THALES

451 Research

2017

THALES DATA THREAT REPORT

#2017DataThreat

TABLE OF CONTENTS

OUR SPONSORS

CenturyLink®

rackspace® the #1 managed cloud company

ARROW

Canon Canon IT Solutions Inc.

CSA cloud security alliance℠

GTRA GOV

OASIS

NUTANIX

QTS

ACCUDATA® SYSTEMS

WICK HILL + zycko®

virtustream®

Part of the NUVIAS group

GuidePoint SECURITY

M.TECH Your Preferred I-Security Partner

peak 10®

INTRODUCTION

One of the fundamental challenges of cybersecurity is dealing with the speed of change. With each new computing paradigm shift – Cloud, Big Data, IoT etc. – come new capabilities and possibilities – along with new security vulnerabilities to be exploited. It's no wonder that the security industry overall now tallies in excess of 1,400 vendors by 451 Research's count, with as many as nine new startups per month and roughly 10 new security categories created each year.

Paradoxically, however, our attitudes and fundamental security strategies are arguably not keeping up with that pace of technical change. To illustrate, 63% of respondents to a new question in this year's survey indicated that their organizations deploy new technologies in advance of having appropriate levels of data security in place.

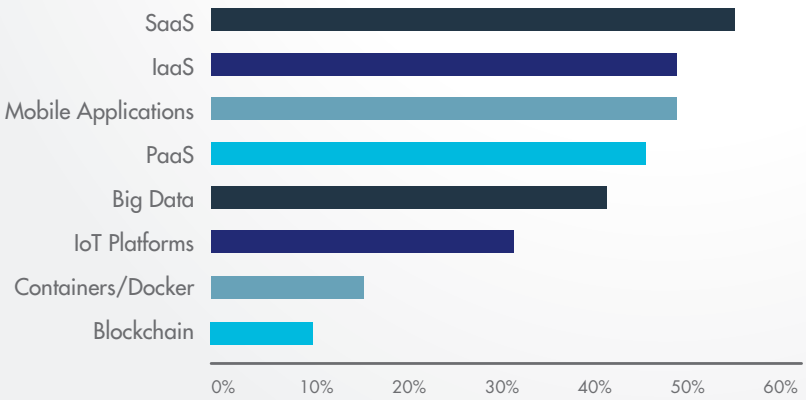
In like spirit, one of the main challenges of the Thales Global Data Threat Report has been to continue to evolve to reflect the latest threats and technologies. For example, past versions of the report focused primarily on the threat presented by insiders, both malicious – as in the renowned case of Edward Snowden – and inadvertent. But as we have learned over the past few years, the global threat landscape is constantly evolving, and one of our biggest challenges is to protect data from a fluid cast of not just insiders but also external threat actors, many of which are well funded, organized and often – though not always – highly sophisticated.

Similarly, the list of people with legitimate access to our data has grown – no longer just employees, but as we have embraced the modern extended enterprise, our resources must now be made available to partners, suppliers and contractors, and potentially our customers. Thus as the line between 'insider' and 'outsider' has blurred, we expanded the scope of our report to add external actors to the mix.

At the same time, more and more enterprise data is being created, transported, processed and stored outside the corporate network boundaries, and thus no longer subject to traditional perimeter-based security controls that rely on the concepts of 'trusted' vs. 'untrusted' or 'internal' vs. 'external'.

As an example, previous studies from 451 Research's Voice of the Enterprise on cloud computing show that nearly two-thirds (63%) of enterprises are using SaaS applications, while the percentage of workloads deployed to the cloud today is expected to jump from 41% to 60% within the next two years. With respect to the Internet of Things (IoT), the most conservative estimates of the number of IoT devices to be deployed within three years top *20 billion*. And as we will discuss in more detail later, we have seen rapid uptake of container technology such as Docker, with nearly 40% of respondents claiming to use containers in production environments, despite being in the market for barely a few years.

Respondents Concerned that Advanced Technologies Deployment is Happening Before Appropriate Data Security is in Place
By Technology Platform



"63% of respondents to a new question in this year's survey indicated that their organizations deploy new technologies in advance of having appropriate levels of data security in place."

Even the very nature of attacks seems to be undergoing a metamorphosis. In one of the most notable incidents of 2016 and a possible sign of things to come, attackers relied on a massive botnet of over 100,000 poorly protected and compromised (IoT) devices to overload the servers at DNS provider Dyn and disrupt Internet services in two-thirds of the U.S., rather than attacking Dyn directly.

In that spirit, we expanded the scope of last year's 2016 Vormetric Data Threat Report to include both external and internal threats to sensitive data, as well as an increased emphasis on emerging technologies such as cloud, Big Data and the IoT. We continue that emphasis in this year's report, while including new questions to capture the rapid growth of container technology, as well as the growing importance of data sovereignty mandates around the world, such as the General Data Protection Regulation (GDPR) recently passed by the European Union.

The 2017 *Thales Data Threat Report* is based on a survey conducted by 451 Research during October and November of 2016. We surveyed 1,100+ senior security executives from across the globe, including from key regional markets in the U.S., U.K., Germany, Japan, Australia, Brazil and Mexico, and key segments such as federal government, retail, finance and healthcare.

"Our 2017 report finds a global situation where spending on security is up – sharply in some sectors – yet successful data breaches are also up significantly."

"Nearly two-thirds (63%) of enterprises are using SaaS applications, while the percentage of workloads deployed to the cloud today is expected to jump from 41% to 60% within the next two years."

EXECUTIVE SUMMARY

Glass half-full, or half-empty?

Similar to last year, the overall assessment of this year's Thales Data Threat Report depends on one's perspective. Security vendors, practitioners and even attackers are likely to find a mixture of both encouraging trends, but also warning signs – all set against a backdrop of attacks that seem to grow more successful each year.

On the positive side, one potentially encouraging sign – at least for security vendors – is that 73% of respondents anticipate security spending increases in the next 12 months, a sharp increase from 58% last year. The primary reason for the jump is that those who anticipate 'much higher' spending (23%) nearly doubled from just 12% last year, also potentially good news for practitioners dealing with security budget constraints. Furthermore, while most security spending remains driven by compliance concerns, security spending in order to implement best practices has moved up again for the second straight year and into the #2 overall spot, a sign that enterprises are starting to do more than the bare minimum to meet regulatory demands. We should also note that 2016 is also shaping up to be a banner year for investment bankers.

