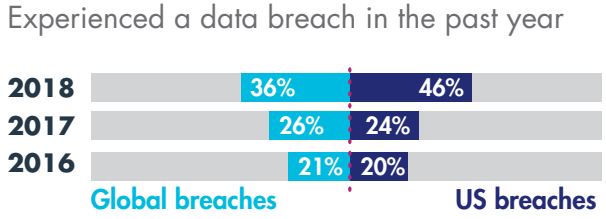


In past reports, compliance has been the primary driver for setting security spending priorities. That changed this year, with the fear of financial penalties from data breaches taking over the top spot, again possibly reflecting the growing number of costly, high profile attacks.

The bad news is that rates of successful breaches have reached an all-time high for both mid-sized and enterprise class organizations, with more than two-thirds (67%) of global organizations and nearly three fourths (71%) in the U.S. having been breached at some point in the past. Further, nearly half (46%) of U.S. respondents reported a breach just in the previous 12 months, nearly double the 24% response from last year, while over one-third (36%) of global respondents suffered a similar fate. In addition to the massive Equifax breach that exposed personal information of 143 million individuals, other noted breaches last year included the education platform Edmodo (77 million records hacked); Verizon (14 million subscribers possibly hacked); and America's JobLink (nearly 5 million records compromised).

"In addition to the massive Equifax breach that exposed personal information of 143 million individuals, other noted breaches last year included the education platform Edmodo (77 million records hacked); Verizon (14 million subscribers possibly hacked); and America's JobLink (nearly 5 million records compromised)."





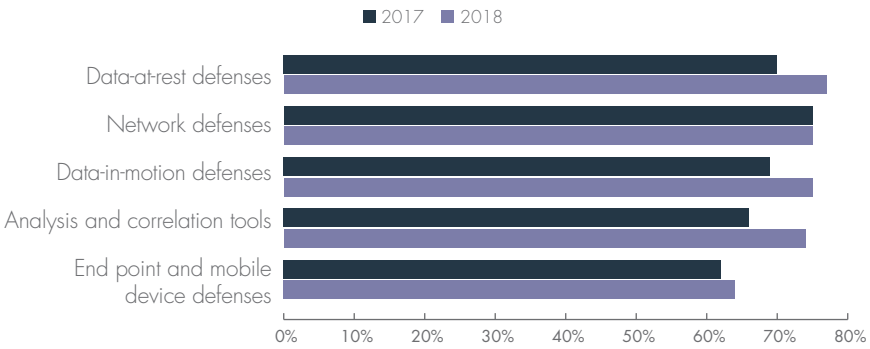
To the least effective go the spoils

As we compare this year's data to that from past surveys, while the numbers may change, the storylines remain essentially the same. We are spending more on security, more respondents view compliance as very effective at preventing data breaches, yet the number of breaches continues to rise.

One notable – and encouraging – change in this year's data was that the perceived effectiveness of securing data at rest (77% globally) surpassed network security (75%) for the first time. At the same time, endpoint security ranked dead last in terms of effectiveness once again, yet has the *highest* planned spending both globally (57%) and in the U.S. (65%) – a stunning disconnect. Conversely, plans for spending on securing data at rest is at the bottom of this list globally (40%) and in the U.S. (44%). In other words, the spending outlook is brightest for tools that we have identified as least effective, and vice-versa. Clearly, more work needs to be done to better align perceptions of effectiveness with the resources committed to support our goals.

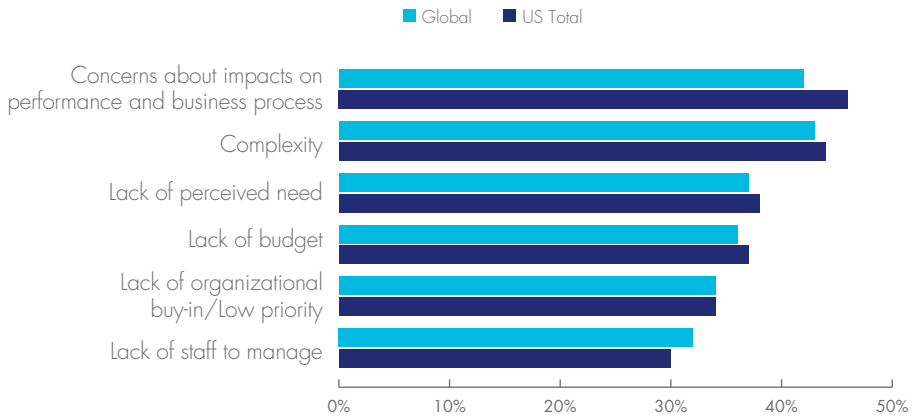
"One notable – and encouraging – change in this year's data was that the perceived effectiveness of securing data at rest (77% globally) surpassed network security (75%) for the first time."

Global increases in IT security spending by technology area



Yet, implemented improperly, data security can be fraught with complexity, and the popularity of hybrid, distributed systems and mobility have certainly contributed to the challenges of deploying data security more broadly. Thus, it is not wholly surprising that complexity –or at least the perception that data security is complex – remains the top barrier to data security in this year's report (43% globally, 44% U.S.), though concerns about performance and business process impact (42% globally, 46% U.S.) have closed the gap considerably from last year.

Perceived reasons that data security is not deployed

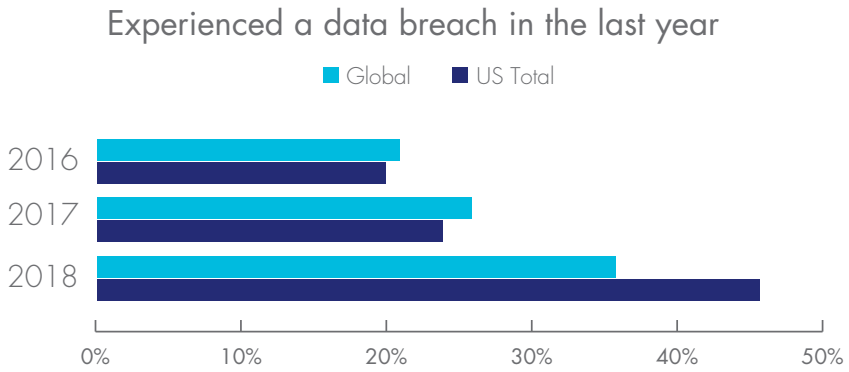


KEY FINDINGS:

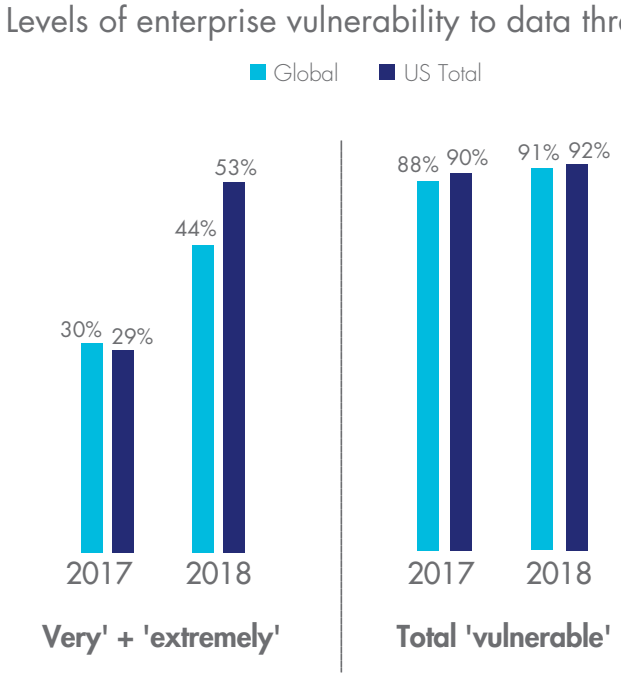
- For the fourth consecutive year, spending on IT security continues its much-needed upward trajectory, with 78% of global organizations planning on upping spending in the year ahead, compared with 73% in 2017. The U.S. is even more aggressive with 86% of firms planning increases.

- On the downside, security breaches are up – and sharply so. More than a third (36%) of global firms were breached last year, up considerably from 26% in 2017 and 20% in 2016. The U.S. was even more dire, with 46% of U.S. firms polled reporting being breached last year having nearly doubled – from 24% last year. More than two-thirds (67%) of global organizations and 71% in the U.S. have experienced a breach at some point.

