THALES

451 Research

2018 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

U.S. HEALTHCARE EDITION

#2018DataThreat

TABLE OF CONTENTS

OUR SPONSORS

GuidePoint SECURITY

CSA cloud security alliance℠

GEOBRIDGE

CRITICALSTART

OASIS

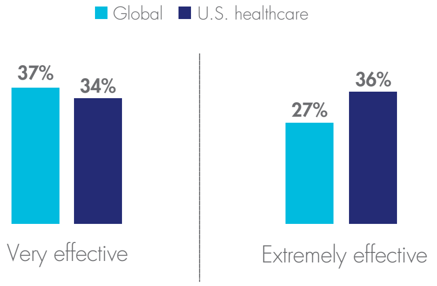
INTRODUCTION

The challenges of data security in U.S. healthcare are as numbingly complex as they are comprehensive. The web of regulations and standards that most healthcare firms face are designed both to protect medical records and personal health information (PHI) and also give patients more control over their health information.

In the U.S., the Health Insurance Portability and Accountability Act (HIPAA) is by far the most pervasive of all regulations. But it is far from the only one. Others include state and federal data security and privacy requirements; Freedom of Information and Privacy Acts; Personal Information Protection Acts (FIPAA/PIPA); and regulations from Occupational Safety and Health Administration (OSHA), to name just a few. Electronic prescriptions for controlled substances (EPCS) are yet another set of regulations that healthcare firms must abide by. Small wonder then that 70% of U.S. healthcare respondents feel that compliance requirements are either 'Very' or 'extremely' effective at preventing data breaches, ahead of the global average of 64%. Of course, being compliant with regulations is more likely to be viewed as highly effective – until the organization is breached.

> *"Small wonder then that 70% of U.S. healthcare respondents feel that compliance requirements are either 'Very' or 'extremely' effective at preventing data breaches, ahead of the global average of 64%."*

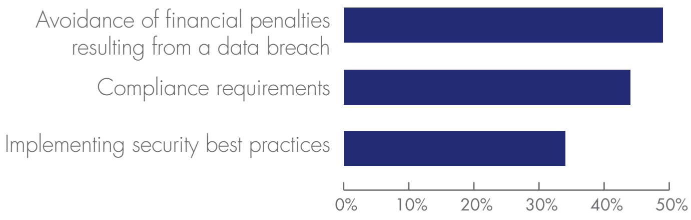
Rates for the effectiveness of compliance for protecting data in 2018



In addition to being pervasive, regulations like HIPAA are not particularly precise in telling healthcare providers exactly what they need to do to maintain compliance. While HIPAA invokes things such as audit trail requirements, secure archival of PHI, tightly controlled access to PHI, and many other regulations, it doesn't provide organizations with detailed instructions on how to accomplish these things. HIPAA is precise, however, in one area – penalties for violations, which range from $100 to $50,000 per violation or per record stolen. No surprise then that avoidance of financial penalties (49%) remains a top driver of spending on security for U.S. healthcare, followed by compliance (44%).

> *"No surprise then that avoidance of financial penalties (49%) remains a top driver of spending on security for U.S. healthcare, followed by compliance (44%)."*

Top impacts on IT security spending within U.S. healthcare organizations in 2018



To complicate the security matter further, the healthcare vertical has emerged as a prime target for hackers. While a stolen credit card has a time-limited value (the card number can be changed), PHI and electronic medical records (EMR) are stuffed with immutable data that can and do fetch hundreds of dollars per stolen record on illegal online markets.

Consolidation has also become a fact of life for many healthcare IT professionals, who have to deal with integration headaches and budgetary constraints that many other industry segments don't have to worry about. Finally, major IT budgetary decisions in hospitals often involve senior physicians and other non-IT professionals, and thus security matters often have to compete with, say, new MRI machines or other equipment with an arguably more measureable ROI than data security. Regulatory and compliance pressures, integration challenges and a steady diet of breaches have combined to create a 'perfect storm' that underlines the case to be made for stronger data protection measures in healthcare.

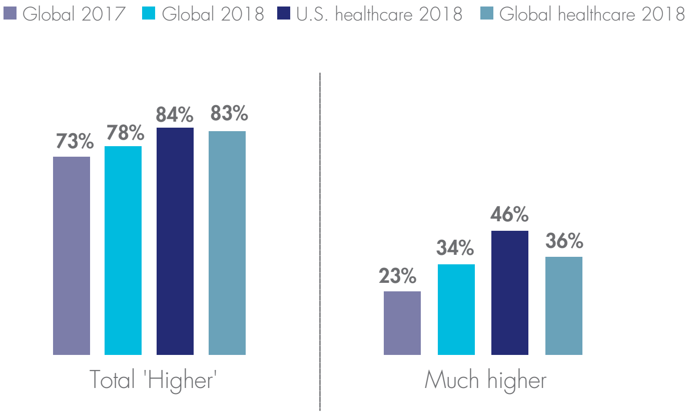
The data in this report are derived from detailed input from 100 senior healthcare security managers in the U.S. and 135 such managers in nine other countries globally – all part of the global Thales 2018 Global Data Threat Report that polled 1,200 security managers in eight countries and across four major vertical markets.

> *"While a stolen credit card has a time-limited value (the card number can be changed), PHI and electronic medical records (EMR) are stuffed with immutable data that can and do fetch hundreds of dollars per stolen record on illegal online markets."*

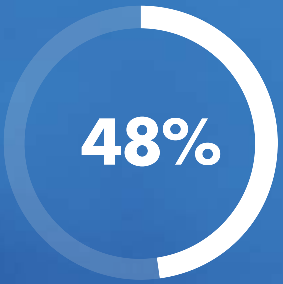
KEY FINDINGS

Planned spending on security in the healthcare sector are above average, with 84% of U.S. healthcare (and 83% of global healthcare) respondents planning to increase spending, ahead of the overall global average of 78% and up slightly from 83% last year.

Planned increases in IT security spending by healthcare organizations



> *"Planned spending on security in the healthcare sector are above average, with 84% of U.S. healthcare (and 83% of global healthcare) respondents planning to increase spending, ahead of the overall global average of 78% and up slightly from 83% last year."*

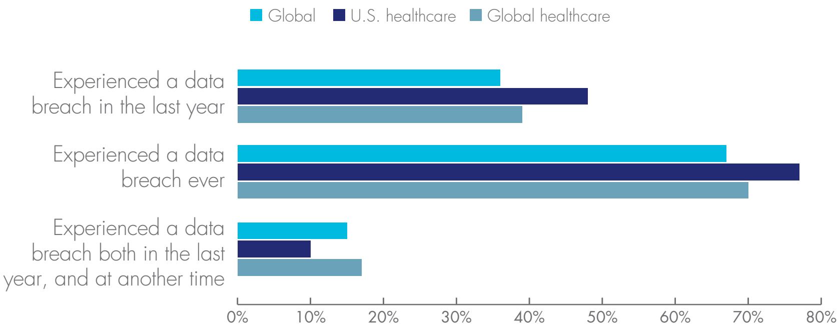


"Yet, despite the rosy spending outlook, nearly half (48%) of U.S. healthcare respondents reported getting breached in the last year alone, well ahead of global healthcare (39%) and the global average (36%)."

