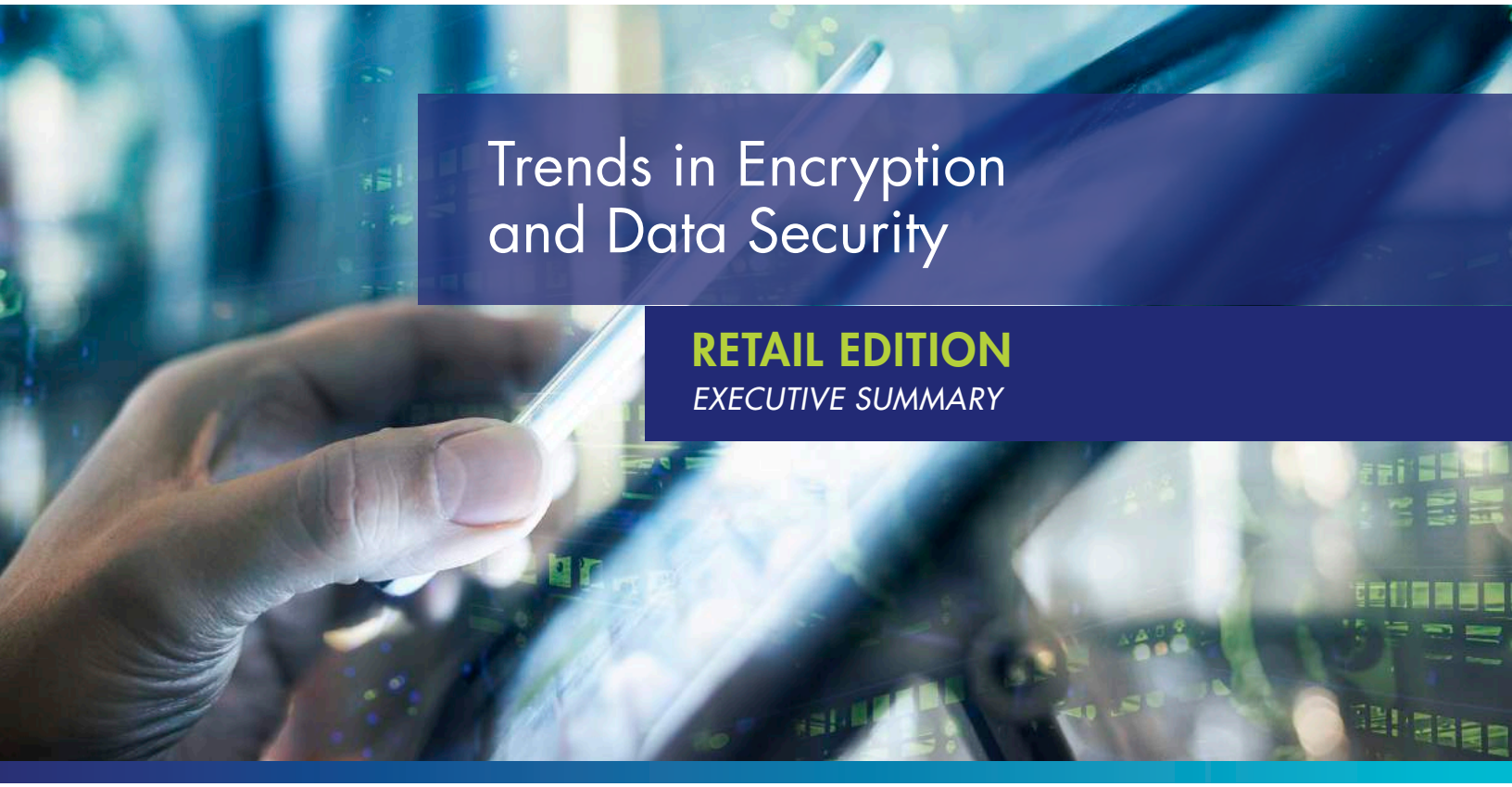
THALES

451 Research

2018 THALES DATA THREAT REPORT



Trends in Encryption and Data Security

RETAIL EDITION

EXECUTIVE SUMMARY

#2018DataThreat

THE TOPLINE

Massive digital transformation and advanced threats are putting U.S. retailer's sensitive data at risk as never before. What will it take to stop the breaches?