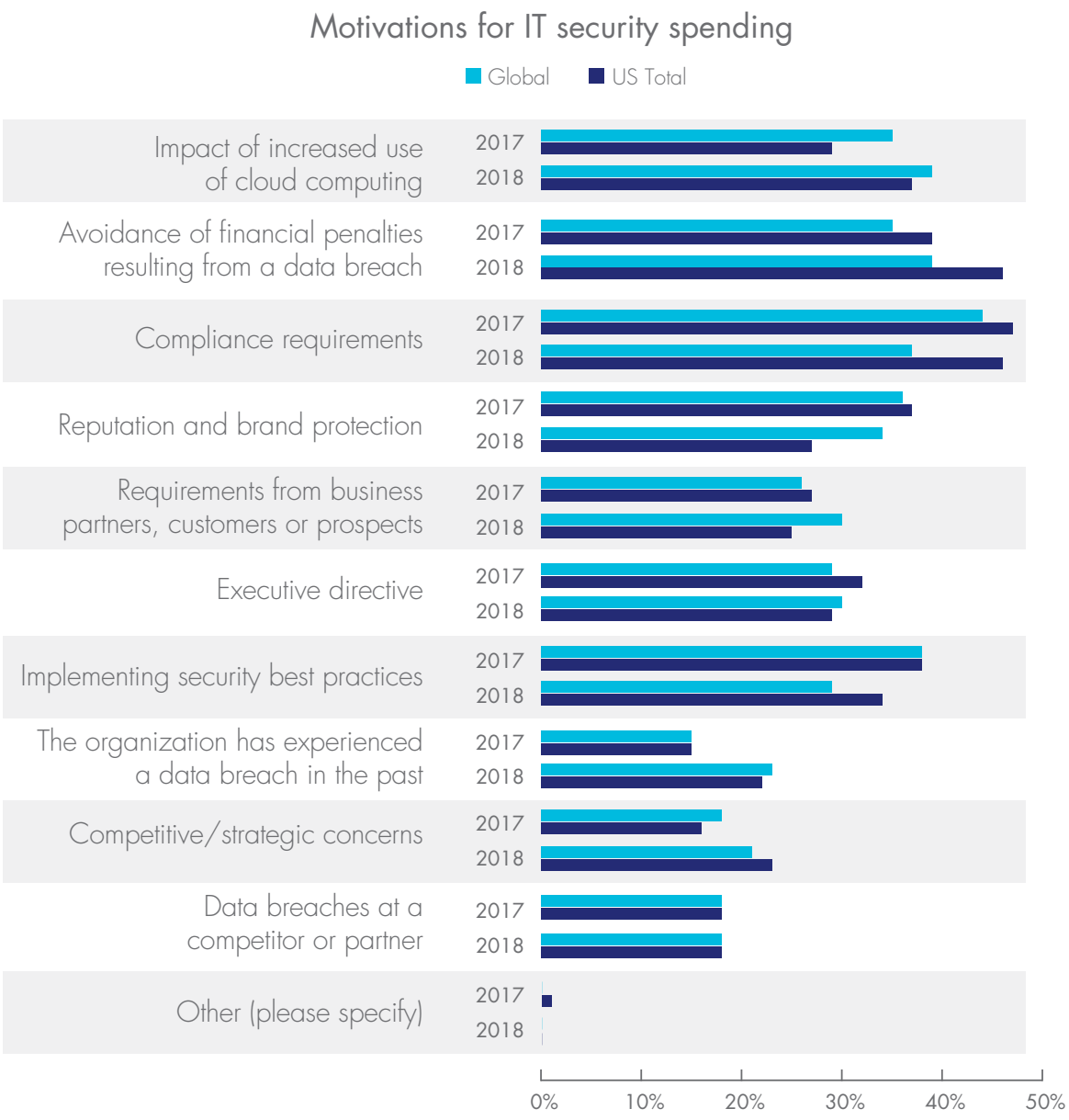
"Being 'very' or 'extremely' vulnerable to security threats are soaring, reaching 44% globally and 53% in the U.S., compared with 30% globally and 29% in the U.S. just one year ago."



- It is no surprise that feelings of being 'very' or 'extremely' vulnerable to security threats are soaring, reaching 44% globally and 53% in the U.S., compared with 30% globally and 29% in the U.S. just one year ago.

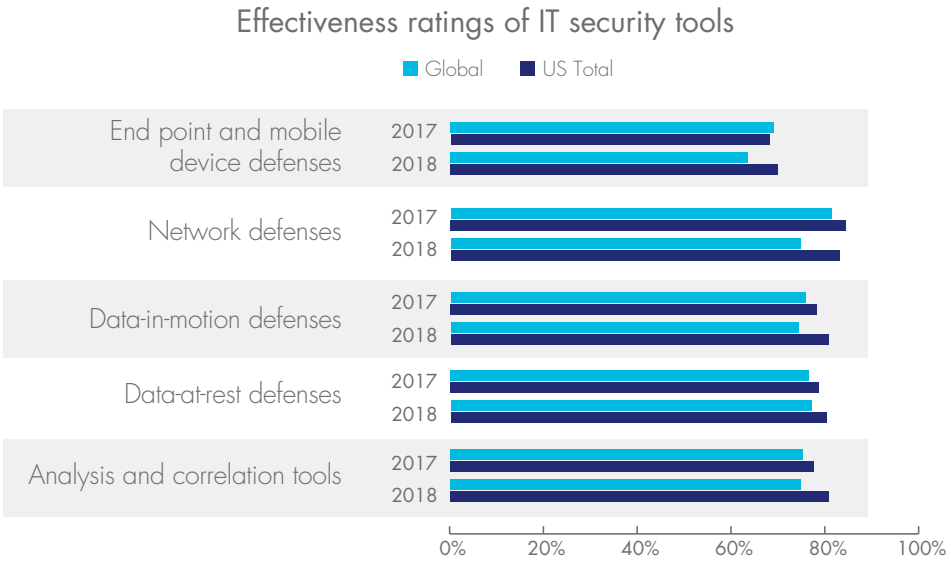


- For the first time, respondents listed avoidance of financial penalties from data breaches (39% vs. 35% last year) along with increased use of cloud (also at 39% globally) as the top stimuli for IT security spending, edging out the former perennial top choice, compliance (37% global, 38% U.S.).



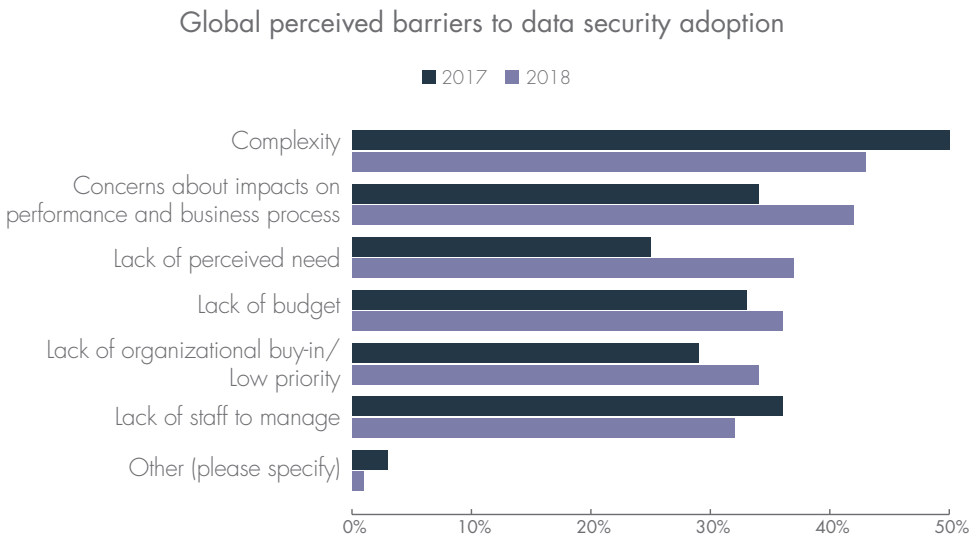
- Yet, more respondents this year feel compliance requirements are 'very' or 'extremely' effective compared with last year (59%), perhaps due to new or updated compliance regulations such as GDPR and PSD2. To illustrate, more global respondents expect to feel the impact of GDPR this year (87%) compared with last (72%).

- The effectiveness of securing data at rest (77% global) for the first time surpassed network security, while endpoint security (64%) was dead last. Yet, endpoint security paradoxically has the highest response rates for planned security spending increases (57% global, 65% U.S.), while data-at-rest ranked dead last for spending increases globally (40%) and in the U.S. (44%).



"The low spending plans for data-at-rest security may be blamed once again on perceptions of complexity, which was once again the top barrier to adopting data security globally (43%) with concerns over performance a close second (42%)."

- The low spending plans for data-at-rest security may be blamed once again on perceptions of complexity, which was once again the top barrier to adopting data security globally (43%) with concerns over performance a close second (42%).

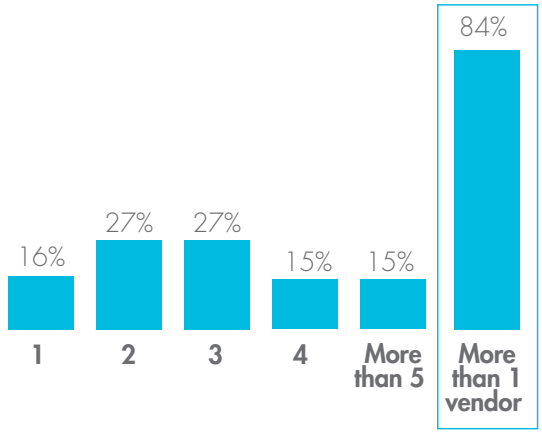


"Encryption remains the technology of choice for ensuring compliance and privacy, with twice as many respondents choosing encryption over the number two choice, tokenization."

- Encryption remains the technology of choice for ensuring compliance and privacy, with twice as many respondents choosing encryption over the number two choice, tokenization. For security in general however, tokenization ranked first in terms of planned deployments, with encryption with bring your own key (BYOK) second and application layer encryption third. Encryption with BYOK is the top choice for securing data in public cloud environments, with encryption with keys held by providers in second place.

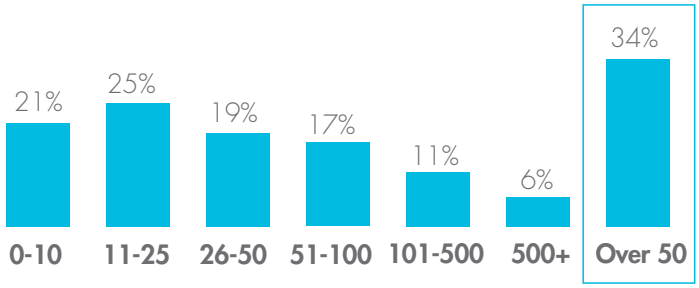
- The vast majority of organizations are opting for a multi-cloud strategy as part of their digital transformation strategies, with 84% globally choosing more than one IaaS vendor and 34% using more than 50 SaaS applications. While cloud providers are increasingly providing their own security features, organizations will need to fill in the blanks themselves and also ensure interoperability amongst their various cloud providers.