However, despite the higher spending (and planned spending) on security, some 26% of respondents said their organizations experienced a breach in the last year, up from 21.7% in 2016, while 42% of respondents experienced a data breach at another time in the past (up from 39.3%). It is no wonder then that nearly one in three respondents feel their organizations are either 'very vulnerable' or 'extremely vulnerable' to threats to sensitive data. Overall, the research suggests that the security industry looks increasingly like a dog chasing its own tail – despite more and more money spent on security each year, our collective problems continue to worsen.

One possible explanation for this vicious cycle is that organizations keep spending on the same solutions that have worked in the past but are no longer the most effective at stopping modern breaches. For example, similar to last year's study, network and endpoint security topped the list of planned spending categories, yet endpoint security ranked at the bottom of the list in terms of effectiveness at preventing data breaches and data theft.

As an example, this year's research surveyed about container usage. Containers, at a high level provide another layer of abstraction that enable flexibility and portability regarding where applications can run, whether on premises, public cloud or private cloud. Just over two years old, Docker – an open source container iteration – is proliferating rapidly in various organizations seeking to speed up application development. One of the more noteworthy data points from this year's study is that nearly 40% of respondents are already using containers in production environments, yet like other emerging technologies, 47% of respondents view security as the main adoption barrier for containers, the number one response other than budget (44%).

KEY FINDINGS:

- More than two in three respondents (67.8%) said their organizations have been breached at some point, an increase of nearly 7% percent over the previous year. And more than one in four (26%) were breached in the last year alone, up from 21.7% the previous year.

- The overwhelming majority of respondents still feel some degree of vulnerability to data threats (88%), down slightly from the previous year (90%), but still at an alarmingly high level. Those feeling 'extremely vulnerable' rose slightly, to 9.1% from 8.2%.

- Compliance (44%) remains the primary reason for spending on data security by a stubbornly wide margin over implementing security best practices, the second strongest driver (38%). However, we found it encouraging that fewer respondents (59.5%) viewed compliance requirements as 'very or extremely effective', a notable drop from 64% last year. Meanwhile brand and reputation plummeted to 36%, down markedly from 50% in last year's study as a primary reason for security spending.

- In a departure from both practical experience and anecdotal evidence, more than 57% of respondents claim 'complete knowledge' of where sensitive data is located, up sharply from 42% last year.

- Data sovereignty has become a hot topic in light of concerns about new regulations, and government snooping. Encryption was identified as the clear choice (64%) to satisfy local data privacy laws such as the EU's recently approved General Data Protection Regulation (GDPR). Tokenization (40%) is listed as a distant second, while migrating data to jurisdictions or choosing local cloud providers are at the very bottom of the list.

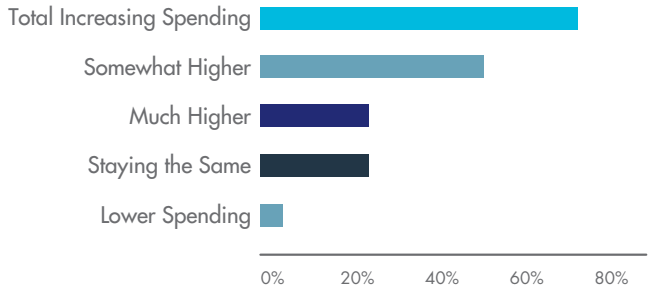
- Complexity remains the top barrier to more aggressive adoption of data security solutions chosen by 50.4% of respondents. 'Lack of staff' trailed by a considerable margin in second place at 36%.

- Though still a nascent technology that's been in the market for barely two years, Docker containers are being used by four in ten respondents for production applications, with a nearly 50-50 split between critical and non-critical applications. Only 13% of respondents have no plans to use Docker containers in the year ahead. Like other emerging technologies like cloud, Big Data and (IoT), not surprisingly, security remains the #1 Docker adoption barrier (46.7% of respondents) and the #1 method for securing containers is encryption.

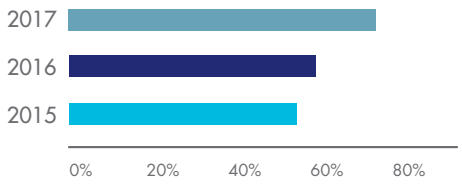
SPENDING INTENTIONS

Against a backdrop of flat or even declining overall IT budgets, 73% of respondents say their organizations will increase security spending next year, up sharply from 59% last year. The main driver of the jump was the number of organizations saying they will have 'much higher' security spending nearly doubled, from 12% last year to 23%.

Next 12 Month Spending Plans to Secure Sensitive Data

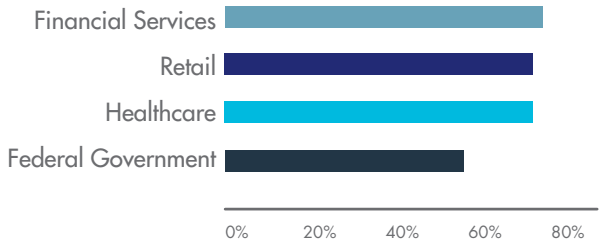


3 Year Trend of Increasing IT Security Spending to Protect Data

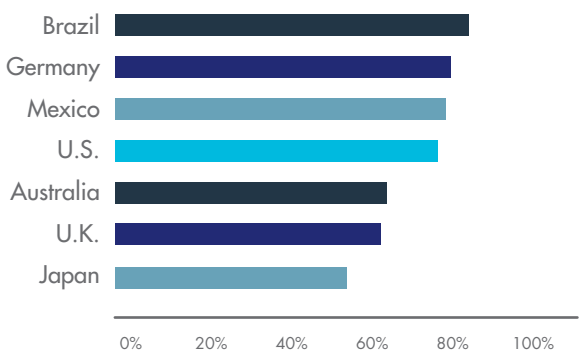


As was the case last year, respondents listed compliance requirements as the top driver of security spending. Thus, it is no surprise that in the two most heavily regulated and compliance-rich vertical markets – healthcare and financial services – 76% and 78% of organizations respectively are planning spending increases. And in retail, which has seen some of the most highly publicized attacks (Target, Home Depot, TJX, British Airways), 77% of organizations will increase security spending. Geographically, the two regions planning to increase their security spending the most were Brazil (85% of respondents from Brazil said their organizations would increase security spending next year, up sharply from 73% last year) and Germany (80% compared to just 63% last year).

