451 Research®

Vormetric Data Security™

2016 VORMETRIC DATA THREAT REPORT

Trends in Encryption and Data Security

CLOUD, BIG DATA AND IoT EDITION

#2016DataThreat

TABLE OF CONTENTS

OUR SPONSORS

INTRODUCTION

The 'triumvirate' of cloud, big-data and the Internet of Things (IoT)[1] can each offer substantial benefits via their ability to generate, collect and use data in novel ways that can both help improve decision making and allow for more agile and adaptive business models.

Unfortunately, as we have seen with historical patterns of IT evolution, security considerations typically take a back seat to establishing a market presence, and only get their due either as as a way to remove barriers to adoption or plug holes after the damage is done. Not surprisingly, then, we have observed a fairly strong positive correlation over time between the maturity of a specific computing model or resource, and the ability to secure that resource - and cloud, big-data and IoT have followed a similar pattern.

As we noted in our recently published Vormetric Global Data Threat Report, to a large extent both security vendors and enterprises are like generals fighting the last war. While the storm of data breaches continues to crest, many remain focused on traditional defenses like network and endpoint security that are clearly no longer sufficient on their own to respond to new security challenges. This disconnect between the old ways of approaching security and the new security approaches required by modern threats is perhaps most evident when looking at emerging areas like cloud, big-data and IoT. Thus this more focused version of our global data threat report will explore the specific concerns security professionals have regarding these new environments ,and also look to provide some insight into how organizations are – and should – be thinking about securing them.

The 2016 Vormetric Data Threat Report is based on a survey conducted by 451 Research during October and November of 2015. We surveyed 1100 + senior security executives from across the globe, including key regional markets in the U.S., U.K. Germany, Japan, Australia, Brazil and Mexico, and in key segments such as Federal government, retail, finance and healthcare.

[1] ***Internet of Things (IoT) devices:*** *any non-PC, server, laptop or mobile phone that is connected to the public Internet to either monitor, collect data or perform a remote control function. IoT devices can include wearable devices (watches, heart rate monitors, etc.), appliances, medical devices, machinery, vehicles, sensors remote control systems, etc.*

"WITHIN THE NEXT 12 MONTHS, 85% OF ALL RESPONDENTS PLAN TO STORE SENSITIVE INFORMATION IN SAAS, PAAS OR IAAS APPLICATIONS OR ENVIRONMENTS."

EXECUTIVE SUMMARY

"70% of respondents were Very or Extremely concerned about security breachs at their cloud service provider."

Security still an afterthought

As noted above, when it comes to adopting new technologies, attention to security practices often take a back seat amidst the rush to stake a claim in a promising new market. Cloud, big-data and IoT have followed similar trajectories, and shoring up these new platforms will require a lot of work – much of which will exceed what many legacy security approaches like network and endpoint security can offer. That said, we are seeing encouraging steps, and not surprisingly, the current state of such efforts largely tracks the maturity of each category.

Cloud providers such as AWS, Box, Google, Microsoft and Salesforce, for example, are leading the way, via some combination of internal development, acquisitions and partnerships, along with a growing group of third-party security vendors with products specifically tailored for cloud environments. Big-data is newer on the scene, and security efforts are accordingly more nascent, but acquisitions by Cloudera and Hortonworks point to increasing awareness of the unique challenges of securing big-data. IoT has vast potential to transform our lives and the way we do business, though not surprisingly IoT security efforts are the least mature, both by member of the IoT ecosystem, as well as third-party security vendors.

In general, the data from our survey reflect similar patterns. For example, when asked where they were most likely to store sensitive data, SaaS (53%), big-data (50%) and IoT (33%) were ranked in descending order as the top three responses. Similarly, regarding what resources were most at risk for loss of sensitive data, databases (54%) and file servers (41%) were the #1 and #2 answers overall, while in terms of emerging categories, SaaS (26%), big-data (21%) and IoT (18%) were the top 3 choices.