Number of **IaaS** vendors used globally this year



"Organizations are opting for a multi-cloud strategy as part of their digital transformation strategies, with 84% globally choosing more than one IaaS vendor and 34% using more than 50 SaaS applications."

Number of **SaaS** vendors used globally this year



- Advanced analytics are a double-edged sword. While two thirds (64%) of global respondents believe AI techniques can increase awareness and detection of attacks before they occur, 43% also see increased breaches owing to AI-based hacking tools.

"63% of survey respondents in 2017 said their organizations were deploying one of more of these nascent technologies (cloud, big data, IoT, mobile and blockchain) ahead of their organization's ability to properly secure them."

BODY OF REPORT

Contradictions, conundrums and enigmas

A key finding in last year's report unearthed a glaring disconnect between organizations' eagerness to deploy emerging technologies that can enable digital transformation, on one hand (Big Data, IoT, and Containers to name just three), and the ability to secure the data stored in them on the other. Nearly two-thirds (63%) of survey respondents in 2017 said their organizations were deploying one or more of these nascent technologies ahead of their organization's ability to properly secure them.

"Organizations are ramping up IT security spending on the same things that, paradoxically, they also deem least effective towards securing data, while investing less in those they deem most effective."

The security spending paradox

Another notable disconnect that appears to have intensified in this year's report is that organizations are ramping up IT security spending on the same things that – paradoxically – they also deem least effective towards securing data, while at the same time investing less in security approaches they deem most effective.

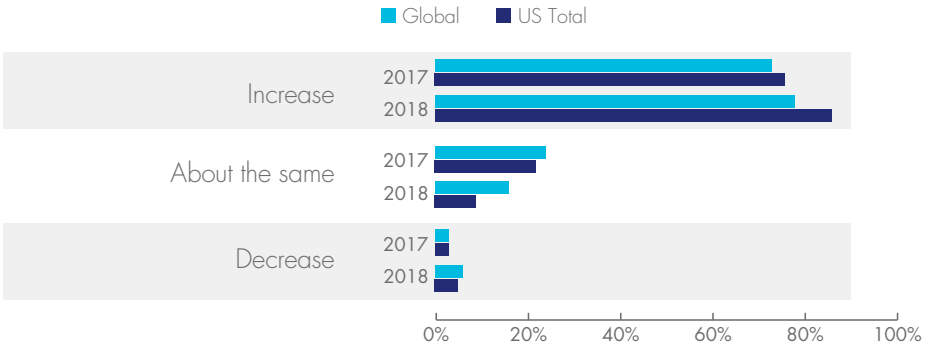
Spending up significantly, but…

Looking first at spending, the good news continues in terms of organizations' willingness to commit money to security. More than three-quarters of respondents plan to increase their spending this year on security (78% of global organizations), up from 73% last year. A large part of the delta was a big jump in respondents expecting their spending to be 'much higher', up from 23% to 34% globally. Most regions posted increases, and for the U.S. specifically, spending plans are even stronger, with 86% planning to increase security spending, up from 76% in 2017). Only in Japan did year-to-year security spending remain unchanged, while in Germany spending actually declined slightly.

"More than three-quarters (78%) of global respondents plan to increase their security spending this year, up from 73% last year. Over one-third (34%) expect spending to be 'much higher'."

In the U.S. Federal market, 93% plan to increase security spending and a full 73% of respondents said their departments would spend 'much higher' on security this year; nearly double the increases posted in any other vertical or country surveyed. In Japan by contrast, while 54% plan to increase security spending (the lowest of any region), only 9% of respondents reported 'much higher' spending intentions, and just 12% in Korea'. Clearly the message of investing more heavily to protect sensitive data is resonating.

Percentages of organizations planning increases in IT security spending



What is driving these spending plans? Organizations are clearly growing more concerned about the potential impact of data breaches and attacks on their bottom lines: 'avoidance of financial penalties' (39%) gained the top spot in terms of reasons for IT security spending, sharing the top spot with 'securing cloud computing' at 39%, edging out the number one spending motivator in past surveys (compliance, 37%). Still, looming data privacy regulations such as GDPR and PSD2 in Europe and ongoing changes to Japan's APPI should ensure compliance remains a significant motivator for security spending.

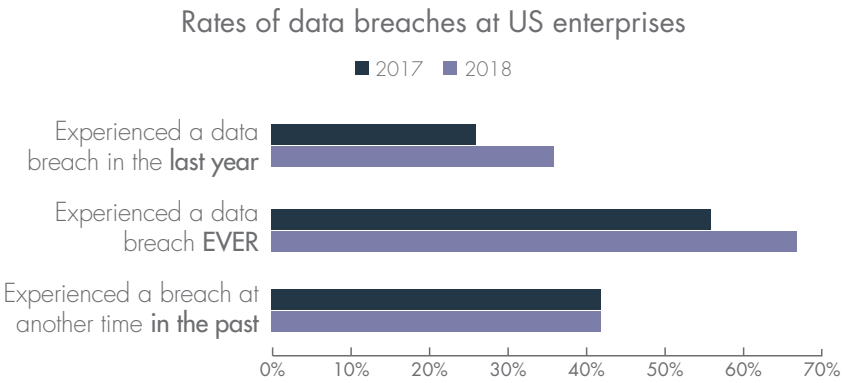
"More than a third of global respondents (36%) saying their organizations suffered a breach within the last year alone, compared with just 26% last year."

...So are data breaches

In past surveys, organizations with substantial projected increases in security spending were no doubt hoping for a corresponding positive impact on data breaches. However, not only did reported breaches not decline, but they rose substantially, with more than a third of global respondents (36%) saying their organizations suffered a breach within the last year alone, compared with just 26% last year – a nearly 40% YoY increase. The comparable figures for the U.S. were even worse – nearly half (46%) were breached in the past year, and at the top of the list is U.S. Federal with 57%, which may partly explain the substantial planned security spending increases noted above.

In terms of geographies, India topped all countries in this dubious category with 56% reporting a breach in the past year, while notable outliers include Japan (9%), Korea (16%) and the Netherlands (27%). Overall, a full 67% of global organizations now report they have suffered a breach at some time in the past, compared with 56% last year. Clearly much remains to be done to better direct security spending increases to those defenses that are the most effective at securing sensitive data.

"Nearly half (46%) were breached in the past year, and at the top of the list is U.S. Federal with 57%, which may partly explain the substantial planned security spending increases."



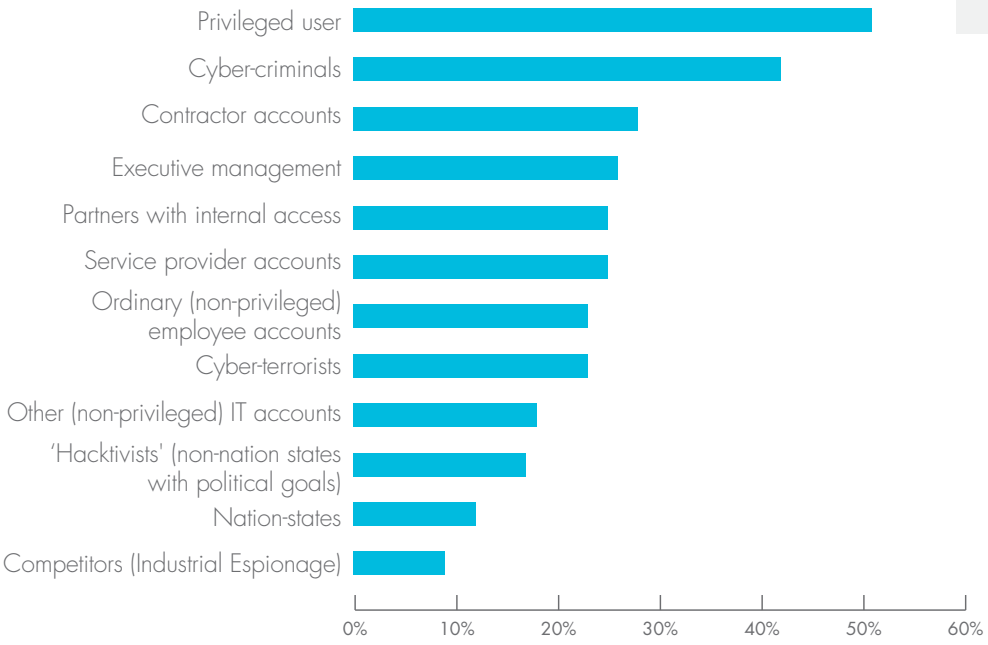
Who are the risky threat actors?

In past reports, we have analyzed the separate threats posed by both external and internal threats separately, in part due to the existence of distinct tools for combatting them. However, for this year we decided to combine them, in large due to the line between insider and external threats blurring, and also since security practitioners are forced to deal with both types of threats on a daily basis.

Thus, while cybercriminals (the top threat among external threat actors in last year's report at 44%) and privileged users (last year's greatest insider threat at 58%) remained the top two concerns, this year's results imply a greater concern for insider attacks than external threats. Privileged users (51%) were the top threat by a wide margin, substantially ahead of cybercriminals at 42%, though we should note that privileged accounts are also a top target for external attackers, as they provide the proverbial 'keys to the kingdom' and allow unfettered access to sensitive resources unless other security measures are in place. It's also worth pointing out that contractors (28%) came in a distant third, illustrating increased concern regarding the risks posed by third-parties.

