TABLE OF CONTENTS

INTRODUCTION 3
EXECUTIVE SUMMARY 5
  Key Findings 7
CLOUD, BIG DATA, IoT AND CONTAINERS:
  DRIVING CHANGE, CREATING COMPLEXITY 8
  Cloud 9
  Big Data 11
Internet of Things 11
Dockers/Containers 13
RECOMMENDATIONS 14
INTRODUCTION

Cloud, Big Data, the Internet of Things (IoT) and increasingly container technology are all being actively embraced, and collectively pack a potentially disruptive punch to the basic ground rules of venerable businesses.

But at the same time, these technologies place more sensitive data in the hands of more people, in more places, and on an ever-increasing number of devices. The inevitable results are greater security vulnerabilities, which are in turn directly linked to the annual uptick in breaches observed in the 2017 Thales Data Threat Report. Not surprisingly, nearly two-thirds (63%) of respondents admit that their organizations deploy new information technologies prior to having appropriate data security measures in place. Indeed, as we observed in the 2016 version of the report a year ago, establishing a market presence typically takes precedence over adequate security provisions amid the rush to deploy new technologies.

Not only that, but spending on security solutions continues to favor infrastructure that is more aligned with the way things used to be done rather than the emerging modus operandi. The biggest spending increases globally this year will go to beefing up network defenses (62%) and endpoint security (56%). Yet sensitive data is increasingly moving beyond internal network boundaries, to the cloud, mobile devices and to the looming Internet of Things (IoT) where perimeter-based security is increasingly less relevant.

Security Professionals Say Their Organizations Are Implementing Advanced Technology Without Data Security

93% Of Organizations Using Sensitive Data In Advanced Technology Environments
Rates of Sensitive Data Use by Advanced Technology Type

“nearly two-thirds (63%) of respondents admit that their organizations deploy new information technologies prior to having appropriate data security measures in place.”
This technology-focused global data report is based on a survey of 1,105 senior security executives across the globe and will take a closer look at these fast-emerging technologies and the concerns prompted by security professionals. The report will also provide insights into how organizations should change course when it comes to securing them.

“SPENDING ON SECURITY SOLUTIONS CONTINUES TO FAVOR INFRASTRUCTURE THAT IS MORE ALIGNED WITH THE WAY THINGS USED TO BE DONE RATHER THAN THE EMERGING MODUS OPERANDI.”
**EXECUTIVE SUMMARY**

Where it comes to deploying the hottest contemporary technologies geared to effecting major changes in both business and IT, it’s a matter of “deploy first, secure later.” That is the clear message echoed in this year’s report, wherein 63% of respondents globally said their organizations are deploying new technologies without first ensuring they are secure. Technologies in this case include cloud (and various public cloud implementations of SaaS); Big Data; IoT; and Containers.

The concern over unsecure deployments is felt most strongly in global retail and in Brazil (both 80%); Mexico (75%); Australia (74%); and in global financial services (73%). Interestingly, U.S. financial services senses this potential threat the least (47%). This finding could reflect the very rigorous financial services compliance and regulatory environment in the U.S., which can be more detailed in spelling out security requirements than some other nations.

The main barrier to adopting better data security globally is the complexity of doing so (50%), particularly as sensitive data increasingly moves beyond corporate firewalls and network perimeter defenses as well as into the devices of more and more users. A distant second to complexity is lack of staff (36%), which is likely to worsen over time as cyber threats gain more attention and competition for security professionals becomes super-heated.

Good news is reflected in security spending plans, where nearly three quarters (73%) of respondents anticipate spending more on security in 2017. This is a significant increase over the 59% of respondents in last year’s Thales report. The flip side of the coin shows that data breaches are also on the rise, with 26% of global respondents citing breaches in the previous year compared with 20% the year prior. Small wonder then that 88% of respondents feel some degree of vulnerability to their sensitive data, albeit a slight decline from last year.

**IT Security Spending Is Up – And So Are Data Breaches**

**Part 1** Increasing IT Security Spending in The Next 12 Months

<table>
<thead>
<tr>
<th>Year</th>
<th>0%</th>
<th>20%</th>
<th>40%</th>
<th>60%</th>
<th>80%</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Part 2** Global Data Breach Rates

- Experienced a data breach in the past
- Had a data breach in the last year

2017 2016

0% 10% 20% 30% 40% 50% 60% 70%
The growing availability of encryption and encryption key management, particularly ‘Bring Your Own Keys’ (BYOK), is easing concerns about cloud services, with 61% globally (66% in the U.S.) saying encryption with a BYOK option would boost their willingness to deploy sensitive data to public clouds.

