THALES

451 Research®

2018 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

U.S. HEALTHCARE EDITION

EXECUTIVE SUMMARY

#2018DataThreat

THE TOPLINE

Healthcare data – Code Red. Over 77% of U.S. healthcare organizations breached to date

Driven by increased attacks from criminal hackers, and pervasive regulations, healthcare organizations in the U.S. are encountering numbingly complex issues when it comes to data security. Healthcare data is more desirable to criminal hackers than ever. While a stolen credit card is valuable only for a limited time (and has a correspondingly lower value), PHI and electronic medical records (EMR) contain immutable personal data that can and does fetch hundreds of dollars per stolen record on illegal online markets. U.S. healthcare organizations are also beset with an intricate web of compliance requirements with the HIPAA/HITECH act only the tip of the iceberg. Federal and state privacy laws, Electronic Prescriptions for Controlled Substances (EPCS) as well as US Food and Drug Administration (FDA) requirements are among others requiring healthcare organizations' compliance.

DATA BREACHES SURGE IN HEALTHCARE

Breached ever

77% More than **3 out of 4** large U.S. healthcare organizations have now been breached ($250M or larger)

Breached in the last year

2.5x

In the last year, almost **half have been breached** – **2.5x** higher than the 2016 results

HEALTHCARE'S DIGITAL TRANSFORMATION ENABLING BETTER HEALTHCARE, CREATING RISKS TO DATA

95% use digital transformation technologies with **sensitive data**

High levels of adoption compound the problem

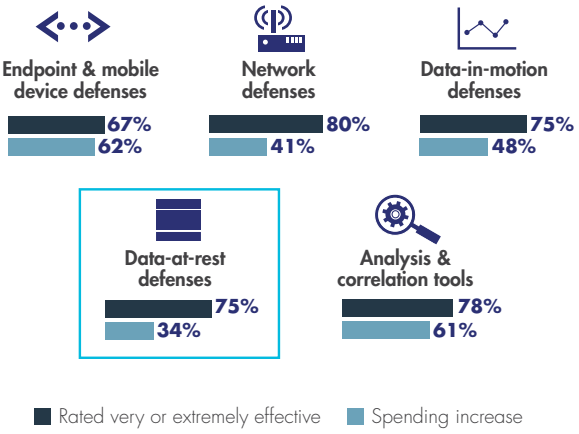
"GIVEN THAT U.S. HEALTHCARE IS AMONG THE MORE AGGRESSIVE IN TERMS OF MULTI-CLOUD ADOPTION, NOT SURPRISINGLY THE TOP CLOUD SECURITY CONCERN IS MANAGING, MONITORING AND DEPLOYING MULTIPLE CLOUD-NATIVE SECURITY TOOLS AT 78%."

—Garrett Bekker, 451 Research Principal Analyst, Information Security

NOT PUTTING THEIR MONEY WHERE THEIR DATA IS

"U.S. HEALTHCARE PLANS TO SPEND THE MOST ON SECURITY FOR ENDPOINT AND MOBILE DEVICES, DESPITE RANKING THESE AS LEAST EFFECTIVE."

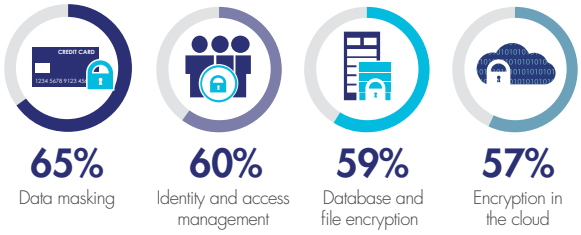
—Garrett Bekker, 451 Research Principal Analyst, Information Security



ENCRYPTION IS THE CRITICAL SOLUTION

Encryption would increase usage of digitally transformative technologies if available

Good news – Encryption tools 3 of the top 4 data security tools being deployed this year:



These pressures are clearly putting healthcare IT security professionals in a tough spot. Although the top motivator for IT security spending is avoiding the financial penalties from a data breach (49%), we've now reached the point where more than three out of four healthcare IT security pros we polled report that their organization has encountered a data breach. In fact, a total of 48% were breached in the last year alone. Clearly, some changes are needed.