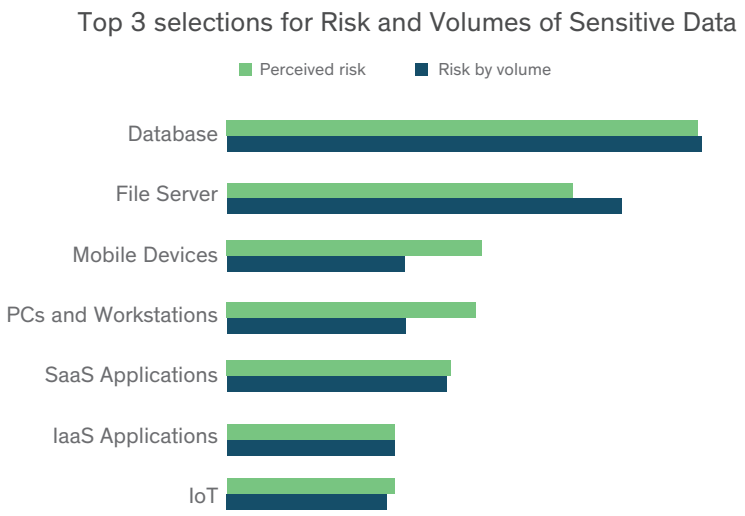

Figure 1: Perceived risk and risk by volume of sensitive data

As noted earlier, a lot of work – and education - needs to be done before we can genuinely feel confident that we are making the right decisions, and when it comes to emerging technologies, the same can be said of enterprise customers. In our global report, we noted that most security executives across the globe still appear to equate compliance with security - nearly two-thirds (64%) viewed compliance requirements as either 'very effective' or 'extremely effective' in preventing data breaches. Equally shocking was that 43% claimed to have 'complete knowledge' of the location of their sensitive data, which contradicts the post-mortems of many publicized data breaches, and is an issue that will likely become more of a challenge as big-data and IoT proliferate – it's worth noting that discovering sensitive data generated by IoT devices was identified as a top concern. Along similar lines, one of the primary concerns about public cloud services remains breaches or attacks at the cloud service provider. Though attacks on cloud providers are rare and most of the latter arguably do a better job of securing their infrastructure than most enterprises, over 70% of respondents were either 'very concerned' or 'extremely concerned' about the potential for such attacks.

On a positive note, we found responses to what are the top choices for securing public cloud environments more encouraging. The number one choice by a wide margin in the 2016 survey was to encrypt data with customer controlled keys, outnumbering encryption with keys managed by the service-provider by a nearly 60%/40% ratio. However, only 33% of respondents indicated they are applying encryption to their big-data environments.

Overall, our Cloud, big-data and IoT report contains a similar mix of encouraging and not-so-encouraging results to those highlighted in our global data threat report. And like that report, the results emphasize that as an industry, we are still focusing too much of our collective energy on fixing yesterday's problems. And while there are positive signs that we are moving in the right direction, there are still hurdles to be overcome. For example, in our global report, we noted that 57% of respondents cited 'complexity' as the main barrier to adoption for data security, with lack of staff to manage (38%) a distant second – both of which could be exacerbated as cloud, big-data and IoT assume a greater piece of the IT landscape. If data security hopes to emerge from the shadow of its network and endpoint security peers, the implicit message for data security vendors is to make products that are simpler to use, require less manpower to implement and maintain, and are applicable across a broader variety of use cases.

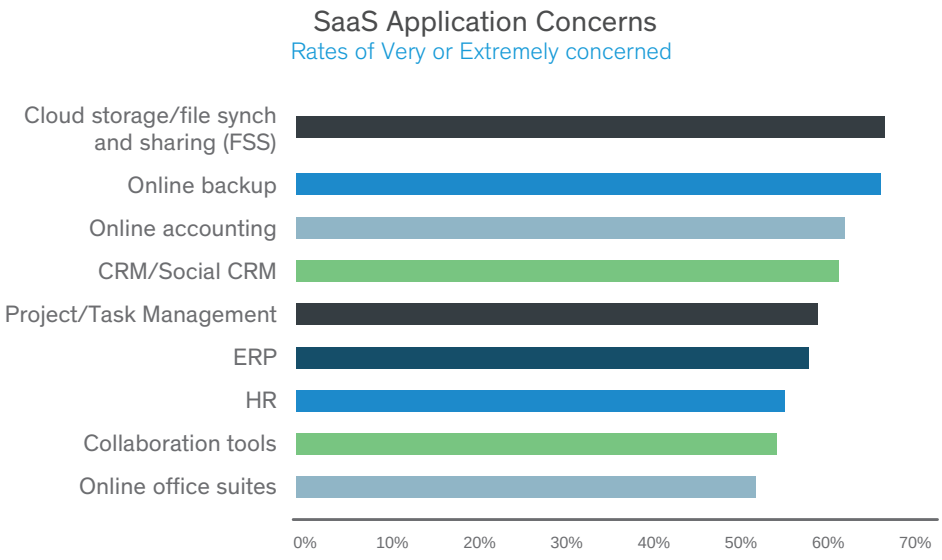

Figure 2: Rates of concern in SaaS applicationss

"57% OF RESPONDENTS CITED 'COMPLEXITY' AS THE MAIN BARRIER TO ADOPTION FOR DATA SECURITY."

KEY FINDINGS:

Overall Sensitivity to Data Loss

- 39% of all respondents identified Cloud as one of the locations which would experience the greatest amount of sensitive data loss as a result of a breach.
- 25% of all respondents identified Big Data as one of the locations which would experience the greatest amount of sensitive data loss as a result of a breach.
- 17% of all respondents identified IoT/smart devices as one of the locations which would experience the greatest amount of sensitive data loss as a result of a breach.

Planned Adoption

- Within the next 12 months, a majority (85%) of all respondents plan to store sensitive information in SaaS, PaaS or IaaS applications or environments.
- Within the next 12 months, half (50%) of all respondents plan to store sensitive information in Big Data environments.
- Within the next 12 months, a third (33%) of all respondents plan to store sensitive information in IoT implementations.

Top Security Concerns for Emerging Technologies

- Though attacks on cloud providers are rare and most of the latter arguably do a better job of securing their infrastructure than most enterprises, over 70% of respondents were either 'very concerned' or 'extremely concerned' about the potential for such attacks.
- While privileged users were viewed as the number one insider risk for sensitive data overall, with respect to cloud specifically, respondents were almost equally concerned with the risk of using shared cloud infrastructure, visibility into the security measures of the cloud provider, lack of control over the location of data and privacy policies.

