thalesesecurity.com

THALES

Executive Summary
2019 Thales Data Threat Report

Global Edition

#2019DataThreat

RESEARCH AND ANALYSIS FROM:

IDC ANALYZE THE FUTURE

Digital transformation is pervasive – and is putting sensitive data at risk

Digital transformation has become a do-or-die proposition for traditional enterprises and a fundamental disruptor that opens the door for new competitors in traditional markets. This year's study found that 97% of organizations surveyed are implementing digital transformation with 37% reporting aggressive transformation – actively disrupting markets or tightly linking their digital transformation efforts to management's vision. However, these efforts are inherently adding risks to their organizations' sensitive data. Not only are 97% using sensitive data within digitally transformative environments, but respondents also had misconceptions about the level of security they are implementing for these environments and the tools that will best protect that information.

97%

of respondents will use sensitive data on digitally transformative technologies.

To a great extent, many organizations seem to be indulging in a false sense of security when it comes to their data. Respondents overwhelmingly believe that their digital transformation implementations are safely deployed, with 66% responding that they are either very or extremely secure. Moreover, encryption, one of the fundamental controls for ensuring that sensitive data is securely deployed, is in use by less than 30% of implementations.

30%

of respondents are using encryption within these environments.

Possible evidence of this false sense of security may also be found when looking at the rate of data breaches reported by digital transformation stance. Those who reported aggressive digital transformation are also encountering the highest rates of data breaches (Figure 1) – with 54% of those in the two most active digital transformation categories having encountered a data breach, while only 23% of those with more basic adoption reporting the same. While higher data breach rates for aggressive digital transformers may be due to the tendency of more advanced organizations also to be better at identifying data breaches in action, another long-term trend may also be in action here – when implementing new technologies, many organizations tend to trade off time-to-market against the security of deployments.

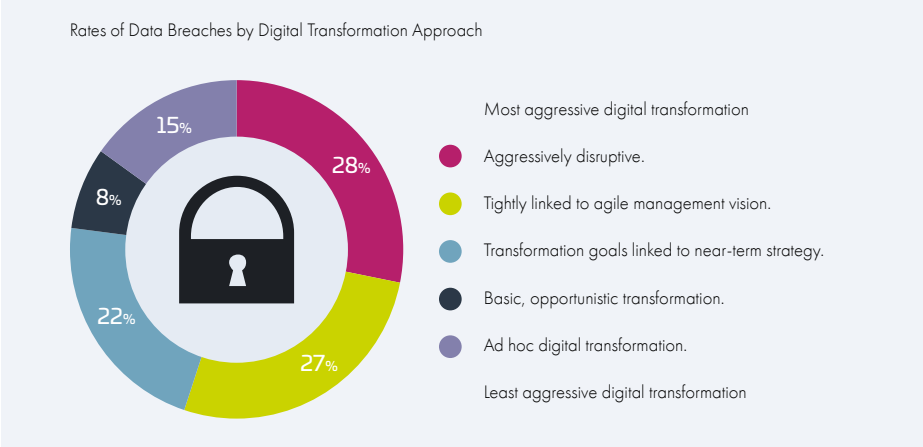


Figure 1 – Aggressive digital transformers have the highest rates of data breaches
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Multi-cloud security is the top digital transformation problem for data

Data now constitutes the "crown jewels" of most organizations as they transition into today's information economy, making the protection of sensitive information a critical priority. However, digital transformation fundamentally changes where data needs protecting and how it needs to be secured, and the cloud is arguably the most dauntingly complex of these environments, and the most widely deployed.

This year's data shows that cloud usage continues to proliferate rapidly: over 90% of all respondents said they plan to use all three of the common cloud environment types –Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) – within 12 months. Moreover, these deployments won't be to just one vendor or one platform, with 45%+ reporting that they will use three or more IaaS or PaaS environments, and 62%+ using 26 or more SaaS environments. Overall, 71% report that they will also use sensitive data within at least one of these cloud environments. This level of multi-cloud usage greatly compounds the difficulties that organizations have to face in protecting their sensitive data, as each environment, and often each implementation within the environment, can require a unique data security approach.