Yet, despite the rosy spending outlook, nearly half (48%) of U.S. healthcare respondents reported getting breached *in the last year alone*, well ahead of global healthcare (39%) and the global average (36%). Further, more than three-fourths (77%) of U.S. healthcare respondents reported at least one breach at some time in the past – the highest among all U.S. verticals. It is not surprising, then, that 56% of U.S. healthcare respondents report feeing either 'very' or 'extremely' vulnerable to sensitive data threats, well ahead of the global average of just 34%.

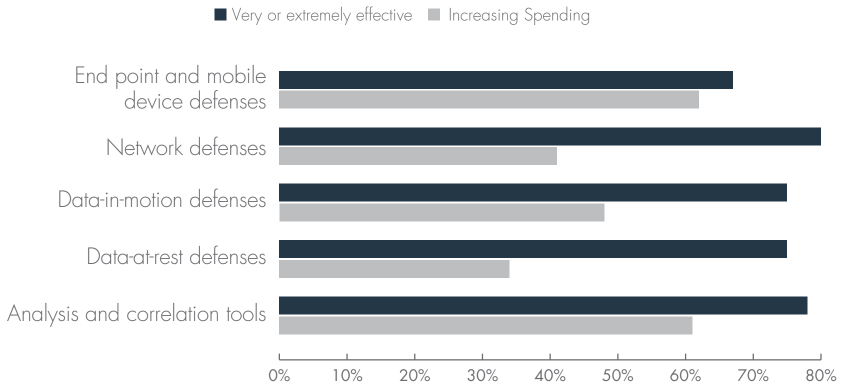
> *"U.S. healthcare has the highest percentage of respondents planning to increase spending for endpoint and mobile device security (62% vs. 57% global), despite ranking them least effective in preventing data breaches. Data-at-rest tools, by contrast, are at the bottom in terms of spending plans for U.S. healthcare despite ranking near the top in terms of effectiveness."*

Rates of healthcare data breaches in 2018



More bad news – U.S. healthcare is not putting its money where it matters most. U.S. healthcare has the highest percentage of respondents planning to increase spending for endpoint and mobile device security (62% vs. 57% global), despite ranking them *least effective* in preventing data breaches. Data-at-rest tools, by contrast, are at the bottom in terms of spending plans for U.S. healthcare despite ranking near the top in terms of effectiveness.

Rates for effectiveness of IT security controls at preventing data breaches and planned increases in data security spending in U.S. healthcare

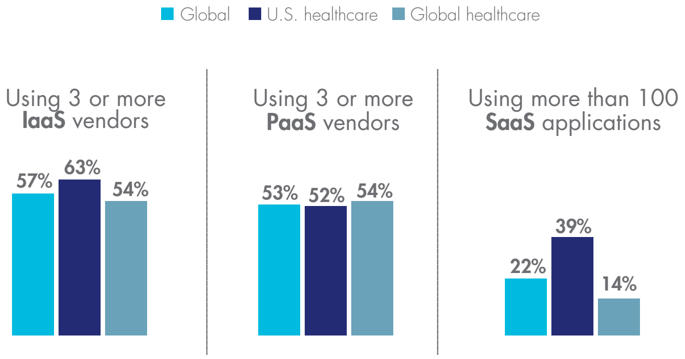


Like other verticals and regions, it is typically the perception of complexity (49%), as well as concerns about impacts on performance and business process (40%) that are holding back healthcare providers from taking a stronger stance with data security. For those who are moving ahead with data security initiatives, encryption and tokenization remain top choices for securing most new environments – such as cloud, IoT and containers – and also for dealing with new data sovereignty requirements such as GDPR.

One notable observation in response to a new question we posed in this year's survey, is that U.S. healthcare is more aggressively pursuing a multi-cloud strategy across IaaS, PaaS and SaaS than the global averages in each category. Specifically, nearly two-thirds (63%) of U.S. healthcare organizations are using 3 or more 3 IaaS providers, compared with 57% globally and 54% for global healthcare. Further, 39% of U.S. healthcare organizations are using more than 100 SaaS applications, nearly twice the global average of 22%, and well ahead of global healthcare at just 14%. Managing, monitoring and deploying multiple cloud native security tools (78%) was also not surprisingly the top security concern, well ahead of the 61% global average (61%) and global healthcare (62%).

"One notable observation in response to a new question we posed in this year's survey, is that U.S. healthcare is more aggressively pursuing a multi-cloud strategy across IaaS, PaaS and SaaS than the global averages in each category."

Healthcare providers use of cloud resources in 2018



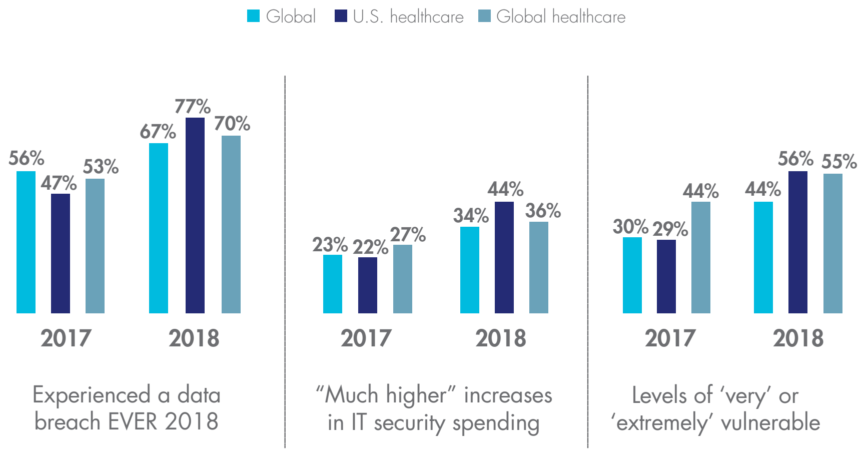
As organizations increasingly engage with multiple cloud providers, who will maintain control over encryption keys has become a huge potential issue, particularly for those who take advantage of native encryption services. On that note, we found it encouraging that U.S. healthcare showed the strongest preferences for locally managed keys in the cloud (48%), compared to the global average of 44% and slightly less than global healthcare (51%).

RISING BREACH COUNTS OUTPACING SPENDING PLANS

Like other sectors, data security spending plans are up year-to year, with 84% of U.S. healthcare planning increases this year, up slightly from 81% last year and ahead of the global average of 78%; global healthcare came in at 83%. The bad news is that reports of successful breaches at U.S. healthcare at 48% are also well ahead of the global average (36%) and global healthcare (39%), and more than double last year's count (20%). Further, nearly three-fourths of U.S. healthcare respondents report being breached at some point in the past (77%), higher than any U.S. vertical and well ahead of both the global average (67%) and global healthcare (70%).