The top three data security concerns for Big Data implementations across all respondents are:

- Security of reports that may include sensitive data (42%)
- Sensitive information may reside anywhere within the environment (41%)
- Privacy violations from data originating in multiple countries (40%)

The top three data security concerns of IoT technologies across all respondents are:

- Protecting sensitive data generated by an IoT device (encryption, tokenization, etc.) (35%)
- Privacy violations related to data generated by an IoT device (30%)
- Identifying or discovering data generated by an IoT device that may be sensitive (29%)

"48% OF ENTERPRISES WOULD INCREASE CLOUD USAGE IF THE SERVICE PROVIDER USED ENCRYPTION, AND ALLOWED THE ENTERPRISE TO MANAGE THE KEYS."

CLOUD, BIG DATA, & IOT – NEW SECURITY CHALLENGES

> *"Historically, security has been treated by developers as an afterthought."*

Much has been made of the unique security challenges posed by the triumvirate of Big Data, IoT and cloud computing. Since the latter two take advantage of resources that largely exist outside of traditional enterprise boundaries, legacy security tools and approaches that rely on a hardened perimeter to enforce existing notions of 'internal' vs. 'external' have limited applicability in the new world order. At the same time, security concerns repeatedly show up as one of the leading barriers to more broad adoption of these new computing models.

Historically, security has been treated by developers as an afterthought. In the rush to stake a claim in an exciting new market, products are often sent to market without investing sufficient effort into ensuring the security of the underlying hardware and software, as well as the data that flows through the. Common sense would dictate that if you build a fragile ship and expect to fix the leaks as they appear, you're bound to take on water.

Considering the numerous security flaws found in many well-known internet routers as a recent example, the tacit assumption has been that the burden of securing such devices and data is ultimately borne by the end user. Only when such weaknesses are exploited and data is compromised is security given real consideration, typically bolted on in a reactionary way. The same unfortunate pattern has repeated itself throughout the evolution of IT , beginning with the introduction of client-server, and repeated again with web-based computing in the mid-2000s.

Given the historical context, it's not surprising that when we consider security for emerging computing models, a maturity model is relevant. For example, a large number of respondents to our survey still view legacy resources such as databases (54%) and file servers (41%) as being at the greatest risk of losing sensitive data. Similarly, concerns about cloud computing, big-data and IoT tend to be highly correlated to their maturity levels and stage of adoption. Within the next 12 months, a majority of respondents (85%) plan to use SaaS, PaaS and IaaS environments to store sensitive or regulated data, while for big-data and IoT, those percentages drop off quite sharply, to 50% and just over 30%, respectively. As enterprises begin to store even more sensitive information in these new environments, including containers, we can expect that these plans to grow accordingly.

Planned Adoption Levels

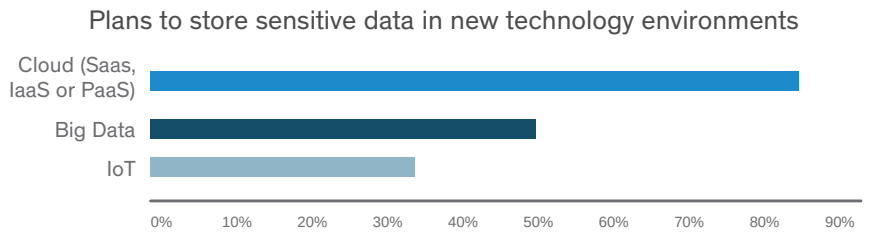

Figure 3: In which of the following new technology environments, if any, does your organization currently store sensitive or plan to store regulated data in the next 12 months?

When asked which locations would experience the greatest amount of data loss in the event of a breach, there was again a strong correlation between adoption rates. Databases and file servers were still the top choices, while cloud apps and Big Data were each ranked third overall, and lead the pack among the various 'next-gen' architectures. Although there is a burgeoning cottage industry devoted to securing SaaS applications, Big Data's showing was a bit of a surprise, and mainly attributable to the dominance of U.S. respondents in the sample, and particularly among financial services firms – most other countries that have been slower to adopt big-data ranked it much lower.

"Though 85% plan to store sensitive or regulated data in public cloud environments, they still have reservations."

Top Cloud Security Concerns

Though 85% plan to store sensitive or regulated data in public cloud environments, as noted above, they still have reservations. One of the primary concerns about public cloud services remains breaches or attacks at the cloud service provider. Though attacks on cloud providers are rare and most of the latter arguably do a better job of securing their infrastructure than most enterprises, over 70% of respondents were either 'very concerned' or 'extremely concerned' about the potential for such attacks. It's also worth noting that while privileged users were viewed as the number one insider risk for sensitive data overall, with respect to cloud specifically, respondents were almost equally concerned with the risk of using shared cloud infrastructure, visibility into the security measures of the cloud provider, lack of control over the location of data and privacy policies.

