THALES

451 Research®

2018 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

RETAIL EDITION

#2018DataThreat

TABLE OF CONTENTS

OUR SPONSORS

VENAFI

GEOBRIDGE

CSA cloud security alliance

GuidePoint SECURITY

CRITICALSTART

OASIS

INTRODUCTION

Continuous reports of major data breaches Globally underscore the harsh realities of the state of cybersecurity today. Increases in IT security spending across a broad swath of vertical markets and geographies have done little to stem the tide of breaches. This ongoing game of cat-and-mouse suggests that the tactics, sophistication, and motivation are helping Global attackers stay at least one step ahead of their often overwhelmed and beleaguered defenders. The obvious – or what should be obvious – question is whether the cyber defenses that are being deployed today need to be re-examined for overall effectiveness and recalibrated.

The U.S. retail sector is certainly emblematic of these trends. Reports of successful breaches, including some of the most infamous and damaging, are soaring even as IT security spending in this sector is up significantly.

U.S. retail faces daunting digital challenges, and IT security is among the biggest. Traditional retailers are struggling to balance brick and mortar businesses with emerging online retail trends, while at the same time battling digital natives like Amazon and Wayfair. 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?"

"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."

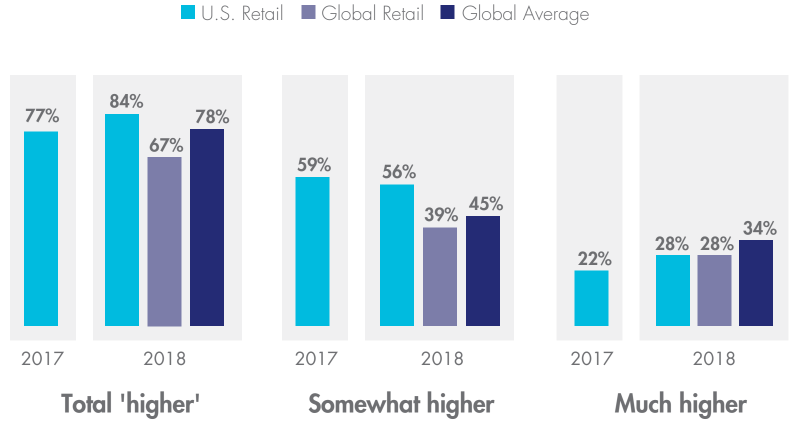
The data in this report are derived from detailed input from 100 senior retail IT security managers in the U.S. and 96 IT security managers from retailers in other countries surveyed and is part of the Global Thales 2018 Global Data Threat Report. The report polled 1,200 IT security managers in eight countries and across four major vertical markets.

KEY FINDINGS

For U.S. retail, this year's report presents a mixture of good news and bad news. Some 84% of U.S. retail respondents plan on increasing IT security spending this year, up from last year's 77% and well ahead of the global average (78%) and particularly global retail (67%).

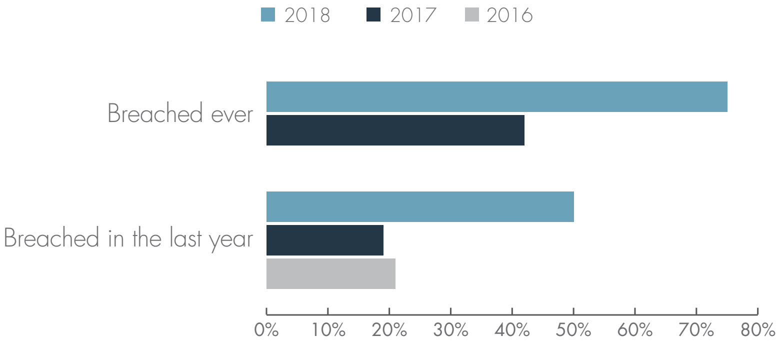
"Some 84% of U.S. retail respondents plan on increasing IT security spending this year, up from last year's 77% and well ahead of the global average (78%) and particularly global retail (67%)."

How IT security spending in 12 months will compare to its current level



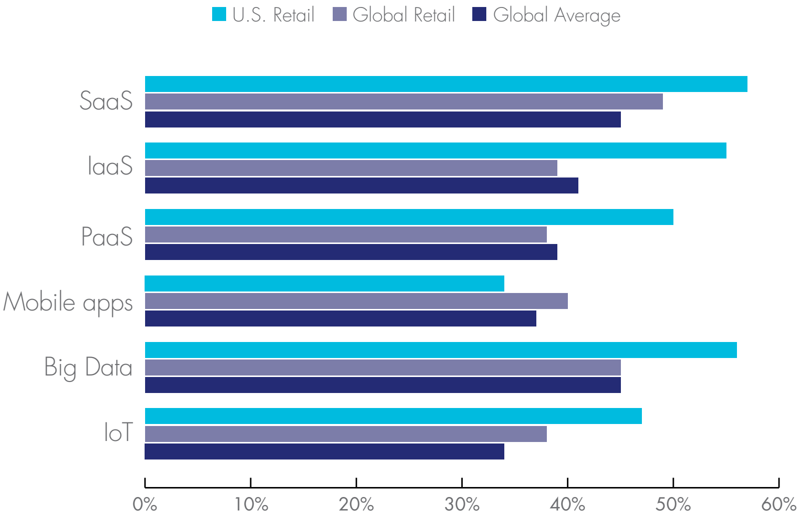
The bad news is that 50% of U.S. retail respondents reported being breached last year, also significantly ahead of the Global average (36%), and second only to U.S. Federal (57%) – and nearly double Global retail (27%). Further, three quarters (75%) of U.S. retail have experienced at least one breach in the past compared with just 60 % for Global retailers.