"Privileged insiders (51%) were the top threat by a wide margin, substantially ahead of cybercriminals at 42%. It's also worth pointing out that contractors (28%) came in a distant third, illustrating increased concern regarding the risks posed by third-parties."

Global ratings for most dangerous threat actors this year



Specifically, the other two 'third-party' choices such as partners with internal access (25%), service provider accounts (25%) came in ahead of nation states (12%) which was second-last, despite screaming headlines regarding cyber threats from North Korea, Russia, China and others. Industrial espionage was also dead last at 9%, suggesting that most organizations have little concern regarding trade secrets or intellectual property being misappropriated by their competitors.

Compliance and security – two sides of the same coin, or distant cousins?

The debate between compliance and security has simmered for years, but more recently the chorus of detractors arguing that compliance alone is not sufficient seems to have grown louder. Yet, when it comes to perceptions of what is most effective at securing sensitive data, nearly two-thirds (64%) of global respondents and three quarters (74%) of U.S. respondents feel that adhering to compliance requirements are either 'very' or 'extremely' effective. Both these figures represent substantial increases over last year's report, when 59% of global respondents and 60% in the U.S. felt similarly.

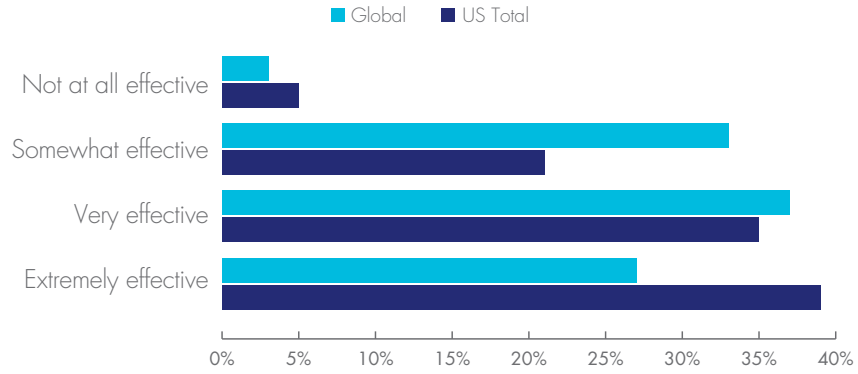
To some extent, such disagreements may stem from a failure to recognize that compliance is typically designed to protect specific data sets. For example with Payment Card Industry Data Security Standard (PCI-DSS), it's possible to be both compliant by protecting credit card data, while simultaneously leaving other sensitive data unprotected without further security measures.

But one critical shortcoming of most compliance mandates is that they change infrequently, while threats evolve constantly, often by the hour or even minute. With threats changing so rapidly, it is nearly impossible to draft regulations that won't quickly become obsolete. The alternative, and more common action is to draft guidelines that are necessarily vague, to the point of leaving practitioners guessing about what actions they need to take to meet the intended standards.

The positive change was driven by the U.S., as noted, and also Germany, which rose to 64% 'very' plus 'extremely' effective from 57% a year earlier. India (85%) and Sweden (68%), both surveyed for the first time in this year's report, also posted numbers in excess of the global average. U.S. Retail led all vertical categories (83%), possibly owing to the strict constructs of various regulations safeguarding credit card usage such as the Payment Card Industry Data Security Standard PCI-DSS). By contrast, faith in compliance seems to be much lower in both Japan (36%) and in Korea (38%).

"Nearly two-thirds (64%) of global respondents and three quarters (74%) of U.S. respondents feel that adhering to compliance requirements are either 'very' or 'extremely' effective."

Ratings for effectiveness of compliance for combating data threats in 2018



Yet, when we look at the main drivers for spending on security, avoidance of financial penalties from breaches moved into top spot for both global (39%, tied with impact of cloud computing), and US (46%), not terribly surprising given rising breach counts. And though confidence in the effectiveness of compliance is growing, as a spending driver, compliance fell globally to third place (37%, down from 44%) and slightly in the U.S. (46%, down from 47%).

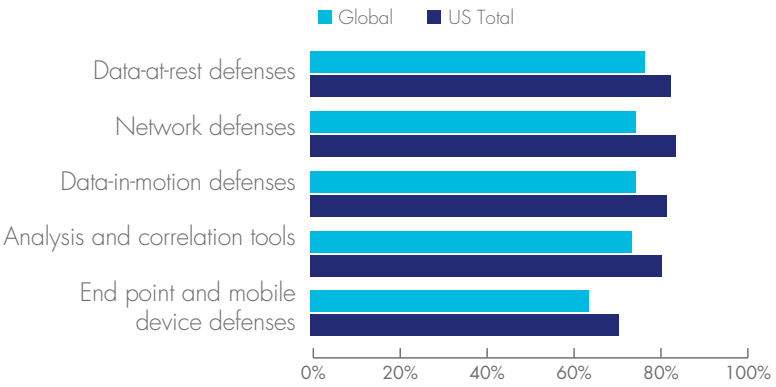
Somewhat surprisingly, implementing best practices plummeted in terms of its perceived effectiveness in protecting sensitive data, falling to the number 6 spot this year from number 2 globally last year. One explanation could be that organizations increasingly find themselves scrambling to avoid fines and penalties as new compliance mandates look, as discussed elsewhere in this report.

Protecting data-at-rest gets its due – sort of

For the first time since we have produced this report, data-at-rest defenses (encryption, tokenization, etc.) was selected as the top defense globally (77%), just ahead of network security and data-in-motion defenses (both at 75%). In the U.S., however, network defenses (84%) maintain a slight edge over data-at-rest (83%) and data-in-motion defenses (82%). By contrast endpoint security continues to decline in terms of perceived effectiveness, being ranked dead last among all defenses both globally (64%) and in the U.S. (71%) – Japan is a notable outlier, with just 39% citing endpoint security as effective at preventing data breaches.

"For the first time since we have produced this report, data-at-rest defenses (encryption, tokenization, etc.) was selected as the top defense globally (77%), just ahead of network security and data-in-motion defenses (both at 75%)."

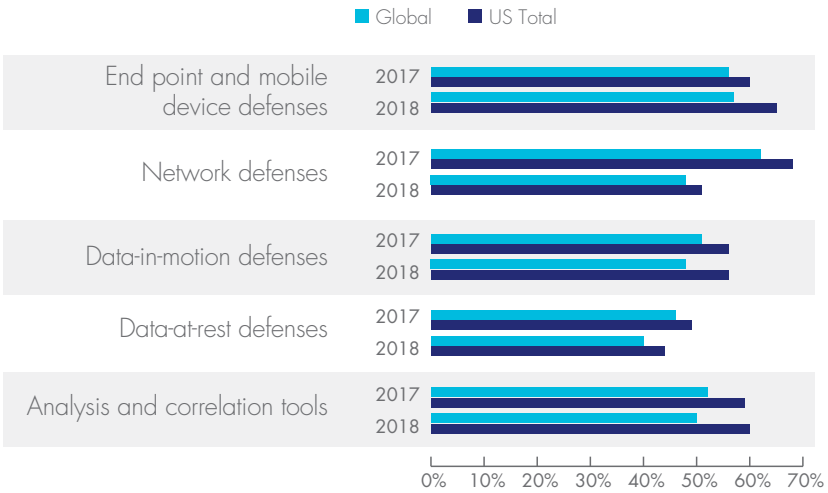
Most effective defenses for protecting data this year



However, herein lies a major disconnect between perceptions of what is most effective at protecting data and preventing breaches and where organizations are actually directing actual spending to bolster IT security. While data-at-rest, was ranked number one globally in terms of effectiveness, it was ranked dead last in terms of planned spending increases (just 40% globally and 44% in the U.S.). In sharp contrast, the biggest planned increases are targeting endpoint security (global 57%, U.S. 65%, up from 60% last year) – the same category deemed least effective in protecting sensitive data. U.S. Retail (72%) and India (81%) are among the highest responses for planned spending on endpoint security.

"While data-at-rest, was ranked number one globally in terms of effectiveness, it was ranked dead last in terms of planned spending increases (just 40% globally and 44% in the U.S.). In sharp contrast, the biggest planned increases are targeting endpoint security (global 57%, U.S. 65%, up from 60% last year) – the same category deemed least effective in protecting sensitive data."

Plans for increases in IT security spending by technology type



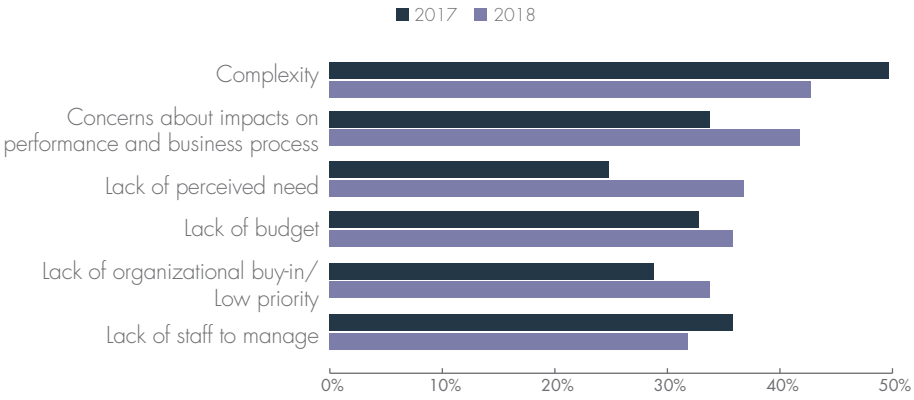
BARRIERS TO SECURITY

This disconnect between planned spending increases and perceptions of what defenses are most effective can be difficult to explain. Part of it could be due to the fact old spending habits die hard. A more likely explanation is that adding more endpoint security is easier from a deployment perspective. And a large part of it could be due to the perceived complexity of data security – not surprising complexity remains at the top of the list of barriers to adopting data security (43% globally).