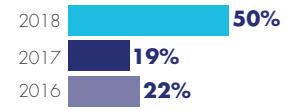
Traditional retailers are caught at the intersection of the absolute requirement to digitally transform their businesses or perish, and mounting attacks against the customer and card data that represent the lifeblood of their operations. Online, retailers face the challenge of mounting attacks against their digital storefronts with a goal of fraud, theft and customer information compromise. The result? Retailer's sensitive data has never been more at risk.

In this environment, IT and data security are now a critical challenge for retailers. With ultra-high volumes of personally identifiable information (PII) and payment card information changing hands with every transaction, the retail industry is one of the most, if not the most, vulnerable targets for cyber-attacks. Not surprisingly the question on the minds of IT and business leaders in U.S. retail is, "What will it take to stop the breaches?"

DATA BREACHES ARE THE NEW REALITY

Breach rates reach new highs

Breach rates accelerate



2.5x Breach rates in the last year are up **2.5X** from the results in 2017

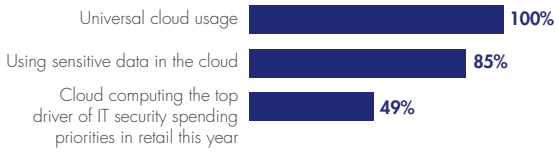
Lack of perceived need is the top reason for not implementing data security in U.S. Retail

DIGITAL TRANSFORMATION EXPANDS DATA THREAT LANDSCAPES

99% use digital transformation technologies with **sensitive data**

(cloud, big data, IoT, containers, blockchain or mobile payments)

Cloud usage the top problem



Multi-cloud usage is high, bringing additional risks

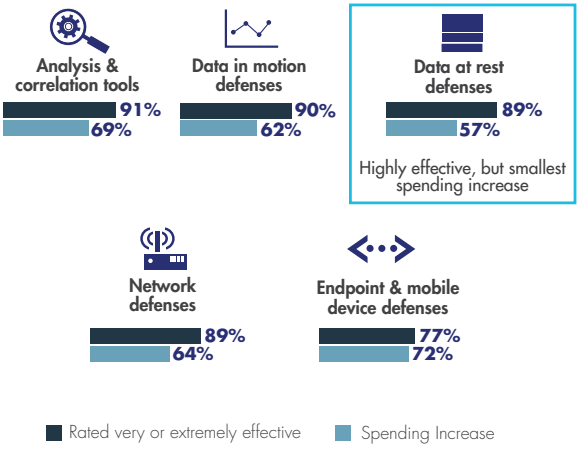
58% Use **3 or more IaaS** vendors

66% Use more than **25 SaaS applications**

57% Using **3 or more PaaS** environments

NOT PUTTING THEIR MONEY WHERE THEIR DATA IS

Respondents report their organizations increasing spending the least on the most effective tools for protecting data



ENCRYPTION IS CRITICAL TO SOLVING DATA SECURITY PROBLEMS

Encryption drives digital transformation and traditional data security

52% **IoT:** Encryption ties with anti-malware as the top tool need for more IoT adoption

49% **Cloud:** Data encryption is a top tool needed to enable more cloud use

46% **Big Data:** Encryption the top tool needed to enable more big data usage

46% **Containers:** Availability of encryption increases adoption

Encryption technologies help to solve new privacy requirements and traditional problems with protecting sensitive data

49% Encryption is the top tool planned for use to meet global privacy regulations such as GDPR

74% Deploying data masking (an encryption technology) this year

67% deploying database and file encryption year

Reports of successful data breaches, including some of the most infamous and damaging, are soaring even as IT security spending in this sector is up significantly. 75% of respondents in retail now report that their organizations encountered a data breach at some time in the past, while 50% of respondents have been breached in the last year alone, up from just 19% in our 2017 report. At the same time, 84% are increasing their IT security spending, with 28% reporting much higher spending than last year.