"Data security spending plans are up year-to year, with 84% of U.S. healthcare planning increases this year, up slightly from 81% last year and ahead of the global average of 78%; global healthcare came in at 83%."

Healthcare data breach rates, IT security spending and vulnerability rise in tandem

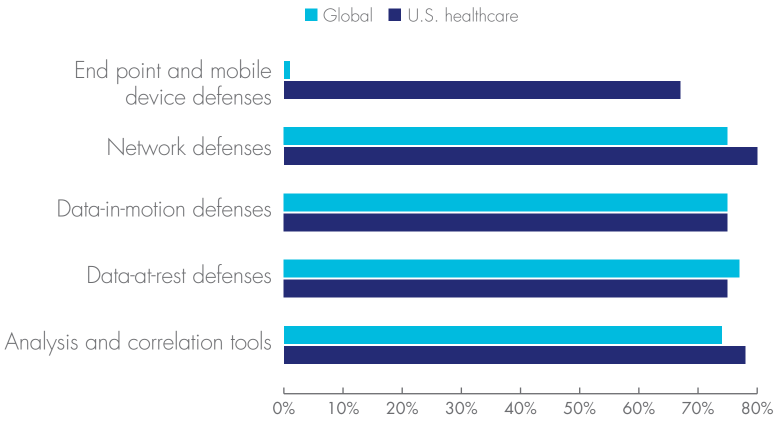


It is no surprise that U.S. healthcare respondents report feeling more vulnerable to sensitive data threats – 56% of U.S. healthcare (55% global healthcare) report feeling either 'very' or 'extremely' vulnerable to data breaches, well ahead of the global average (34%).

U.S. healthcare respondents are also not putting their budgets where their data is. U.S. healthcare respondents rank network security as most effective (80%) at protecting sensitive data, while endpoint and mobile defenses (67%) ranked last, by a considerable margin. Data-in-motion protections, however, (75% each) tied for third in terms of effectiveness.

Yet for the first time, U.S. healthcare plans to spend the most on endpoint and mobile devices (62% vs. 57% for the global average, despite ranking these as least effective, with analytics and correlation tools a close second (61%). Similarly, global healthcare ranked data-at-rest protections dead last at 34%, barely half the amount who plan to increase spending on endpoint and mobile security. Such wide disparities between effectiveness and spending intentions have obvious implications for the long-term effectiveness of cyber security efforts in healthcare.

Ratings for effectiveness of IT security tools for protecting data in 2018



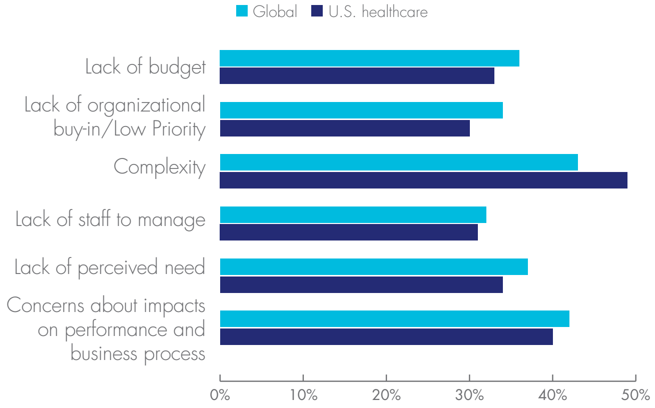
"Nearly three-fourths of U.S. healthcare respondents report being breached at some point in the past (77%), higher than any U.S. vertical and well ahead of both the global average (67%) and global healthcare (70%)."

"U.S. healthcare respondents are also not putting their budgets where their data is. for the first time, U.S. healthcare plans to spend the most on endpoint and mobile devices (62% vs. 57% for the global average), despite ranking these as least effective at preventing breaches."

As with most other sectors, one of the top barriers to broader adoption of data security tools and techniques is complexity, or at least the common perception that data security has to necessarily be a complex undertaking. Indeed, nearly half of U.S. healthcare respondents (49%) rank complexity as the main barrier to adopting data security – the highest of any vertical, and ahead of the 43% global average. Concerns about impacts on performance and business processes are a distant second (40%) for U.S. healthcare.

"It's no surprise that the top reasons given for spending on security include avoidance of financial penalties (49% compared to the global average of 39%). Compliance ranked second among U.S. healthcare as a driver of security spending (44%)."

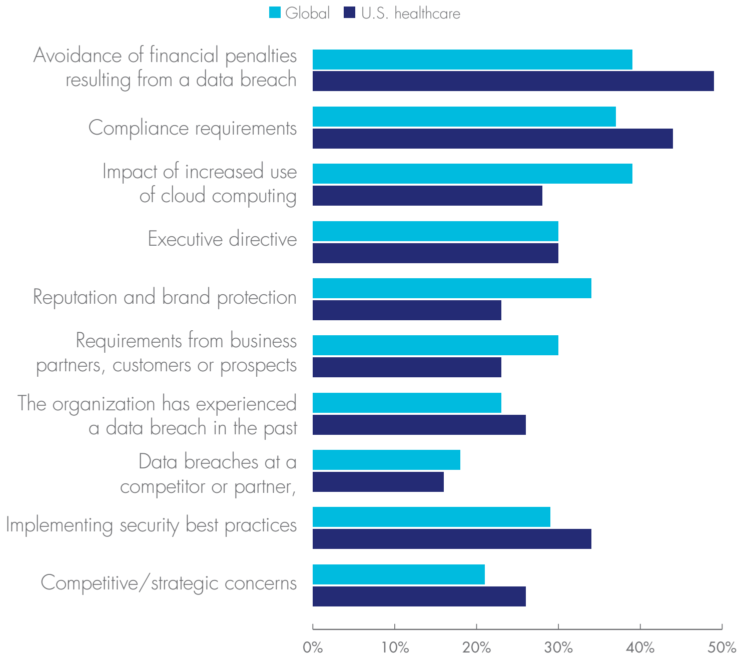
Perceived barriers to deployment of data security tools