If there is a silver lining, it's that complexity declined as an adoption barrier, from 50% a year ago, and also that complexity barely edged out other adoption barriers such as concerns about performance impacts, which surged to 42% globally from 34% last year. Moreover, performance concerns topped the list in the U.S. at 44%, with complexity a close second at 42% – a first for our survey. Lack of budget was the top hurdle for adopting data security for both the U.S. (53%) and Global federal (52%) sectors and Korea (56%). Notably, lack of staff dropped from 36% last year to 32% and into fifth place, despite increasing industry awareness of chronic shortages of skilled cybersecurity talent.

"Perceptions of complexity remain the top barrier to broader data security adoption, though performance impacts have narrowed the gap. Lack of budget looms large in both U.S. and Global federal sectors, as well as Korea."

Global perceived barriers to data security deployment

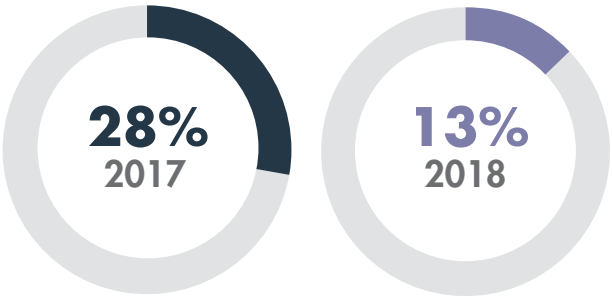


Encryption as antidote for proliferating data sovereignty mandates

The imminent arrival of privacy mandates around the globe (such as GDPR in May 2018) appear to be having a large impact on most organizations' thinking about security – only 13% of global respondents say they will not be impacted by privacy regulations – a steep drop from 28% last year. Among those nations sensing they will be most greatly impacted are Korea (1% will not be impacted), Netherlands (8%); and Sweden (11%).

"The imminent arrival of privacy mandates around the globe (such as GDPR in May 2018) appear to be having a large impact on most organizations' thinking about security – only 13% of global respondents say they will not be impacted by privacy regulations – a steep drop from 28% last year."

Global impact of data privacy and sovereignty laws

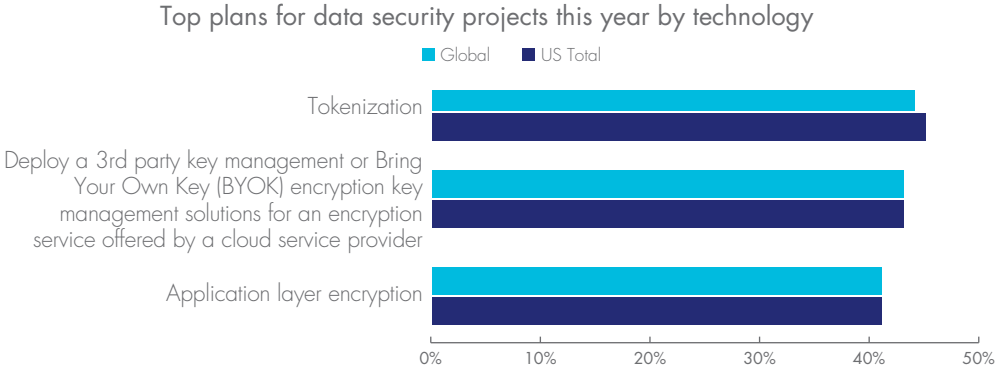


Our organization will not be impacted by any local, national or regional data privacy/sovereignty regulations

And how do most organizations plan to deal with these mandates? For 42% of global respondents, encryption remains the tool of choice, more than double the amount that chose the second-best option, tokenization (20%). Both Sweden (59%) and Korea (53%) lead the encryption charge, while U.S. Federal somewhat surprisingly lags all other countries and verticals at 24%. Only one country (or vertical for that matter), the Netherlands, preferred tokenization (32%) to encryption (29%).

Encryption and tokenization top the list of data security projects

Encryption – and also tokenization – rank at or near the top of respondents' lists for those who are looking to implement data security, including for many emerging technology environments that are driving digital transformation. When asked which encryption and data security tools are in plan for next year, respondents ranked tokenization as the top tool (44% globally, 45% U.S.) – up from third place globally a year ago, barely edging out encryption with BYOK (43% globally and in U.S.) and application layer encryption (41% globally and in the U.S.) and hardware security modules (41% global, 42% U.S.).



For securing public cloud, encryption topped the global tools list at 44% compared with 47% in the U.S. For securing IoT environments, encryption/tokenization top the list (48% global, 47% U.S.). For Big Data environments, however, encryption falls to third place at 35% both globally and in the U.S., trailing strong authentication (38% globally) and monitoring and reporting (36%).

STRATEGIES FOR A MULTI-CLOUD WORLD

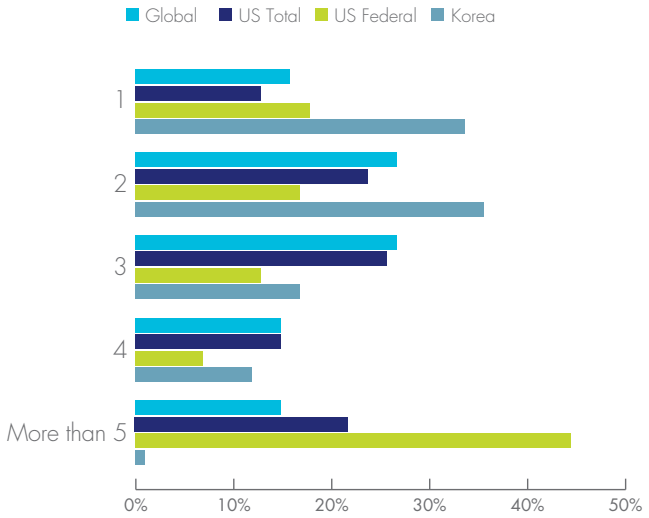
Several of the new questions we included to this year's report revolve around adoption of cloud resources, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Part of the motivation was to see to what extent firms were using single-source providers, or instead were adopting multiple cloud providers and applications. From a security perspective, cloud usage patterns have implications for how organizations deploy security in the cloud, and whether they rely primarily on services from cloud providers themselves, from independent third-party security vendors, or a combination of both.

Overall, we found strong evidence of multi-cloud adoption across all three flavors of public cloud. For SaaS and PaaS, this was perhaps less surprising, since organizations have been using SaaS apps for over ten years, and it's become fairly common knowledge in security circles that most organizations are using a wide range of SaaS apps.

For IaaS, however, we were somewhat surprised at the strength of the evidence in favor of using multiple clouds. Despite the continued dominance of cloud behemoths like AWS, only 16% of global respondents are single-sourcing IaaS from one cloud provider; more than half of (54%) are using two or three IaaS providers; and 57% use three or more. In the U.S., nearly two-thirds (63%) use three or more IaaS providers, while at the low end of the spectrum, in Korea only 30% of respondents report using three or more IaaS providers.

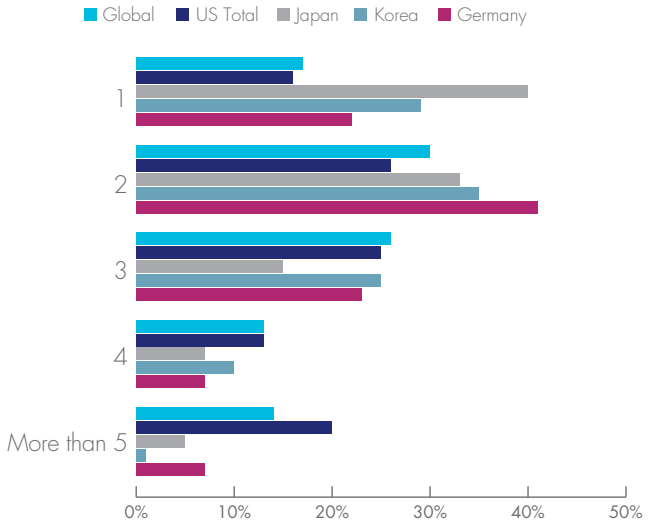
"Only 16% of global respondents are single-sourcing IaaS from one cloud provider."

IaaS: Rates of multiple cloud usage by enterprises this year



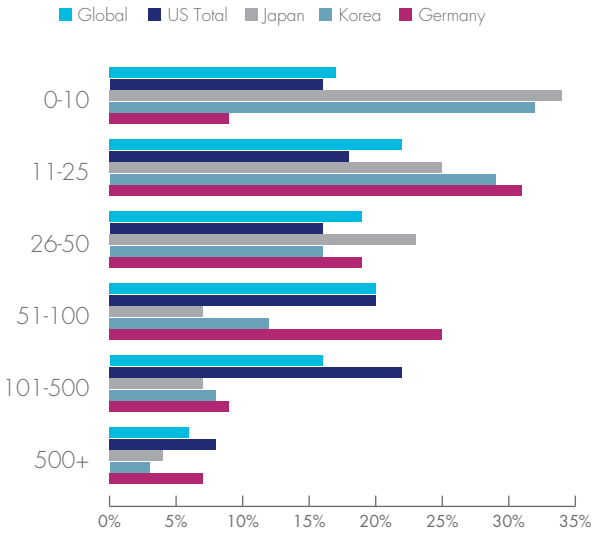
Similarly, with PaaS users, just 17% globally use only one provider, while 56% report using 2 or 3. At the low end, in Japan only 27% are using three or more PaaS providers; Korea 36%; and Germany 37%.