HEALTHCARE DATA – CODE RED

Data breaches are surging in healthcare

In healthcare organizations, patient care is always the priority – with IT in place to serve technical and business needs. But today, we use electronic personal health records (ePHRs) to share patient information across healthcare providers, and many treatments require the deep use of electronic analysis with digital technologies or cutting-edge technical treatments, or even net-connected devices. These changes result in "honey pots" of data that hackers find extremely valuable, and have resulted in additional compliance requirements on healthcare organizations for data security. Some of these requirements have strong "teeth" in the form of penalties for lost personal information or consequences on failure to meet an audit requirement. The result – IT is now front and center not only in enabling patient care, but also in protecting patient data. The problem lies in the fact that, in spite of regulations and requirements, healthcare IT security is not succeeding when it comes to protecting data.

Overall, IT security pros in healthcare reported that their organizations have been breached more than reported by their counterparts in U.S. federal agencies, U.S. retail organizations and U.S. financial services enterprises. The results show a rate of 77% of healthcare organizations being breached at some time in the past and 48% in the last year alone. Only two years ago in 2016, this rate of "breaches in the last year" for healthcare providers was only 18% – It's now two and a half times higher. How has this affected the healthcare IT security pros we polled? They are worried. In results from last year's survey, only 7% showed as very or extremely vulnerable to threats against their data. Today, 37% show as very or extremely vulnerable – up more than five times last year's rate.

Breached ever

77%

More than **3 out of 4** large U.S. healthcare organizations have now been breached ($250M or larger)

Breached in the last year

2.5x

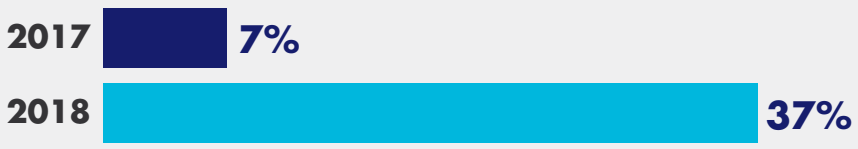
In the last year, almost **half have been breached** – **2.5x higher** than the 2016 results

Breached more than once

10%

Have been breached both in the **last year and previously**

Rates of extremely vulnerable to data threats



"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."

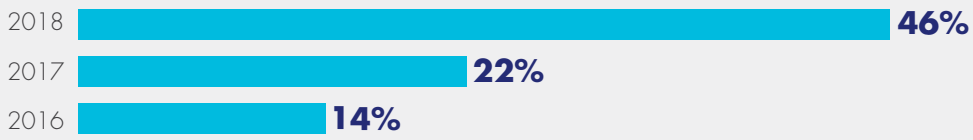
—Garrett Bekker, 451 Research Principal Analyst, Information Security
Author of the 2018 Thales Data Threat Report

Good news

We also see a trend of good news. As noted earlier, the top impact on IT security spending among the healthcare IT security pros that we polled was avoiding the financial penalties resulting from a data breach at 49%, while the top motivation last year was meeting compliance requirements at 57%. It seems clear that the penalties for data breaches are starting to hurt, and motivating healthcare organizations to go beyond compliance requirements and stop the pain.

Penalties and breaches also seem to be affecting organizations' spending for IT security – The purse strings are loosening to help protect their organizations. While 84% overall report that IT security spending is increasing, 46% are reporting that their spending in the next year will be "much higher" versus only 22% reporting "much higher" spending last year. At the same time, lack of budget has not been the top reason for failing to increase data security spending. Lack of budget was cited by only 33% of respondents as a reason for not deploying more data security tools in both our 2017 and 2018 report data sets. Last, IT security budget assigned to data security is being well spent on the technologies that should make a big difference in protecting data. Three of the top four are encryption technologies that place protecting for data with the data itself – protecting information even from compromised accounts or malicious insiders; Data masking (65%), Database and file encryption (59%) and encryption in the cloud (57%).