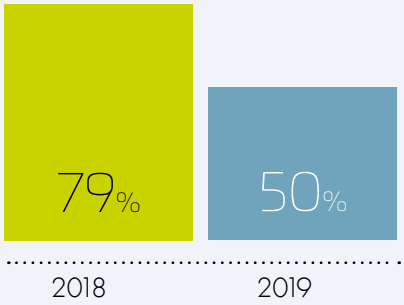
> "This level of multi-cloud usage greatly compounds the difficulties that organizations have to face in protecting their **sensitive data**, as each environment, and often each implementation within the environment, can require a unique data security approach."

Tools that reduce multi-cloud data security complexity are critical

Complexity was identified by respondents as the top barrier to data security deployment at 44%. Moreover, as organizations need to stretch their IT security budgets to cover not only internal security but multiple outside environments, budget is also a critical concern. With IT security spending increases declining this year to 50% from last year's 79% (Figure 2), organizations will need to get the highest possible return from their IT resources and spending in order to meet the IT and data security needs of increasing deployments in cloud and other digital transformation technologies. Data security platforms and service offerings that can help organizations to manage the complexity of spanning cloud, on-premises and other environments are critical to meeting these needs – with encryption and tokenization solutions providing some of the strongest protections from today's threat environment.

Encryption technologies are the top tools needed

Respondents clearly understand what tools were most effective for protecting their data. The top two selections of technologies needed to alleviate data security concerns for cloud were both encryption technologies, with both data encryption and Hardware Security Modules (HSMs) for cloud use selected by over 38%.



IT security spending increases decline

A tapering off of spending increases, combined with the complexity of protecting data across multi-cloud environments, leads to the need for data security platform and service solutions that can keep costs in line, while reducing complexity.

Figure 2 – IT security spending
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

No one is safe from data breaches

Not only are data breach rates high, but heavy investments in IT and data security have not proven to provide immunity. There's a distressing pattern to the rates of data breaches identified (Figure 3), half of all organizations breached were breached in the last year, and half of those breached in the last year have been breached previously. The raw numbers show that 60% have been breached at some time in the past, 30% were breached in the last year, and 14% were breached both in the last year and previously.

For many, preventing data breaches is not an IT security spending priority

One explanation for this may be the emphasis that organizations place on their IT security spending priorities. The results showed that avoiding data breaches, and having previously encountered a data breach, are at the bottom of this year's IT security spending priorities – both at around 30% of respondents. What were the top IT security spending priorities? Best practices (40%), followed by compliance (35%) and cloud computing (35%). If preventing data breaches isn't a priority, no wonder breach rates continue to increase, while we find many repeat offenders who are serially breached.

Higher investments in IT security don't correlate to lower rates of data breaches

Also, the results showed that even organizations investing heavily in IT and data security have high breach rates, and in fact, their breach rates are higher than those with lower investments in IT security. One data point, organizations spending 10% or less of the IT budget on IT security, had breach rates of 17% in the last year, while those with greater than 10% spending had breach rates of 34% in the last year. This may seem counterintuitive, but there are some good reasons that this makes sense. First, organizations that "have a target on their backs" because their business models include the use of sensitive financial and personal data are forced to spend more on IT security as a preventive measure. Thus, their heavy spending doesn't ensure that they won't encounter a data breach; it simply helps them to avoid "more" breaches. Second, a long-term industry observation is that organizations that are less sophisticated in their IT security implementations may simply not be aware that they have been breached, leading them to report lower numbers than their more sophisticated brethren.