PaaS: Rates of multiple cloud usage by enterprises this year



Not surprisingly, SaaS applications usage rates are much higher, with 42% of global respondents using 50 or more SaaS applications; 22% more than 100; and 6% more than 500. By comparison, in Japan only 18% of respondents report using 50 or more SaaS applications, and 23% in Korea. In practice, however, given the well-known 'Shadow IT' issue, it is highly likely that most organizations are using many more SaaS apps than security offers or senior management are aware of. Cloud security vendors with the ability to discover unsanctioned SaaS applications routinely find that larger enterprises typically have in the vicinity of 800 or more SaaS apps running in their environment.

SaaS: Rates of multiple cloud usage by enterprises this year



The security implications of the above are fairly straightforward. For one, the proliferation of cloud environments and applications increases the potential for putting sensitive data at risk. To illustrate, 45% of global respondents and 49% in the U.S. say they are storing sensitive data in SaaS environments (though that figure fell from last year's 55%), 41% in IaaS and 39% in PaaS.

Further, with so many SaaS providers to account for in so many organizations, ensuring data protection in SaaS environments is a complex task that in one sense could put digital transformation efforts at risk. While many cloud providers are increasingly offering their own security features, organizations still need to somehow manage those features across multiple cloud environments, and also provide security for those SaaS applications that do not provide their own security functionality.

New security challenges from emerging technologies

By their very nature, 'modern' technologies like Big Data, IoT and cloud mean accessing, processing and storing often outside the traditional enterprise security perimeter. Thus today, the traditional concepts of 'trusted' and 'untrusted' environments are disappearing altogether, due to new technologies but also the rise of the modern extended enterprise that relies increasingly on 'outsiders' such as contract workers, consultants, outsourced service providers, suppliers and other third-party vendors.

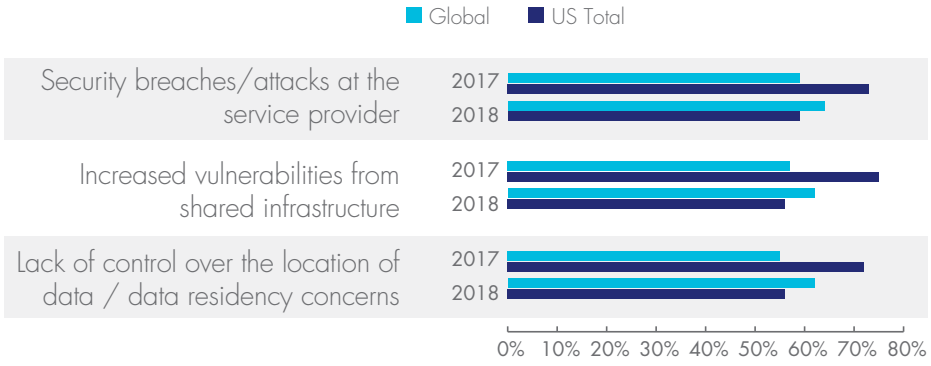
As noted earlier, one of the biggest security challenges modern technologies present is that most of them are prime locations for storing sensitive data, and in many cases before adequate steps are taking to secure them. For example, 45% of global respondents are already storing sensitive data in SaaS applications (49% in U.S.) and Big Data environments (46% U.S.).

So what are the main concerns that these 'digitally transformative' technologies pose for security practitioners? For the cloud specifically, the top concerns are similar to those listed a year ago, led by attacks and breaches at the service providers (64% global and 73% U.S.,) both of which are up considerably from last year (59% global), particularly for the U.S. (50% last year). Although plausible arguments can be made that most cloud providers are more secure than the average enterprise, publicized breaches at service providers such as Verizon and OneLogin have likely dented the confidence in the security of cloud providers, and certainly highlighted the catastrophic consequences that can follow.

Second on the list of cloud security concerns are once again vulnerabilities from shared infrastructure (62% global, 75% U.S., again up smartly from 57% global and 56% U.S. last year). Data residency/data sovereignty concerns rounded out the top three (57% global, 56% U.S., up from 51% global and 50% U.S. last year).

"More respondents were concerned about attacks and breaches at cloud service providers (64% global, up from 59%), particularly in the U.S. (73% vs. 50% last year. Although plausible arguments can be made that most cloud providers are more secure than the average enterprise, publicized breaches at service providers such as Verizon and OneLogin have likely undermined confidence."

Top perceived cloud environment vulnerabilities

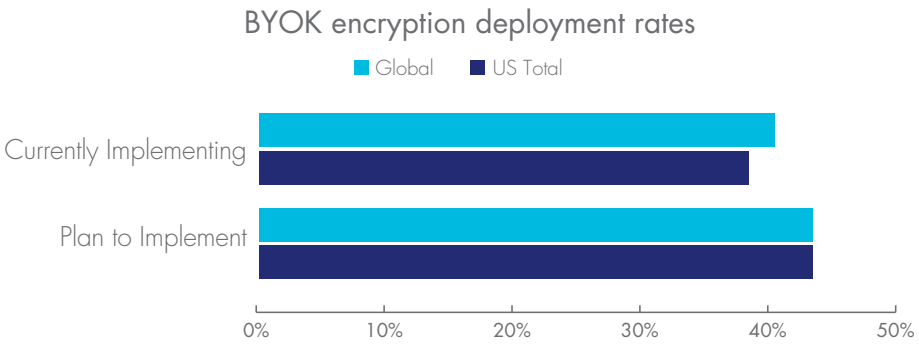


Encryption with key management an essential cloud security control

Given growing concerns about the security of cloud providers. Encryption in general remains the top means of securing data in the cloud. Encryption can be highly effective in protecting sensitive data in the cloud in the event of a breach, can also help meet new data sovereignty requirements, and with customer managed keys or BYOK, can also help guard against attacks by rogue admins. Not surprisingly, encryption with options for local key control or BYOK once again the top choice (44% global, 47% U.S.), ahead of encryption with key control resting with the service provider (41% global).

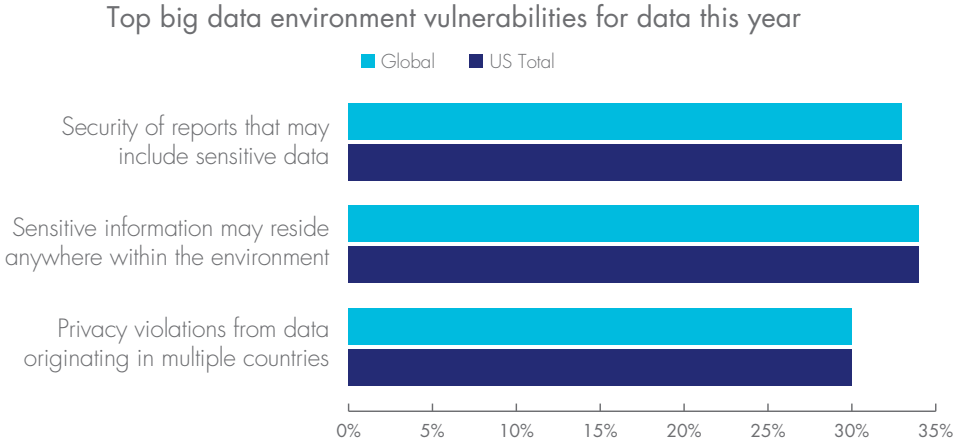
Already today 40% of global respondents and 38% in the U.S. have implemented BYOK, and another 43% in both segments will do so this year, bringing the totals to over 80%. However, only 51% of global respondents are implementing encryption in the cloud today, while as many as 12% have no plans to use encryption in the cloud.

"Already today 40% of global respondents and 38% in the U.S. have implemented BYOK, and another 43% in both segments will do so this year, bringing the totals to over 80%."



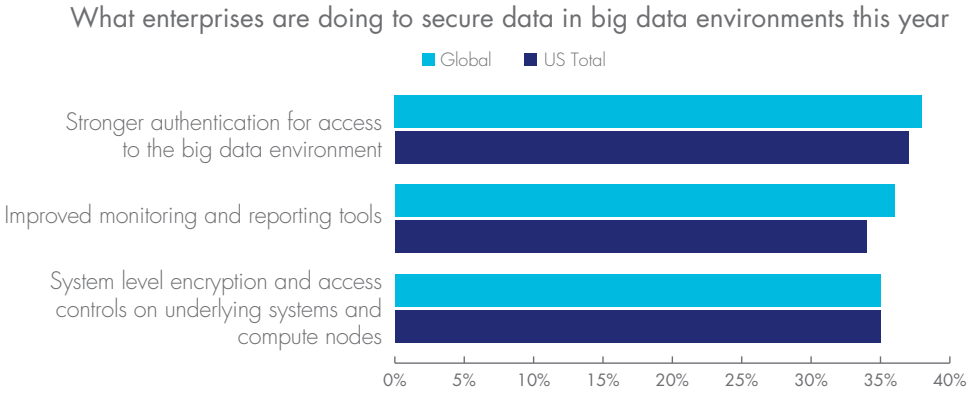
BIG DATA, BIG QUESTIONS

Despite its many advantages, Big Data presents its own security challenges, what are often referred to as the 'Three 'V's: Volume, Variety and Velocity'. In short, compared to traditional relational databases, the data generated and stored within Big Data environments can be orders of magnitude larger, less homogeneous, and perhaps most importantly, change rapidly. Thus, the top Big Data security issue is that sensitive data can be anywhere – and therefore everywhere – a concern expressed by 34% of global and U.S. respondents. A related concern is that Big Data-generated reports could contain sensitive data (33% global and U.S.), while concerns over privacy regulations at 30% global round out the list of top issues.