Healthcare IT security spending increases
Rates of "Much Higher" spending increases by year



Top data security tools planned to be implemented this year for healthcare

HEALTHCARE'S DIGITAL TRANSFORMATION

Enabling better healthcare – Creating new risks to data

Digital transformation has evolved as a significant driver for healthcare data threats. The overall adoption of Cloud and SaaS applications, Big Data implementations, IoT, containers, mobile payments and blockchain technologies also raises security risks owing to their relative newness, the unique approaches required to protect data within each environment and the sheer scale of deployments. And sensitive data will be used within these environments to create extensive data sets, analyze results, collaborate and store critical information – as reported by 95% of respondents.

In widest use for digital transformation in healthcare were cloud (100%) and big data (96%), while other technologies like IoT are within the adoption curve, with IoT leading the pack – 45% of healthcare organizations are already using IoT with medical devices.

95% use digital transformation technologies with sensitive data

High levels of adoption compound the problem

Multi-cloud operations creating the biggest concerns

Healthcare organizations appear to have gone "all in" on the use of cloud services. 58% are using more than 50 Software as a Services (SaaS) services, matched in our survey of industries only by U.S. federal agencies, and well ahead of financial services (45%) as well as retail (43%). With 63% also using more than three Infrastructure as a Services (IaaS) offerings and 52% more than three 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 levels of complexity driven by the unique requirements for protecting, and retaining control of, data within this range of environments.

Only **32%** are using encryption to protect cloud data today

Levels of concern are high

In a traditional data center, not only was data physically secured within the four walls of the enterprise, but all of the infrastructure underlying implementation tools and networks were also under the direct control of the healthcare organization. Now, for IaaS and PaaS, a specific data security plan must be created for each deployment and environment, then enforced by policy, operational methods and tools. For SaaS environments, the case is more complex. In many SaaS environments, organizations are given 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. Healthcare organizations need their data under their control. Encryption – with local encryption key control – required.

Massive adoption compounds the problem

63% Using **3 or more IaaS** providers

52% Using **3 or more PaaS** providers

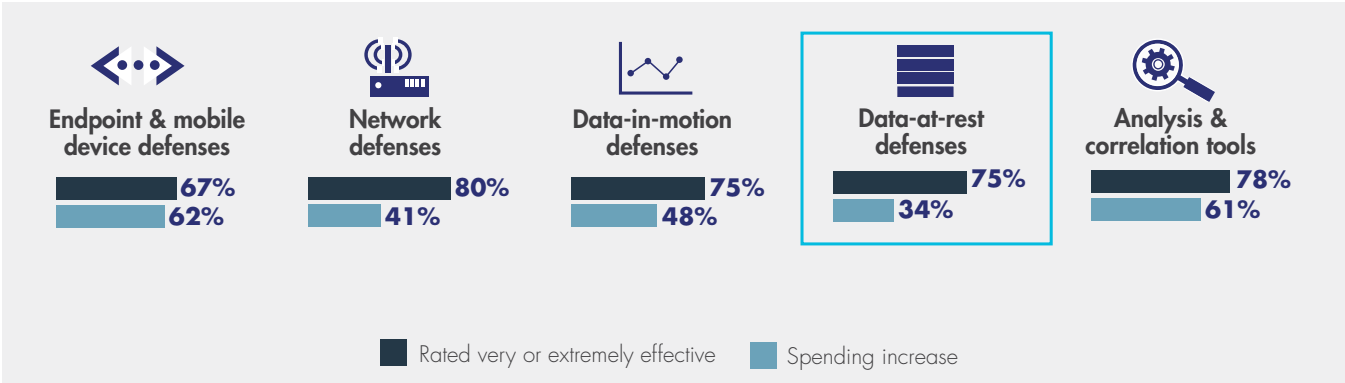
58% Using more than **50 SaaS applications** – Where data is inherently harder to control

Cloud computing is low on the Healthcare IT security spending priority list

NOT PUTTING THEIR MONEY WHERE THEIR DATA IS

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

This year for the first time in our polling, we found that respondents recognize the defenses designed specifically for protecting data are the most effective tools for doing so – except in healthcare. Respondents from federal agencies, retail enterprises and financial services organizations all rate data-at-rest and data-in-motion tools as most effective at protecting data – but respondents from healthcare organizations did not. Network (80%) and analysis and correlation tools (78%) were top rated in effectiveness, with data-at-rest and data-in-motion tools tied at 75% each in ratings of very or extremely effective.