U.S. retail breach rates accelerate



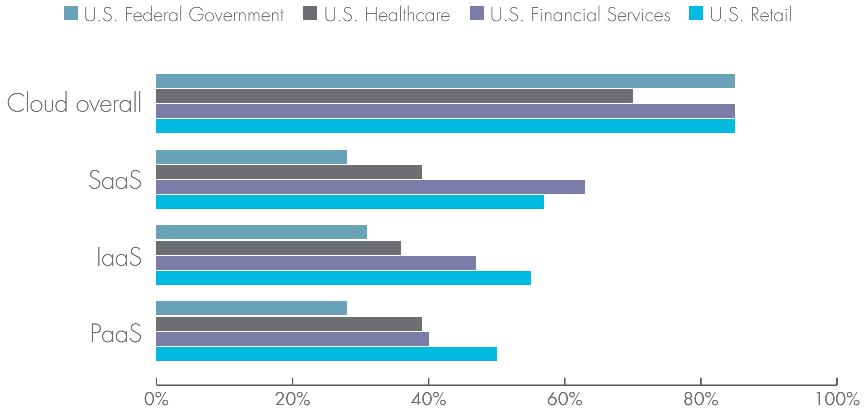
U.S. retail is also more inclined to store sensitive data in the technology environments used for digital transformation, compared with the global average.

Storing sensitive data in environments for digital transformation



"The bad news is that 50% of U.S. retail reported being breached last year, also significantly ahead of the global average (36%). Further, three quarters (75%) of U.S. retail have experienced at least one breach at some point in the past."

Rates of sensitive data use in the cloud for U.S verticals



Other key findings include:

- U.S. retail ranked analysis and correlation tools (91%) as the most effective solution for stopping breaches, and data-in-motion (90%) second. Yet spending plans are the highest for endpoint/mobile defense solutions, despite their being ranked as the least effective defenses.

- Despite having a higher propensity to store sensitive data in the cloud, only 26% of U.S. retail is implementing encryption in the cloud today, compared with 30% both in Global retail and the Global average.

- However, encryption/tokenization remain the top choices for securing emerging environments.

    - For public cloud, encryption with keys managed locally and with service providers tied for #2 for U.S. retail (49%), compared to 44% and 41% Global respectively, trailing the top answer, detailed physical and IT architectural and security implementation information (53%).

    - Top choices for U.S. retail for securing Big Data are the ability to analyze and use encrypted or tokenized data (46%) (compared with 31% for Global retail) and system level encryption (44%).

    - For IoT, the top security controls for U.S. retail are encryption/tokenization (52%) and anti-malware (48%).

    - Moreover, top security controls needed to expand adoption of containers for U.S. retail includes anti-malware was (54%), followed by encryption (46%) and vulnerability scanning (42%).

84%

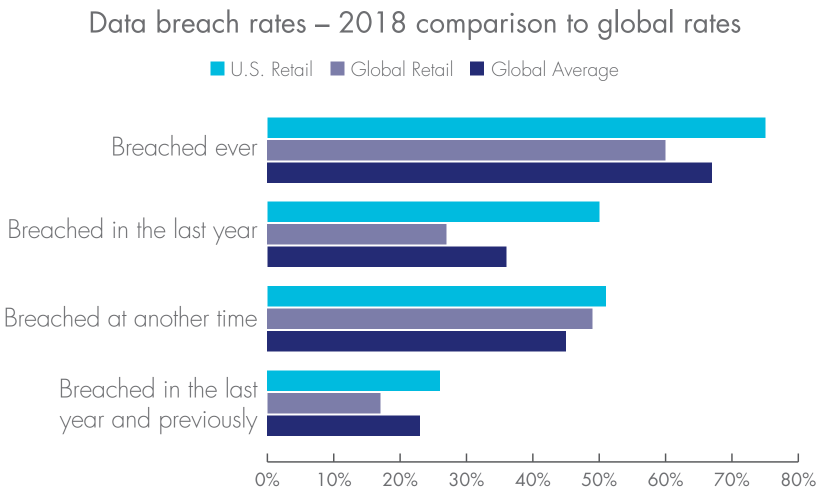
"84% of U.S. retail respondents say their organizations will increase IT security spending this year, up sharply from last year (77%) and well ahead of both the Global average (78%) and Global retail (67%). More than a quarter of both U.S. retail and Global retail (28%) say their spending this year will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

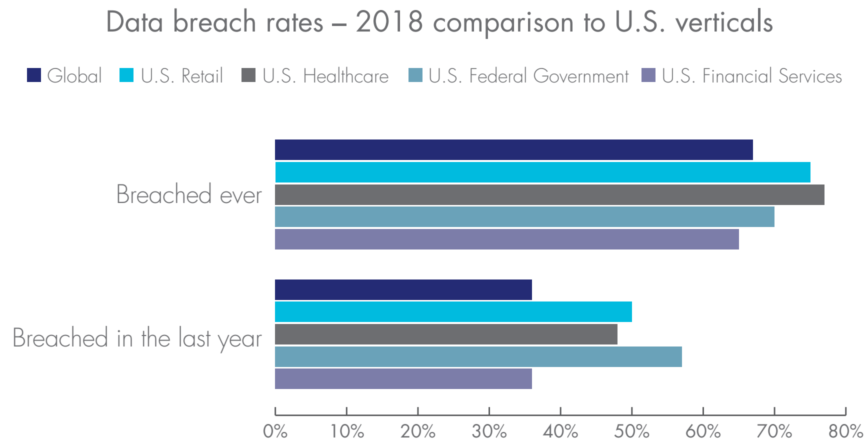
SPENDING MORE, ENJOYING IT LESS

Quite possibly in response to an uptick in breaches, 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.'

However, as mentioned earlier, retail is a prime cybercrime target, especially in the U.S. Exactly half (50%) of U.S. retail were breached in the past year alone, well ahead of the Global average (36%) and nearly double Global retail (27%). Further, three quarters (75%) of U.S. retail have been breached at least once in the past, again ahead of 67% Globally and just 60% for Global retail.