A core problem is that even as threats evolve and increase against traditional data stores within enterprise networks and data centers, retailer's digital transformation efforts are putting sensitive data into cloud, big data, IoT, mobile payments, blockchain and other technologies. These environments are as large a component of the problem as evolving threats, or even more so. In retail, this transformation is a do-or-die requirement, but each new environment and instance adds new attack surfaces and data security problems that need to be addressed.

It also doesn't appears that increases in IT security spending will be deployed effectively to protect retailer's data in this rapidly evolving landscape. Increases in spending are tending toward the tools that were best at protecting our organizations in the past, rather than what's needed today to protect sensitive, regulated and protected information.

DIGITAL TRANSFORMATION REQUIRES A NEW DATA SECURITY APPROACH

Digital transformation drives efficiency and scale for existing products and services, while also making possible new business models that drive growth and profitability. Although all sectors of industry are grappling with this change, the retail industry seems most affected. Traditional retailers are having to defend their turf against new challengers that started with online storefronts, and the competition is brutal – integrating online with brick-and-mortar operations via digital transformation is a make-or-break proposition. For sensitive data, the risk is that the rush to deployment can leave sensitive data at risk. With these market forces in play, we found massive adoption of cloud, big data, IoT, mobile payments and blockchain technologies by retailers. Cloud usage is now universal, with other technologies adoption rates all at the 90%+ level.

Each of these environments has unique data security challenges that must be addressed for secure usage with sensitive data, but the cloud is the most problematic. Cloud usage with sensitive data was especially high at 85%, with multiple cloud usage also at elevated levels, creating the new problem of how to secure sensitive data across multi-cloud deployments.

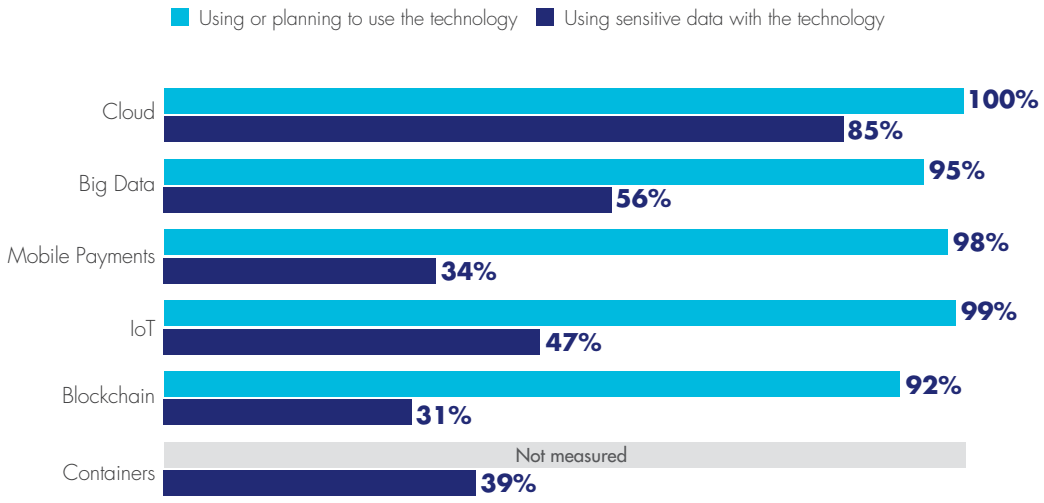
Digital transformation initiatives have high usage of sensitive data

99% use digital transformation technologies with **sensitive data**

(cloud, big data, IoT, containers, blockchain or mobile payments)

49% **Cloud computing** is the second most important item impacting IT security spending decisions

Implementations levels and sensitive data usage with digital transformation technologies



Multi-cloud operations creating big concerns

We found that 66% of respondents identified that their enterprise uses more than twenty-five Software as a Service (SaaS) offerings, 58% were also using three or more Infrastructure as a Services (IaaS) offerings and 57% three or more platform as a service (PaaS) offerings. This level of cloud service usage drives innovation and efficiency, but comes at a price for data security – and it can be measured by the unique requirements for protecting, and retaining control of, data within this range of environments.