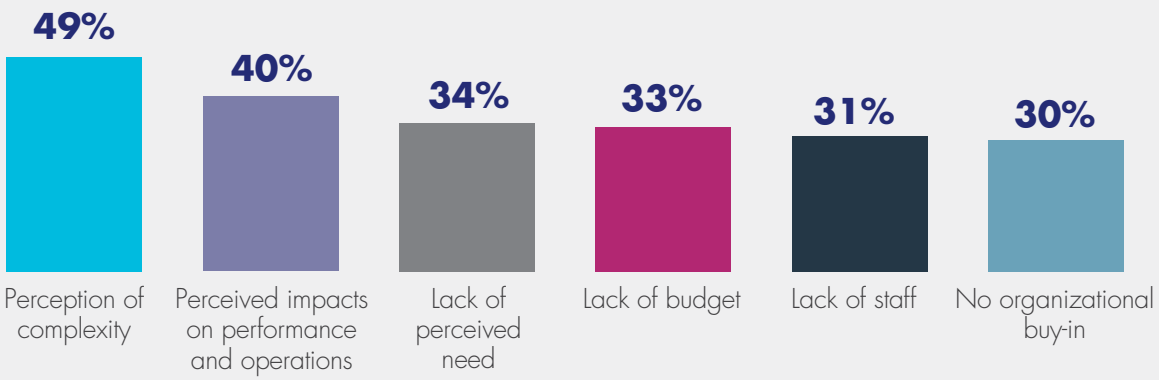


Defenses around data also weren't top priorities for spending increases – in fact increases in data-at-rest defenses were dead last in responses from healthcare providers at 34%. Endpoint and mobile defenses were rated least effective at protecting data (at 67%), yet getting the largest spending increase (62%). It's worth noting that some of this emphasis on the endpoint may be due to last year's rash of ransomware incidents at hospitals and other healthcare providers, giving justification for this increase due to an industry-specific problem. But there are also some misconceptions. At the moment, network defenses which were rated as most effective at protecting data (80%), 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 off a network with network-based security controls. The most effective solutions are security controls that provide an additional layer of protection directly around data sets. Data-at-rest and data-in-motion security tools can reduce attack surfaces, and provide the information needed to quickly find and stop attacks in progress around large data sets. But, unlike their counterparts in other industries, healthcare IT security pros have yet to realize this fully.

> "U.S. healthcare plans to spend the most on endpoint and mobile devices, despite ranking these as least effective."
>
> *—Garrett Bekker, 451 Research Principal Analyst, Information Security*
> ***Author of the 2018 Thales Data Threat Report***

In part, the usual concerns about budget and priorities are cited as reasons for low data security adoption. But perhaps a larger part of the reason for the disconnect may be the perception that data security is hard, expensive and has a high impact on operations. Usually, this perception is the result of having experience with older "legacy" data security tools. Modern tools have lower costs than in the past, extremely low-performance overhead (as a result of using hardware encryption capabilities built into today's CPUs) and a resulting lack of impact on business processes and operations. In some cases, no changes are required to applications and operations on the deployment of data security tools.