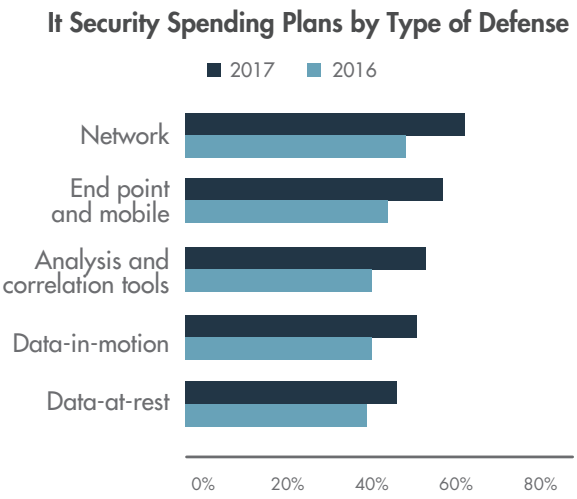
Planned Spending Increases to Protect Data by *Industry*

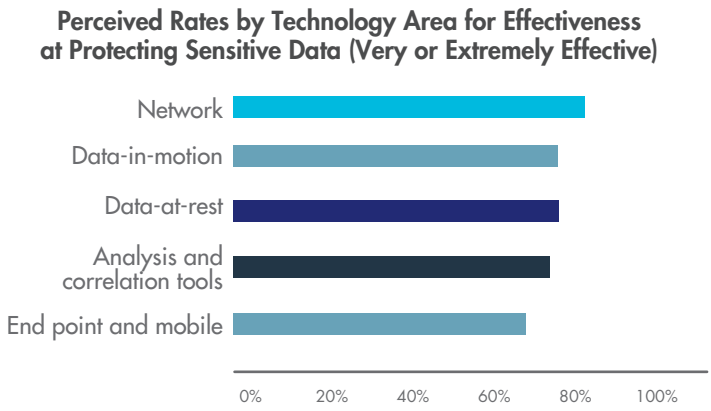


Planned Spending Increases to Protect Data by *Region*



The sobering news is that the spending still favors old habits-spending on network and endpoint security once again top the list. What's more surprising – is that planned spending on these two areas also showed the largest year over year increases of any security category (network security +13.7%; endpoint security +12.3%) So not only do network and endpoint security still dominate spending plans, they also appear to be widening the gap with other security categories – despite being ranked least effective, at least in the case of endpoint security.

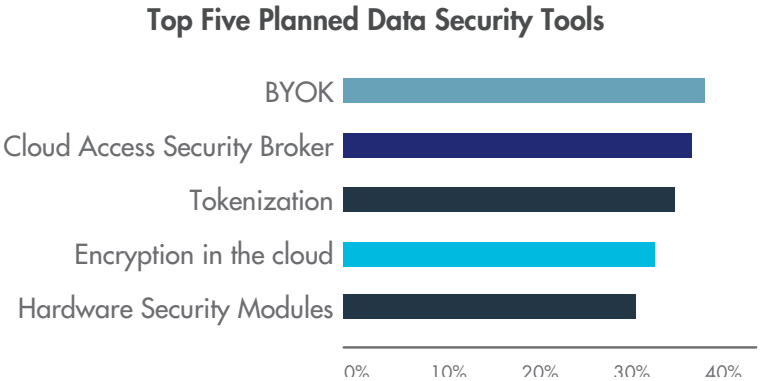




Conversely, spending plans for data-at-rest encryption ranked dead last, even though respondents ranked encryption of data-at-rest as more effective (75.7%) in protecting sensitive data than endpoint security (69.3%). These disconnects between what people actually plan to spend their budgets on and what are perceived as the most effective defenses can have lingering harmful consequences as the threat environment evolves. Ideally, it is hoped that the ongoing adoption of new technologies like Cloud, Big Data, IoT and containers will provoke more investment in forms of security that are better suited to the new security challenges they pose.

As far as security techniques and solutions organizations are planning to implement next year, encryption with bring-your-own-encryption-key or BYOK topped the list, displacing last year's top choice of application layer encryption, which slipped all the way to 6th place. Behind BYOK is cloud access security broker (CASB), with tokenization remaining in third place.

"FOR THE FIRST TIME, 4 OF THE TOP 5 DATA SECURITY TOOLS PLANNED FOR IMPLEMENTATION ARE RELATED TO CLOUD. BYOK, CASB, ENCRYPTION IN THE CLOUD AND HARDWARE SECURITY MODULES."



"Network security and endpoint security topped the list in terms of spending plans, but also showed the largest YOY increases."

"SPENDING PLANS FOR DATA-AT-REST ENCRYPTION RANKED DEAD LAST, EVEN THOUGH RESPONDENTS RANKED DATA-AT-REST ENCRYPTION AS MORE EFFECTIVE (75.7%) THAN ENDPOINT SECURITY (69.3%) AT PROTECTING DATA."

COMPLIANCE CONTINUES TO LEAD

One of the notable themes from past reports was the high degree of faith that many industry verticals and regions place in compliance mandates. Indeed, last year nearly two-thirds (64%) of respondents said compliance requirements were either 'very' or 'extremely' effective in securing data. Yet while compliance can serve as an effective tool for establishing security baselines, the rising tide of breaches each year should serve to highlight the limitations of compliance mandates in terms of establishing a comprehensive and technologically current security policy.

