gemalto
security to be free

Your Data. Their Cloud.

Three Steps to Securing Data in Any Cloud Environment

of total IT and data processing requirements are met using cloud resources. This is expected to increase to 45% in the next two years.

Ponemon Institute and Gemalto, The 2016 Global Cloud Data Security Study, May 2016

Meet Jack.

Jack is the IT manager at an established, but growing, enterprise.

His team is responsible for protecting the organization's data assets, including the need to secure customer information, employee data, company financials, and more.

Back when everything was stored in the data center, securing the company's data was so much easier. Jack was in control.

Employees could only access business applications on-premises through the network. It was simple for Jack's team to manage the authentication of users, while keeping a watchful eye on who had access to company applications and information.

Keeping sensitive data secure at all levels of the technology stack was easier too. Everything was located in the traditional data center and inside of the company's protected perimeter. Jack's team only had to worry about bad guys outside of the firewall.

Times have changed.

The Cloud: Big Benefits. Bigger Risk?

These days, Jack and his team are faced with more security threats, more compliance mandates, and more data to protect. Departments across the company have also adopted cloud technology on their own, which means his team is juggling even more isolated requests and projects.

Jack knows the cloud comes with big benefits. It helps his company to:

- Get products and services to market faster
- Reduce storage and infrastructure costs
- Provide access to business applications and information anytime, anywhere, and from any device
- Process, analyze, and put data to use sooner

The cloud will also help Jack's team manage growing data demands in today's connected and competitive digital world.

> But what happens when data leaves his network and moves to the cloud? With so many new cloud initiatives, Jack's team needs a more unified and holistic approach to data security.

73%

of IT professionals consider cloud computing applications and platform solutions very important or important to their organizations' operations. That is expected to increase to 81% over the next two years.

Ponemon Institute and Gemalto, The 2016 Global Cloud Data Security Study, May 2016

You Can't Secure the Cloud with Old School Technology

Moving to the cloud means Jack's team no longer has a clearly defined perimeter to secure and data can be accessed by devices that are not always company-owned. The old school data protection approach and technologies they once relied on, such as securing the network perimeter, just won't work in the cloud. It will leave sensitive data exposed, and that's not cool.

With his company's data in their cloud...

- Can he trust it there?
- Will he lose control over sensitive corporate, employee, and customer information?
- Can he make sure the company compliance and regulatory requirements are met?
- How will he prevent unauthorized users, administrators and bad guys from accessing data?
- How will he keep data safe as it is migrated to, stored in, moving across, or even deleted from the cloud?
- Will government entities have access to data if the cloud service provider is subpoenaed?

The cloud comes with great benefits, but Jack knows that you can't secure it with the same old school technology. He needs a new approach to cloud security – one that puts him back in control.

Three Ways to Maintain **Control in the Cloud**

The good news for Jack is that there is a way to maintain control of his data in the cloud and achieve compliance. His team must deploy cloud-ready data security solutions that will:

Encrypt Sensitive Data

Secure and control sensitive data wherever it goes

Control Access

Ensure only authorized users can access cloud-based applications

Own and Manage Encryption Keys

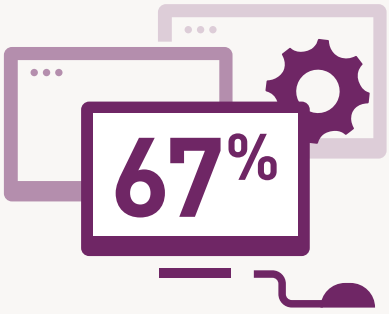
Centrally manage and prove ownership of your encryption keys

Let's learn more about how Jack can apply this new approach to cloud security with Gemalto's portfolio of SafeNet Identity and Data Protection solutions.

Control Access to Cloud-based Applications

Like many businesses, Jack's company wants to take advantage of cloud-based SaaS applications, such as SalesForce, Microsoft Office 365, and Amazon Web Services, to support employee mobility and easily scale to meet business needs. But, they can't risk exposing sensitive company data to unauthorized users.

A multi-factor authentication solution can ensure only approved users access the company's cloud-based applications by combining something the user knows, like their ID and password, with something they have, like a token or one-time password delivered to their mobile device.



67% of organizations say managing user identities is more difficult in the cloud than on-premises.

Ponemon Institute and Gemalto, The 2016 Global Cloud Data Security Study, May 2016

With a multi-factor authentication solution from Gemalto, Jack's team can also:

- Centrally define and enforce policies for network, web-, and cloud-based applications from a single backend
- Deploy a proven solution without changing the company's existing infrastructure
- Increase user convenience with a single identity for logging in to the company's network, on-premises, and cloud applications
- Offer secure access with frictionless methods such as contextual, pattern-based, and single-tap push authentication
- Gain centralized visibility into access events taking place throughout the IT environment for simplified audits and compliance

> Jack's team can now prevent the bad guys from accessing the company's Microsoft Office 365 accounts and viewing sensitive corporate information. It's a win-win for everyone...even Jack.