Perceived barriers to data security



ENCRYPTION IS A CRITICAL TOOL NEEDED TO PROTECT SENSITIVE DATA

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

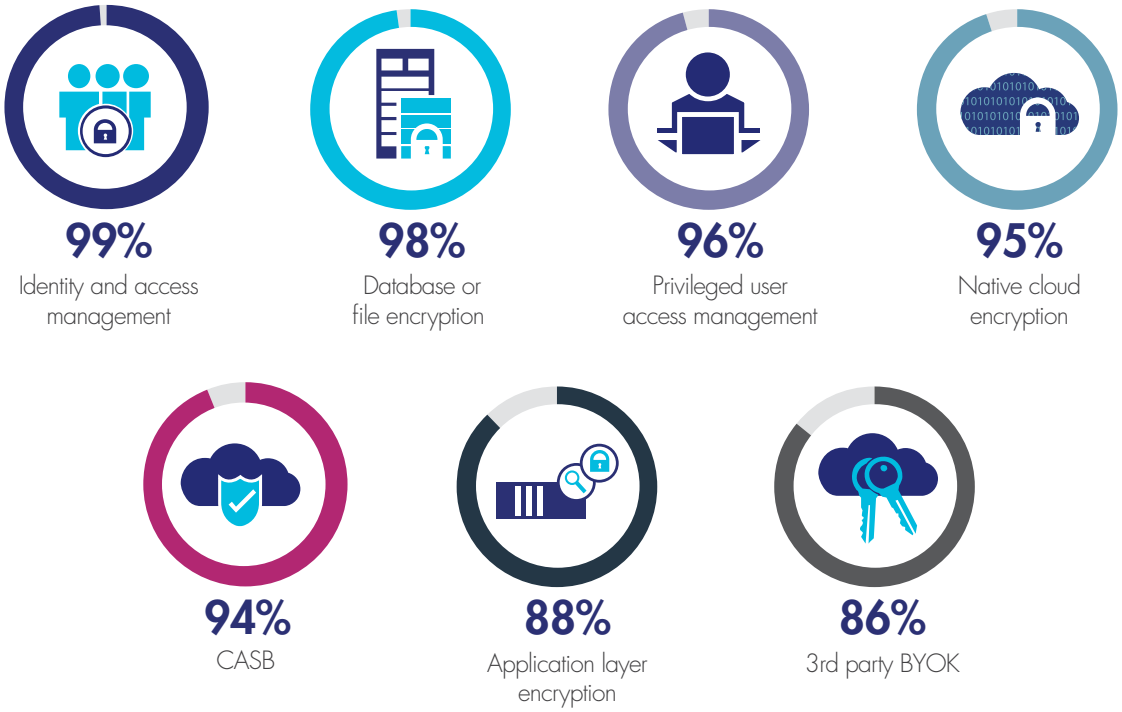
Based on our data, it's not clear that the healthcare organizations whose IT security pros we polled understand that they are now the custodian of not only their patients' physical and mental health and wellbeing but their financial health and wellbeing as well. Healthcare data is a prime source for the information that enables highly profitable identity theft activities. Once compromised, this healthcare data is permanently "in the wild" and available to hackers and criminals to compromise identity for financial gain, again and again. Consumers who encounter financial fraud based on this data are permanently at risk due to the depth of personal information exposed. Medical fraud can be even more devastating but is much less common.

What are the best controls to prevent this permanent loss? Encryption, access controls and monitoring of data access activities. Properly implemented wherever there is a data store or data transmission, these controls immensely reduce the attack surface, and make it possible to catch data thieves in action. Healthcare organizations need to take this into account in their planning and keep in mind that modern tools change what used to be a difficult, complex and resource intensive process, into an everyday tool that protects both their organization and their patients.

Good news

There's some good news to mix in with the other results this year. Although spending on data-at-rest technologies is getting the lowest spending increases, there are still projects underway to help safeguard data within healthcare organizations. Respondents identified a range of solutions that they are already implementing, or plan to implement this year, including cloud encryption, database/file encryption, identity and access management, BYOK, application encryption and more. Implementation of these tools represents solid progress towards protecting data across both newer environments used for digital transformation and traditional data centers, but may well be limited to specific implementations and uses, rather than all sensitive data that needs protection.

Implementing or planning to implement data security tools in healthcare this year



Encryption is also a clear leader among tools that healthcare IT security professionals are looking for to increase usage of cloud, big data, IoT and containers. Cloud encryption tools such as encryption gateways and third-party encryption key managers for cloud environments are also showing strong plans for adoption as ways that respondents are looking at to bring cloud-based data back under agency control.

