

Gemalto & Ponemon Institute Study: Cloud data security still a challenge for many companies

- *Half of all cloud services and corporate data stored in cloud not controlled by IT departments*
- *Only a third of sensitive data stored in cloud-based applications is encrypted*
- *More than half of companies do not have a proactive approach for compliance with privacy and security regulations for data in cloud environments*
- *Simple measures by IT organizations provide protection for both corporate data and “shadow IT” needs.*

Amsterdam, July 26, 2016 – Despite the continued importance of cloud computing resources to organizations, companies are not adopting appropriate governance and security measures to protect sensitive data in the cloud. These are just a few findings a Ponemon Institute study titled “The 2016 Global Cloud Data Security Study,” commissioned by [Gemalto](#) (Euronext NL0000400653 GTO), the world leader in digital security. The study surveyed more than 3,400 IT and IT security practitioners worldwide to gain a better understanding of key trends in data governance and security practices for cloud-based services.

On July 28 at 10 a.m. EDT, Gemalto and the Ponemon Institute will host a webinar to discuss the full results of the study. Click on the following link to register: <https://www.brighttalk.com/webcast/2037/216247>.

According to 73 percent of respondents, cloud-based services and platforms are considered important to their organization’s operations and 81 percent said they will be more so over the next two years. In fact, thirty-six percent of respondents said their companies’ total IT and data processing needs were met using cloud resources today and that they expected this to increase to forty-five percent over the next two years.

Although cloud-based resources are becoming more important to companies’ IT operations and business strategies, 54 percent of respondents did not agree their companies have a proactive approach to managing security and complying with privacy and data protection regulations in cloud environments. This is despite the fact that 65 percent of respondents said their organizations are committed to protecting confidential or sensitive information in the cloud. Furthermore, 56 percent did not agree their organization is careful about sharing sensitive information in the cloud with third parties such as business partners, contractors and vendors.

“Cloud security continues to be a challenge for companies, especially in dealing with the complexity of privacy and data protection regulations,” said Dr. Larry Ponemon, chairman and founder, Ponemon Institute. “To ensure compliance, it is important for companies to consider deploying such technologies as encryption, tokenization or other cryptographic solutions to secure sensitive data transferred and stored in the cloud.”

“Organizations have embraced the cloud with its benefits of cost and flexibility but they are still struggling with maintaining control of their data and compliance in virtual environments,” said Jason Hart, Vice President and Chief Technology Officer for Data Protection at Gemalto. “It’s quite obvious security measures are not keeping pace because the cloud challenges traditional approaches of protecting data when it was just stored on the network. It is an issue that can only be solved with a data-centric approach in which IT organizations can uniformly protect customer and corporate information across the dozens of cloud-based services their employees and internal departments rely every day.”

Key Findings

Cloud security is stormy because of shadow IT

According to respondents, nearly half (49 percent) of cloud services are deployed by departments other than corporate IT, and an average of 47 percent of corporate data stored in cloud environments is not managed or controlled by the IT department. However, confidence in knowing all cloud computing services in use is increasing. Fifty-four percent of respondents are confident that the IT organization knows all cloud computing applications, platform or infrastructure services in use – a nine percent increase from 2014.

Conventional security practices do not apply in the cloud

In 2014, 60 percent of respondents felt it was more difficult to protect confidential or sensitive information when using cloud services. This year, 54 percent said the same. Difficulty in controlling or restricting end-user access increased from 48 percent in 2014 to 53 percent of respondents in 2016. The other major challenges that make security difficult include the inability to apply conventional information security in cloud environments (70 percent of respondents) and the inability to directly inspect cloud providers for security compliance (69 percent of respondents).

More customer information is being stored in the cloud and is considered the data most at risk

According to the survey, customer information, emails, consumer data, employee records and payment information are the types of data most often stored in the cloud. Since 2014, the storage of customer information in the cloud has increased the most, from 53 percent in 2014 to 62 percent of respondents saying their company was doing this today. Fifty-three percent also considered customer information the data most at risk in the cloud.

Security departments left in the dark when it comes to buying cloud services

Only 21 percent of respondents said members of the security team are involved in the decision-making process about using certain cloud application or platforms. The majority of respondents (64 percent) also said their organizations do not have a policy that requires use of security safeguards, such as encryption, as a condition to using certain cloud computing applications.