> *"Retail is a prime cybercrime target, especially in the U.S. Exactly half (50%) of U.S. retail were breached in the past year alone, well ahead of the Global average (36%) and nearly double Global retail (27%). Further, three quarters (75%) of U.S. retail have been breached at least once in the past, again ahead of 67% Globally and just 60% for Global retail."*





> *"Not surprisingly, 49% of U.S. retail report feeling 'very' and 'extremely' vulnerable to attacks on sensitive data."*

Not surprisingly, 49% of U.S. retail report feeling 'very' and 'extremely' vulnerable to attacks on sensitive data, compared with a much lower Global average (34%) mirrored by Global retail (35%).

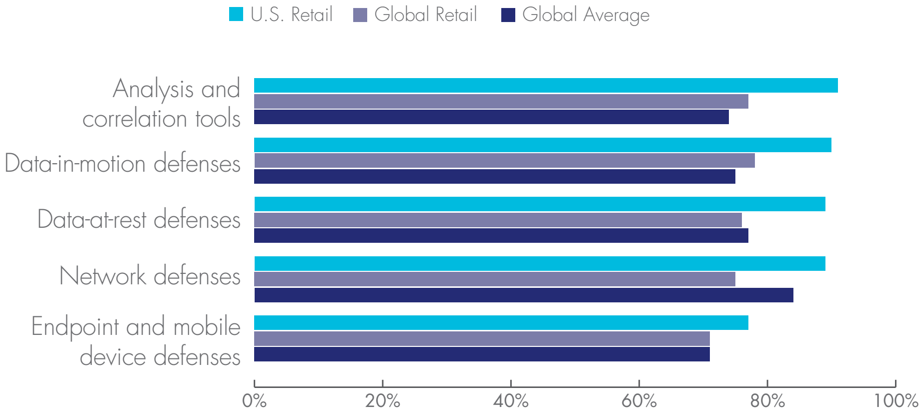
Spending in all the wrong places

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. For example, analysis and correlation tools were ranked as the most effective defense against security breaches by 91% of U.S. retail, followed closely by data-in-motion defenses at 90%. Endpoint/mobile defenses (77%), conversely, were ranked as least effective, yet ranked as the top in terms of planned spending increases by U.S. retail (72%) and by Global retail (52%). Meanwhile, data-at-rest (57%) and data-in-motion (62%) defense were ranked at the bottom of spending priorities for U.S. retail despite having much higher results for effectiveness.

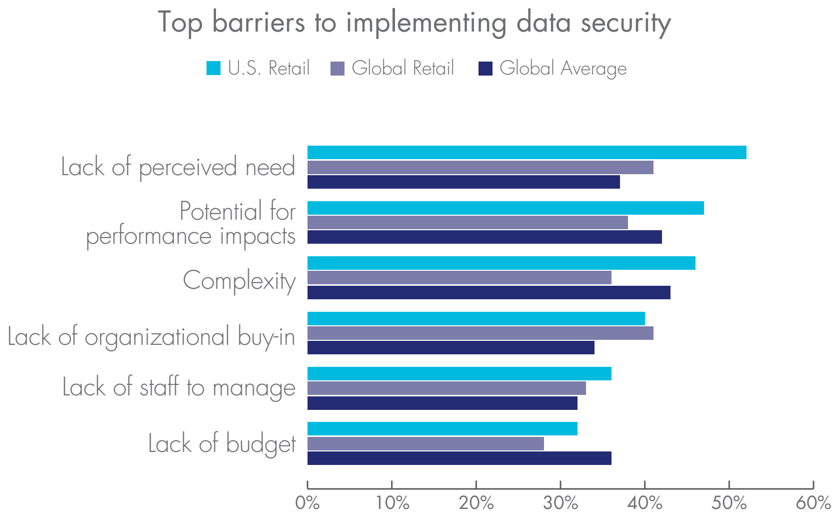
> *"Endpoint/mobile defenses (77%), conversely, were ranked as least effective, yet ranked as the top in terms of planned spending increases by U.S. retail (72%) and by Global retail (52%). Meanwhile, data-at-rest (57%) and data-in-motion (62%) defense were ranked at the bottom of spending priorities for U.S. retail despite having much higher results for effectiveness."*

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, particularly for heavy adopters of public cloud resources such as the U.S. retail sector. However, data security tools such as discovery/classification, encryption or tokenization can provide increased protection to known and unknown sensitive data found within advanced technology environments like cloud, containers, Big Data and IoT.

Ratings for effectiveness of defenses when protecting sensitive data



It is certainly a conundrum as to why data security does not gain more spending attention. Across most verticals and geographies, the perception of complexity (43%), as well as concerns about business performance (42%), are cited as top barriers to implementing data security. For U.S. retail, however, lack of perceived need is the top barrier (52%), followed by impacts on business performance (47%) and perceptions of complexity (46%). The new data privacy regulation from the EU (GDPR) may put more of a focus on data security overall, and in the U.S. and Global retail specifically.

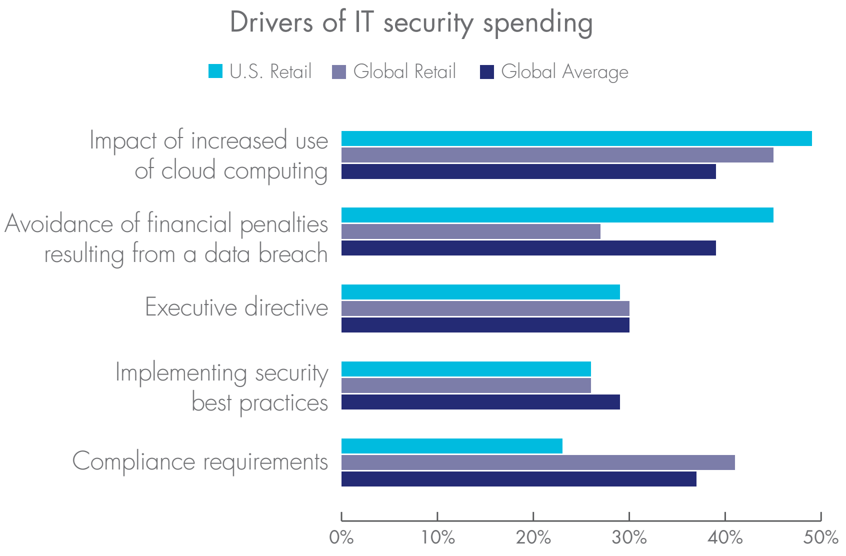


> *"For U.S. retail, as relatively higher adopters of cloud computing, not surprisingly the increased use of cloud tops the list of IT security spending drivers at 49%, well above the Global average of 39%."*