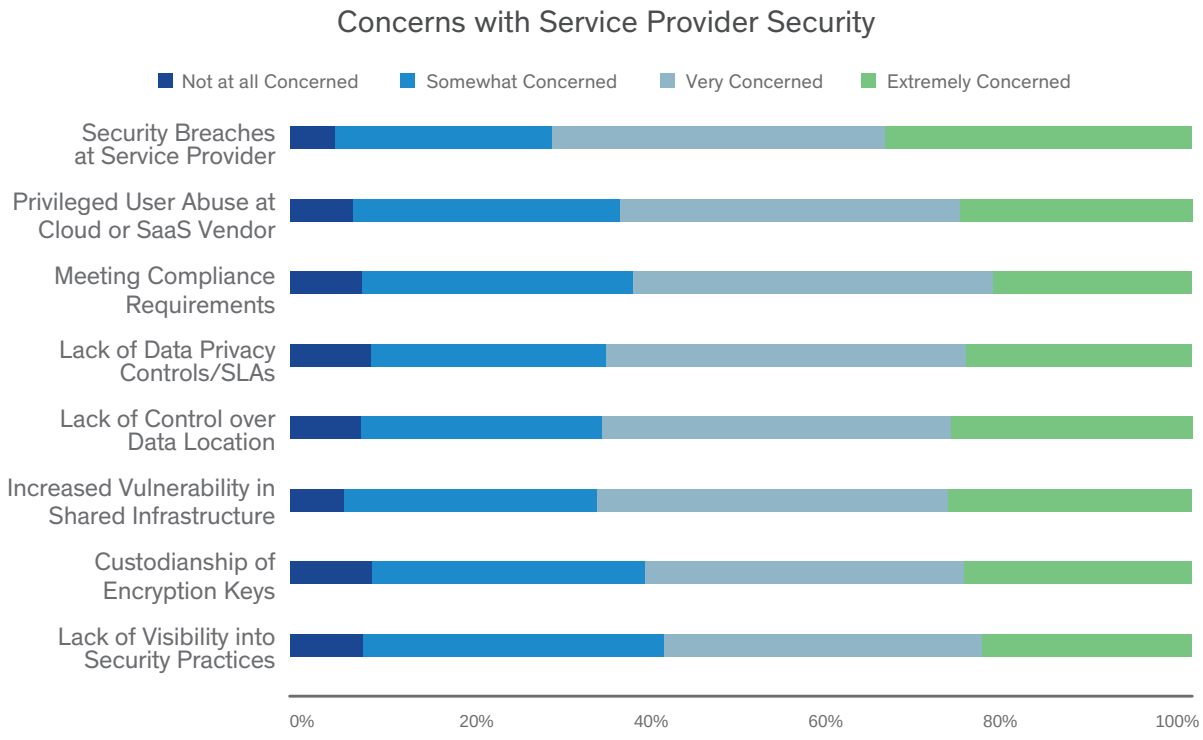

Figure 4: How concerned are you about the following data security issues as they relate to public cloud services?

ENCRYPTION COULD EASE CLOUD SECURITY CONCERNS

So what are respondents' top choices for addressing their concerns about public cloud? Encrypting sensitive data stored at cloud providers has emerged in recent years as a top consideration for addressing cloud security concerns, and 451 Research expects that over the coming years, all cloud providers housing sensitive enterprise data will have to offer encryption services to be considered viable options.

This year's data once reflects that view, though, one key issue that is shaping up to be critical in terms of security for SaaS applications is encryption key management, and more specifically, whether the service provider or the customer maintains control over the keys. Interesting test cases were presented earlier this year as both Salesforce and Box launched their own native encryption solutions., with Box offering customers the ability to maintain administrative control over encryption keys, and Salesforce's Shield service offering only a vendor-controlled option.

Maintaining local control over keys is a critical requirement for many compliance mandates, and so not surprisingly the number one choice by a wide margin in the 2016 survey was to encrypt data with customer controlled keys, outnumbering encryption with keys managed by the service-provider by a nearly 60%/40% ratio.

Further, while deploying encryption with service provider control over keys was the third-ranked option at 35%, the gap between the two deployment options for key management is widening in favor of local control – last year's survey elicited nearly identical responses for both options. We anticipate the gap between the two key management options will continue to widen over time, and thus foresee more cloud providers offering encryption with local key management as an inducement to attract more customers. We also see an increased role for more granular access controls as some of the emerging vendors that 451 refers to as 'Cloud Application Control' (CAC) or others refer to as CASB vendors.

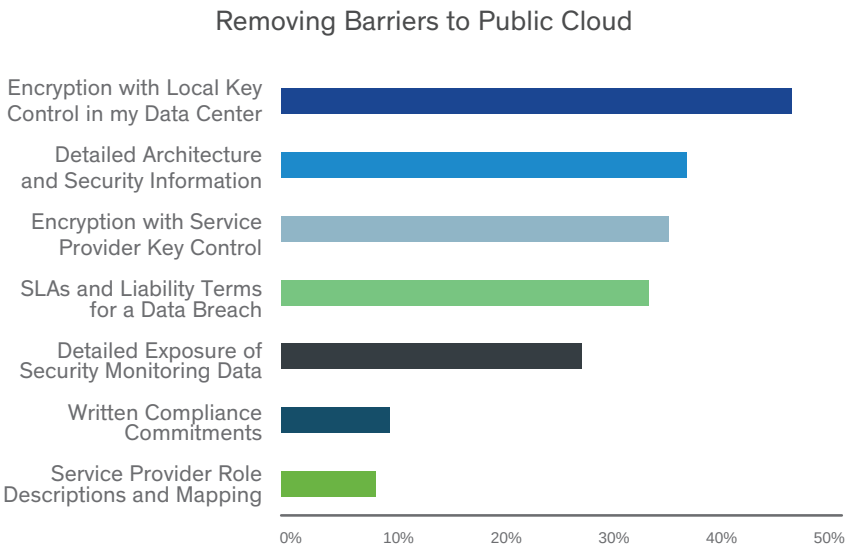

Figure 5: What would increase your willingness to move use a public cloud service?