In a traditional data center, not only is data physically secured within the four walls of the enterprise, but all of the infrastructure underlying implementation tools and networks are also under the direct control of the organization. Now, for IaaS, a specific data security plan must be created for each deployment and environment, then enforced by policy, operational methods and tools. For SaaS and PaaS environments, the case is more complex. In many of these environments, organizations retain little control over how their data is stored or protected, and in some cases where data security controls are available (such as AWS S3 storage buckets or Salesforce implementations) managing encryption keys, and access controls become a new task, requiring new expertise and tools. Third party offerings that reduce this complexity with integrated management of encryption technologies for multiple environments are starting to become available, but are not yet widely recognized. Organizations are going to need them – A basic security maxim is that whoever controls the keys, controls the data. Encryption – with encryption key control either local or remote from the cloud environment managed – is required.

> "As organizations increasingly engage with multiple cloud providers, who maintains control over encryption keys has become a huge potential issue, particularly for those who take advantage of native encryption services."
>
> *—Garrett Bekker, 451 Research Principal Analyst, Information Security*
> ***Author of the 2018 Thales Data Threat Report***


75%
"Of particular concern for retail is not only the elevated rates of breaches being encountered (75% in total), but also that half of all retailer IT security pros surveyed responded that their organization had been breached in the last year."
+6.5%
78%
CTMX
FTR
CSCO
CHK
AAPL
PRTO
AMZN
TSLA
AVGO
SIRI
0.45
-0.23
-2.34%
-1.01
-1.89%
0.02
-0.65

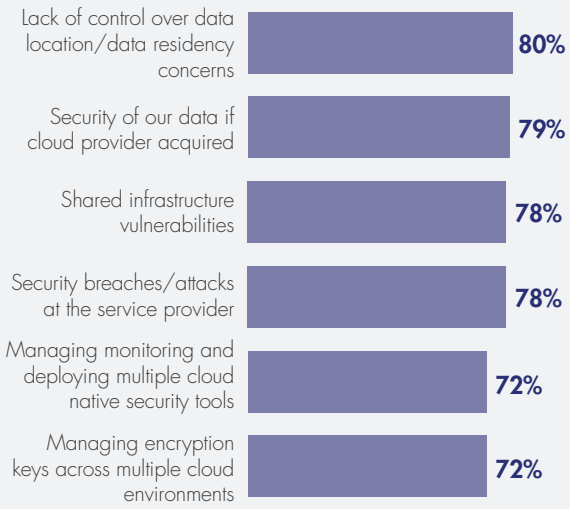
Multi-cloud usage brings additional risks

58%
Use **3 or more IaaS** vendors

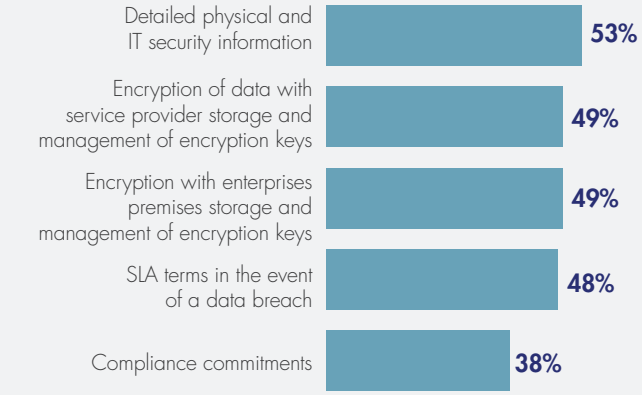
66%
Use more than **25 SaaS applications**

57%
Use **3 or more PaaS** environments

Top concerns with cloud computing



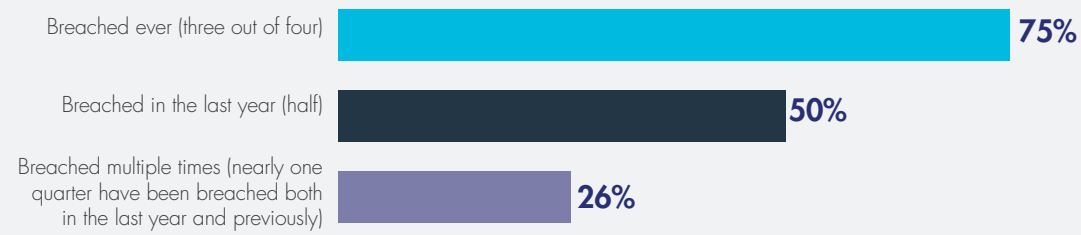
Top IT security tools needed to expand cloud computing use