Also, considering that for Global retail a lack of organizational buy-in was tied with lack of perceived need as top barriers to implementing data security (41%), the implication is that either management doesn't care enough about data security or that IT has not done the job of selling its importance upstream. Moreover, it's certainly more than ironic that one of the sectors most besieged by breaches would have lack of perceived need as the main reason for not adopting data security tools. Regardless, the lack of attention towards data security is alarming given the continued targeting of the retail sector by cyber-criminals.

Drivers of IT security spending

For U.S. retail, as relatively higher adopters of cloud computing, not surprisingly the increased use of cloud tops the list of IT security spending drivers at 49%, well above the Global average of 39%. This is followed in U.S. retail by avoidance of financial penalties (45% vs. a Global average of 39%), and reputation and brand protection (33% for U.S. retail) – the latter was chosen as the top reason by Global retail (47%).



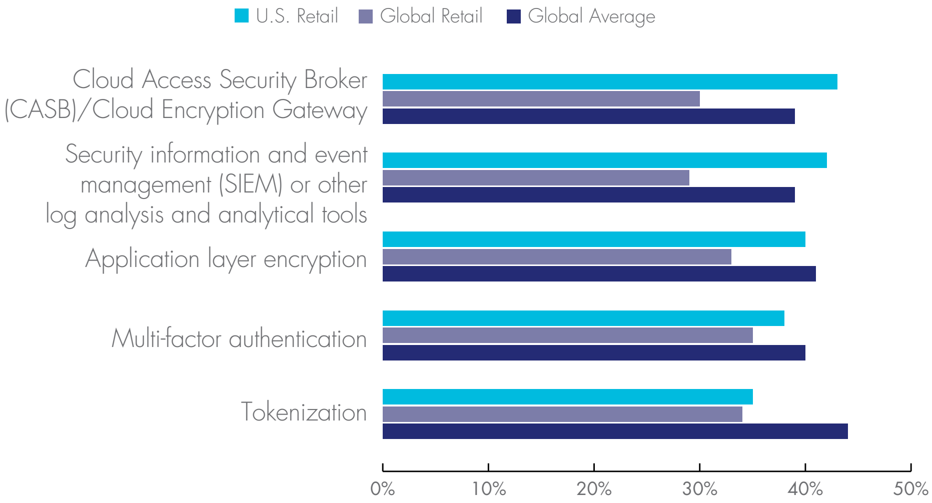
Interestingly, compliance declined as a strong driver of spending on IT security in U.S. retail (23% vs. 37% Global average and 41% Global retail), offset by an increase in responses for cloud computing despite the impact of PCI-DSS on spending plans for retail merchants. The higher Global average was likely influenced by this year's arrival of GDPR in Europe, though we also note that this was only the second year that the impact of cloud computing was offered as a response option.

Yet, 83% of U.S. retail respondents feel compliance requirements are 'very'+ 'extremely effective' in preventing breaches compared to 64% Global average and 53% last year, and 65% for Global retail. It should be remembered that most compliance regulations focus on specific data sets, such as PCI DSS and credit card data, and are limited in their governance over other data types. Also, compliance regulations often lag leading-edge trends in threat vectors and cyber-attacks.

> *"83% of U.S. retail respondents feel compliance requirements are 'very'+ 'extremely effective' in preventing breaches compared to 64% Global average and 53% last year, and 65% for Global retail."*

For U.S. retail the highest-ranked data security technology in terms of planned deployments is CASB (43% vs. 39% Globally), with SIEM a close second at 42% and application layer encryption slightly behind at 40%. Global retail priorities differ, however, with encryption with BYOK the top choice at 42%, well ahead of 30% for U.S. retail; identity and access management rank second (40%). We also note that tokenization is a much lower priority for both U.S. and Global retail than for the Global average. Part of the discrepancy between encryption and tokenization could be due to regulations, which sometimes specify encryption or tokenization, as well as differences in the types of data that need to be secured.

Planned implementation of encryption and data security tools



> *"Globally, the number one choice to satisfy local data privacy laws (GDPR, Korea's PIPA, and APPI in Japan) by a wide margin is encryption (42%), with tokenization a distant second (20%)."*

> ***"14% of U.S. and Global retail say they won't be impacted by privacy mandates such as GDPR, in-line with the 13% Global average."***

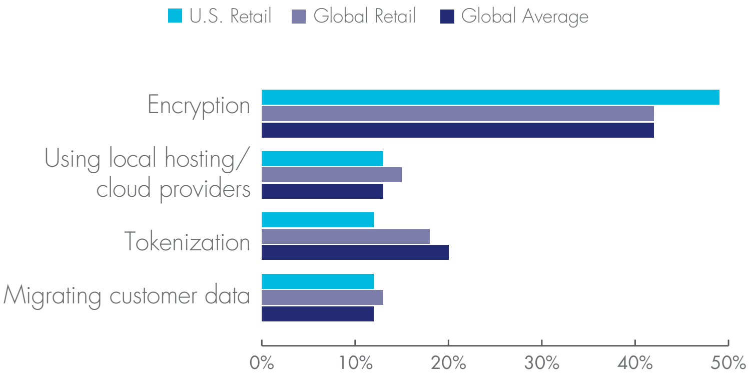
DATA SOVEREIGNTY

With the advent of GDPR this month, data sovereignty is a major IT security concern for all organizations doing business with any EU citizen. Not surprisingly, just 14% of U.S. and Global retail say they won't be impacted by privacy mandates such as GDPR, in-line with the 13% Global average.