"ONE KEY ISSUE THAT IS SHAPING UP TO BE CRITICAL IN TERMS OF SECURITY FOR SAAS APPLICATIONS IS ENCRYPTION KEY MANAGEMENT."

BIG DATA

> ***"50% of all respondents plan to store sensitive information in Big Data environments within the next 12 months, though big-data was selected by only 18% of respondents as one of the locations most at risk for loss of sensitive data."***

As noted earlier, for most architectural shifts in IT, security is often an afterthought, and the evolution of 'big data' has followed a similar tack. As adoption of Big Data increases globally, organizations will be housing a growing share of sensitive data in these environments. Vendors and service providers alike have been scrambling to add an element of security to their offerings, hoping to entice customers to move their big-data workloads out of test and development and into production.

From a security perspective, the 'three Vs' of big data – volume, velocity and variety – present several new challenges when it comes to protecting sensitive data. For starters, the velocity of big data requires tools that can operate at line speed and don't introduce latency. Furthermore, given the sheer volume of data created, customers may often be completely unaware of potentially sensitive personally identifiable information (PII) residing within a Hadoop cluster, or where it may be located. For example, a company may want to do analytics on a click stream from a social media site or on a Twitter feed, but may have no idea if the data contains Social Security numbers or other PII.

And while it may be hard enough to know where your sensitive data is located, it's even harder to classify it and determine its level of sensitivity, particularly when it is constantly changing. As an example, data that might not normally be considered sensitive might become so once it has been applied to a big data experiment and yields results that may be highly proprietary.

The obvious question, then, is what is being done to ensure the security of this sensitive data? Do organizations even understand what it will take in order to keep the data stored and/or generated in these environments safe? What are organizations most concerned about when it comes to securing big-data?

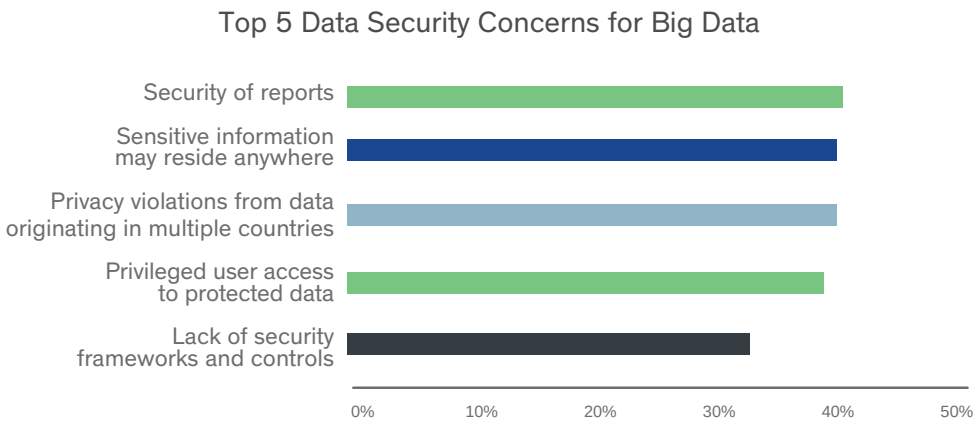

Figure 6: Data concerns, ranked highest to lowest, all responses

As noted earlier, 50% of all respondents plan to store sensitive information in Big Data environments within the next 12 months, though big-data was selected by only 18% of respondents as one of the locations most at risk for loss of sensitive data. The top three global concerns regarding security for their organization's Big Data implementations were the security of reports that may include sensitive data (42%), the knowledge that sensitive information may reside anywhere within the environment (41%) and the possibility of privacy violations from data originating in multiple countries (which

speaks to growing global concerns about data sovereignty addressed in our global report). One of the unique challenges of big-data is locating and identifying data that might be sensitive, yet discovering sensitive data in a big-data environment was the second-lowest ranked concern, chosen by just 23% of respondents.

In addition to effective access controls, encryption would be a logical starting point for helping address big-data security concerns, though only 33% of respondents indicated they are applying encryption to their big-data environments. We suspect this may speak to not only the early stage of adoption of big-data, but more likely the 'double jeopardy' that big-data environments typically present - the difficulty of difficult of identifying which data should be encrypted, on one hand, as well as the sheer volume – and variety - of big-data deployments on the other. In an extreme, but increasingly common example, big-data experiments can be run in public cloud environments, which can add additional complexity and thus additional risks to the equation.

"Only 33% of respondents indicated they are applying encryption to their big-data environments."