Encrypt and Secure Sensitive Data

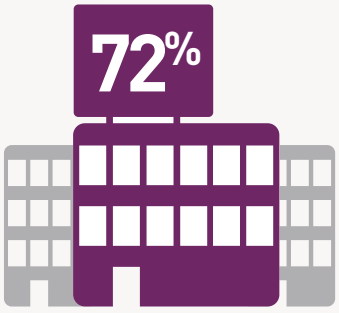
Jack's company is finding more value in data than ever before. However, as company data produced, processed, and stored in the cloud grows, it also becomes a prime target for attack.

Encryption is a critical last line of defense because it applies protection and access controls directly to the data wherever it resides or as it moves across the company's cloud, hybrid, virtual, and on-premises environments.

With an enterprise-ready encryption solution from Gemalto, Jack's team can:

- Secure both structured and unstructured data at rest in applications, databases (column- and file-level), files and folders, storage (DAS/SAN/NAS), and virtual machines in any cloud
- Apply granular access controls to ensure only authorized users or processes can view protected data, including privileged users and administrators
- Monitor access to protected data with comprehensive logging and auditing
- Keep data secure that's moving to and from the cloud with high speed network encryption

> Jack is happy that learn that anything he can do in his on-premises data center, he can do in the cloud. The data is secure, and his company is compliant. Now, let's take care of those encryption keys.



72% of organizations say the ability to encrypt or tokenize sensitive or confidential data in the cloud is important, and 86% say it will become more important over the next two years.

Ponemon Institute and Gemalto, The 2016 Global Cloud Data Security Study, May 2016

Maintain Control and Ownership of Encryption Keys

With the company's sensitive data encrypted, Jack's team needs a new way to centrally and securely manage and store the encryption keys used to protect his data in his cloud, hybrid, and on-premises environments.

He also wants to ensure that the ownership of these keys stays with him, not a cloud provider or third party vendor. This is important because only Jack and authorized users in his company will be able to access secured data in any cloud environment. In addition, his team will ultimately be held responsible if there is a data breach.

With a centralized enterprise key management solution from Gemalto, Jack's team can:

- Always prove ownership of encryption keys and data
- Centrally manage the lifecycle and storage of encryption keys
- Control and address any access requests for his company's encrypted data
- Define and control data access permissions for company personnel, partners, vendors, customers, etc.
- Prevent government entities from accessing the encryption key or gaining access to the company's data through a cloud service provider (Jack or his company may be forced to provide the key, but the company will know about it and be able to respond accordingly.)
- Ensure data is securely decommissioned from the cloud

Jack now owns and centrally manages his keys and data in the cloud, and across his on-premises environments, knows his keys are stored separately from his data, and has deployed an added layer of security for key storage and cryptographic operations within a tamper-resistant hardware security module. There's nothing old school about that.

55%

Only 55% of organizations control their encryption keys when data is encrypted in the cloud.

Ponemon Institute and Gemalto, The 2016 Global Cloud Data Security Study, May 2016

Simplify the Way Your Team Works

The mandate to move the company to the cloud gave Jack the opportunity to evaluate his data security strategy not only for the cloud, but his on-premises environments too. He quickly discovered sensitive data in locations his team didn't know about, and data protection solutions in use across the company that they did not deploy.

Through 2020, 95% of cloud security failures will be the customer's fault. Risks associated with user behavior and configuration of the cloud environments are the responsibility of the customers and not the cloud service provider.

Gartner, Market Trends:
Are Cloud Providers Becoming Security Vendors?, May 31, 2016

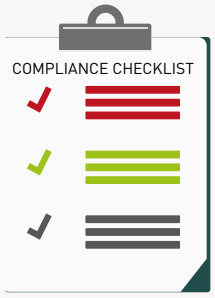
With Gemalto, Jack can now move past silo-constrained identity and data protection. He can deploy solutions across all of the company's cloud and on-premises environments centrally, uniformly, and at scale as an IT service for the organization. This helps Jack's team to:

Strengthen security

Security policies can be both centrally managed and broadly deployed, and sensitive keys are tightly secured.

Strengthen compliance and reduce audit costs

With a unified, cohesive view of cryptographic activity across the enterprise, Jack's team has the visibility needed to ensure compliance.



Reduce IT costs

Jack has established proven security processes that can be repeated across the organization - saving time and money.

Increase IT and business agility

With a centrally managed platform, Jack's team has become more nimble and can focus their efforts on new technology projects and challenges.