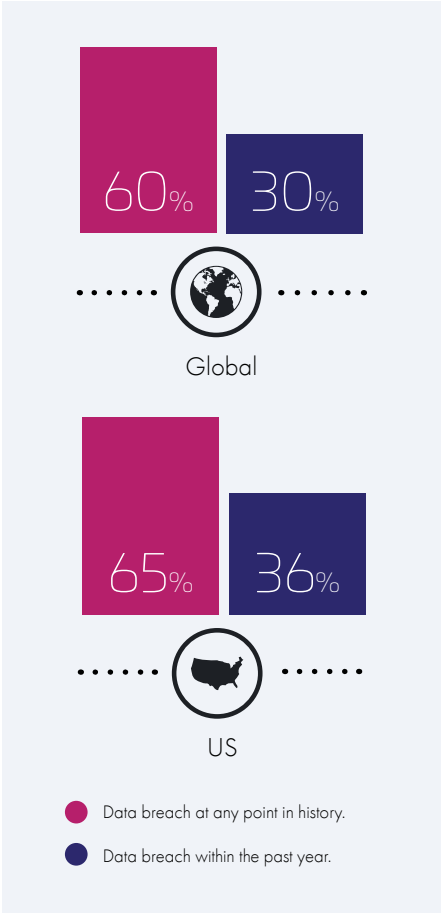


Figure 3 – Aggressive digital transformers have the highest rates of data breaches
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Regulatory and compliance changes introduce new challenges

Data privacy regulations and compliance standards continue to be top drivers for the use of data security controls across both industries and nations (Figure 4), registering as the second highest priority for IT security spending this year, and within the top three drivers for the previous three years. While industry specific standards such as the Payment Card Industry Data Security Standard (PCI DSS) are priorities within retail and other card dependent industries around the world, the severity and number of government data privacy and sovereignty regulations is now a top factor, with over 100 of these regulations in place worldwide. Regulations include industry specific regulations in the U.S. such as: Sarbanes Oxley (SOX) in financial services, HIPAA HITECH in healthcare, and FedRAMP, NIST, FISMA, and FIPS in the Federal Government. As well as regulations that apply to all organizations using citizens' private data, examples include the EU's GDPR regulations, which went into full effect in 2018, Germany's BDSG, new California and New York standards on data privacy, Brazil's Data Protection Law, the amended APPI law in Japan, PIPA in South Korea, and Mexico's Federal Law on the Protection of Personal Data held by Private Parties (LFPDPPP) to name just a few.

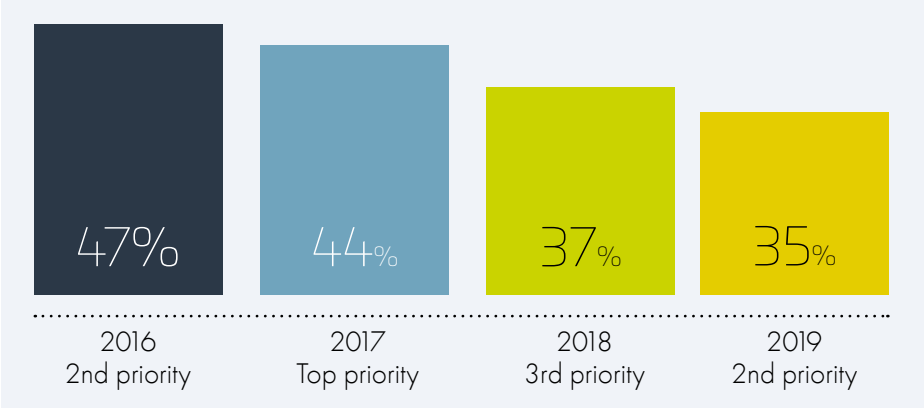


Figure 4 – Top drivers for IT security spending
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

As the complexity and number of compliance and regulatory requirements have increased, so have organizations' failure rates when audited for implementation of these standards. Results from our survey showed that while only 13% of organizations had a compliance audit failure for data security more than twelve months previously, 23% – almost twice that number – had an audit failure for data security in the last year.

As the severity of penalties and audit requirements continue to increase around the world, with the potential for severe penalties from regulations such as the EU's GDPR of up to 4% of global sales, organizations are taking steps to address these requirements. Enterprises' plans center around encryption and tokenization (an encryption technology) with the top selection being encryption at 44% with tokenization the second highest selection at 19%.

