THALES

Multi-cloud use and compliance requirements shape encryption strategy, finds latest Thales Global Encryption Study

Encryption with public cloud services experienced double digit growth

San Jose, Calif. – April 5, 2018 – Thales, a leader in critical information systems, cybersecurity and data security, announces the results of its 2018 Global Encryption Trends Study. The report, based on independent research by the Ponemon Institute and sponsored by Thales, reflects some of the changes and challenges organizations are experiencing in a world marked by widespread cloud deployments, use of multiple public cloud providers and new regulations such as the EU General Data Protection Regulation (GDPR).

Click to Tweet: #Encryption in public #cloud services sees double digit growth, according to new @thalesesecurity report https://bit.ly/2uAPMPi

This year, 43% of respondents report that their organization has an encryption strategy applied consistently across their enterprise. This strategy is leveraged to protect sensitive data against cyber criminals, help organizations address complex compliance requirements, and guard against human error. Encryption, which is achieved with software or hardware tools such as hardware security modules (HSMs), is often coupled with best practice-based key management. Encryption is also playing an increasingly large role in protecting the enormous adoption of organizations deploying to the cloud.

Among the findings:

- 84% of respondents either use the cloud for sensitive/non-sensitive applications and data today, or will do so in the next 12-24 months
- 61% of respondents are using more than one public cloud provider, and 71% plan to in the next two years
- 39% encrypt in public cloud services (such as Amazon Web Services, Microsoft Azure and Google Cloud), a number that has risen 11% since last year's report
- Overall HSM use grew to 41% -- the highest level ever. The most common use cases for HSMs are SSL/TLS and application level encryption, with 20% of respondents reporting that they use HSMs with blockchain applications
- 49% of enterprises are either partially or extensively deploying encryption of IoT data on IoT devices and platforms

This year's statistics are encouraging, but the report does show areas of challenge. Data discovery rates as the top data encryption planning/execution challenge by 67% of respondents, a number that is 8% higher than 2017. Respondents from the UK, Germany, the US and France have the most challenges, which likely points to activities associated with preparation and compliance of data privacy regulations such as GDPR which comes into effect in May this year.

When considering the majority of organizations polled are using more than one public cloud provider, the report also raises questions about how organizations are enforcing consistent encryption and key management policies across multiple cloud vendors. Securing data in a multi-cloud environment can be especially problematic for organizations seeking compliance, particularly if they are attempting to instantiate a single organizational policy using different native tools from multiple cloud providers. Not surprisingly, policy enforcement is second only to performance as a most valued feature of encryption solutions in this year's study.

Dr. Larry Ponemon, chairman and founder of The Ponemon Institute, says:
"While enterprises are rightfully encrypting cloud-based data, 42% of organizations indicate they will only use keys for cloud-based data-at-rest encryption that they control themselves. Similarly, organizations that use HSMs in conjunction with public cloud-based applications prefer to own and operate those HSMs on-premises. These findings tell us control over the cloud is highly important to companies increasingly under pressure from data security threats and compliance requirements."

John Grimm, senior director of security strategy at Thales eSecurity, says:
"Companies navigating today's threat landscape are understandably seeking out fast, scalable encryption tools that encompass enterprise and cloud use cases, and enforce policy consistently across both models. Fortunately, enterprises have more data protection choices today than when the race to the cloud began. These options include bring your own key (BYOK) and bring your own encryption (BYOE) solutions, which allow enterprises to apply the same encryption and key management solution across multiple platforms."

The Global Encryption Trends Study is now in its thirteenth year. The Ponemon Institute surveyed more than 5,000 people across multiple industry sectors in the United States, United Kingdom, Germany, France, Australia, Japan, Brazil, the Russian Federation, Mexico, India, Saudi Arabia, the United Arab Emirates, and Korea.

The new 2018 Global Encryption Trends Study can be downloaded here.

Industry insight and views on the latest data security trends can be found on the Thales eSecurity blog at blog.thalesesecurity.com.

Follow Thales eSecurity on Twitter @Thalesesecurity, and on LinkedIn, Facebook and YouTube**.**

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-premises, in the cloud, in data centres 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 organisation needs to protect and manage its data, identities and intellectual property, and meet regulatory compliance – through encryption, advanced key management, tokenisation, and privileged-user control and high-assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organisation's digital transformation. Thales eSecurity is part of Thales Group.

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 65,000 employees in 56 countries, Thales reported sales of €15.8 billion in 2017.

Contact:

Constance Arnoux
Thales Media Relations – Security
+33 (0)6 44 12 16 35
constance.arnoux@thalesgroup.com

Liz Harris
Thales eSecurity Media Relations
+44 (0)1223 723612
liz.harris@thales-esecurity.com