SECURITY AND SPENDING

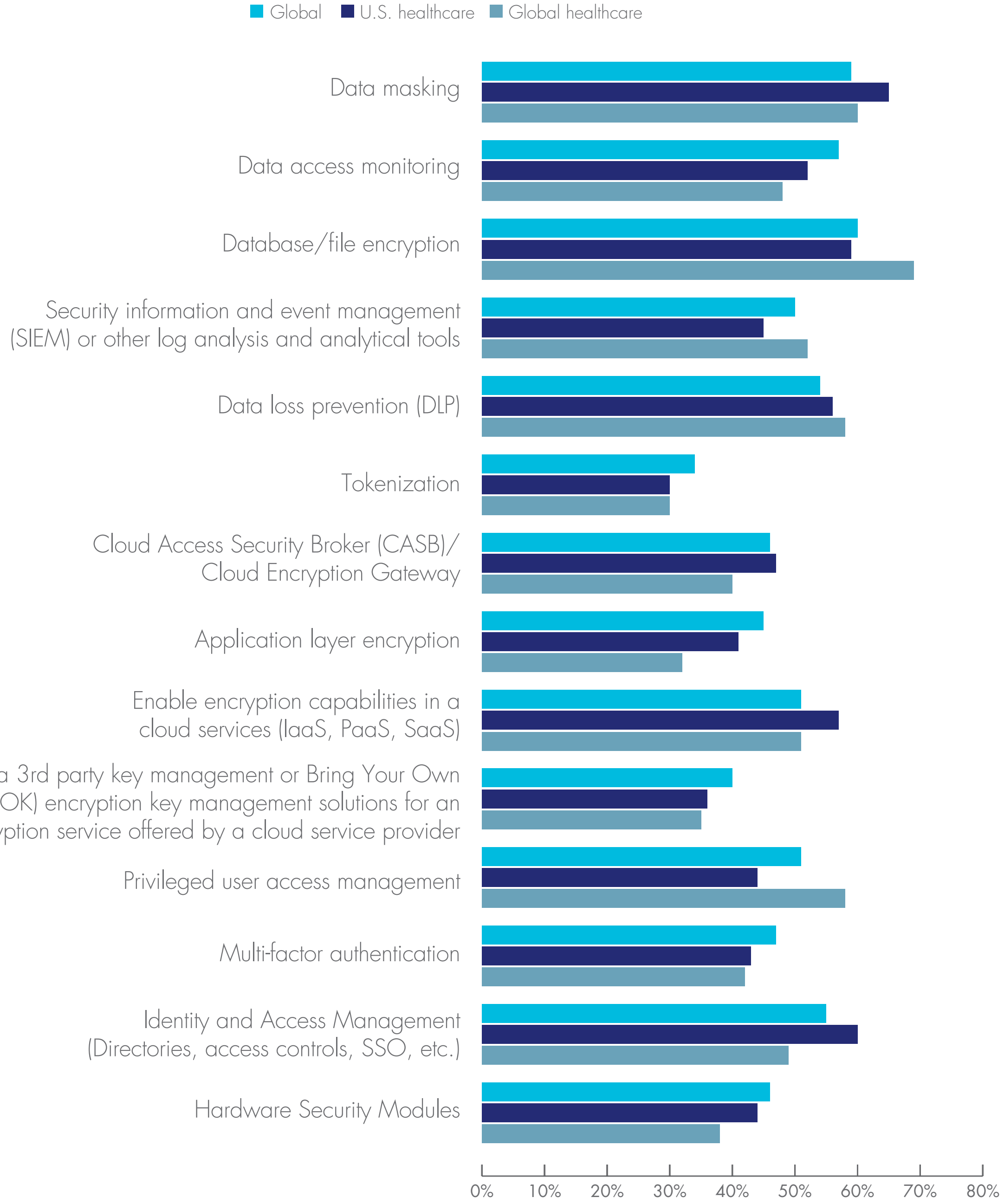
Given the wide variety of regulations and potentially large penalties faced by most U.S. healthcare companies, it's no surprise that the top reasons given for spending on security include avoidance of financial penalties (49% compared to the global average of 39%). Compliance ranked second among U.S. healthcare as a driver of security spending (44%), but was ranked number one with global healthcare at 51%, higher than any other sector and significantly head of the global average (37%).

Impacts on IT security spending plans in 2018



As far as allocating money towards specific security tools, top on the list for U.S. healthcare was privileged user access management with 52%, ahead of all verticals and well ahead of the global average (38%) and global healthcare (31%). Encryption with BYOK ranked second for U.S. healthcare (50% vs. 43% for the global average), while notably global healthcare had the highest preference for BYOK of any vertical (55%).

Data security tools being implemented in 2018



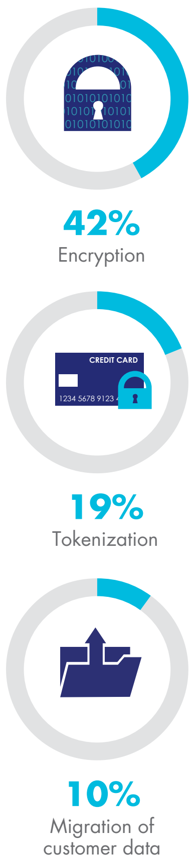
Meeting data sovereignty requirements:

"Encryption is the top choice for complying with local privacy regulations (42%), followed distantly by tokenization (19%) and migrating customer data (10%). Encryption also ranked first for global healthcare (36%), with tokenization again a distant second (21%)."

DATA SOVEREIGNTY

Given looming deadlines for GDPR, data sovereignty is highly topical these days. For U.S. healthcare, properly handling private data for EU citizens may be less of an issue for global organizations. Still, encryption is the top choice for complying with local privacy regulations (42%), followed distantly by tokenization (19%) and migrating customer data (10%). Encryption also ranked first for global healthcare (36%), with tokenization again a distant second (21%).

U.S. healthcare top 3 planned approaches to meeting national data sovereignty and privacy requirements in 2018

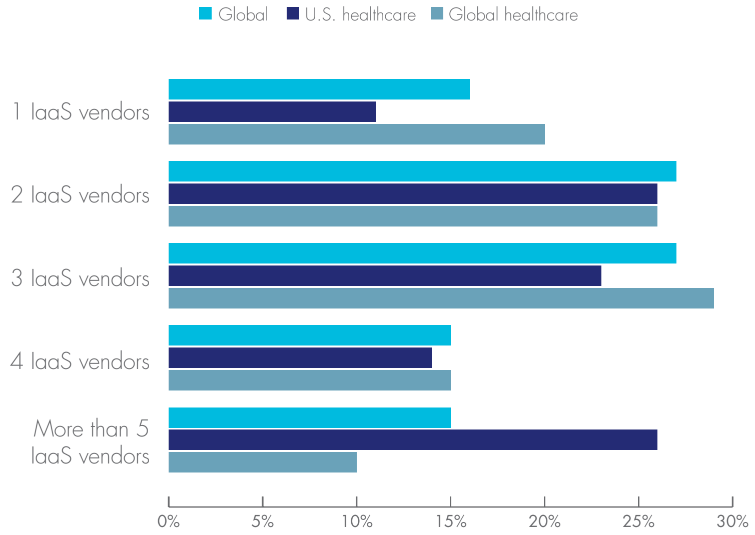


SECURING SAAS, BIG DATA AND IoT

Globally, most organizations are pursuing a multi-cloud strategy, and there is strong evidence that multi-cloud strategies are also becoming the norm for U.S. healthcare, though somewhat less so for global healthcare. However, using multiple cloud providers can also introduce unique security challenges, much of which are related to the potential lack of interoperability across multiple clouds, and also the wide variety of security options offered by many cloud providers. For example, each cloud provider may offer encryption and key management options that are unique compared to other cloud providers, and most often, encryption keys are not exposed externally for customers to manage as they see fit. Thus, it can be challenging to implement a consistent data security policy for firms that are using a wide range of IaaS, PaaS or SaaS vendors, and the complexity of which increases as the vendor counts rise. And as we noted earlier, managing, monitoring and deploying multiple cloud native security tools (78%) was not surprisingly the top security concern among U.S. healthcare, well ahead of the 61% global average (61%) and global healthcare (62%).