INTERNET OF THINGS (IOT)

Though IoT promises to present a security hurdle of epic proportions, security concerns likewise reflect IoT's early stage of adoption. With the exception of Australia, most regions currently see little risk from data generated by IoT devices, and given the sheer volume of devices that are anticipated, securing sensitive data generated by IoT devices is the primary concern of most security professionals (36%), as well as privacy violations related to data generated by IoT devices (30%). And while most recipients expressed overall confidence in their ability to locate their sensitive data, with respect to IoT specifically, discovering sensitive data generated by IoT devices is a top concern and only slightly trails the prior concerns

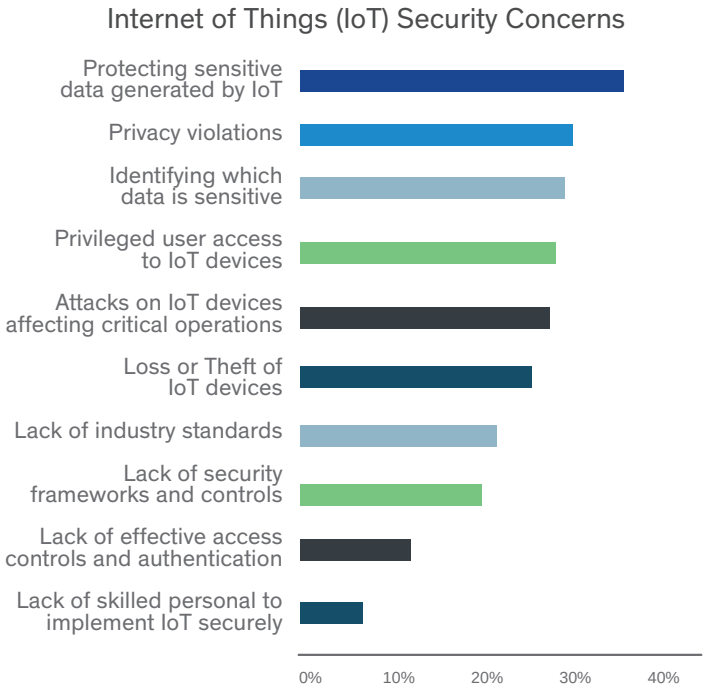

Figure 7: Security concerns by category

CLOUD, BIG DATA AND DATA SOVEREIGNTY DRIVING BROADER POTENTIAL USE CASES FOR ENCRYPTION

"Given the risks, why isn't encryption a higher priority, and why hasn't it been deployed more broadly through most enterprises? "

As noted below, products that can directly help mitigate data theft – data-in-motion and data-at-rest defenses such as encryption - were near the bottom of the list in terms of overall spending intentions at 40% and 39%, respectively. (Figure 4) also noted above and in our global data threat survey, encryption is still most frequently applied to things like PCs, laptops, hard drives and emails. These stats beg the following questions: why isn't encryption a higher priority, and why hasn't it been deployed more broadly through most enterprises?

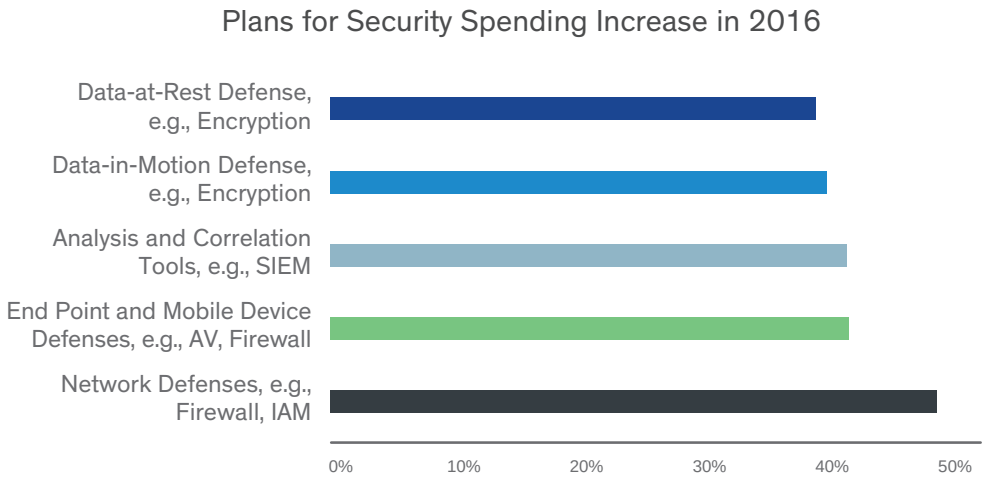

Figure 8: Spending increases for 2016

As we will discuss in more detail below, one of the barriers to more widespread adoption of encryption has been existing perceptions about complexity, as well as costs and potential staffing requirements. As with most areas of security, a tradeoff applies with encryption as well – the greater the degree of protection, the greater the added cost and complexity. And as we will discuss below, a related issue is the sheer number of varieties of encryption and potential use cases that may call for encryption, adding more complexity to the mix.

Broadly speaking, encryption has traditionally been broken down into two high-level groups: data-in-motion, and data-at-rest. Data-in-motion defenses are used to protect the transmission of data between networks, and include virtual private networks (VPNs) - long a staple of most firms' security arsenals - that rely on rely on either Internet Protocol Security (IPSec) or Secure Sockets Layer (SSL) encryption, as well as Secure Shell (SSH) and the embedded web security protocol HTTPS. Data-at-rest defenses include an even broader variety of technologies and use cases that can range from full disk encryption for protecting laptops and hard drives from loss or theft, to file-level encryption and access controls to address system-level attacks and insider privilege abuse, and finally to application layer controls such as encryption, tokenization and data masking to protect against higher-level attacks such as Structured Query Language(SQL) injection and rogue database administrators. Additionally, many of the aforementioned products currently available are also designed for specific platforms or operating systems.

