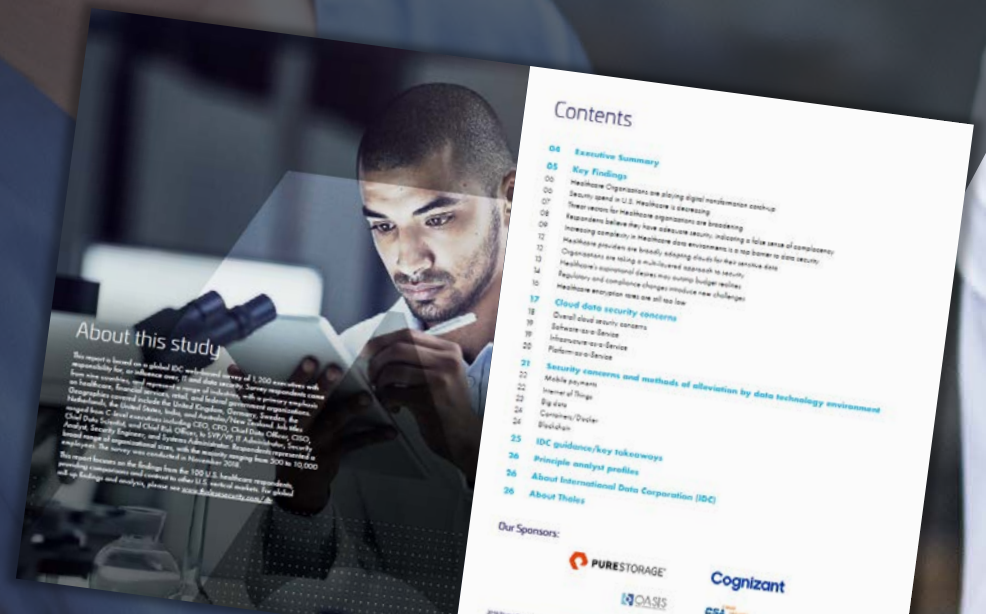

THALES

The Changing Face of Data Security

2019 Thales Data Threat Report

Healthcare Edition



THALES

Healthcare organizations universally use digital transformation technologies with sensitive data

THALES

100%

of respondents will **use sensitive data** with **digitally** transformative technologies.

THALES

less than

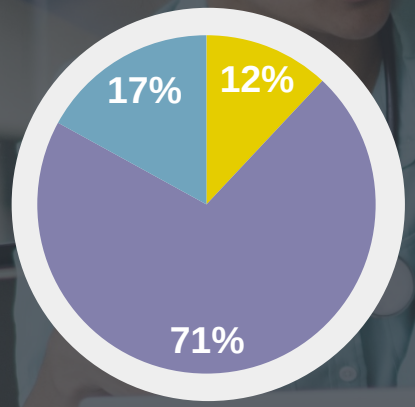
38%

of respondents are using data encryption within these environments

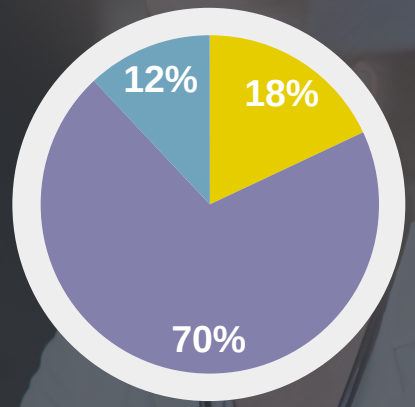
The reality of the multi-cloud enterprise

Multi-cloud environments make the job of protecting data more complex.