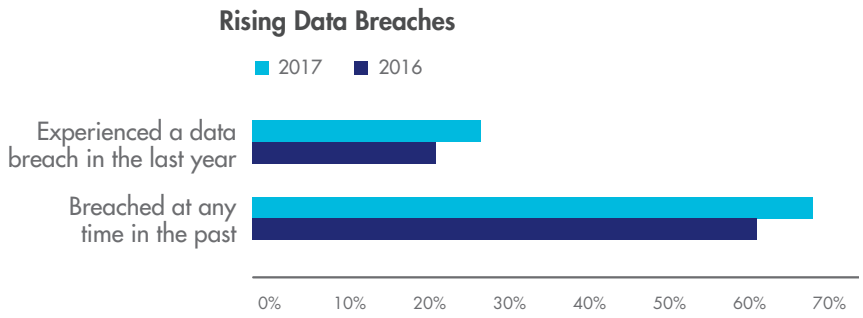
Thus we were slightly encouraged that the corresponding metric for this year fell significantly to just over 59% this year. Although it appears that the belief in compliance requirements effectiveness rose in Japan and Australia from last year, most other regions surveyed decreased their overall enthusiasm for compliance requirements. A plausible reason for this decline is mounting evidence that compliance adherence is just not enough in this fast-changing threat environment. We are also encouraged that implementing security best practices continues to gain in importance, and moved decisively into the second position as a driver of security spending (38%). That said, compliance still holds a lot of sway in certain regions that trust its effectiveness such as Brazil, (70%), Mexico (68%) and Australia (66%), and as we noted above, compliance remains the top driver of security spending globally (44%).

"59% of respondents said compliance requirements were either 'very' or 'extremely' effective in securing data, down from 64% last year, while implementing best practices moved up into second place."

BREACHES

Increased spending on security notwithstanding, this year's study saw the percentage of organizations that have been successfully breached at some time in the past rise to 67.8%, up considerably from 61.1% last year, while those breached in the past 12 months also rose significantly to 26.1%, up from 21.7% a year earlier. Among the hardest hit geographies and industry verticals were Australia, where a full 44% of respondents reported a breach in the past year, and retail (43% globally).

"Organizations breached in the past 12 months rose sharply, to 26.1% from 21.7% last year."



"PRIVILEGED USERS WERE THE TOP INSIDER THREAT IN ALL REGIONS SAVE JAPAN."

Riskiest threat factors

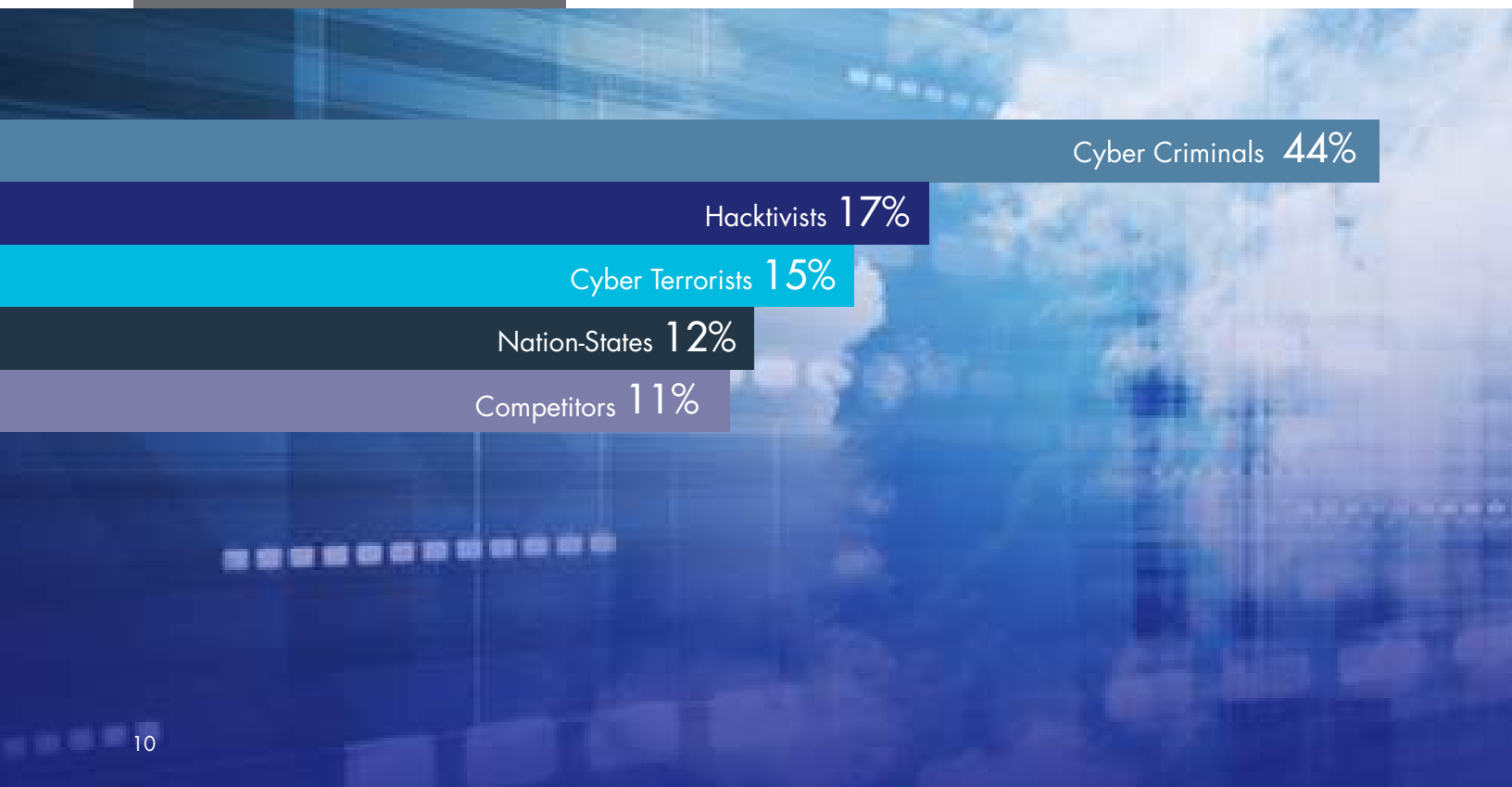
When it comes to which insiders are deemed as a threat, privileged users remain far ahead of all user categories, selected by nearly 59% of respondents – a slight increase from 58% last year. The concern with privileged users is understandable, given the attention focused on certain high-profile cases of insider abuse (e.g. Snowden), the potential damage that can be done by a rogue insider that has the proverbial 'keys to the kingdom', as well as the increasingly common occurrence of privileged credentials being compromised. Privileged users were the top insider threat in all regions save Japan, which places a slightly greater emphasis on ordinary (non-privileged) employees (49% vs. 48%), though notably by a much smaller margin than previous surveys.

"57% of respondents say they have 'complete knowledge' of where their sensitive data is located, up dramatically from 43% last year."

