THALES

PRESS RELEASE
26.01.2017
PARIS LA DÉFENSE

2017 Thales Data Threat Report: security spending decisions leave sensitive data vulnerable

Group – Civil Aerospace – Defence Aerospace – Space - Transportation - Defence - **Security**

©Thales

Thales, a leader in critical information systems, cybersecurity and data security, announces the results of its 2017 Thales Data Threat Report, issued in conjunction with analyst firm 451 Research. Sixty-eight percent of respondents have experienced a breach with 26 percent experiencing a breach in the last year – both numbers that rose from last year. Paradoxically, overall security spending is also up; in 2017 73 percent of organizations increased IT security spending – a marked jump from 2016 (58 percent).

Old Habits Die Hard

The report, which is in its fifth year, polled 1,100 senior IT security executives at large enterprises around the world and indicates an ongoing disconnect between the security solutions organizations spend money on and the ability of those solutions to protect sensitive data. While 30 percent of respondents classify their organizations as 'very vulnerable' or 'extremely vulnerable' to data attacks (and the number of breaches continues to rise) the two top spending priorities are network (62 percent) and endpoint (56 percent) protection solutions. Counterintuitively, spending on data-at-rest solutions (46 percent) comes last.

Garrett Bekker, senior analyst, information security at 451 Research and author of the report says:

"*One possible explanation for this troubling state? Organizations keep spending on the same solutions that worked for them in the past but aren't necessarily the most effective at stopping modern breaches. Data protection tactics need to evolve to match today's*

> Key Points

- Thales announces the results of its 2017 Thales Data Threat Report, issued in conjunction with analyst firm 451 Research.
- Trends: Breaches and security spendings have increased respectively by 22% and 15% from last year.
- Visit Thales at booth #S1007 South Expo, RSA Conference, Moscone Center, San Francisco, February 13-16, 2017.

threats. It stands to reason that if security strategies aren't equally as dynamic in this fast-changing threat environment, the rate of breaches will continue to increase."

Compliance the top driver for IT security spending

The reasons behind security spending decisions are varied, but the key driver remains constant: compliance. Almost half (44 percent) of respondents list meeting compliance requirements as their top spending priority, followed by best practices (38 percent) and protecting reputation/brand (36 percent). Fifty-nine percent also believe compliance is 'very' or 'extremely' effective at preventing data breaches. While compliance regulations provide a data security blueprint, they are by no means are the only consideration when building a security strategy robust enough to withstand today's sophisticated attackers.

External and Internal Cyber Actors the top threat

As in years past, the 2017 Data Threat Report explored threat perceptions. All vertical industries polled identified cyber criminals as the top threat (44 percent), followed by hacktivists (17 percent), cyberterrorists (15 percent) and nation-states (12 percent). With respect to internal threats, 58 percent of respondents believe privileged users are the most dangerous insiders (a slight decrease from last year's 63 percent). At 44 percent, executive management is seen as the second-most-risky insider, followed by ordinary employees (36 percent) and contractors (33 percent).

Securing Data from Future Threats: Promise or Peril?

In this age of the cloud and SaaS enterprise deployments, more and more enterprise data is being created, transported, processed and stored outside corporate network boundaries, making traditional perimeter-based security controls and legacy network and endpoint protection solutions increasingly less relevant. Other new, popular technologies also bring added security challenges. For example, nearly 40 percent of respondents are using Docker containers for production applications. At the same time, 47 percent cite security as the 'top barrier' to broader Docker container adoption.

To offset the data breach trend and take advantage of new technologies and innovations, organizations should, at a minimum, adhere to the following practices

- Leverage encryption and access controls as a primary defense for data and consider an 'encrypt everything' strategy
- Select data security platform offerings that address a variety of use cases and emphasize ease-of-use
- Implement security analytics and multi-factor authentication solutions to help identify threatening patterns of data use.

Source/Methodology

The data in this study is based on Web and phone interviews of 1,105 senior executives in Australia, Brazil, Germany, Japan, the UK and the U.S. Most have a major influence on or are the sole decision maker for IT at their respective companies.
Respondents represented the following industries: automotive; education; energy; engineering; federal government; healthcare; IT; retail; and telecommunications.

About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America,

« Enterprises today must inevitably confront an increasingly complicated threat landscape. Our world, which now includes the cloud, big data, the IoT and Docker, calls for robust IT security strategies that protect data in all its forms, at rest, in motion and in use. Businesses need to invest in privacy-by-design defense mechanisms – such as encryption – to protect valuable data and intellectual property and view security as a business enabler that facilitates digital initiatives and builds trust between partners and customers. »

Peter Galvin, *Vice president of strategy, Thales e-Security*

Please visit

- Thales Group
- Security
- 2017 Thales Data Threat Report

Press contact

Thales, Media Relations Security

Dorothée Bonneil
+33 (0)6 84 79 65 86
dorothee.bonneil@thalesgroup.com

Thales e-Security Media Relations

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

@ThalesPress

Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

About Thales e-Security

Thales e-Security is the leader in advanced data security solutions and services, delivering trust wherever information is created, shared or stored. We ensure that company and government data is secure and trusted in any environment – on premise, in the cloud, in data centers and in 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 meeting the highest standards of certification for high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales e-Security is part of Thales Group. www.thales-esecurity.com

About Thales

Thales is a global technology leader for the Aerospace, Transport, Defence and Security markets. With 62,000 employees in 56 countries, Thales reported sales of €14 billion in 2015. With over 25,000 engineers and researchers, Thales has a unique capability to design and deploy equipment, systems and services to meet the most complex security requirements. Its exceptional international footprint allows it to work closely with its customers all over the world.

Positioned as a value-added systems integrator, equipment supplier and service provider, Thales is one of Europe's leading players in the security market. The Group's security teams work with government agencies, local authorities and enterprise customers to develop and deploy integrated, resilient solutions to protect citizens, sensitive data and critical infrastructure.

Thales offers world-class cryptographic capabilities and is a global leader in cybersecurity solutions for defence, government, critical infrastructure providers, telecom companies, industry and the financial services sector. With a value proposition addressing the entire data security chain, Thales offers a comprehensive range of services and solutions ranging from security consulting, data protection, digital trust management and design, development, integration, certification and security maintenance of cybersecured systems, to cyberthreat management, intrusion detection and security supervision through cybersecurity Operation Centres in France, the United Kingdom, The Netherlands and Hong Kong.