Globally, the number one choice to satisfy local data privacy laws (GDPR, Korea's PIPA, and APPI in Japan) by a wide margin is encryption (42%), with tokenization a distant second (20%).

Similarly, for U.S. retail the preferred way of complying with local data privacy rules by an even wider margin is encryption (49% vs. 42% Globally), and also by a wide margin over other options such as tokenization (12%), migrating customer data (12%) or using local hosting/cloud providers (13%).

Plans to comply with local data privacy rules



CLOUD

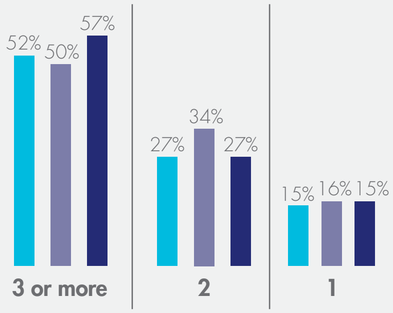
As is true across most all vertical sectors and geographies, U.S. retail is aggressively pursuing a multi-cloud strategy. For example, more than half (52%) of U.S. retail report using 3 or more IaaS providers vs. 57% Globally. Only 14% of U.S. retail respondents use just one PaaS provider while 52% use up to 3 vs. 56% Globally.

SaaS usage rates run even higher. For U.S. retail, 23% use from 11-25 SaaS applications vs. 22% Globally and 33% for Global retail. One in four (25%) of U.S. retail use between 51-100 apps vs. 20% Globally. Moreover, more than half (57%) of U.S. retail say they store sensitive data in SaaS applications, compared to 45% Globally and 49% for Global retail.

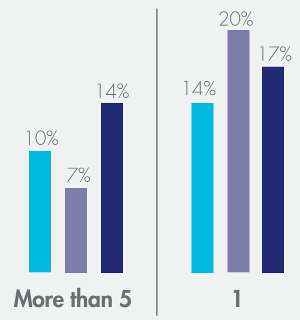
Overall, U.S. retail is much more concerned about the IT security threats posed by the use of public cloud, likely because U.S. retail organizations are more likely to both use cloud and store sensitive data within cloud resources. For example, U.S. retailers are much more likely to store sensitive data in each of the main public cloud categories than other sectors. Along with financial services, 85% of U.S. retailers are storing sensitive data in either an IaaS, PaaS or SaaS service.

■ U.S. Retail ■ Global Retail ■ Global Average

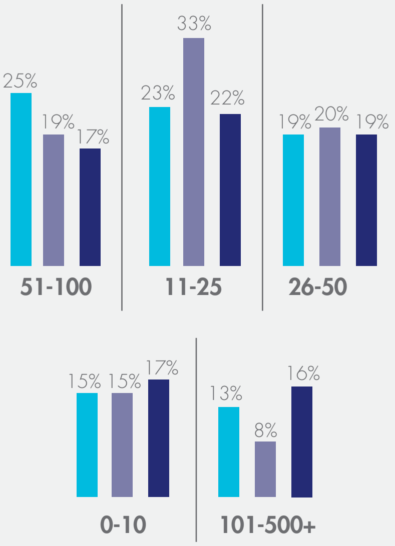
Number of **IaaS** providers currently used or planned to use



Number of **PaaS** providers currently used or planned to use



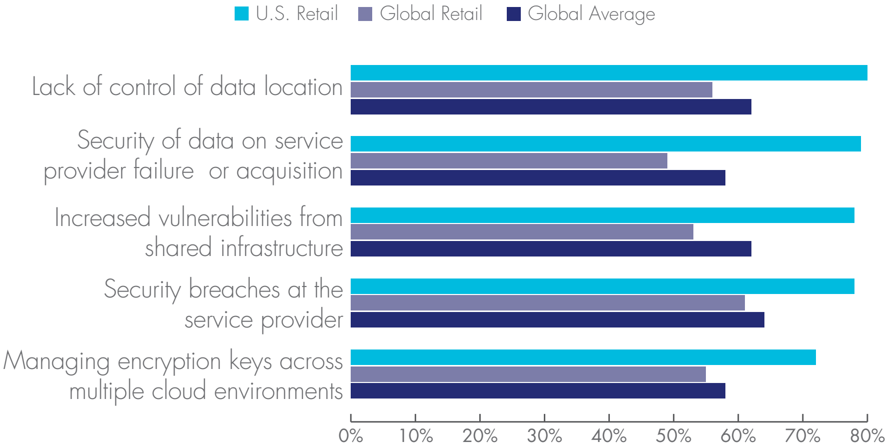
Number of **SaaS** apps currently used or planned to use



Globally, attacks and breaches at the cloud provider remain the top cloud security concern at 64%, up from 59% last year. This is also the top concern for Global retail (61%). Thus far, attacks on cloud providers have been relatively rare, and arguably cloud providers have much more extensive security measures in place than most enterprises. That said, when breaches do occur, they can be devastating to the extent that they impact critical applications. For U.S. retail, however, the top concern is data residency at 80% vs. just 56% for Global retail. By comparison, data residency was selected by just 62% Globally, likely due to the impact that GDPR may have on U.S. based retailers doing business in the EU.

> *"U.S. retail is aggressively pursuing a multi-cloud strategy. For example, more than half (52%) of U.S. retail report using 3 or more IaaS providers vs. 57% Globally. Only 14% of U.S. retail respondents use just one PaaS provider while 52% use up to 3 vs. 56% Globally."*

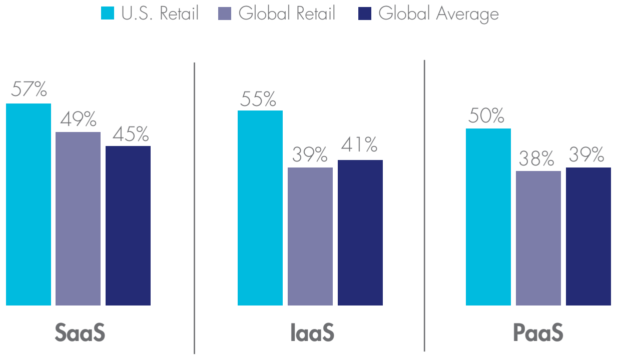
Data security concerns about public cloud services



GDPR is also a likely factor for why breaches at the cloud provider dropped from the number one answer in last year's survey (57%). Security of organization's data if the cloud provider fails or is acquired was a close second at 79% followed closely by security breaches and Increased vulnerabilities from shared infrastructure with 78%.