Encryption is the critical solution to the problem

As digital transformation results in a migration of data away from enterprise premises, the solutions that IT security organizations relied on in the past to protect their data are no longer sufficient. Fundamentally, implementing digital transformation, and especially cloud-based solutions and tools, changes what needs protecting and how it needs to be protected.

Yet organizations' IT security stances often seem stuck in the past. As breach rates have increased across the board, we've seen a consistent pattern in previous years of this report that IT security spending clusters around the areas that have protected networks and systems in the past. For the most part, these are network and end-point protections, rather than the best solutions for protecting sensitive data, data-at-rest and data-in-motion security tools. Essentially, people continue to protect against today's threats, in the newest technology environments, with yesterday's tools. Change is required to protect today's IT landscape, and encryption is the keystone technology required.

> "For the most part, these are network and end-point protections, rather than the **best solutions** that are best for protecting sensitive data, data-at-rest and data-in-motion security tools."

Another key finding this year is that although organizations have strong plans for adopting data security technologies, the actual implementation rates are low. When asked where encryption technologies are deployed today to protect not only cloud environments but also big data, IoT, containers, mobile payments, social media, and blockchain, results in every category were 30% or less. At the same time, use of sensitive data in these environments was from 71% for cloud environments, in the 40% or higher range for most other digital transformation technologies, and in the 32% range for blockchain and containers. This leads to the conclusion that in spite of good intentions, sensitive data within these environments may be fundamentally at risk.

30%

or fewer of enterprises say they use encryption for the vast majority of use cases studied.

Nevertheless, IT security pros that we polled clearly understood what's needed to solve the problem. When selecting the IT security technologies that they most needed in order to expand their usage of these critical environments, encryption was a top choice (Figure 5).

- For Cloud: Encryption was the top tool needed to enable more cloud use (38.8%).
- For Big Data: Encryption (45.3%) and Secure Identity (47.8%) are needed to drive Big Data adoption.
- For IoT: Encryption was the top IT security tool identified that was needed to increase enterprise ability to use IoT (42.3%).
- And with Containers: 47% identified encryption as a critical technology needed to expand use.

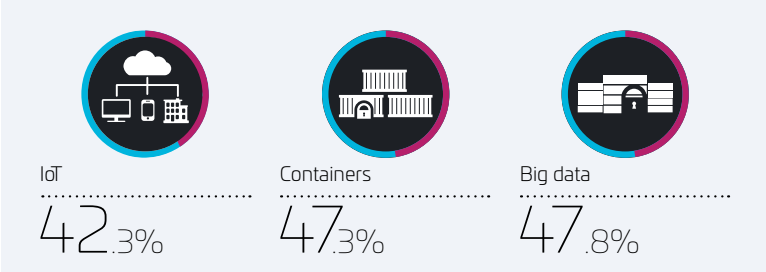


Figure 5 – Encryption for Big Data, IoT and Containers adoption
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Data security is hard

But it's vitally important. Organizations need to take a fresh look at how they provide data security. Against this backdrop, analysts recommend that security professionals consider the following:

- Focus on all threat vectors.
- Invest in modern, hybrid and multi-cloud-based data security tools and measures that scale to modern architecture.
- Look for solutions that let you do more with less.
- Prioritize compliance and sovereignty issues.
- Data security, starting with encryption, is an important part of the mix.

To download the full 2019 Thales Data Threat Report Global Edition, visit thalesesecurity.com/DTR #2019DataThreat

About Thales Cloud Protection & Licensing

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

Our Sponsors:

PURESTORAGE®

Cognizant

Canon Marketing Japan Inc.

OASIS Open standards. Open source.

CSA cloud security alliance℠

MOTIV

carahsoft.

THALES

2860 Junction Ave, San Jose, CA 95134, USA

+1 888 267 3732
+1 408 433 6000

> thalesesecurity.com <

thalesesecurity.com/DTR

#2019DataThreat