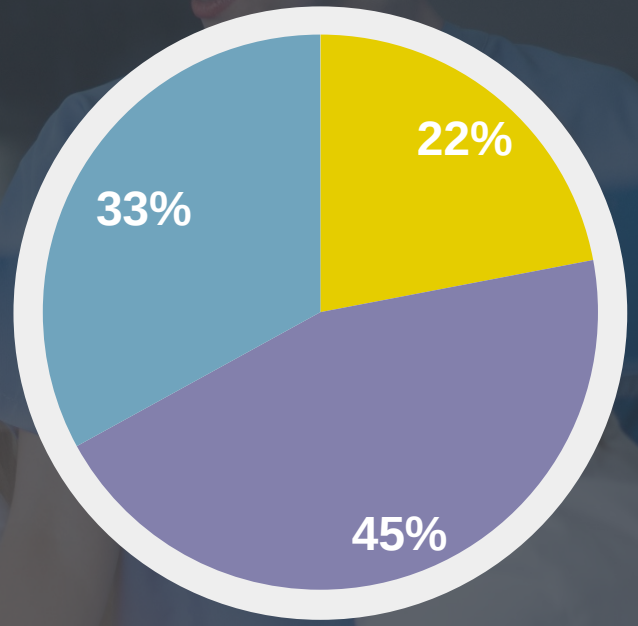
Number of cloud environments



IaaS



PaaS



SaaS

- 4 or more
- 2 or 3
- 1

- More than 50
- 11 - 50
- 10 or less

THALES

Driven by the need to protect digital transformation's complex data environments,

46%

rated complexity as the top barrier to implementing data security.

Data breach resistance: no one is immune

Healthcare has the highest breach rates

U.S. Healthcare reported the highest rates of data breaches of any industry segment surveyed.

70%

of U.S. healthcare enterprises say that they have been breached at any time in their history, with…

33%

... experiencing a breach within the past year alone.

Encryption rates are low

Despite recognizing the importance of protecting sensitive data, encryption rates throughout the enterprise are surprisingly low.

• **The Patient Protection and Affordable Care Act of 2010 (PPACA)** created new care delivery and reimbursement models, such as accountable care organizations (ACOs) and value-based purchasing plans, focused on reimbursing for care coordination, improving quality, and improving patient outcomes rather than paying providers on a fee-for-service or volume basis. As a result of the PPACA, more electronic patient health information (ePHI) has been created and shared with other entities, increasing the risk of a privacy/security breach.

• **Under ARRA's HITECH Act, the HIPAA Omnibus Rule** published in January 2013 implements the new privacy and security provisions proposed. As a result, privacy breach notification, minimum use, and disclosure reporting requirements become more stringent. The risks and liabilities associated with privacy breaches increase and annual penalties for violations can total up to $1.5 million per provision, up from $25,000. Security professionals must consider the complex healthcare environment with its highly mobile and transitory workforce.

• **The Drug Enforcement Agency's Electronic Prescription of Controlled Substances (EPCS)** passed in 2010 requires two-factor authentication for each electronic prescription authorized physicians write for controlled substances.

• **The SUPPORT for Patients and Communities Act** signed into federal law in 2018 includes an electronic prescribing requirement for all controlled substance prescriptions for a covered Medicare Part D plan. The compliance deadline is January 1, 2021. In an effort to combat the opioid crisis many states are implementing similar laws to mandate EPCS.

"Compliance requirements are clearly driving a significant portion of the organizations' data security efforts."

These compliance requirements are clearly driving a significant portion of the organizations' data security efforts. When asked which statement best matched their data privacy/sovereignty stance, encryption was the strategy cited most often by healthcare respondents, and it was the healthcare industry that used encryption at the highest rate for sensitive data – 50% (see Figure 13).

Figure 13 – Data privacy/sovereignty stance
Source: 2019 Thales Data Threat Report Survey, IDC, November, 2018

Healthcare encryption rates are still too low

As they look to safeguard sensitive data, the good news for U.S. healthcare organizations is the rate at which they use encryption is higher than their global counterparts, and higher than the global sample as a whole. The bad news is that at rates of between 25% and 38% depending on the type of data, these rates of encryption are still too low, especially given the encryption requirements set forth in HIPAA (see Figure 14). This points to greater vulnerability if IT systems are infiltrated because it implies that administrative, financial AND clinical data is available to bad actors in clear text. Lost mobile devices would also pose a similar risk.

"Greater use of encryption of files and fields in databases can help guard against infiltration and theft of data."

Figure 14 – Encryption use rates
Source: 2019 Thales Data Threat Report Survey, IDC, November, 2018

The top use cases for U.S. healthcare organizations to use encryption are full-disk encryption within their own datacenters, files and fields in databases, and within public cloud environments. Each of these is practiced by 38% of the U.S. healthcare sample, rates much higher than the global sample. And while it's obviously a positive to use FDE, it should also be noted that the protection FDE provides is limited to loss, theft, or improper disposal of drives. While this is good for lost or stolen computers, it only "checks the box" for compliance purposes and provides little to no protection for other types of datacenter threats such as system compromises, insider threats, and application-level attacks on data.