"72% OF ENTERPRISES OVERALL WILL BE IMPACTED BY PERSONAL DATA PRIVACY AND SOVEREIGNTY REQUIREMENTS WITH 38% REPORTING A 'SIGNIFICANT IMPACT' ON THEIR USE OF CLOUD COMPUTING."

With respect to external threat actors, cyber criminals once again led the way by a wide margin (86%) over the next-closest group, hacktivists (67%), and cyber terrorists (66%). Notably, nation states fell to the bottom of the list (35%), which is curious in light of ongoing discussions of cyber activities by China, North Korea, Iran and Russia. It's worth noting that our survey was conducted in advance of the recent U.S. election, and thus the widespread allegations of Russian interference were likely not fully captured in the results.

TOP EXTERNAL THREAT ACTORS



Data location

It has often been said that you can't secure what you don't know, and one of the common objections to data security tools in general is that many organizations have limited knowledge of the types of data they may have, how sensitive it might be, or where it may be located. Last year we decided to test this hypothesis and were somewhat shocked at the results: just less than half of respondents (43%) claimed 'complete' knowledge of their sensitive data, while 47% claimed 'some' idea. Conversely, less than 10% claimed they had little to no idea where their sensitive data might be, which is at odds with most of our frequent conversations with industry sources.

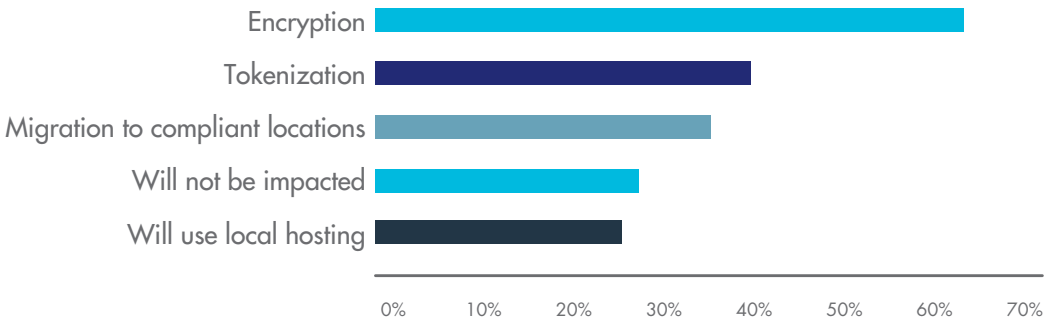
Thus, we were more than a bit surprised that this year, 57% of respondents say they have 'complete knowledge' of where their sensitive data is located, up dramatically from 43% last year. One potential explanation is that the scope of what most respondents consider "sensitive" is fairly narrow. Another is that this may represent a case of 'ignorance is bliss' – it's not uncommon for firms to discover data or data stores they never knew existed once they run a discovery scan as part of another project. However, if we are to believe the results it would be a reassuring sign given that data is more distributed than ever thanks to the rise of cloud, mobility, Big Data and IoT. Indeed, when it comes to public cloud services such as SaaS, IaaS and PaaS, 55% of respondents listed "lack of control over the location of data" as a very or extremely high concern.

A related issue is data sovereignty, which has been a hot topic of late in light of new regulations in many countries, often driven by allegations of mass surveillance by intelligence agencies such as the NSA, as well as concerns for personal privacy. One of the most sweeping of such laws is the EU's GDPR, which goes into effect in May of 2018 and affects any organization collecting any personal data on any resident within the 28-nation European Union. Thus interest in data sovereignty – the notion that digital data is subject to the laws of the country where the data is located – is running high.

451 Research's recent *Voice of the Enterprise: Cloud Transformation 2016* study shows that nearly 38% of global respondents cite data sovereignty as having a 'significant impact' on their organization's use of cloud computing. As such, we added a new question to our survey this year around data sovereignty and found that nearly two-thirds (64%) of respondents plan to encrypt any personal data that will be subject to local privacy or security regulations such as GDPR. Global financial services firms (66%) and respondents from Mexico (70%) are particularly keen on encryption in this matter.

"NEARLY TWO-THIRDS (64%) PLAN TO ENCRYPT PERSONAL DATA SUBJECT TO LOCAL PRIVACY OR SECURITY REGULATIONS SUCH AS GDPR, WHILE 40% PLAN TO USE TOKENIZATION."

Global Plans For Meeting Personal Data Privacy and Sovereignty Regulations

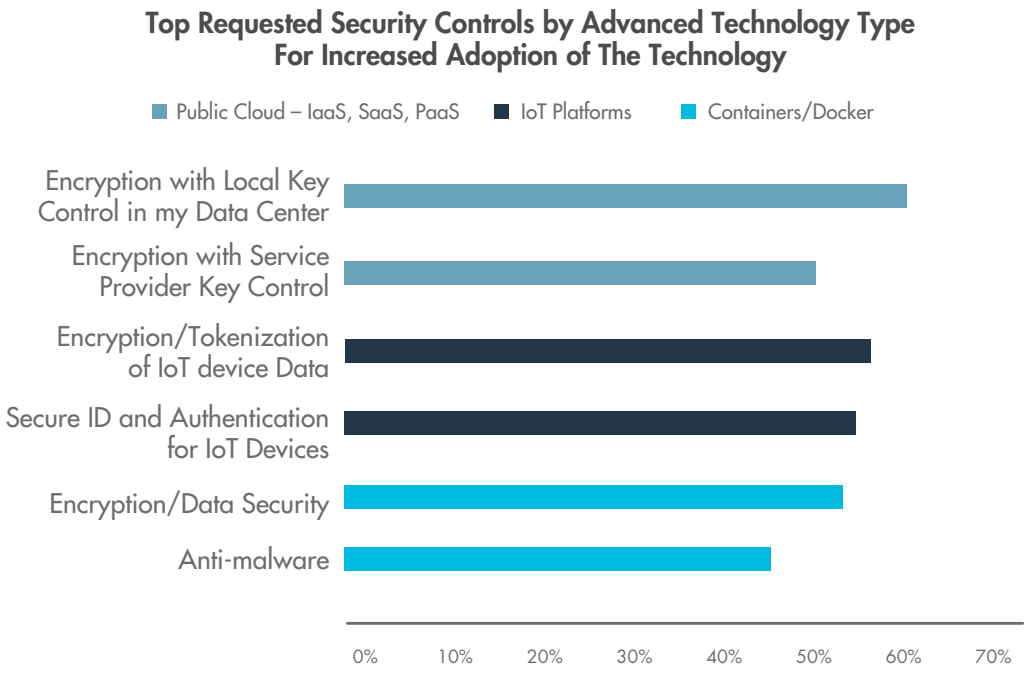


A distant second is tokenization (40%), however, just over one in four global respondents plan to address data sovereignty requirements by either migrating data (28%) or transitioning to a local cloud provider (26%). We found this a bit surprising, particularly given that many cloud providers and security vendors with cloud-based services have been quietly setting up operations in countries or regions in which privacy concerns run high, such as Germany, Canada, Australia and APAC to deal with both data sovereignty issues as well as performance and latency concerns. We suspect the results can be explained in part by the difficulties of migrating large amounts of legacy data to cloud providers, particularly those located overseas.