Without question, encryption and tokenization are seen as the top choice for securing emerging environments such as SaaS (61%); IoT (56%); and in addressing concerns over data sovereignty (64%).

Encryption and Tokenization Are the Top Choices to Secure Advanced Technologies and Quell Concerns Over Data Sovereignty

Part 1 Encryption Availability Would Increase Enterprise Adoption of Advanced Technologies

Part 2 Encryption The Top Method Planned to Meet Data Privacy and Data Sovereignty Regulations
KEY FINDINGS:

- Although three-quarters (73%) of respondents globally are spending more on security this year than last (compared with just 59% last year), data breaches continue to rise – up 30% year to date. And feelings of vulnerability remain high – 88% report feeling some degree of vulnerability, down slightly from 90% last year.

- Organizations continue spending most heavily on network defenses (62%) and endpoint security (56%), while attackers increasingly target security weaknesses outside the corporate firewall.

- Nearly-two thirds (63%) of respondents feel their organizations are deploying new technologies before they are adequately secured. Yet 57% plan to store sensitive data in Software-as-a-Service (SaaS), 49% in Infrastructure-as-a-Service (IaaS), and 44% in Platform-as-a-Service (PaaS).

- While compliance (44%) remains the top reason for IT security spending, increased cloud use within the organization (a new option for this year’s report) debuts in the #3 spot with 35%.

- Surprisingly, four in ten respondents (40%) already use Containers for production applications, and nearly one in five (19%) respondents globally will store sensitive data in Containers. Like cloud, Big Data and IoT, security is the main barrier to container adoption (47%).

- Encryption and tokenization are the top choices for securing sensitive data in public cloud (61%), IoT (36%) and Containers (53%). For public cloud, encryption with customer-managed keys (61%) is preferred by a wide margin over encryption with service-provider managed keys (48%).

- Encryption (64%) is also the clear choice globally for protecting sensitive data subject to data sovereignty requirements such as the upcoming GDPR, with tokenization a distant second (40%). Surprisingly, organizations are less likely to migrate data to new locations to comply with such requirements (36%) and, even less likely (26%) to leverage local cloud providers to meet sovereignty regulations.

“NEARLY-TWO THIRDS (63%) OF RESPONDENTS FEEL THEIR ORGANIZATIONS ARE DEPLOYING NEW TECHNOLOGIES BEFORE THEY ARE ADEQUATELY SECURED. YET 57% PLAN TO STORE SENSITIVE DATA IN SOFTWARE-AS-A-SERVICE (SAAS), 49% IN INFRASTRUCTURE-AS-A-SERVICE (IAAS), AND 44% IN PLATFORM-AS-A-SERVICE (PAAS).”
CLOUD, BIG DATA, IOT AND CONTAINERS: DRIVING CHANGE, CREATING COMPLEXITY

You likely wouldn’t use an ATM if you felt the machine was not secure. Yet 63% of global respondents are concerned their organizations are deploying advanced technologies without assurances that sensitive data will be protected. Indeed, data from the global Voice of the Enterprise study from 451 Research shows that the percent of all workloads running in SaaS will leap from 12% in 2016 to 20% in 2018, while workloads deployed to IaaS will double from 6% to 12% - underscoring the considerable appetite for public cloud deployments. And what they are most concerned about are deployments of sensitive data to public cloud: SaaS (55%); IaaS (49%); and PaaS (46%).

Securing SaaS data - as well as sensitive data in IoT, Big Data and Containers - carries the added challenge of gaining control of data outside the boundaries of the legacy infrastructure and its security framework. This is certainly true of IaaS offerings such as AWS or Azure, where security is generally a shared responsibility between the enterprise and the cloud provider. SaaS is perhaps the most extreme case, and presents new security challenges since enterprises have little ability to touch, manage or make modifications to a SaaS providers’ resources. Security thus becomes a main barrier to more aggressive adoption of advanced technologies.

Concerns notwithstanding, respondents globally are charging ahead with plans this year to store and access sensitive data on SaaS (57%); Big Data platforms (47%); IaaS (49%); PaaS (44%); IoT devices (31%); and even the very young container environment (19%).

---

Advanced Technologies Use For Sensitive or Regulated Data Storage
Percentage of respondents whose organizations store sensitive data in the following environments

<table>
<thead>
<tr>
<th>Environment</th>
<th>2017</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IaaS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PaaS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Big Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IoT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Containers</td>
<td>Not Measured</td>
<td></td>
</tr>
<tr>
<td>Block Chain</td>
<td>Not Measured</td>
<td></td>
</tr>
</tbody>
</table>

---

"Voice of the Enterprise study from 451 Research shows that the percent of all workloads running in SaaS will leap from 12% in 2016 to 20% in 2018, while workloads deployed to IaaS will double from 6% to 12%.”