Greater use of encryption of files and fields in databases can help guard against infiltration and theft of data, much like in the Target attack several years ago. Cybercriminals gained access to the network via the HVAC system, then accessed the customer credit card database and exfiltrated that data which was in clear text and not encrypted.

THALES

38% or less

of healthcare organizations polled say they use encryption for the vast majority of use cases studied.

Data privacy and sovereignty regulations impact nearly all

Enterprises in healthcare face a daunting array of privacy and compliance regulations including HIPAA/HITECH, PPACA, the Patients and Communities Act, and EPCS.

THALES

90%

will be affected by data privacy and sovereignty regulations.

THALES

62%

will use encryption and tokenization to meet these requirements.

Data Security doesn't have to be hard

It's vitally important. Organizations need to take a fresh look at how they provide data security.

Visit thalesesecurity.com/DTR-healthcare to download the full report, including IDC recommendations.

IDC guidance/key takeaways

Data security is not easy, particularly for healthcare organizations, many of which are working diligently to achieve the benefits of digital transformation. And as healthcare organizations continue along their DX journey, they need to reexamine their data security stances. In particular, IDC recommends healthcare security professionals consider the following:

- **Focus on all threat vectors.** Today's threats come from all over, and healthcare organizations need to remain vigilant. As bad actors continue to evolve their methods, security professionals need to keep their guard up and continually evolve to protect against them. As guardians of sensitive patient data, and with stringent penalties for noncompliance, healthcare organizations and must take this responsibility seriously.
- **Invest in modern, hybrid and multi-cloud-based data security solutions that scale to modern architectures.** Yesterday's perimeter-security defenses are no longer sufficient to protect against the myriad of data threats facing the organization. With more devices at the edge, the expanding threat surface is increasingly borderless, so the legacy perimeter approach doesn't work. Healthcare providers must recognize the increased complexity of today's security environment and implement solutions that span legacy concerns as well as modern, cloud-based digital transformation technologies. "As a service" and "as a platform" solutions that cross environments can help eliminate much of this complexity and cost – making the job much more manageable.
- **Prioritize compliance issues.** Federal regulations governing healthcare organizations have significant penalties for non-compliance. And in today's unpredictable political environment, it's hard to know what may be around the corner. Healthcare providers need to ensure they are not only diligently following current regulatory compliance mandates, but that they also have sufficient flexibility built into their technologies to handle new requirements when they occur.
- **Data security, starting with encryption and access management, is an important part of the mix.** As healthcare providers continue to place greater amounts of their data in the cloud, they must adopt new data security strategies. Even selecting a top-tier cloud provider doesn't remove the burden of an organization doing its part to provide data security, and this starts with encryption, authentication, and access management.

Principal analyst profiles

Frank Dickson
Frank Dickson is a Program Vice President within IDC's Security Products research practice. In this role, he provides thought leadership and guidance for clients on a wide range of security products including endpoint security, identity and access management, authentication, threat analytics, and emerging products designed to protect transforming architectures and business models.

Lynne Dunbrack
Lynne Dunbrack is Research Vice President for IDC Health Insights responsible for the research operations for IDC Health Insights. She manages a group of analysts who provide research-based advisory and consulting services for payers, providers, accountable care organizations, IT service providers, and the IT suppliers that serve those markets. Lynne also leads the IDC Health Insights' Connected Health IT Strategies program. Specific areas of Lynne's in-depth coverage include mobile, constituency engagement, interoperability, health information exchange, privacy, and security. Technology coverage areas include clinical mobility (physician facing) and mobile health (consumer facing), health information exchange, end-to-end remote patient health monitoring for health, wellness and chronic conditions, Internet of Things (IoT), personal health records and member, patient, provider portals, kiosks, videoconferencing and online care, unified communications, aging in place, and social.

About International Data Corporation (IDC)

IDC is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,100 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries.

IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG), the world's leading media, data and marketing services company that activates and engages the most influential technology buyers.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Thank you to our sponsors:

RESEARCH AND ANALYSIS FROM:

Decisive technology for decisive moments

thalesesecurity.com/DTR-healthcare

#2019DataThreat