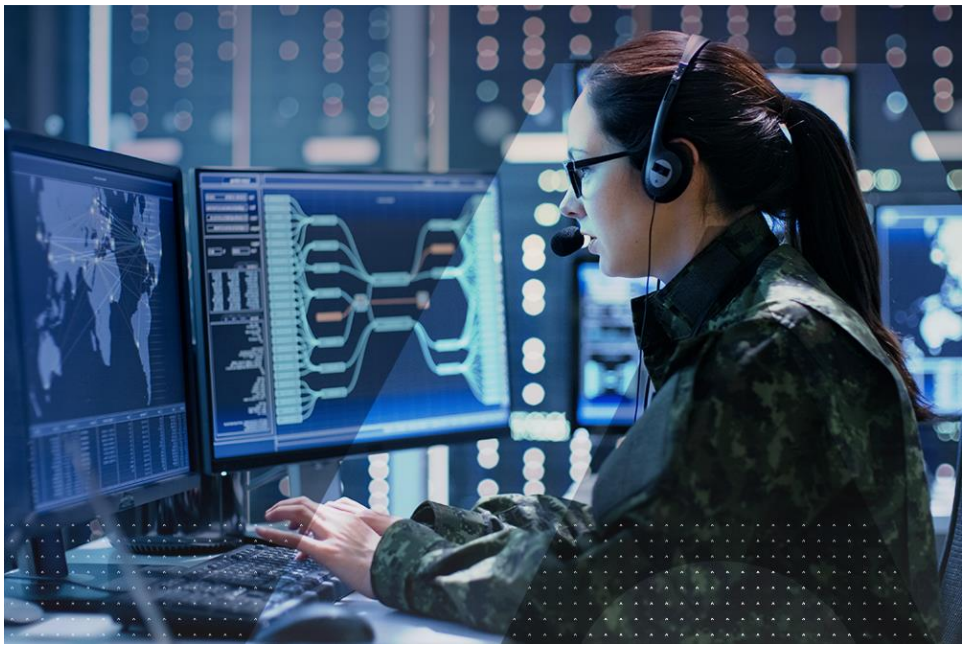
THALES

PRESS RELEASE
1 May 2019
Paris La Défense

Digital Transformation Efforts are Putting Sensitive Government Data at Risk

- Agencies struggling with cloud complexity as demand for digitally transformative technologies outpaces security adoption
- Despite increase in data breaches, proper investment in data protection is low for agencies
- Report finds data privacy and regulatory compliance are driving need for encryption and tokenization



©Thales

Thales, a leader in critical information systems, cybersecurity and data protection, announces that the push towards digital transformation in the U.S. government is putting sensitive data at risk, according to its 2019 Thales Data Threat Report – Federal Edition. The research, conducted by analyst firm IDC, indicates that as agencies embrace new technologies, such as multi-cloud deployments, they are struggling to implement proper data security.

"As digital transformation expands the number and position of attack vectors, the layers of security must expand and be repositioned to address new needs," said ***Frank Dickson, program vice president for security products research, IDC****. "As a result, agencies require flexible, consolidated security platforms that will enable them to manage greater amounts of complexity, spanning legacy on-premises as well as cloud-based and edge-oriented technologies."*

Almost all (98%) of respondents from federal agencies report that they are using sensitive data within digital transformation technology environments In fact, usage of digitally transformative technologies is high, as over 80% already use or plan to use these technologies within the next year. These

technologies include cloud, big data, mobile payments, social media, containers, blockchain and IoT. Yet, less than a third of respondents are using data encryption within these environments today even though it was identified as a key solution for securing sensitive data when using it on digitally transformative technologies. So, the question that federal agencies need to ask is whether digital transformation deployments are *really* secure?

"In many cases, security problems arise from well-known, long-standing vulnerabilities that agencies have not addressed, including limited use of data encryption and the abuse of privileged user policies," said ***Nick Jovanovic, VP, federal, Thales Cloud Protection & Licensing****. "Modernization and transformation efforts can create new vulnerabilities that result in data breaches, with security measures often being applied after the fact. As such, agencies need platforms that help them to better manage these environments and enable protection down to the data layer."*

The Reality of the Multi-Cloud Agency

The report found that agencies continue to move to multi-cloud environments as part of their digital transformation efforts with 78% of respondents using sensitive data in the cloud. Specifically, 66% of respondents have 26 or more Software-as-a-Service (SaaS) applications, 52% have three or more Infrastructure-as-a-Service (IaaS) applications and 41% have three or more Platform-as-a-Service (PaaS) applications. It comes as no surprise that 43% perceive complexity as the top barrier to deploying data security.

Despite Increase in Data Breaches Agencies Still Not Focused on Prevention

Although 60% of respondents have encountered a data breach and 35% have had one during the past year, prevention is at the bottom of the IT security spending priority list. The bottom three security spending priorities include managing previous data breaches (30%), addressing compliance/privacy requirements (27%) and avoiding data breach penalties (24%). Furthermore, over 80% of agencies are feeling vulnerable, with more than a third feeling extremely vulnerable.

Data Privacy and Sovereignty Regulations Impact all Agencies

Agencies across the government face a myriad of security-related laws and initiatives – such as FIPS, FISMA and FedRAMP. That said, roughly a quarter indicated they failed a compliance audit in the last year. To combat these challenges, over half of the respondents identified encryption and tokenization as the leading strategies to meet regulatory concerns.

For more key findings and security best practices, download a copy of the new 2019 Thales Data Threat Report -- Federal Edition. Thales also will host a webinar on Thursday, May 30 at 2:00 PM ET about "The Changing Landscape of Data Security for U.S. Federal Agencies." To join, please visit the registration page.

Follow Thales on Twitter, LinkedIn, Facebook and YouTube**.**

PRESS RELEASE
1 May 2019
Paris La Défense

About Thales

The people we all rely on to make the world go round – they rely on Thales. Our customers come to us with big ambitions: to make life better, to keep us safer. Combining a unique diversity of expertise, talents and cultures, our architects design and deliver extraordinary high technology solutions. Solutions that make tomorrow possible, today. From the bottom of the oceans to the depth of space and cyberspace, we help our customers think smarter and act faster - mastering ever greater complexity and every decisive moment along the way. With 80,000 employees in 68 countries, Thales reported sales of €19 billion in 2018.

PRESS CONTACT

Thales, Media Relations
Security
Constance Arnoux
+33 (0)1 57 77 91 58
constance.arnoux@thalesgroup.com

PLEASE VISIT

Thales Group
Security
Download HD photos

@Thalesgroup