"Respondents globally are charging ahead with plans this year to store and access sensitive data on SaaS (57%); Big Data platforms (47%); IaaS (49%); PaaS (44%); IoT devices (31%); and even the very young container environment (19%)."
CLOUD

The movement to cloud globally is akin to a giant boulder rolling downhill, inexorably gathering momentum. 451 Research’s Voice of the Enterprise 2016 study revealed that the 40% of all enterprise workloads globally deployed to the cloud in 2016 will jump to 57% by 2018 – an increase of 42%. As mentioned in the section above, deployments to public cloud SaaS and IaaS platforms will experience particularly rapid growth at a time when concerns about security of the public cloud continue to linger. This is reinforced by one of the major findings in the 2017 Thales Data Threat Report: nearly two thirds of organizations (63%) are deploying advanced technologies ahead of having adequate security measures in place.

To be sure, protecting data in public cloud environments has unique challenges for enterprises, primarily dealing with an off-premises, shared environment where they no longer maintain 100% control. That said, data breaches at cloud service providers to date have been rare, and generally not serious. Most major cloud providers have larger staffs of highly trained security professionals than any enterprise, and their scalability and redundancy can provide protection from the kinds of DDOS attacks that can plague on-premises workloads.

Perhaps because of the recognition of these public cloud security realities, security concerns overall for public cloud are waning. For example, global data protection concerns for the most common SaaS applications such as cloud storage/file synch, online backup, and project management all fell significantly in the 2017 Thales Data Threat Report compared with a year ago. And those respondents listing “service provider security breaches” as a top concern fell to 59% this year globally compared with 70% in last year’s survey. While vulnerabilities from shared infrastructure (57%) was listed as the #2 public cloud security concern, data sovereignty followed at 55%. It’s perhaps noteworthy that compliance ranked at the bottom of the list of concerns, possibly reflecting growing confidence in public cloud.

![Data Security Concerns for Public Cloud Services](image-url)
Still, while concerns about cloud security are dropping, they are still significant. Security remains a top barrier to further cloud adoption, and encryption with locally managed keys or BYOK (61%) is far and away seen as the technology that would most increase willingness to use public cloud globally, up sharply from 48% a year ago. Encryption with keys managed by the service provider came in a distant second at 51%.

Similarly, cloud-related technologies also scored high with respect to overall data security spending plans. More than one-third (39%) of global respondents plan on deploying ‘Bring Your Own Key’ encryption strategies this year, while slightly less (38%) will use a cloud encryption gateway; and 36% will use tokenization or enable encryption at the cloud provider.

Public Cloud Security Incentives and Implementation Plans

**Part 1**
Offerings from CSPs That Will Increase Enterprise Cloud Adoption

- Encryption with locally managed keys (BYOK)
- Encryption with keys managed by the CSP
- SLA and Liability Agreements for Data Breaches
- Detailed Security Implementation Data

**Part 2**
Top 5 Planned Implementations of Data Security Tools in 2017

- 3rd Party BYOK
- CASB/Cloud Encryption Gateway
- Enable encryption capabilities in the cloud
- Tokenization
- Hardware Security Modules
BIG DATA

As with cloud, Big Data is a global juggernaut. Just as enterprises globally wrestle with determining which Big Data is potentially valuable to the organization, they wrestle as well with determining the relative sensitivity of that data, and therefore how it needs be secured. Also with the potential of Big Data deployments springing up on an ad hoc basis outside of IT’s purview, concerns arise about whether adequate defenses are in place enterprise-wide.

With Big Data the ‘three V’s’ come into play: Volume, Velocity and Variety, each carrying unique security concerns. By most estimates, data volumes are doubling roughly every two years (volume and velocity). Most of that growth is in unstructured data (variety) from a host of mostly external sources, the security of which is difficult to assure.

Not surprisingly the top global security concerns globally for Big Data center on discovery and awareness of the existence of Big Data (45%) and the existence of reports generated that use Big Data (44%). Nearly half (47%) of respondents currently house sensitive data in Big Data environments such as Hadoop, Spark and NoSQL, or plan to in 2017. And the top means to secure this data is data-at-rest encryption (36%), up from 33% a year ago.

INTERNET OF THINGS

Enterprises globally are going all-in for IoT. Data from the recent Voice of the Enterprise Internet of Things Study from 451 Research shows 71% of enterprises globally are already aggregating data for IoT initiatives. These global organizations plan on growing IoT-related spending by a robust 33% this year. However, security is cited as the top impediment to IoT deployments in the study.