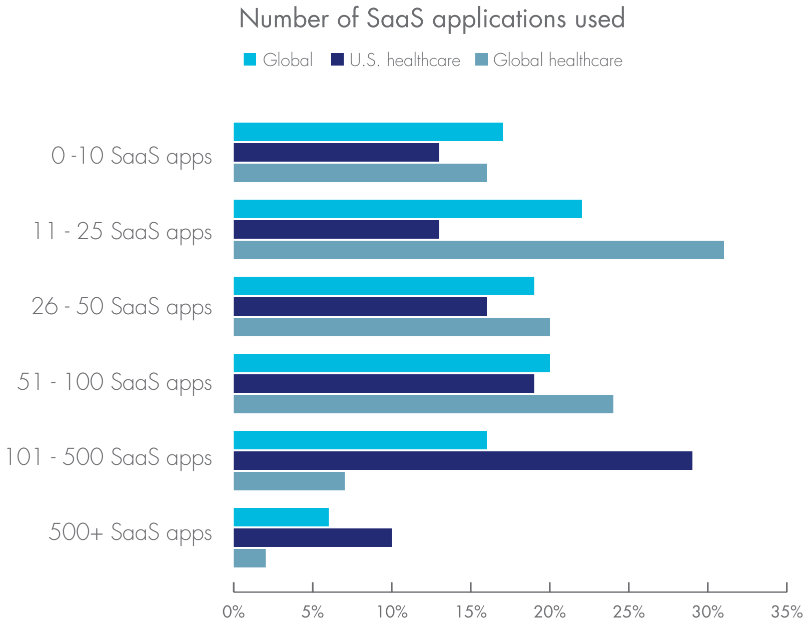
Only 11% of U.S. healthcare respondents report using just 1 IaaS provider, versus 16% globally, while nearly two-thirds (63%) are using more than three IaaS providers, vs. 57% globally and 54% for global healthcare.

Number of IaaS vendors used



"Only 11% of U.S. healthcare respondents report using just 1 IaaS provider, versus 16% globally, while nearly two-thirds (63%) are using more than three IaaS providers, vs. 57% globally and 54% for global healthcare."

The results are similar for PaaS and SaaS. Just 19% of U.S. healthcare reports using only 1 PaaS vs. 17% of the global average and 18% of global healthcare. More than half of U.S. healthcare respondents (55%) report using 3 or more PaaS providers, slightly ahead of the 53% global average and 52% for global healthcare. With respect to SaaS, a full 39% of U.S. healthcare organizations are using over 100 SaaS applications – nearly double the 22% reported by the global average. In contrast, just 14% of global healthcare respondents are using 100 or more SaaS apps – among the lowest of all reported verticals and well below U.S. healthcare.

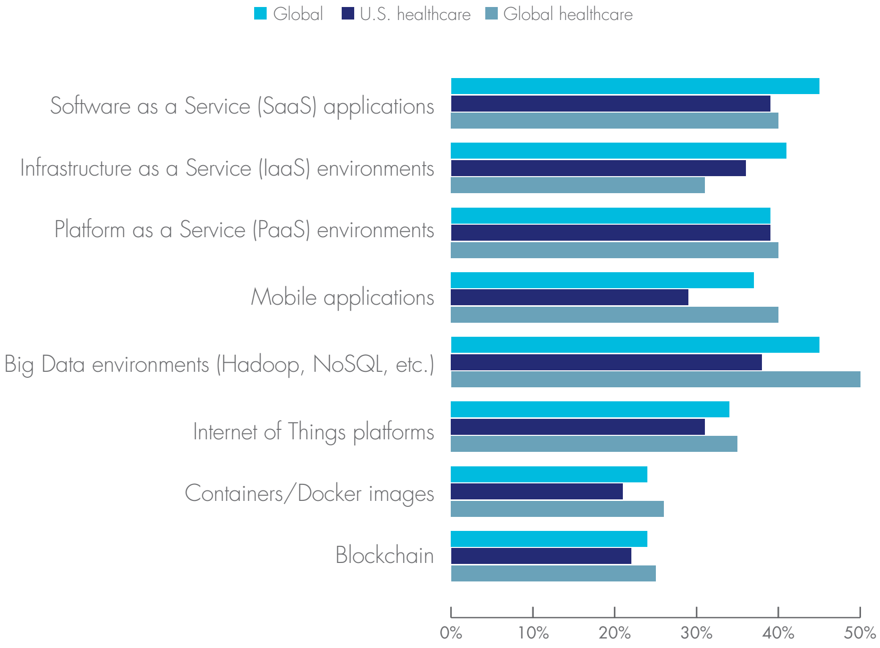


SENSITIVE DATA TRENDS IN NEW OR EMERGING TECHNOLOGY ENVIRONMENTS

In general, U.S. healthcare respondents are less likely to store sensitive data in 'new' or 'emerging' technologies than the global average. Still, while lower than the global average of 45%, an alarmingly high number of U.S. healthcare respondents (39%) report storing sensitive data in SaaS apps. Similarly, more than one-third (36%) of U.S. healthcare respondents report storing sensitive data in IaaS (vs. the global average of 41%), and 29% of U.S. healthcare report storing sensitive data on mobile applications (vs. 37% globally). One of the challenges with securing sensitive data in these new platforms is that they are all architected differently, and as such can have widely divergent methods and techniques for securing them.

"In general, U.S. Healthcare respondents are less likely to store sensitive data in 'new' or 'emerging' technologies than the global average."

Rates of using sensitive data in new or emerging technology environments

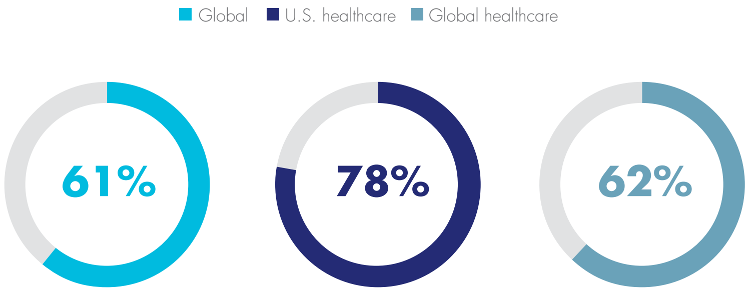


Cloud

As mentioned earlier, multi-cloud strategies can make data security very challenging. Each vendor may offer its own encryption and key management schemes, with the result that enterprises are forced to make sense of it all and manage yet another console.