48%

Cloud: Data encryption is the top tool needed for more cloud use

35%

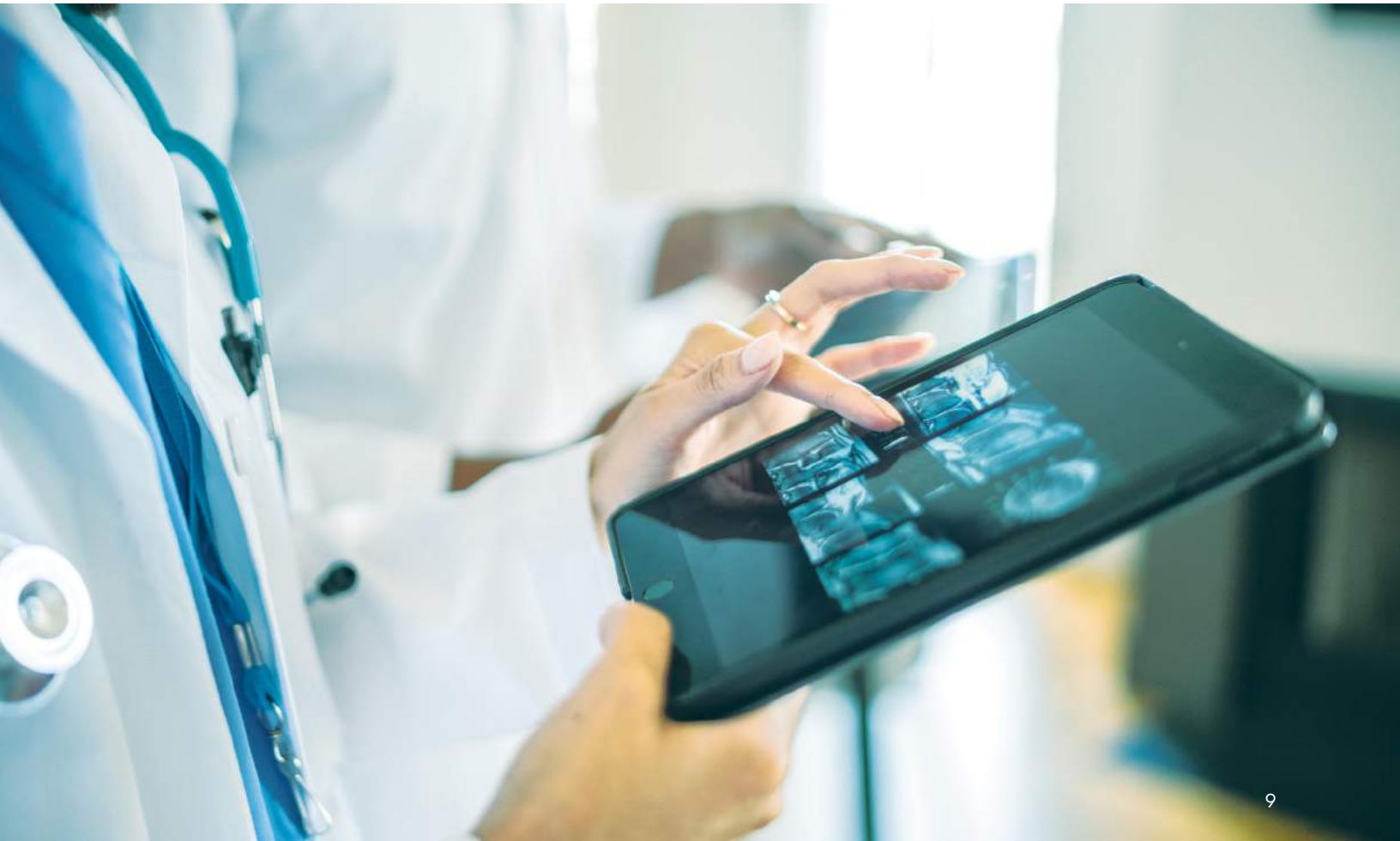
Big Data: System level encryption and access controls

49%

IoT: Secure authentication (an encryption technology) a top tool need for more IoT adoption

31%

Containers: Availability of encryption tools would increase adoption



"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."

"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."

"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 feeling either 'very' or 'extremely' vulnerable to sensitive data threats."

—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

GuidePoint SECURITY

cloud security alliance℠

GEOBRIDGE

CRITICALSTART

OASIS

THALES

www.thalesesecurity.com