There is good reason for this concern. By definition, IoT implies hundreds if not thousands of interconnected digital devices in a single enterprise. Merely maintaining security updates on each of them can be daunting. In addition, security leaders must provide assurance for authentication and identification of each device.
and IoT application running on those devices. And secure communications and data protection must be assured for each IoT endpoint, the networks that carry their data, and for the back-end systems that process the data.

In our survey for the 2017 Thales Data Threat Report, we found that the overwhelming majority of respondents (86%) are planning IoT deployments. The top security concerns of doing so include protecting sensitive IoT data (36%), and the discovery of sensitive IoT data (30%)—figures largely unchanged from a year ago.

Similar to our findings for public cloud, global respondents would be more likely to deploy IoT solutions with the availability of encryption and tokenization for IoT data (56%), followed closely by secure identification and authentication for IoT devices (55%).

“THE RECENT VOICE OF THE ENTERPRISE INTERNET OF THINGS STUDY FROM 451 RESEARCH SHOWS 71% OF ENTERPRISES GLOBALLY ARE ALREADY AGGREGATING DATA FOR IOT INITIATIVES.”
DOCKERS/CONTAINERS

Though the most nascent among the emerging technologies discussed in the 2017 Thales Data Threat Report, nearly 40% of global respondents will be using Containers in production environments, and 19% of those respondents will store sensitive data in Containers this year. But just as with the emerging IoT environment, there remains a lack of enterprise-grade security controls in most container environments today, owing largely to their relative immaturity. And when deployed to the cloud, Containers still lack secure infrastructure controls as well as the ability to safeguard against rogue admins, since most Containers run as 'root'.

Thus, as with all advanced technologies in our study, security is once again cited as the top barrier for container adoption (47%), followed closely by budget (44%) and staffing (33%). Among container-specific security concerns globally, unauthorized access to Containers topped the list at 43% followed by the spread of malware between Containers at 39%.

Security as the Top Barrier to Container Adoption

Part 1 Top Barriers to Container Adoption

- Security
- Budget
- Staffing
- Compliance

Part 2 Security Concerns for Containers

- Unauthorized Access to Containers
- Spread of Malware Among Containers
- Privacy Violations from Shared Resources
- Vulnerabilities in Container Images
- Untrusted 3rd Party Container Images
- Patching and Updated Containers
- Lack of Image Compliance Certifications

Part 3 Security Controls that Would Increase Enterprise Container Adoption

- Encryption
- Anti-Malware
- Vulnerability Scanning
- Monitoring Tools for Containers
- Digital Signature-base Image Validation
- Role-based Access Controls
- Security Reporting Tools
- Image Compliance Certifications

“Nearly 40% of global respondents will be using Containers in production environments, and 19% of those respondents will store sensitive data in Containers this year.”
As with Big Data and IoT, encryption ranked as the top security technology (53%) that would boost willingness to deploy Containers more actively, a wide margin over the number two choice, anti-malware (45%) and scanning for container vulnerabilities (42%). However, only 16% of respondents are currently using data-at-rest encryption with existing container deployments.

"AS WITH BIG DATA AND IOT, ENCRYPTION RANKED AS THE TOP SECURITY TECHNOLOGY (53%) THAT WOULD BOOST WILLINGNESS TO DEPLOY CONTAINERS MORE ACTIVELY, A WIDE MARGIN OVER THE NUMBER TWO CHOICE, ANTI-MALWARE (45%) AND SCANNING FOR CONTAINER VULNERABILITIES (42%)."

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 endpoint and network security are no longer sufficient. When implemented as a part of the initial development (for ease of implementation versus retrofitting later), data security offers increased protection to known and unknown sensitive data found within advanced technology environments. Look for data security tool sets that offer services-based deployments or platform offerings, integrate with cloud provider’s security tools, and include automation for reduced deployment and maintenance complexity. |
| DISCOVER AND CLASSIFY | Get a better handle on the location of sensitive data, particularly for new environments like Cloud, Big Data and IoT where data is highly decentralized. |
| 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 | **Cloud:** Encrypt and manage keys locally for both IaaS/PaaS and SaaS environments, utilize BYOK options where available or consider cloud encryption gateway or tokenization.  
**Big Data:** Employ discovery as a complement to encryption and access control within the environment, and also consider data masking or tokenization.  
**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 or tokenization of data at rest on IoT devices, back end systems and in transit to limit data threats  
**Data Sovereignty:** Encryption and tokenization are top alternatives to migrating data or choosing local cloud providers. |
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.

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 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.