ENCRYPTION

For most legacy on-premises environments, databases (48%) and file servers (40%), as well as PCs and mobile devices (33% each) are the most likely to store and be at risk for loss of sensitive data. And the most common tools and techniques for protecting those resources include database/file encryption (72%), database activity monitoring (70%); and data loss prevention (DLP; 63%). Indeed, aside from databases and file servers, our study also showed that encryption is also widely deployed to protect data-at-rest on PCs (53%), email (45%) and mobile devices (44%).

With respect to protecting sensitive datacenter servers specifically, respondents were nearly equally divided between full disk encryption (FDE; used by 41% of respondents) and file/volume encryption (39%). This is a bit of a reversal from last year's study, in which file/volume encryption was chosen by a 46% to 40% advantage over FDE. It is important to note that FDE offers protection only from physical loss or theft within the data center, while file/volume encryption combined with access controls can help protect against threats within the system itself.



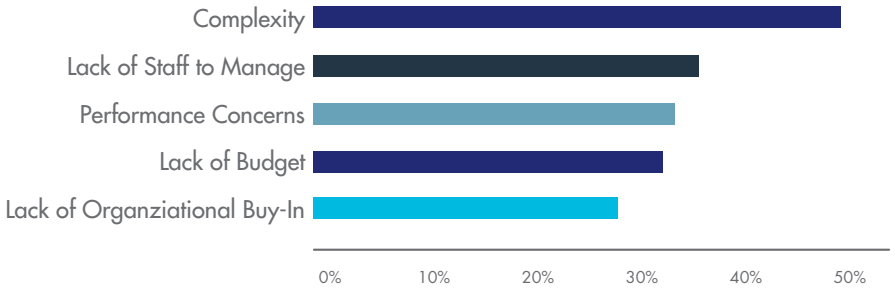
However, when we consider emerging technology categories such as cloud, Big Data, IoT and now containers, encryption takes on even greater significance as a primary security control. For example, encryption with the ability for organizations to store and manage their own encryption keys, often known as 'Bring Your Own Key' or (BYOK), was the top security control (61%) that would make respondents more willing to use public cloud (either IaaS, PaaS or SaaS) while encryption with keys controlled by the service provider was the number two answer at 51%. Similarly, encryption or tokenization of data generated by IoT devices (56%) was the number one security control that would make respondents more comfortable moving to IoT and also the top choice for data sovereignty mandates such as GDPR (64%).

COMPLEXITY AND LACK OF SKILLED STAFF STILL A HURDLE FOR DATA SECURITY

If data security is so effective at preventing threats, why does it still trail both network and endpoint security in terms of spending plans? Part of the answer is that both network and endpoint security are fairly transparent, in the sense that end users typically have little idea when a new firewall appliance or anti-malware software has been installed. The same isn't always true for data security, or at least that's the common perception. Thus, it was not a complete surprise that complexity (50.4%) was once again chosen as the as the #1 barrier to data security adoption. Of course, complexity to some extent goes hand-in-hand with staffing requirements since complex deployment, tuning and management requirements for security products typically require more people to manage them – this was particularly an issue in the US Federal market (53%) as well as respondents in Mexico (46%) and Japan (41%). The most notable change from last year's report is that concerns about impacts to performance and business operations moved up from fifth place into third overall (34%), while lack of budget slipped from third to fourth place (33%), but is a substantial hurdle for both the global federal (47%) and global retail industry verticals (53%).

The lack of skilled security staff has been a consistent theme in 451's research efforts the past few years, and in conjunction with complexity, makes a strong case for data security functionality delivered as a service, particularly those functions that are perceived to be labor intensive and require substantial resources and expertise to keep up and running, such as encryption key management or DLP.

Top Perceived Global Barriers to Adopting Data Security



"THE TOP TWO CHOICES FOR SECURITY IOT WERE ENCRYPTION/ TOKENIZATION (56%) AND AUTHENTICATION/IDENTIFICATION OF IOT DEVICES (55%)."

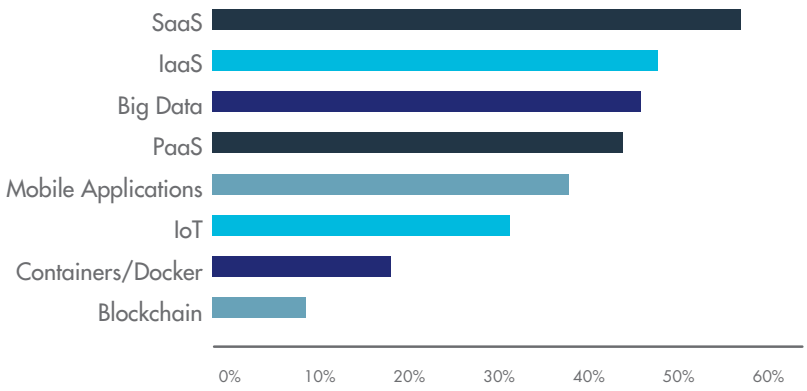
SECURING CLOUD, BIG DATA AND IOT

One of the unique security challenges posed by the triumvirate of cloud, Big Data and IoT is that the latter utilize resources that often exist outside of traditional enterprise boundaries, and thus security tools that rely on traditional notions of "internal" versus "external" have limited applicability. With respect to cloud specifically, data from 451 Research's Voice of the Enterprise survey on cloud computing shows that SaaS applications are the most widely deployed type of cloud resource, with 62.8% of respondents currently having deployed SaaS applications. Further, the percentage of workloads deployed as software-as-a-service (SaaS) is expected rise from 14% today to 23% of all workloads in two years.