"The top Big Data security concern is that sensitive data can be anywhere – and everywhere – expressed by 34% of global and U.S. respondents. The top choices to secure Big Data were stronger authentication and access controls, monitoring and encryption."

We asked a new question this year to gain insight into what organizations are doing to combat these potential trouble spots, and the top answers were stronger authentication and access controls (38% global, 37% in the U.S.), improved monitoring and reporting tools (36% global, 34% U.S.) and encryption and access controls for underlying platforms (35% global and U.S.). We also noted a fairly strong regional bias in the responses: stronger authentication was preferred in the UK (45%) and the Netherlands (44%), improved monitoring in India and Korea (45% each) and Germany (43%), while the highest responses for system-level encryption came from the Netherlands (40%) and India (38%).



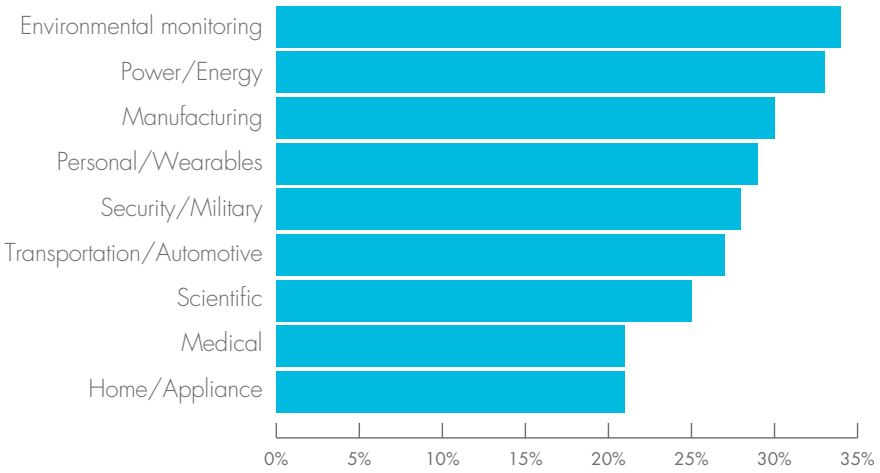
IoT RISING, BUT SO ARE IoT SECURITY CONCERNS

With nearly three-fourths (71%) of organizations aggregating data from the millions of IoT devices already in use, security concerns are predictably starting to mount. As we saw with the Mirai botnet attacks in 2016, hackers pulled off a major, successful DDOS attack that took out large chunks of the Internet in Europe and the U.S. by lashing together a botnet of 100,000 poorly protected IoT devices.

Paradoxically, some of the top IoT security concerns have declined from a year ago. Sharing the top spot globally are concern over protecting the data generated by IoT devices (26% compared with 36% last year), and attacks impacting critical operations (also 26%, up from 24% last year). Not too far behind in third place is discovering sensitive data generated by IoT devices (23% compared with 30% last year).

We also expanded our probe of IoT in this year's report with a new question regarding the most popular IoT devices currently in use, with environmental monitoring devices the most common (34% globally), followed by power and energy (33%); and manufacturing (30%). Notably, and perhaps surprisingly given high-level concerns in the media, medical devices (21%) and home appliances (21%) ranked last. It's also perhaps noteworthy that Sweden and India led the way in terms of deployments for most categories of IoT devices.

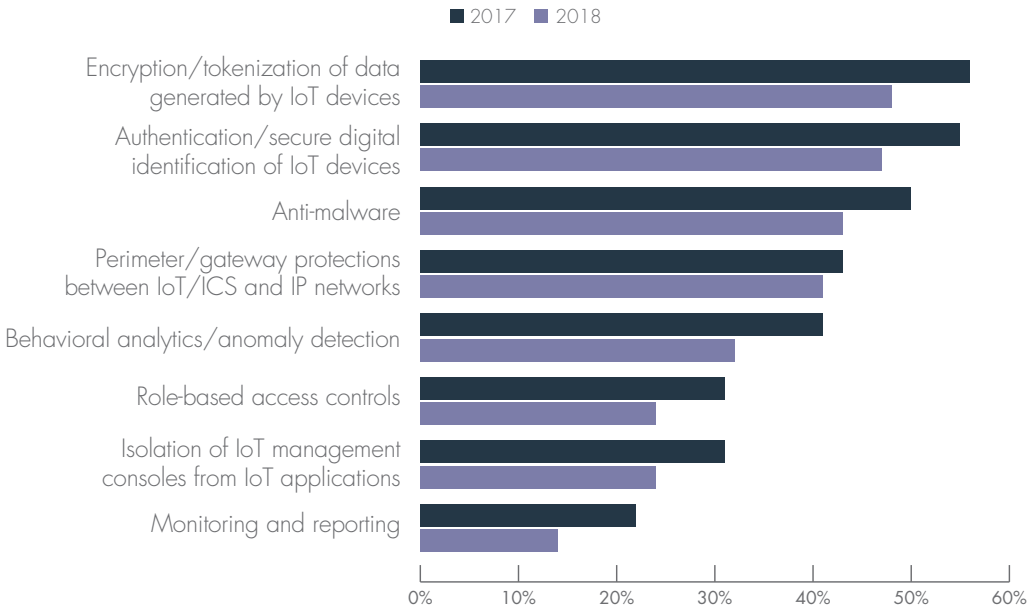
IoT: Deployment plans by use case globally this year



"With respect to IoT security controls, encryption and tokenization emerged globally as the top technology that would spur greatest use of IoT devices (48%), slightly ahead of proper digital identification of IoT devices (47%) and anti-malware (43%)."

With respect to IoT security controls, encryption and tokenization emerged globally as the top technology that would spur greatest use of IoT devices (48%), slightly ahead of proper digital identification of IoT devices (47%) and anti-malware (43%). By combining both encryption and authentication, the IoT explosion will likely serve as a new driver of demand for public key infrastructure (PKI), as well as hardware security modules (HSMs) to manage the encryption keys used to in IoT security implementations.

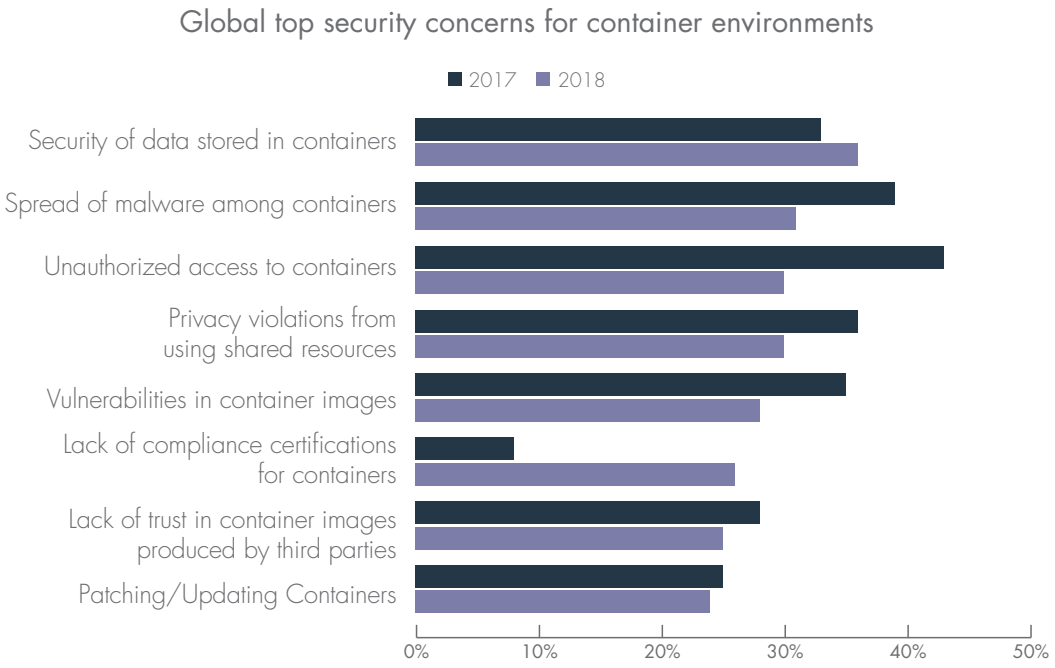
Technologies needed to speed IoT deployment globally



DOCKER/CONTAINERS

Our predictions of a 40% CAGR for the growth of containers through 2020 are proof positive of the rapid acceptance of this emerging technology that is barely four years old. Globally, nearly one-quarter (24%) of respondents report they are already using containers in production, split between non-critical production applications (13%) and critical production applications (11%), similar to the 23% overall response in the U.S. Production use of containers is highest in India (38%) and in Germany (36%), with Sweden (16%) and the U.K. (18%) trailing the rest of the pack and the global average.

However, we observed considerable change among the top container security concerns from last year's survey. Specifically, the top global container security concern this year is the security of data stored in containers (36%), which moved all the way up from fifth place last year. The spread of malware (31%) remained the second biggest concern, while last year's top choice – unauthorized access to containers – dropped into a tie for fourth place with privacy violations (30%).