IT SECURITY SPENDING IS UP – AND SO ARE DATA BREACHES

Of particular concern for retail is not only the elevated rates of breaches being encountered (75% in total), but also that half of all retailer IT security pros surveyed responded that their organization had been breached in the last year and that 26% had been breached both in the last year and previously. Let's look at this another way. Over half of the organization surveyed that were breached in the last year had been breached previously. This statistic is especially troubling, as it indicates that organizations are not learning from previous mistakes about how to protect their sensitive data, or they are simply not making it a priority.

Data breaches reported in U.S. Retail



There is some evidence that a key component of the problem is that organizations have decided not to make data security a priority. When asked about the barriers to data security within their organizations, the top item identified was "lack of perceived need" at 52%.

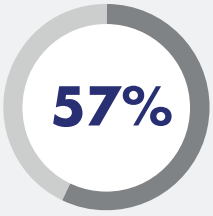
However, our results also show good news as well. IT security budgets are starting to expand to counteract these threats. 84% are increasing their IT security spending, with 28% reporting that IT security spending will be much higher this year.

HOW WILL ORGANIZATIONS MITIGATE THESE RISKS?

Increasing IT security spending

Overall increasing spending

Much higher spending



Will increase data-at-rest spending this year

"Look for data security toolsets that offer services-based deployments, platforms, and automation that reduce usage and deployment complexity for an additional layer of protection for data."

—Garrett Bekker, 451 Research Principal Analyst, Information Security
Author of the 2018 Thales Data Threat Report

ORGANIZATIONS NEED TO CHANGE HOW THEY PROTECT THEIR DATA

Respondents report biggest spending increases in tools that no longer protect data effectively

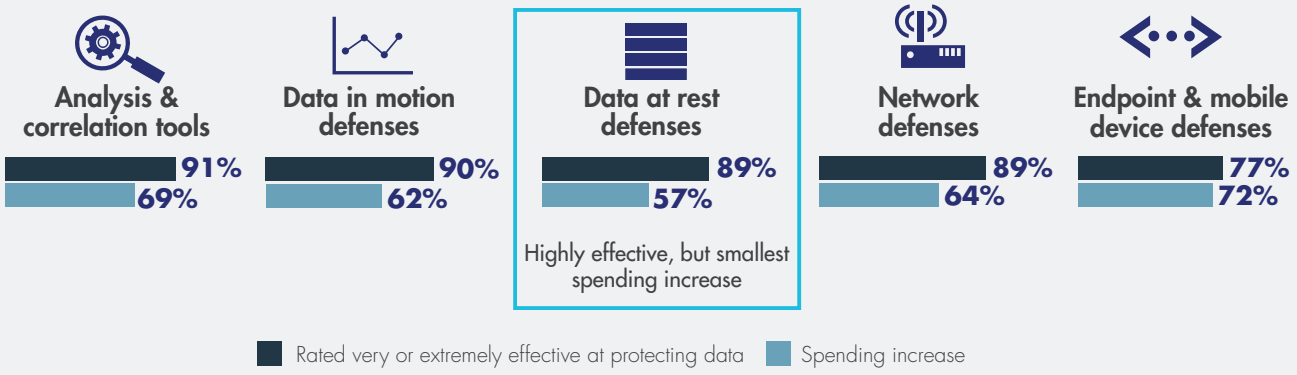
We found that respondents clearly recognize the defenses designed specifically for protecting data are the most effective tools for doing so. Data-at-rest and data-in-motion defenses were rated as two of the top three tools for protecting data, with 89% and 90% responding that they were either 'very' or 'extremely' effective. Analysis and correlation tools, such as Security Information and Event Management (SIEM) or big data for security systems are also highly effective at helping to identify threats to data, and rated slightly higher at 91%.

However, data-at-rest security tools, among the best methods for protecting data repositories, are not getting a high priority in spending increases. In fact, the data-at-rest defenses that are the most effective at protecting large data stores are the lowest priority for increases in IT security spending, with 54% increasing spending in this area – the lowest of all our categories measured.