> *"Overall, U.S. retail is much more concerned about the IT security threats posed by the use of public cloud, likely because U.S. retail organizations are more likely to both use cloud and store sensitive data within cloud resources."*

Sensitive data stored in the cloud



"Globally, attacks and breaches at the cloud provider remain the top cloud security concern at 64%, up from 59% last year. This is also the top concern for Global retail (61%)."

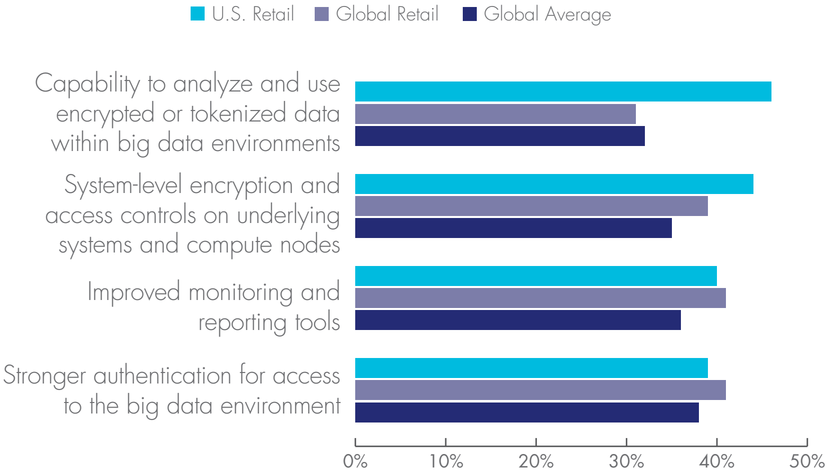
BIG DATA

Topping the list of Big Data security concerns for U.S. retail is the reality that sensitive data may reside anywhere in a Big Data environment (43% vs. 34% Globally) – also the top concern for Global retail (32%). This concern is followed by concerns over the security of reports that may contain sensitive data (38% U.S. retail vs. 33% Globally).

A new question this year addressed what security controls would be needed to expand adoption of Big Data? The top answers were the ability to analyze and use encrypted or tokenized data within big data environments (46% U.S. retail compared with 32% Globally and 31% for Global retail). System-level encryption and access controls were the second most popular response (44% U.S. retail).

"Topping the list of Big Data security concerns for U.S. retail is the reality that sensitive data may reside anywhere in a Big Data environment (43% vs. 34% Globally) – also the top concern for Global retail (32%)."

Security that would increase willingness to use big data



IoT

Another new question probed for the most popular types of IoT devices in use. Topping the list for U.S. retail is manufacturing (42%) followed by power/energy (39%). Environmental monitoring is #1 for Global retail (40%). Power/energy and personal/wearables tied for #2 (30%).

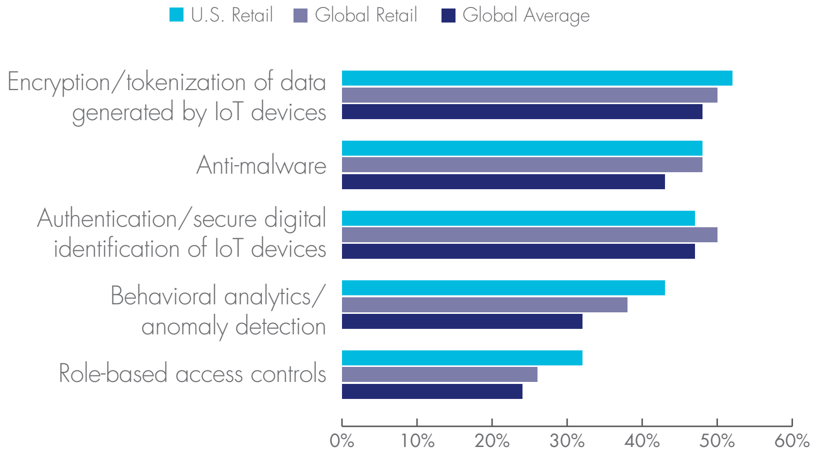
Generally speaking, IoT devices are perceived as presenting a lower security risk compared to other 'new' tech environments, similar to last year. The greatest IoT security concerns for U.S. retail are attacks on IoT devices that may impact critical operations (33%), followed by protecting sensitive data generated by an IoT device (32%). Privacy violations related to data generated by an IoT device tops the list for Global retail at 30%, possibly owing to GDPR. Protecting sensitive data generated by an IoT device was #2 (29%). However, an attack on IoT devices that may impact critical operations was #1 Globally (26%).

"The greatest IoT security concerns for U.S. retail are attacks on IoT devices that may impact critical operations (33%), followed by protecting sensitive data generated by an IoT device (32%). Privacy violations related to data generated by an IoT device tops the list for Global retail at 30%."

And finally, the top security controls needed to expand IoT usage for U.S. retail are encryption/tokenization (52%) and anti-malware (48%). For Global retail, the top choice is authentication and encryption/tokenization (50%). Authentication is #3 for U.S. retail (47%).

"The top security controls needed to expand IoT usage for U.S. retail are encryption/tokenization (52%) and anti-malware (48%). For Global retail, the top choice is authentication and encryption/tokenization (50%). Authentication is #3 for U.S. retail (47%)."