That complexity can be magnified when cloud, big-data and IoT are added to the mix. With cloud, for example, different potential encryption scenarios exist for each of the various cloud architectures that require varying levels of integration work. For example, IaaS and PaaS providers often provide file or folder-level encryption, either natively or via a third-party partner, and offer several options for key management. SaaS applications, on the other hand, are a bit more challenging since the SaaS provider controls the entire stack and file and folder-level encryption aren't really a viable option. Most SaaS encryption models are applied at the application layer, and either require the encryption to be directly baked into the application by the service provider, or rely on an external proxy gateway that onboards some of the application logic

for crypto processing. And there are various methods for handling encryption keys – as noted above, encryption with customer-managed keys and service provider-managed keys were the #1 and #3 in terms of removing barriers to cloud adoption, though the preference for the former seems to be growing.

To add to that complexity, many existing SaaS encryption solutions have been architected to address a single, or at most a few SaaS applications, and the same generally holds true for big-data. Of the few big-data encryption offerings that currently exist, most target specific fields or columns are are commonly focused on Hadoop, though some solutions are also incorporating data discovery as well as role-based access controls and secure communications with other applications. And with IoT, there is the potential to deploy encryption thoughout the entire implementation – IoT devices, communications between devices and back end servers, as well as during storage and processing operations. The end result is that when considering both the varied requirments of both cloud and big-data environments, many firms that would like to adopt a more comprehensive encryption strategy have been forced to deal with a growing assortment of point products and vendors.

Still, several factors suggest the sands are slowly shifting towards more widespread use of encryption and related techniques. For one, as we've argued earlier, traditional security tools are no longer doing a good enough job, and across the industry, there is growing recognition that multi-layer attacks will eventually succeed at penetrating even the most hardened networks. Second, as we noted earlier, further adoption of public cloud resources and big data will provide data-at-rest encryption with a higher place of prominence given the limitations of legacy security tools in environments where enterprises no longer control the underlying resources upon which they are built.

Thus it's not surprising to us that the data security technologies with the largest plans to implement were application layer encryption (40%), tokenization and MFA (39%), and cloud encryption gateways (38%), each of which is particularly suitable for addressing cloud, big data and also data residency/sovereignty use cases (Figure 9).