Move Your Business to the Cloud Securely with Gemalto

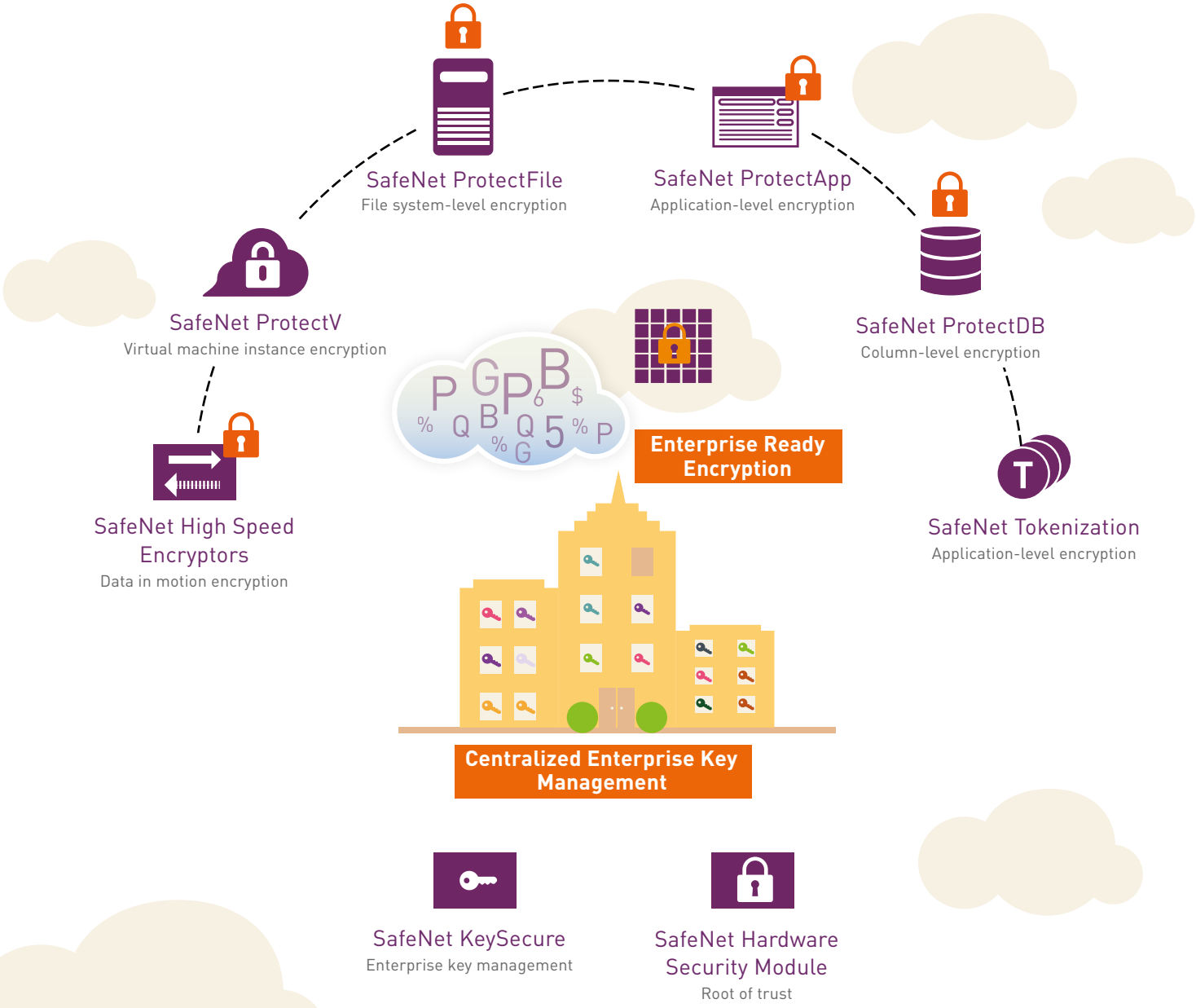
Gemalto's portfolio of SafeNet Identity and Data Protection solutions provides centralized, enterprise-ready data protection across all on-premises, cloud, and hybrid environments. Centralized and proven multi-factor authentication, encryption, and enterprise key management ensures your business can control access to cloud-based applications, secure sensitive data wherever it goes, prove ownership of keys and secure them in shared environments, and minimize the risk of running your business in the cloud.

These solutions integrate with a growing ecosystem of cloud providers and cloud-enabled applications and tools to keep data safe now, and into the future as your business needs evolve.

Apply Strong Multi-factor Authentication with SafeNet Identity Protection Solutions

Integrates with more than 240 of today's leading business applications

Secure Your Data and Keys in the Cloud with SafeNet Data Protection Solutions



Integrates with more than 420 cloud providers, applications, databases, and tools, including Amazon Web Services, Microsoft Azure, IBM SoftLayer, Google Cloud Platform, VMware, Cloud Foundry, Docker, Chef, MongoDB, and more

Ready to be like Jack?

Jack knows that times have changed and that an old school approach to securing data just isn't cool in the cloud.
It's time for your enterprise to take a new approach to cloud security too.

Be like Jack.

Get to know Gemalto.

GEMALTO.COM/CLOUD-SECURITY

Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments and data – from the edge to the core. Gemalto's newly expanded portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

GEMALTO.COM