Security controls that would increase willingness to adopt IoT



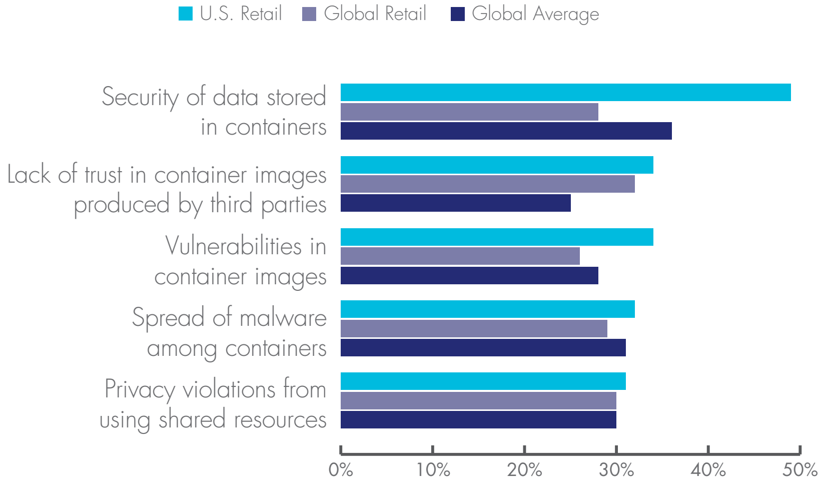
DOCKERS/CONTAINERS

As we have noted in past reports, container technologies are being adopted quite rapidly with many firms using Docker containers or Kubernetes, even in production environments. However, as with most 'new' or 'emerging' technologies, security risks can pose a significant adoption hurdle.

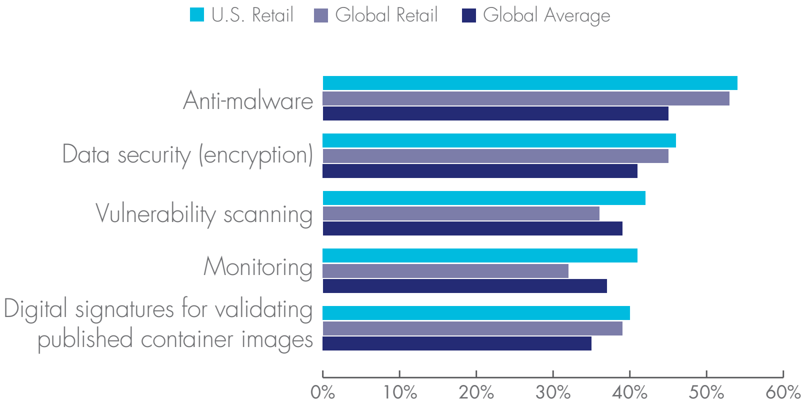
Topping the list of container security concerns for U.S. retail is the security of data stored in containers (49% vs. 36% Globally), followed by lack of trust in container images produced by third parties (34%) and vulnerabilities in containers (also 34%). The top security controls required to expand adoption of containers for U.S. retail includes anti-malware (54%), followed by encryption (46%) and vulnerability scanning (42%). It's worth noting that encryption was the top answer in 2017 (56%). For Global retail, the top two responses were also anti-malware (53%), and encryption (45%), followed by digital signatures (39%).

"The top security controls required to expand adoption of containers for U.S. retail includes anti-malware (54%), followed by encryption (46%) and vulnerability scanning (42%). It's worth noting that encryption was the top answer in 2017 (56%). For Global retail, the top two responses were also anti-malware (53%), and encryption (45%), followed by digital signatures (39%)."

Container security concerns



Security controls that would increase willingness to use containers



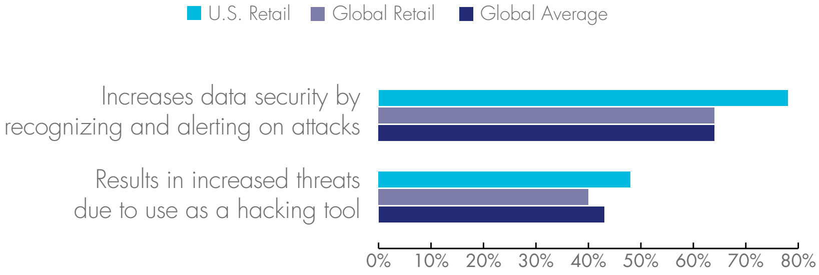
AI / MACHINE LEARNING – A DOUBLE-EDGED SWORD

A new question in this year's data set sought opinions of AI/Machine learning as security tools. Like most security tools, AI can be used both for beneficial and malicious uses – the 'Yin and Yang' of security. The good news is that perceived positive uses of AI greatly outnumber the perceived negative responses with 78% of U.S. retail (vs. 64% for Global retail and 64% Globally) believe that use of machine learning or AI helps increase data security by recognizing and alerting on attacks.

However, it is also clear that bad actors are also leveraging the automation and scale benefits of AI, as 48% of U.S. retail (vs. 40% of Global retail) perceive increased breaches due to smarter hacking tools as a result.

> *"Like most security tools, AI can be used both for beneficial and malicious uses – the 'Yin and Yang' of security. The good news is that perceived positive uses of AI greatly outnumber the perceived negative responses with 78% of U.S. retail (vs. 64% for Global retail and 64% Globally) believe that use of machine learning or AI helps increase data security by recognizing and alerting on attacks."*