Given that U.S. healthcare is among the more aggressive in terms of multi-cloud adoption, not surprisingly the top cloud security concern is managing, monitoring and deploying multiple cloud native security tools at 78%, well ahead of the 61% global average and 62% reported by global healthcare. U.S. healthcare is also more concerned about compliance requirements and increased vulnerabilities from shared infrastructure (both at 75%), well ahead of the global averages of 54% and 62%, respectively. Global healthcare is more inline with global averages at 57% and 64%, respectively.

Top cloud concern for healthcare:
Managing monitoring and deploying multiple cloud native security tools



"The top Big Data security concern here for U.S. healthcare respondents is that sensitive data can reside anywhere in a Big Data environment (35%), in line with the global average (34%)."

Strong preference for multi-cloud adoption is also reflected in responses towards cloud security controls. Key control is a potentially enormous issue, since organizations who cede control over keys to their service provider effectively relinquish full control over their data. Further, in a multi-cloud environment, leaving keys in the hands of cloud providers also introduces potential key management nightmares, particularly as the number of external cloud providers grows. On that note, it's an encouraging sign that U.S. healthcare is more likely to use encryption with local key control (48%), ahead of the global average of 44%, while global healthcare is among the highest at 51%. Conversely, just 29% of U.S. healthcare respondents are likely to use encryption with keys managed by the CSP than any other vertical, well below the 41% global average. However, it's worth noting that like the rest of the world, roughly just one-third of U.S. healthcare (32%) are implementing encryption in the cloud now (in line with the global average of 30% and global healthcare at 33%). Given both strong adoption of public cloud resources – and the fact that roughly 40% of firms on average are storing sensitive data in the cloud – clearly work remains to be done in terms of improving the security of valuable resources.

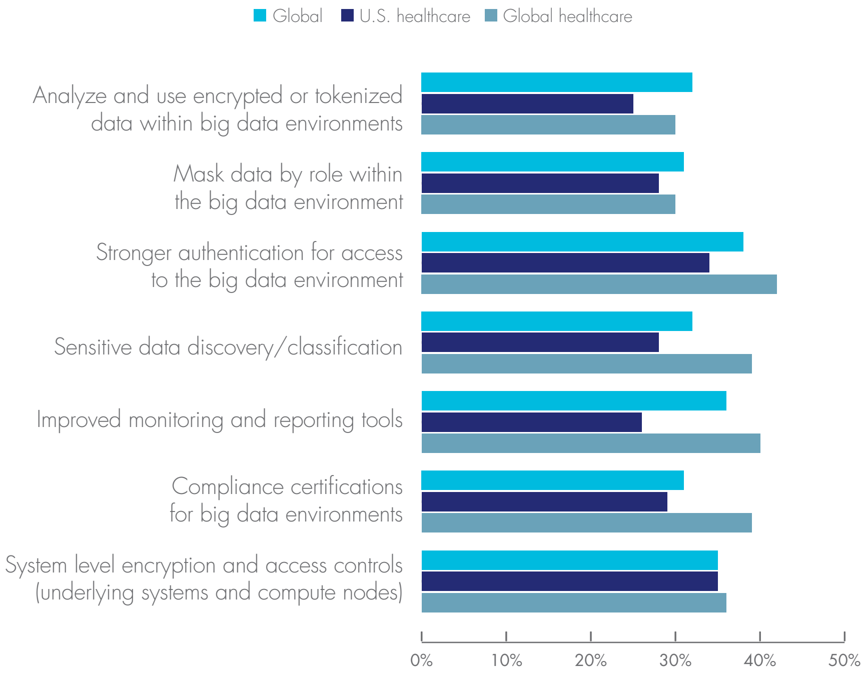
> *"It's an encouraging sign that U.S. healthcare is more likely to use encryption with local key control (48%), ahead of the global average of 44%, while global healthcare is among the highest at 51%."*

BIG DATA

The top Big Data security concern here for U.S. healthcare respondents is that sensitive data can reside anywhere in a Big Data environment (35%), in line with the global average (34%) and global healthcare (31%). Privacy violations from data originating in multiple countries was ranked second (28%), slightly below the global average of 30%.

The top choices for securing Big Data for U.S. healthcare – a new question posed this year – include system level encryption and access controls (35%) followed by stronger authentication (34%). In contrast stronger authentication ranks first for global healthcare (42%), followed by improved monitoring and reporting tools (40%).

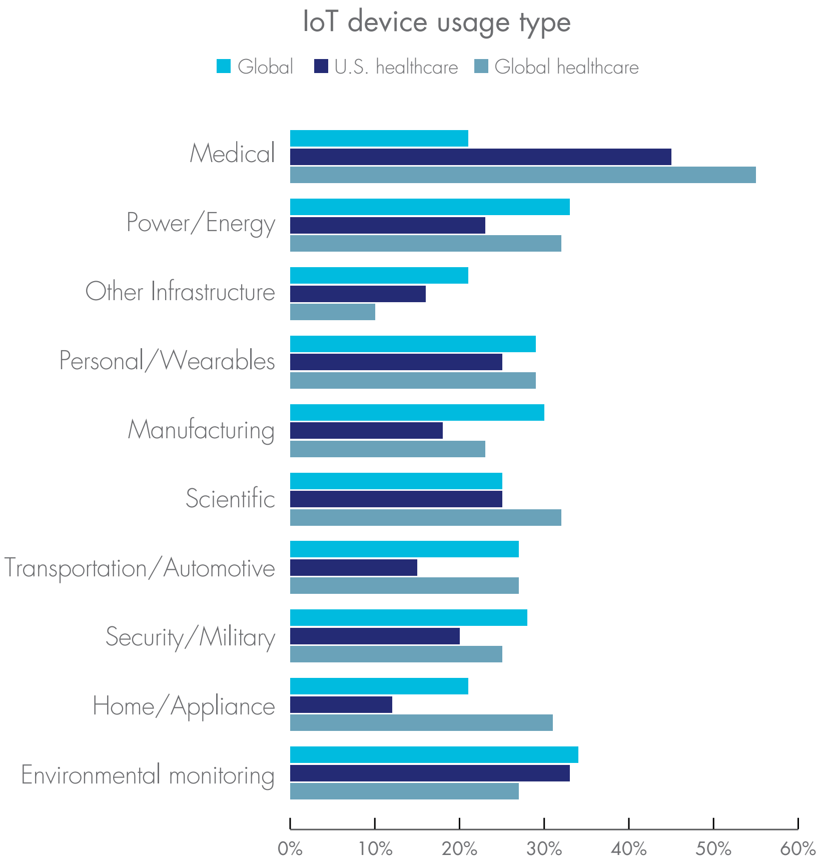
Capabilities needed to expand use of big data environments



IoT

Given the rapid increase in interest in IoT, and also IoT's potential impact on overall IT, we added several questions related to the topic this year. We added a new question to try to get a handle on the most popular types of IoT devices in use. For U.S. healthcare, not surprisingly, medical devices lead the list at 45%, more than double the global average of 21%; global healthcare is even higher at 55%. Environmental monitoring (33%) and scientific (25%) devices round out the top three for U.S. healthcare.