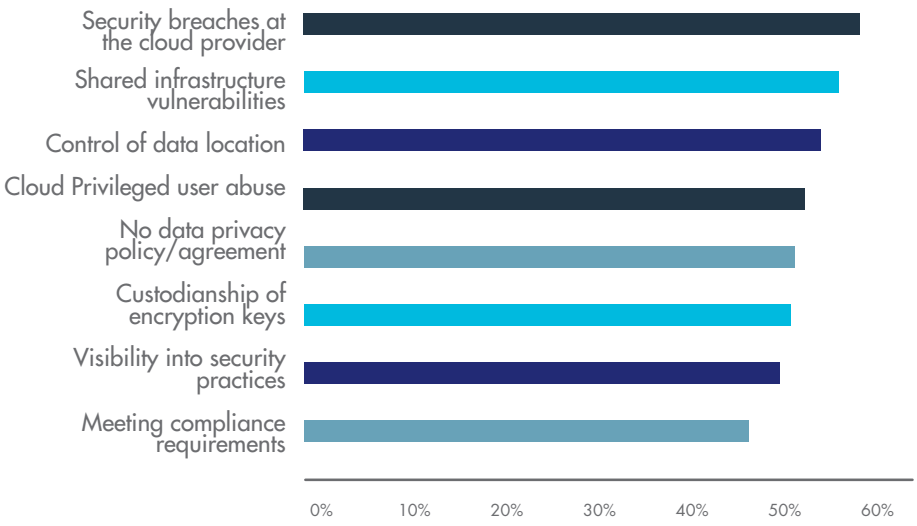
Not surprisingly SaaS also topped the list of technologies about which respondents are most concerned from a security perspective (55%). SaaS applications are also the most at risk of loss of sensitive data for all 'emerging' technology categories (28%) followed by Big Data (21%), IoT (20%), and IaaS/Paas (15%), and also where respondents plan to store the most sensitive data (SaaS at 57%, IaaS at 49%, Big Data at 47%, PaaS at 44% and IoT at 31%).

What are respondents most concerned about? Similar to last year, attacks or breaches of the cloud provider is the top cloud security concern (59%), followed by perceived vulnerabilities from shared infrastructure (57%) and lack of control over data location (55%).

Advanced Technology Environments Where Organizations Plan to Store Sensitive Data



Top Cloud Security Concerns



"Though Docker has barely been around for more than a few years, nearly 40% of respondents are using Docker containers for production applications – not simply development and testing as is often the case with new technologies like IaaS."

Cloud

And what are the most popular means of securing against cloud security threats? Far and away the ability of cloud service providers to offer encryption with the ability for firms to manage and control their own encryption keys (BYOK) is cited as the top control (61%) that would lead to greater willingness to use public cloud services, followed by encryption with keys managed by the cloud provider. Yet only 35% of all respondents either currently implement or have plans to implement BYOK encryption as a part of their organization's overall data security strategy. That said, the adoption level of BYOK parallels the adoption levels of cloud overall, and thus, we expect interest in BYOK encryption to increase as data increasingly migrates to the cloud.

Big Data

In terms of which 'new' technology environments do respondents plan to store sensitive or regulated data, Big Data once again retains the third spot overall, trailing SaaS and IaaS. However, in terms of which of those new technologies respondents are most concerned about, Big Data fell into fifth slot, behind SaaS and IaaS, but also PaaS and mobile applications. Security concerns for Big Data center on the fact that sensitive organizational data may reside anywhere in the system (45%) and that Big Data reports might contain highly sensitive data (44%).

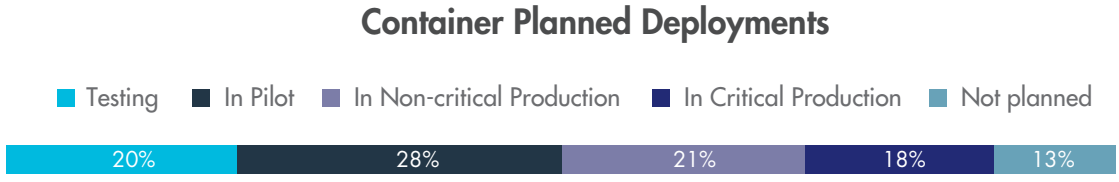
IoT

Overall, as with last year's study, the perception of IoT risk remains low, at least relative to other emerging technologies. As we noted previously, the sheer magnitude of IoT promises to be unprecedented, with conservative estimates suggesting over 20 billion IoT devices could be deployed within three years. And similar to other new technologies like cloud and Big Data, security is the number one barrier to broader adoption of IoT.

Yet among all emerging technologies, IoT still ranks fairly low (32%; sixth overall) and trails other categories like SaaS and IaaS in terms of security concerns. The biggest IoT-specific security concerns were protecting the data generated by IoT devices (36%) and identifying or discovering sensitive data generated by an IoT device (30%). With respect to options for securing IoT, respondents once again chose encryption/tokenization of IoT data as the best defenses for protecting data generated by IoT devices (56%) with authentication and secure identification of IoT devices a close second (55%).