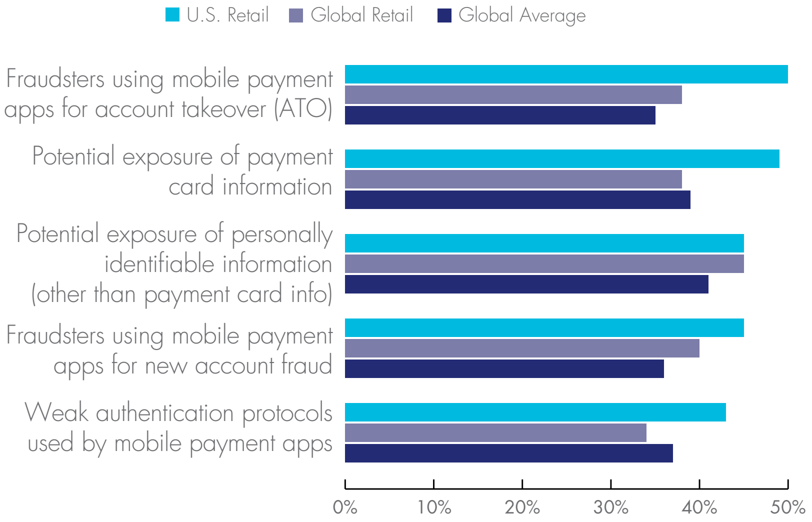
Impacts of machine learning or AI technologies on organization's data



MOBILE PAYMENTS

Another new question this year addressed security concerns for mobile payment applications. For U.S. retail, fraudsters using mobile payment applications for account takeover were the top concern at 50%, followed closely by potential exposure of payment card information at 49%. Potential exposure of PII (other than payment card info) was the top answer Globally (41%) and also for Global retail (45%).

Security concerns for mobile payment applications

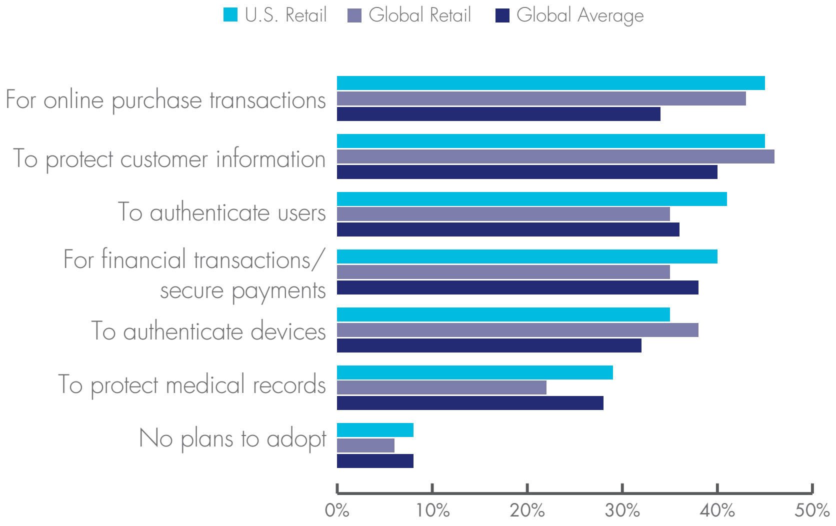


> *"Another new question this year addressed security concerns for mobile payment applications. For U.S. retail, fraudsters using mobile payment applications for account takeover were the top concern at 50%, followed closely by potential exposure of payment card information at 49%. Potential exposure of PII (other than payment card info) was the top answer Globally (41%) and also for Global retail (45%)."*

BLOCKCHAIN TRENDS

Blockchain ranks as one of the most significant new developments in IT security in years, at least in terms of hype and industry 'buzz'. Though still very early for commercial implementations of blockchain, just 8% Globally have no plans to adopt blockchain, and the same was true for U.S. retail (8%) and Global retail (6%). The main use cases for U.S. retail defined by this new question include online purchase transactions and protecting customer information (45% each), followed by authenticating users (41%). For Global retail, protecting customer data is # 1 at 46%, followed by online purchase transactions (43%).

Blockchain use cases



> *"Though still very early for commercial implementations of blockchain, just 8% Globally have no plans to adopt blockchain, and the same was true for U.S. retail (8%) and Global retail (6%)."*

RECOMMENDATIONS

RE-PRIORITIZE YOUR IT SECURITY TOOLSET

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, particularly for heavy adopters of public cloud resources such as the U.S. retail sector. 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 like cloud, containers, Big Data and IoT.

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.

DISCOVER AND CLASSIFY

Get a better handle on the location of sensitive data, particularly to deal with Big Data, IoT and data sovereignty mandates such as GDPR that are a major consideration for retailers operating Globally.

DON'T JUST CHECK OFF THE COMPLIANCE BOX

More than two-thirds of U.S. retail respondents still have considerable faith in compliance mandates. However, retail organizations should consider moving beyond compliance and adopting security tools such as encryption or tokenization that may be more appropriate as new technologies like cloud are adopted.

ENCRYPTION AND ACCESS CONTROL

Encryption needs to move beyond laptops and desktops.

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

Data Sovereignty: Consider both encryption and tokenization as a way to avoid hefty fines from violating nascent privacy laws

> *"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, particularly for heavy adopters of public cloud resources such as the U.S. retail sector."*

> *"Retail organizations should consider moving beyond compliance and adopting security tools such as encryption or tokenization."*

ANALYST PROFILE

Garrett Bekker
Principal Analyst
451 Research

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

ABOUT 451 RESEARCH

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

ABOUT THALES eSECURITY

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

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

PLATINUM PARTNER – GEOBRIDGE

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

PLATINUM PARTNER – VENAFI

Venafi is the cyber security market leader in machine identity protection, securing machine-to-machine connections and communications. Venafi protects machine identity types by orchestrating cryptographic keys and digital certificates for SSL/TLS, IoT, mobile and SSH. Venafi provides global visibility of machine identities and the risks associated with them for the extended enterprise – on premises, mobile, virtual, cloud and IoT – at machine speed and scale. Venafi puts this intelligence into action with automated remediation that reduces the security and availability risks connected with weak or compromised machine identities while safeguarding the flow of information to trusted machines and preventing communication with machines that are not trusted.

With 31 patents currently in its portfolio, Venafi delivers innovative solutions for the world's most demanding, security-conscious Global 2000 organizations. Venafi is backed by top-tier investors, including Foundation Capital, Intel Capital, Origin Partners, Pelion Venture Partners, QuestMark Partners, Mercato Partners and NextEquity. For more information, visit: www.venafi.com.

THALES

www.thalesesecurity.com