At the same time, increases in IT security spending are greatest for end point (72%) and network defenses (64%), even as these tools are no longer wholly effective against attacks designed to compromise data. The combination of spear phishing with zero-day exploits available to criminal hackers makes it almost impossible to keep intruders away from critical data stores solely with network and endpoint-based security controls. As respondents recognize, the most effective solutions are security controls that provide an additional layer of protection directly around data sets, and to help identify attacks underway against data based on analytics such as data access patterns. Data-at-rest and data-in-motion security tools can reduce attack surfaces, and provide the information that analytics tools need to quickly find and stop attacks designed to mine critical data while in progress. Cloud computing also makes network security tools less relevant as new infrastructure is increasingly not implemented within the four walls of the enterprise.

NOT PUTTING THEIR MONEY WHERE THEIR DATA IS

Respondents report their organizations increasing spending the least on the most effective tools for protecting data



> "A common theme we have observed across virtually every vertical and geographic market in the Thales 2018 Global Data Threat Report also held true for U.S. Retail: namely spending the most on defenses deemed least effective."
>
> *—Garrett Bekker, 451 Research Principal Analyst, Information Security*
> ***Author of the 2018 Thales Data Threat Report***

ENCRYPTION IS A CRITICAL TOOL FOR PROTECTING SENSITIVE DATA – WHEREVER IT RESIDES

Protects data in traditional data centers, cloud, big data, and wherever sensitive information is used or stored

Good news. Not only did our respondents at U.S. retailers identify that encryption technologies are the most effective way to protect data, but in spite of lower comparative spending levels for data security, projects are underway to implement encryption for data protection at fairly high levels. Data masking and database/file encryption were two of the top 3 data security tools planned to be implemented this year, and encryption was also recognized as the top tool needed to meet global data privacy requirements such as GDPR.

Top 5 data security tools that are being implemented this year:

75%
Data access monitoring

74%
Data masking

67%
Database/file encryption

63%
DLP

63%
Identity and access management

Encryption drives digital transformation and traditional data security

52%

IoT: Encryption ties with anti-malware as the top tool need for more IoT adoption

49%

Cloud: Data encryption is a top tool needed to enable more cloud use

46%

Big Data: Encryption the top tool needed to enable more big data usage

46%

Containers: Availability of encryption increases adoption

Encryption technologies help to solve new privacy requirements and traditional problems with protecting sensitive data

49%
Encryption is the top tool planned for use to meet global privacy regulations such as GDPR

74%
Deploying data masking (an encryption technology) this year

67%
deploying database and file encryption this year

"Firms should consider greater use of encryption and BYOK, especially for cloud and other advanced technology environments to both address growing compliance mandates and also to move closer to industry best practices."

—Garrett Bekker, 451 Research Principal Analyst, Information Security
Author of the 2018 Thales Data Threat Report

"84% of U.S. retail respondents say their organizations will increase IT security spending this year, up sharply from last year (77%) and well ahead of both the Global average (78%) and Global retail (67%). More than a quarter of both U.S. retail and Global retail (28%) say their spending this year will be 'much higher.'"

"With increasingly porous networks, and expanding the 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 at a later date), data security offers increased protection to known and unknown sensitive data found within advanced technology environments."

"Look for data security toolsets that offer services-based deployments, platforms, and automation that reduce usage and deployment complexity for an additional layer of protection for data."

—Garrett Bekker, 451 Research Principal Analyst, Information Security
Author of the 2018 Thales Data Threat Report

ENCRYPTION IS THE SOLUTION

Encryption technologies are critical to protecting data at rest, in motion and in use. Encryption secures data to meet compliance requirements, best practices and privacy regulations. It's the only tool set that ensures the safety and control of data not only in the traditional data center, but also with the technologies used to drive the digital transformation of the enterprise.

ABOUT THALES

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

CLICK HERE TO TO READ THE FULL REPORT

OUR SPONSORS

VENAFI

GEOBRIDGE

CSA cloud security alliance

GuidePoint SECURITY

CRITICALSTART

OASIS

THALES

www.thalesesecurity.com