Containers

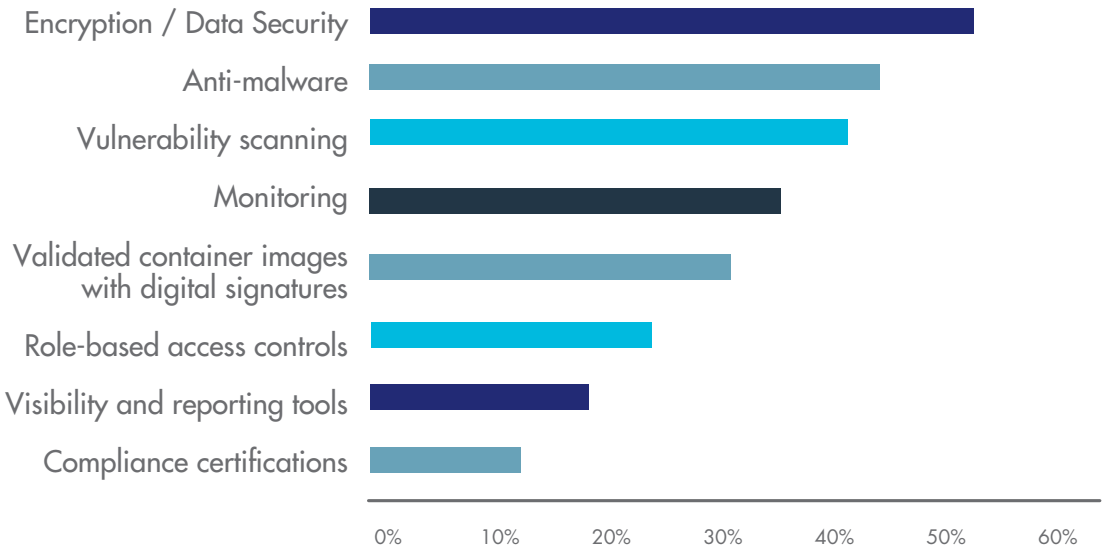
A new question we asked in this year's survey investigated respondents' concern with the use of container technology such as Docker. This was in part due to both Docker's rapid growth and also its likely impact across a broad swath of IT. Indeed, both usage and interest in containers have soared in the last 24 months. in a sense, containers can be viewed as a natural progression of virtualization. Docker greatly automates the deployment of applications within software 'containers', which are essentially self-contained run-time environments comprising an application and all its dependencies, configuration files, and libraries.



Though Docker has barely been around for more than a few years, nearly 40% of respondents are using Docker containers for production applications – not simply development and testing as is often the case with new technologies like IaaS. Furthermore, the percentage of respondents using containers for production applications was pretty evenly split between mission critical and non-mission critical applications. This lofty deployment of mission-critical container production applications underscores tremendous interest while ratcheting up security concerns. Globally, Brazil is among the most aggressive in terms of container usage, with 29% using containers for mission-critical production applications – conversely, Australia (22% for production apps) and Japan (24% for production apps) lag behind other geographies in terms of current use of Docker containers.

As is typical with any fast-emerging technology, security concerns abound. Indeed, security is cited as the top barrier to broader Docker container adoption by nearly 47% of respondents, and was particularly a concern with US federal institutions (60%). The main security concerns respondents identified include unauthorized access (43%), followed by the spread of malware (38.6 %). To combat these concerns, respondents rank encryption as the top security antidote (53.4%), well ahead of anti-malware (45%) and vulnerability scanning (41.7%), a sentiment echoed across virtually all geographies and vertical markets. Some of the unique challenges and requirements of securing containers include providing visibility into container access patterns, policies that will persist and travel with containers as they are copied or moved, and the ability to isolate data between containers and provide granular access controls using a default-deny framework.

Tools that would increase willingness to use containers



"SECURITY IS THE TOP BARRIER TO CONTAINER ADOPTION, AND THE TOP CHOICES FOR SECURING CONTAINERS INCLUDE ENCRYPTION (53.4%), ANTI-MALWARE (45%) AND VULNERABILITY SCANNING (41.7%)."

RECOMMENDATIONS

In recent years, we have witnessed traditional models of computing being figuratively – and in some cases literally – turned upside down and inside out. And as the technology landscape has shifted, so too has the threat environment, as well as the various methods of defending against those threats. Information security will always be a cat-and-mouse game as technology providers look to keep up with the ever-changing threat landscape and attackers. But a main theme of 451 Research's ongoing analysis – and also one of the main theses of this report – is the misalignment between current threats and the appropriate defenses needed to truly protect an organization's assets from compromise. To the extent that security spending continues to increase each year, a defensible argument could be made that, at worst, much of that money is being wasted, or at best, sub-optimally allocated.

Simply put, as our corporate boundaries become increasingly porous and our resources are on the move, traditional endpoint and network security approaches are no longer sufficient in and of themselves. Indeed, research from 451's Voice of the Enterprise survey on cloud computing in Q3 2015 shows that the security tools that are most important in the 'old world' – firewalls, anti-malware, etc., are less relevant in the cloud, while those security controls that are less popular – including identity management, DLP and encryption – become more so in the new world.

But as we have discussed previously, data security is not without its own challenges, primarily complexity (or at least the perception that data security is complex) but also lack of skilled staff. One of the ways the data security industry is beginning to address both complexity and the growing security skills shortage is via more services-based offerings, including DLP, encryption and key management all offered as a service. Another recurrent theme of 451's ongoing research and focus of our recent Trends in Information Security report is the need for more automation to help reduce both complexity and also lower the requirements for human capital in the security process.

It's also important to recognize that an effective and comprehensive data security strategy cannot be accomplished in a single step, but should be viewed as a journey. And given that data is now distributed across a broad array of applications, devices and resources, discovery is a good place to start. Despite the optimism of our earlier stats, nearly half of global respondents don't have a great handle on where all their data is located.

Once firms have a better idea of where their sensitive data may reside, applying more comprehensive data controls such as encryption would be a logical next step. However, encryption is no longer just for laptops, PCs and mobile devices. Regardless of which new technology is chosen – whether SaaS, IaaS, Big Data, IoT or containers, the preferred means of securing each of them was encryption.

Lastly, it's important to recognize that it's no longer enough to just check off compliance boxes. Indeed, new global privacy regulations such as GDPR carry extensive fines for non-compliance that could have serious financial consequences rather than just a slap-on-the-wrist. And firms who are concerned with data sovereignty and also either attacks on cloud service providers or privilege abuse should consider encryption with BYOK as an option.

RECOMMENDATION SUMMARY

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 for an additional layer of protection for data.
DISCOVER AND CLASSIFY	Get a better handle on the location of sensitive data, particularly for Cloud, Big Data, Containers and IoT.
DON'T JUST CHECK OFF THE COMPLIANCE BOX	Global and industry regulations can be demanding, but firms should consider moving beyond compliance to greater use of encryption and BYOK, especially for cloud and other advanced technology environments.
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. **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 Principal 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.

"A MAIN THEME OF 451 RESEARCH'S ONGOING ANALYSIS – AND THIS REPORT – IS THE MISALIGNMENT BETWEEN CURRENT THREATS AND THE APPROPRIATE DEFENSES."

ABOUT THALES E-SECURITY

Thales e-Security 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-premise, 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 e-Security is part of Thales Group.

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

THALES

www.thales-esecurity.com