> *"For U.S. healthcare, not surprisingly, medical devices lead the list at 45%, more than double the global average of 21%; global healthcare is even higher at 55%. Environmental monitoring (33%) and scientific (25%) devices round out the top three for U.S. healthcare."*



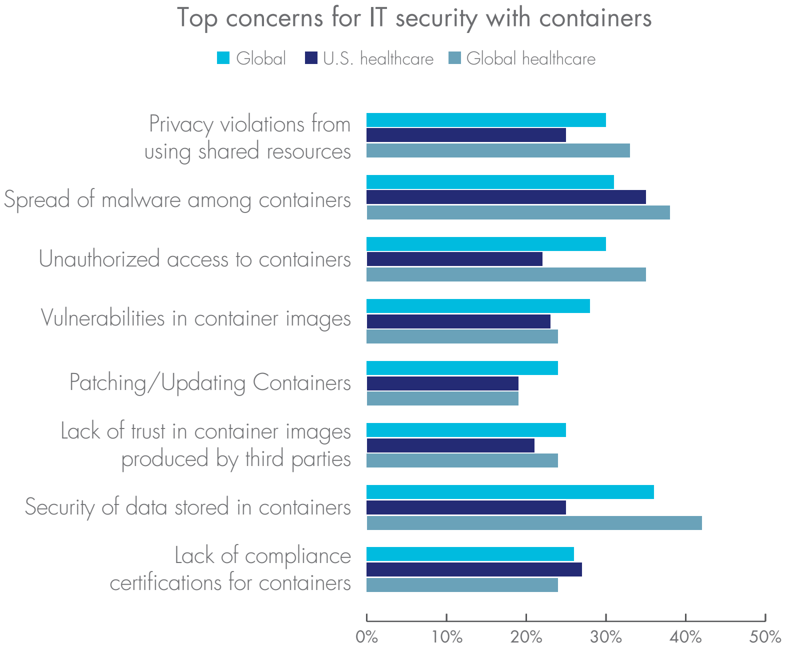
The biggest IoT security concerns for U.S. Healthcare are protecting sensitive data generated by an IoT device 25% (27% for Global Healthcare); followed by attacks on IoT devices (24%); and loss or theft of IoT devices (20%). Meanwhile, though encryption and tokenization is the top control globally (48%), and for Global Healthcare (57% - higher than any other vertical), the top IoT security controls for U.S. Healthcare are authentication and secure digital identification (49%), with encryption/tokenization in second place (42%).

“Top IoT security controls for U.S. Healthcare are authentication and secure digital identification (49%), with encryption/tokenization in second place (42%).”

DOCKERS/CONTAINERS

Nearly 21% in U.S. healthcare and 19% for global healthcare report using containers for 'production' applications, below the global average of 24%. Globally, the top security concern is the security of data stored in containers (36%), and also for global healthcare (42%). U.S. healthcare respondents, however, are most concerned with the spread of malware between containers (35%), followed by lack of compliance certifications (27%).

> *"Nearly 21% in U.S. healthcare and 19% for global healthcare report using containers for 'production' applications, below the global average of 24%."*



Despite being most concerned about malware, anti-malware was less of a priority for U.S. healthcare when it comes to technologies that would boost usage of containers (35%), well below the global average of 45%; digital signatures for containers was number two. For global healthcare, anti-malware was the clear top choice (56%), followed by encryption at (44%).

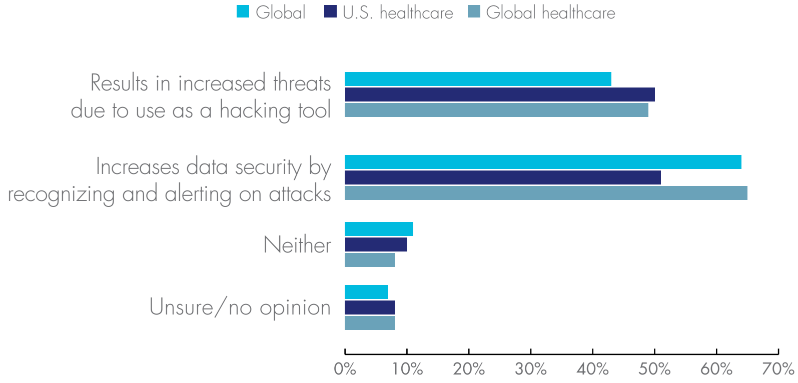
AI/MACHINE LEARNING – A DOUBLE-EDGED SWORD

Like most security tools, artificial intelligence and machine learning can be used both for beneficial and malicious uses. Vulnerability scanners are a good example – they can be used both by 'good guys' to scan their networks for vulnerabilities as part of a pen test, but also by attackers to find a way to infiltrate a network. Thus, we asked a similar question about the impact of AI and ML on security, and found that both are broadly seen as potentially having both positive and negative consequences for security.

The good news is that perceived beneficial uses of AI (64%) outnumber the malicious uses (43%) for the global average. But for U.S. healthcare, there is more of an even split – 51% believe AI/Machine learning increases security, while 50% believe it gives an edge to potentially malicious uses. Global healthcare, by contrast, is more in line with global averages, with 65% viewing AI and ML as enhancing security, with 49% recognizing increased threats.

> *"The good news is that perceived beneficial uses of AI (64%) outnumber the malicious uses (43%) for the global average. But for U.S. healthcare, there is more of an even split – 51% believe AI/Machine learning increases security, while 50% believe it gives an edge to potentially malicious uses."*

