

89 Percent of Retail IT Security Pros Feel Vulnerable to Data Threats, Yet Data Breach Prevention a Low Spending Priority

*Spending to protect data increasing, but concentrated in least effective security controls
2016 Vormetric Data Threat Report – Retail Edition*

SAN JOSE, Calif. – June 14, 2016 – Vormetric, a Thales company, and a leader in enterprise data protection for physical, virtual, big data, and cloud environments, today announced the results of the [Retail Edition of the 2016 Vormetric Data Threat Report](#) (DTR). The report is issued in conjunction with analyst firm 451 Research, reporting responses from 1,100 senior IT security executives at large enterprises worldwide, including over 100 in U.S. retail organizations. This edition of the fourth annual report extends earlier findings of the [global report](#), focusing on responses from retail organizations, detailing IT security spending plans, perceptions of threats to data, rates of data breach failures and data security stances.

“The good news is that U.S. retailers, are protecting data for the right reasons, and nearly half have a good track record of safeguarding sensitive data. Protecting reputation and brand integrity was the top reason for securing sensitive information at 55 percent, and 44 percent claimed they had never experienced a data breach or failed a compliance audit,” said Garrett Bekker, senior analyst, information security, at 451 Research and the author of the 2016 Vormetric Data Threat Report. “But IT security spending plans tell another story. Spending on network defenses (55 percent) and end point and mobile device defenses (48 percent) are increasing faster than on security controls that are more effective at protecting data, data-at-rest defenses (44 percent) and data-in-motion defenses (42 percent).”

Spending to protect data is increasing fastest in areas that have been shown to be ineffective at protecting against multi-stage attacks. Network defenses (65 percent) and endpoint and mobile device defenses (58 percent) still see the highest increase in spending, while approaches like data-at-rest defenses that have been proven to be effective at protecting data after perimeter defenses have been bypassed are at the bottom (48 percent).”

Other key findings:

- 89 percent feel vulnerable to data threats
- 51 percent have already experienced a data breach, with more than one in five (21 percent) indicating a breach in the last year
- At 55 percent, protecting reputation and brand was the top IT security spending priority, followed closely by meeting compliance requirements at 49 percent
- Complexity at 61 percent is identified as the top barrier to adoption of better data security
- A bright spot is that 44 percent are increasing spending on data-at-rest defenses this year

[Click to Tweet:](#) Retailers in the cross hairs – 89% say their data is vulnerable #2016DataThreat
<http://bit.ly/1Oe1Civ>

Top external and internal threat actors

After years of high profile, well publicized data breaches, retailers already know that they are a primary target for cybercriminals and malicious insiders. Unsurprisingly, the top external threat actors identified were cybercriminals, a top selection for 48 percent of respondents. The top internal threat actors identified were privileged users. Privileged user accounts typically have access to all the resources and systems they manage, unless restrained by additional security controls, and their account credentials are primary targets in cyberattacks.

Reputation and brand protection are top data protection drivers for retail, but data breach prevention is at the bottom of the list

Retail's IT security spending priorities as measured in the report:

- Reputation and brand protection (55 percent)
- Compliance (49 percent)
- Best practices (37 percent)
- Executive directive (35 percent)
- Preventing data breaches (31 percent)

With preventing data breaches the lowest priority for IT security spending, the large number of data breaches from retailers over the last few years should be no surprise. But the finding that reputation and brand protection are the top priority is at odds with the low priority of preventing data breaches. When a data breach happens, damage to reputation and brand directly result.

Compliance is also still a top driver of IT security spending in retail as well. With adherence to credit card and privacy regulations a requirement of business, it's no surprise that IT security professionals in retail focus on meeting compliance mandates. However, compliance is not enough, as retailers that have met their compliance requirements have frequently been breached over the last two years.

Cloud usage and concerns for data are high

Retail organizations are worried about their use of sensitive data in cloud environments, with 75 percent citing security breaches at the cloud provider as a concern, but this concern has not stopped sensitive data moving to the cloud. Current levels of sensitive data use within cloud environments:

- SaaS – 69 percent
- IaaS – 58 percent
- PaaS – 58 percent

The ability to encrypt data in the cloud was the number one factor that would increase willingness to increase their cloud usage, at 51 percent of responses.

Getting more right

A number of positive results indicate that retail organizations are taking steps in the right direction to recognize and deal with the problems surrounding their use of sensitive information.

- 61 percent are increasing spending to protect sensitive data
- 55 percent are looking to implement data security for brand and reputation protection
- 44 percent, plan to invest in data-at-rest defenses this year

“With frequent, high profile data breaches occurring, it seems a complete miss that preventing them is at the bottom of a retailer’s IT security spending priority list,” said Tina Stewart, vice president of marketing for Vormetric. “Surprisingly, they are also failing to connect the dots about the best solutions to use. With tremendous sets of detailed customer behavior and personal information in their custody, and with retailers a prime target for hackers, we’d expect to see more investments in data security, than in less than fully effective tools like network and anti-virus security.”

The research report is available from Vormetric and can be found [here](#).

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

About Vormetric, a Thales company

Vormetric’s comprehensive high-performance data protection platform helps companies move confidently and quickly. Our seamless and scalable platform is the most effective way to protect data wherever it resides—any file, database and application, in any server environment. Advanced transparent encryption, powerful access controls and centralized key management let organizations encrypt everything efficiently, with minimal disruption. Regardless of content, database or application—whether physical, virtual or in the cloud—Vormetric Data Security enables confidence, speed and trust by encrypting the data that builds business. Vormetric Data Security was recently acquired by Thales Group and is now a Thales company.

Please visit: www.vormetric.com and find us on Twitter @Vormetric.

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 22,000 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.

Drawing on its strong cryptographic capabilities, Thales is a global leader in data protection and one of the world leaders in cybersecurity products and solutions for defence, critical infrastructure and

telecommunication operators, industrial and financial companies. Covering the entire cybersecurity chain, Thales offers a comprehensive range of services and solutions that includes: cybersecurity consulting and testing, cyber-secured software centric system design / development / integration and certification, provision and through-life management of data protection products and services, secured IT outsourcing and cloud computing solutions, as well as managed security services based on our network of Security Operation Centers in France, the United Kingdom and the Netherlands.

Contact:

Andy Kicklighter
Vormetric Media Relations
+1 408-908-6260
akicklighter@vormetric.com

Dorothee Bonneil
Thales Media Relations – Security
+33 (0)1 57 77 90 89
dorothee.bonneil@thalesgroup.com

Liz Harris
Thales e-Security Media Relations
+44 (0)1223 723612
liz.harris@thales-eseurity.com