We also noticed some changes in terms of the security technologies that would boost usage of containers. Anti-malware, last year's second ranked container security technology globally, moved into the top spot (45%), taking over the lead from last year's leader, encryption (41%), largely due to declines in the U.S. and Germany. Vulnerability scanning also moved down a notch to third (39%).

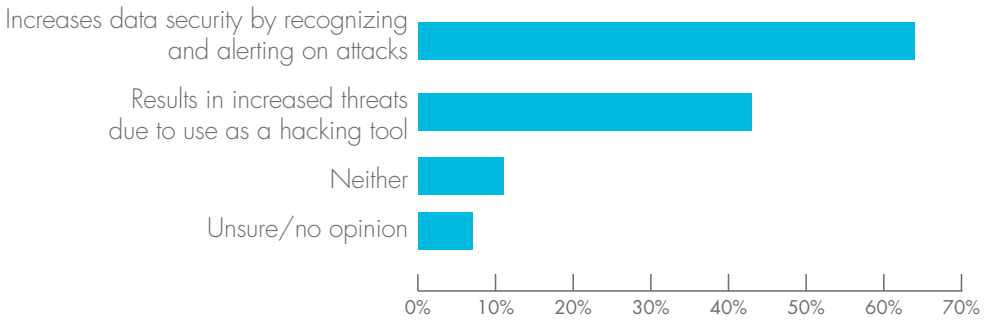
AI/MACHINE LEARNING

New this year, we included questions to address the impact of artificial intelligence (AI) and machine learning (ML). Advanced analytics have become a mainstay of many security vendors, who are using a combination of AI and ML to address areas such as risk-based or adaptive authentication, behavioral biometrics and user behavior

analytics to name just a few. Like most security tools, however – and most of technology for that matter – there is a 'dual nature' to such efforts. In the right hands and used properly, AI has already proven to be valuable aid to help spot and identify previously unnoticed behavioral and usage patterns that can foretell an imminent attack. In the hands of hackers, however, these same tools can be used as a weapon for malicious self-learning attacks such as hivenets and swarmbots. The latter are potentially massively scalable and much more damaging than botnets, able to control an attack without the central command and control instruction that standard botnets require.

We attempted to address this duality in this year's report, and found that overall, 'white hat' uses of AI and ML outnumber the 'black hat' responses. Specifically, nearly two-thirds (64%) of respondents believe AI is a boon to data security effort, while slightly less than half (43%) feel the future will bring an increase in breaches owing to misuse of these same tools by 'the bad guys' to steal sensitive data or deny critical services. Such concerns were most apparent with respondents from Korea (51%) and India (48%), though interestingly both nations were also among the most positive with respect to the impact of AI and machine learning (India 79%, Korea 75%).

Global IT security impact of machine learning/AI this year

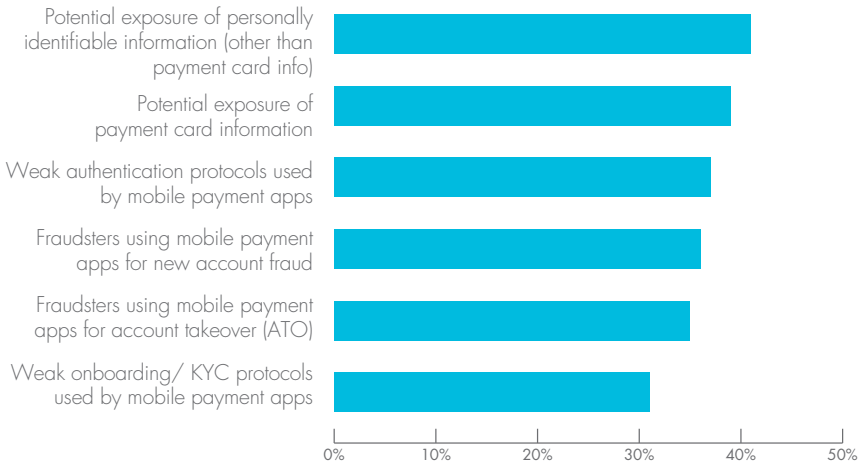


MOBILE PAYMENTS

Among millennials, mobile payments are booming as smartphone makers' pile on payment features into the latest generation of hardware and mobile apps. Thus for the first time we included questions on mobile payments in this year's report, specifically addressing the security risks posed by mobile payments. Topping the list of concerns was the potential for exposing customer identifiable information (41%), with India the highest at 54%. Potential exposure of personally identifiable information (PII) was a close second at 40% globally, followed by weak authentication protocols used by most mobile payments apps.

In terms of regional and vertical highlights, not surprisingly U.S. Retail expressed high concern about exposure of credit card information (49%), as did Korea (45%), Sweden (45%) and the U.K. (42%). India (54%) and the Netherlands (40%) were more concerned about PII exposure, while the biggest concern in Germany was account takeover by fraudsters (43%).

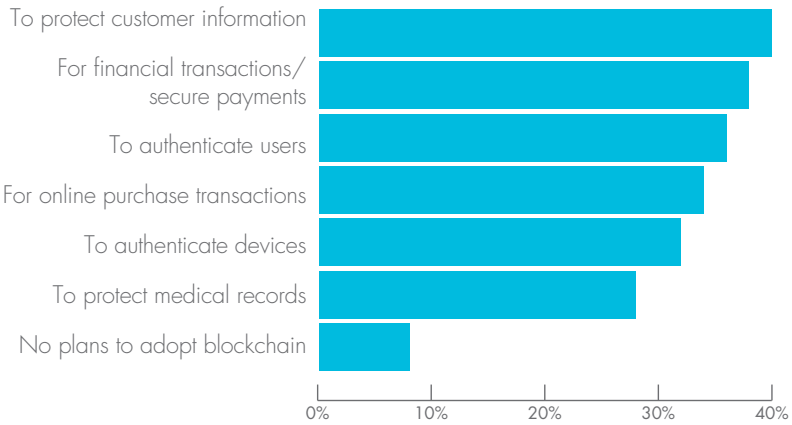
Global mobile payments security risks this year



BLOCKCHAIN TRENDS

Blockchain has the potential to be one of the most significant new developments in security in years, and there has certainly been plenty of industry buzz around blockchain, certainly with respect to crypto currencies. We believe blockchain and the applications it will support may well disrupt nearly all business models when it comes to displacing timeworn, traditional means of securing transactions and protecting data. To illustrate, while blockchain is a very recent phenomenon, just 8% of global respondents say they have no plan to adopt blockchain, with responses as low as 1% in India, 2% in Sweden and 3% in Germany and the Netherlands – in other words, nearly all organizations plan to take advantage of blockchain at some point.

Global blockchain usage plans this year



While it may be too early for actual security tools based on blockchain, there is an emerging consensus around the primary areas where blockchain can be applied. The main use cases emerging globally include protecting customer information (40%), followed by financial transactions/secure payments (38%), and user authentication (36%).

RECOMMENDATIONS

RE-PRIORITIZE YOUR IT SECURITY TOOL SET	With increasingly porous networks, and expanding use of external resources (SaaS, PaaS and IaaS most especially) traditional end point and network security are no longer sufficient. Look for data security tool sets that offer services-based deployments, platforms and automation that reduce usage and deployment complexity and staffing requirements.
LOOK FOR MULTI-CLOUD COVERAGE	Consider solutions that will work both with existing tools from cloud service providers, but also across multiple clouds and cloud apps.
DON'T JUST CHECK OFF THE COMPLIANCE BOX	Global and industry regulations can be demanding, but firms should consider greater use of encryption and BYOK, especially for cloud and other advanced technology environments to both address growing compliance mandates and also move closer to industry best practices.
ENCRYPTION AND ACCESS CONTROL	Encryption needs to move beyond laptops and desktops. **Data center:** FDE offers very limited protection in the data center – consider file and application level encryption and access controls **Cloud:** Encrypt and manage keys locally, BYOK is an enabler for enterprise SaaS, PaaS and IaaS use and secures against insider threats. **Big Data:** Employ discovery as a complement to encryption and access control within the environment **Containers:** Encrypt and control access to data both within containers and underlying data storage locations **IoT:** Use secure device ID and authentication, as well as encryption of data at rest on devices, back end systems and in transit to limit data threats

ANALYST PROFILE

Garrett Bekker is a Principle Analyst in the Information Security Practice at 451 Research. He brings a unique and diverse background, having viewed enterprise security from a variety of perspectives over the past 15 years. Garrett spent more than 10 years as an equity research analyst at several investment banking firms, including Merrill Lynch, where he was the lead enterprise security analyst, as an investment banker, and also in sales and marketing roles with early-stage enterprise security vendors. Throughout his career, Garrett has focused on a wide variety of subsectors within enterprise security and is now focusing primarily on identity and access management (IAM) and data security, with a special interest in applying the former to cloud-based resources.

Garrett Bekker
Principal Analyst
451 Research

ABOUT 451 RESEARCH

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

ABOUT THALES eSECURITY

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

Please visit **www.thalesesecurity.com** and find us on Twitter **@thalesesecurity**.

PLATINUM PARTNERS – GEOBRIDGE

Established in 1997, GEOBRIDGE emerged as one of the first information security solutions providers to support cryptography and payment applications for payment processors, financial institutions and retail organizations. Today, GEOBRIDGE is a leading information security solutions and compliance provider that provides Cryptography and Key Management, Payment Security , Compliance, and HSM Virtualization solutions and services to our clients. Our client list includes Fortune 500 companies, financial institutions, healthcare organizations and government clients across North America and around the globe. GEOBRIDGE leverages our team's expertise in data protection, program development, enforcement and governance to help architect solutions to help mitigate risk for our clients.

THALES

www.thalesesecurity.com