Machine learning and AI – threat or benefit

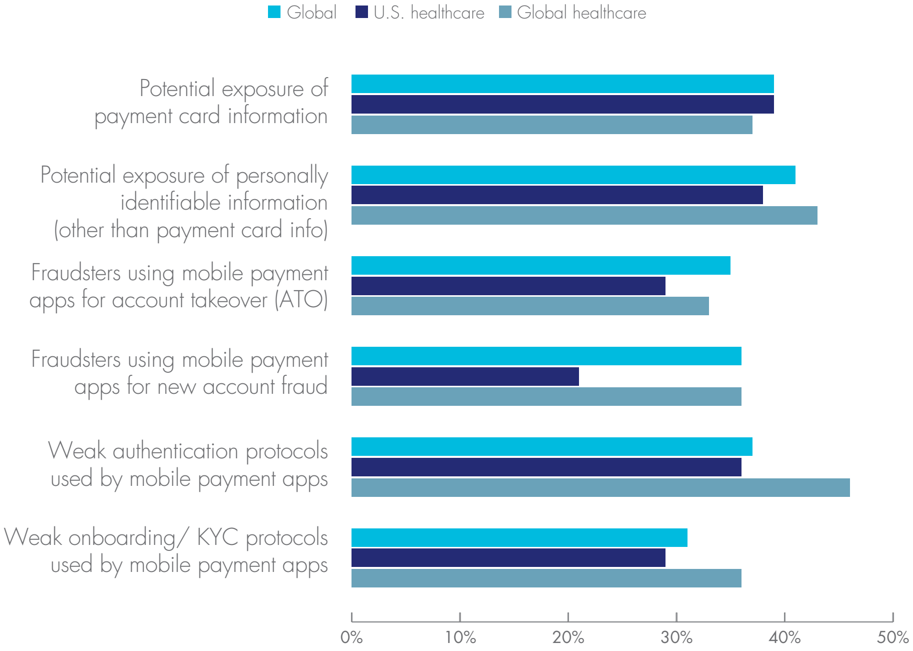


MOBILE PAYMENTS

Another new area of question surrounds the impact and security implications of increased use of mobile payments technologies. The top security concerns for mobile payment applications for U.S. Healthcare are the potential exposure of payment card information (39%, in line with the global average), followed closely by potential exposure of personally identifiable or PII at 38% versus the global average of 41%. For Global Healthcare, weak authentication protocols used by mobile payment applications are the top concern at 46%.

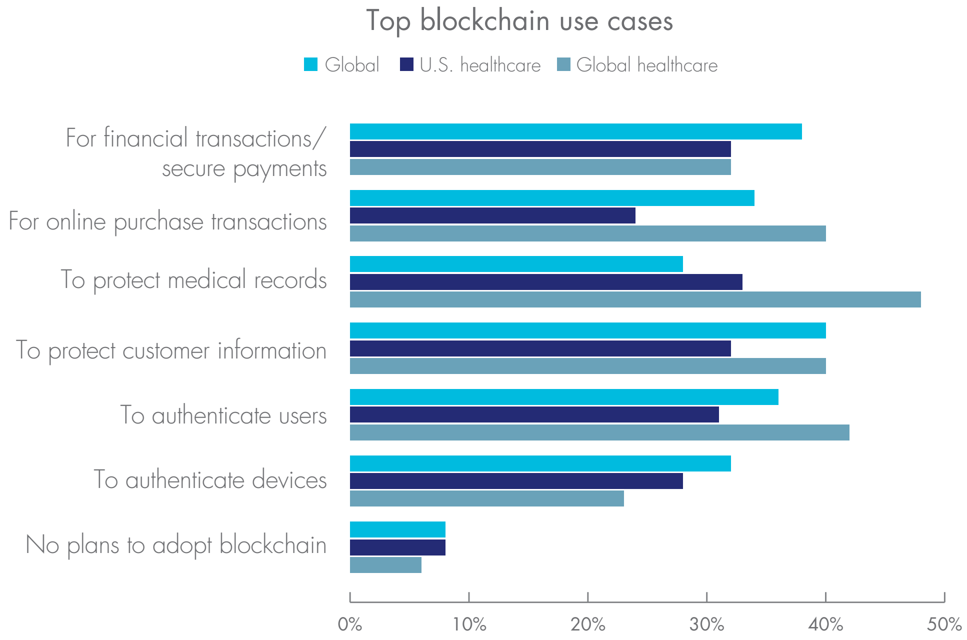
> *"The top security concerns for mobile payment applications for U.S. healthcare are the potential exposure of payment card information (39%, in line with the global average), followed closely by potential exposure of personally identifiable or PII at 38% versus the global average of 41%."*

Security concerns for mobile payments



BLOCKCHAIN

Blockchain could be one of the most significant new developments in security in years. And while much of the buzz has been around Bitcoin and cryptocurrencies, blockchain also has applications securing transactions, protecting data and managing identities, to name a few. Though it is still very early for commercial implementations of blockchain, just 8% of U.S. healthcare and 6% of global healthcare respondents have no plans to adopt blockchain, in line with global averages. Currently, the main use cases for blockchain in U.S. healthcare include protecting medical records (33% vs. 38% for the global average, and 48% for global healthcare). Financial transactions and secure payments are in second place for U.S. healthcare (32%), tied with protecting customer information.



“Though it is still very early for commercial implementations of blockchain, just 8% of U.S. Healthcare and 6% of Global Healthcare respondents have no plans to adopt blockchain, in line with global averages.”

RECOMMENDATIONS

RE-PRIORITIZE YOUR IT SECURITY TOOL SET	With increasingly porous networks, and expanding use of external resources (SaaS, PaaS and IaaS), especially among rapid adopters pursuing multi-cloud strategies like U.S. healthcare, traditional end point and network security are no longer sufficient, yet remain a top spending priority. Data security offers increased protection to known and unknown sensitive data found within advanced technology environments, and platform offerings and those that provide automation help 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 privacy mandates like HIPAA and GDPR.
DON'T JUST CHECK OFF THE COMPLIANCE BOX	Given heavy compliance burdens, U.S. healthcare respondents continue to have more faith in compliance mandates than other sectors. While compliance can serve as an important signpost on the path to greater security, however, healthcare organizations should consider moving beyond compliance and adopting security tools such as authentication, encryption or tokenization that may be more appropriate as healthcare agencies increasingly adopt new technologies like cloud, mobile apps, Big Data and IoT.
ENCRYPTION AND ACCESS CONTROL	Encryption needs to move beyond laptops and desktops. **Cloud:** Less than one-third of healthcare respondents encrypt sensitive data in public cloud environments. U.S. healthcare organizations should consider doing more to encrypt data and also manage keys locally to retain full control over sensitive data in multi-cloud environments. **Big Data:** Deploy system-level encryption and access controls and strong authentication. **Containers:** Deploy anti-malware to prevent the spread of malware between containers and also encrypt and control access to data within containers. **IoT:** Use secure device ID and authentication, as well as encryption to protect data generated by medical IoT devices. **Data Sovereignty:** Consider both encryption and tokenization as a way to avoid hefty fines for violating privacy laws like GDPR and healthcare-specific regulations such as HIPAA. **Mobile payments:** Encryption and/or tokenization can also help address the main risk from mobile payments: loss of PII **Blockchain:** While it may be early for commercial implementations, blockchain promises to play a big role in terms of securing transactions, authenticating users and securing data from tampering.

ANALYST PROFILE

Garrett Bekker
Principal Analyst
451 Research

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 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 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 eSecurity is part of Thales Group.

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

PLATINUM PARTNERS – 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.

THALES

www.thalesesecurity.com