Encryption is important but not yet pervasive in the cloud

Seventy-two percent of respondents said the ability to encrypt or tokenize sensitive or confidential data is important, with 86 percent saying it will become more important over the next two years, up from 79 percent in 2014. While the importance of encryption is growing, it is not yet widely deployed in the cloud. For example, for SaaS, the most popular type of cloud-based service, only 34 percent of respondents say their organization encrypts or tokenizes sensitive or confidential data directly within cloud-based applications.

Many companies still rely on passwords to secure user access to cloud services

Sixty-seven percent of respondents said the management of user identities is more difficult in the cloud than on-premises. However, organizations are not adopting measures that are easy to implement and could increase cloud security. About half (forty-five percent) of companies are not using multi-factor authentication to secure employee and third-party access to applications and data in the cloud, which means many companies are still relying on just user names and passwords to validate identities. This puts more data at risk because fifty-eight percent of respondents say their organizations have third-party users accessing their data and information in the cloud.

Recommendations for Data Security in the Cloud

The new realities of Cloud IT mean that IT organizations need to set comprehensive policies for data governance and compliance, create guidelines for the sourcing of cloud services, and establish rules for what data can and cannot be stored in the cloud.

IT organizations can accomplish their mission to protect corporate data while also being an enabler of their "Shadow IT" by implementing data security measures such as encryption that allow them to protect data in the cloud in a centralized fashion as their internal organizations source cloud-based services as needed.

As companies store more data in the cloud and utilize more cloud-based services, IT organizations need to place greater emphasis on stronger user access controls with multi-factor authentication. This is even more important for companies that give third-parties and vendors access to their data in cloud.

About the Survey

The survey was conducted by the Ponemon Institute on behalf of Gemalto and surveyed 3,476 IT and IT security practitioners in the United States, Brazil, United Kingdom, Germany, France, Russian Federation, India, Japan and Australia who are familiar and involved in their company's use of both public and private cloud resources. Industries represented among the respondents include Financial Services, Retail, Technology & Software, Public Sector, Healthcare and Pharmaceutical, Utilities & Energy, Education, Transportation, Communications, Media & Entertainment, and Hospitality.

Related Resources

- Report: [Gemalto 2016 Global Cloud Data Security Study](#)
- Infographic: [Gemalto Cloud Data Security Infographic](#)
- Web Site: [Gemalto 2016 Global Cloud Data Security Study Findings](#)
- Video: [Gemalto Cloud Security Solutions Overview](#)
- Web Site: [You Can't Secure the Cloud with Old School Technology](#)

About Gemalto

Gemalto (Euronext NL0000400653 GTO) is the global leader in digital security, with 2015 annual revenues of €3.1 billion and customers in over 180 countries. We bring trust to an increasingly connected world.

Our technologies and services enable businesses and governments to authenticate identities and protect data so they stay safe and enable services in personal devices, connected objects, the cloud and in between.

Gemalto's solutions are at the heart of modern life, from payment to enterprise security and the internet of things. We authenticate people, transactions and objects, encrypt data and create value for software – enabling our clients to deliver secure digital services for billions of individuals and things.

Our 14,000+ employees operate out of 118 offices, 45 personalization and data centers, and 27 research and software development centers located in 49 countries.

For more information visit www.gemalto.com or follow [@gemalto](https://twitter.com/gemalto) on Twitter.

Gemalto media contacts:

Philippe Benitez
North America
+1 512 257 3869
philippe.benitez@gemalto.com

Peggy Edoire
Europe & CIS
+33 4 42 36 45 40
peggy.edoire@gemalto.com

Vivian Liang
大中华地区 (Greater China)
+86 1059373046
vivian.liang@gemalto.com

Ernesto Haikewitsch
Latin America
+55 11 5105 9220
ernesto.haikewitsch@gemalto.com

Kristel Teyras
Middle East & Africa
+33 1 55 01 57 89
kristel.teyras@gemalto.com

Shintaro Suzuki
Asia Pacific
+65 6317 8266
shintaro.suzuki@gemalto.com