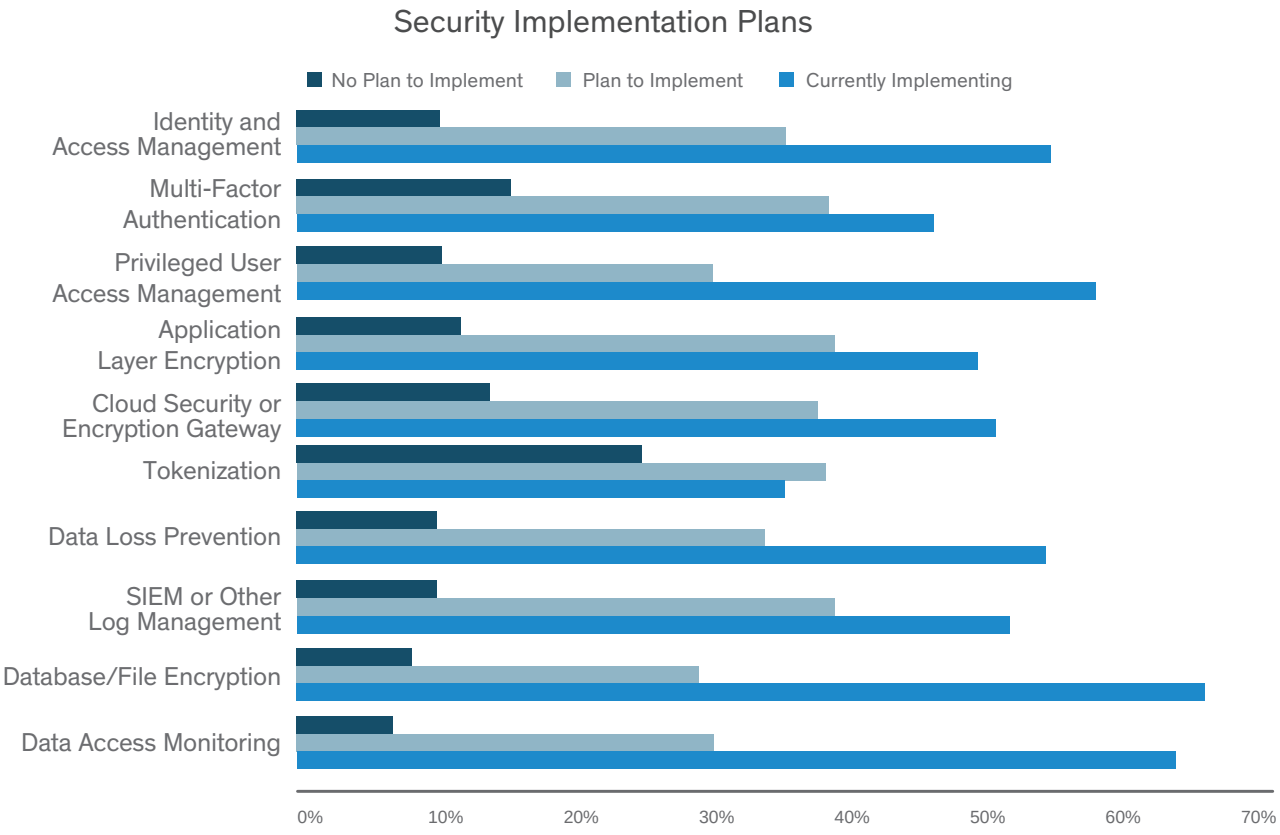

Figure 9: Plans to implement security

RECOMMENDATIONS

The past few years have been challenging ones for the information security industry as a whole, and nearly everyone has been affected – end users, enterprises and security vendors alike. If we have learned anything in that time, it is that our old ways of doing business and securing our resources are no longer working as they once did. As they saying goes, if you have a hammer, everything looks like a nail, and if you have a networking background, it's tempting to try to address new security challenges by adding another firewall, IPS, WAF or other network-based tool. To use another metaphor, Albert Einstein's oft-used quote is fitting – if doing the same thing over and over and expecting a different result isn't the definition of insanity, it is certainly a recipe for placing your critical assets at risk.

"As firms grow to accept the limitations of traditional security approaches, data security is likely to become a more critical component of a comprehensive security strategy. "

So where do we go from here? There is a considerable amount of innovation taking place in the security industry, and 451 Research is tracking a lengthy list of vendors that are applying new techniques to prevent attacks as well as detect potential threats and narrow the window of exposure. That said, none of these emerging techniques can offer a silver bullet, particularly as cloud, big-data and IoT present their own unique security challenges.

As firms grow to accept the limitations of traditional security approaches, data security is likely to become a more critical component of a comprehensive security strategy. But, as we have discussed, data security is not without its own challenges, many of which are magnified when considering emerging technologies like cloud, big-data or IoT. For starters, we believe firms need to get a better handle on where their sensitive data is located, and what its level of sensitivity might be so that the appropriate securities can be put in place. Thus we see the ability to discover and classify data growing in importance as data is increasingly distributed beyond the enterprise network confines and across cloud, big-data and IoT environments.

While things like better discovery of sensitive data can apply across all categories in varying degrees, the subtle differences among cloud, big-data and IoT may warrant slightly different approaches. Thus in the following sections, we will offer a few brief recomndations that are relevant to each environment.

Cloud

As noted earlier, a total of 83% of all respondents indicated that encryption would increase their organization's use of public cloud services (SaaS, IaaS or PaaS), either with keys controlled by the customer or by the service provider. As such, 451 Research expects that within the coming years all cloud providers housing sensitive enterprise data will need to offer encryption services to be considered viable options, and thus we expect to see a growing variety of both native and third-party encryption options. Enterprises will need to consider internal security policies, industry best practices and applicable compliance mandates to determine the best option, though we anticipate a growing preference for customer-managed keys over time.

Big-data

As noted above, the highly distributed nature of big-data highlights the importance of sensitive data discovery. It also points to the need for broad-based encryption and access control solutions that can span both traditional data repositories, as well as multiple big-data platforms such as Hadoop, NoSQL and others and a variety of deployment options. In addition to standard encryption, format-preserving or field-level encryption as well as data masking might also be viable choices for certain situations where either data needs to be protected but not restored to its original value, or only specific components need protection.

IoT

Given that IoT devices were identified as one of the primary intial IoT security concerns, a good starting point would be a focus on device authentication and access controls to the devices themselves, as well as encrypting data on and in transit from such devices. And since all data ultimately finds its way to a database, back-end systems should also be built to include both fine-grained access controls and encryption. In addition, given the vast amounts of data that could theoretically be generated by IoT devices and platforms, enterprises would be well-served to develop corporate policies that clearly delineate what will be collected, who will have access, how the data is used, and how long it will be retained.

Lastly, we suggest enterprises explore, in addition to encryption, new security analytics techniques that can offer an extra layer of protection above and beyond what encryption alone can provide. For example, 451 is following new developments in threat analytics and techniques to monitor data access patterns that can establish baselines of 'normal' activity which can be used to identify potential breaches and provide a greater degree of visibility into potentially compromised resources.

CLOUD	Encrypt sensitive data stored in the cloud. Internal policies, industry best practices and compliance mandates should determine the best options for key management.
BIG-DATA	Look for broad-based encryption and access control solutions that can span traditional data repositories, as well as multiple big-data platforms.
IOT	Focus on device authentication and access controls to IoT devices, as well as encrypting data on and in transit from such devices.

METHODOLOGY

- The data in this study (with the exception of Figure 3) is based on web and phone surveys of 1,114 senior IT executives with influence on or responsibility for IT security purchases in their organizations.
- Respondents represented a representative range of company sizes, from $50 million U.S. to $2 billion-plus U.S.
- There was also a representative sample of vertical industries.
- 451 Research conducted the surveys in October and November of 2015.

ANALYST PROFILE

Garrett Bekker is a Senior 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
Senior 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 VORMETRIC

Vormetric's comprehensive high-performance data security platform helps companies move confidently and quickly. Our seamless and scalable platform is the most effective way to protect data wherever it resides–any file, database and application in any server environment. Advanced transparent encryption, powerful access controls and centralized key management let organizations encrypt everything efficiently, with minimal disruption. Regardless of content, database or application–whether physical, virtual or in the cloud–Vormetric Data Security enables confidence, speed and trust by encrypting the data
that builds business.

Please visit **WWW.VORMETRIC.COM** and find us on Twitter **@VORMETRIC**.

Vormetric Data Security™

Vormetric.com/DataThreat/2016