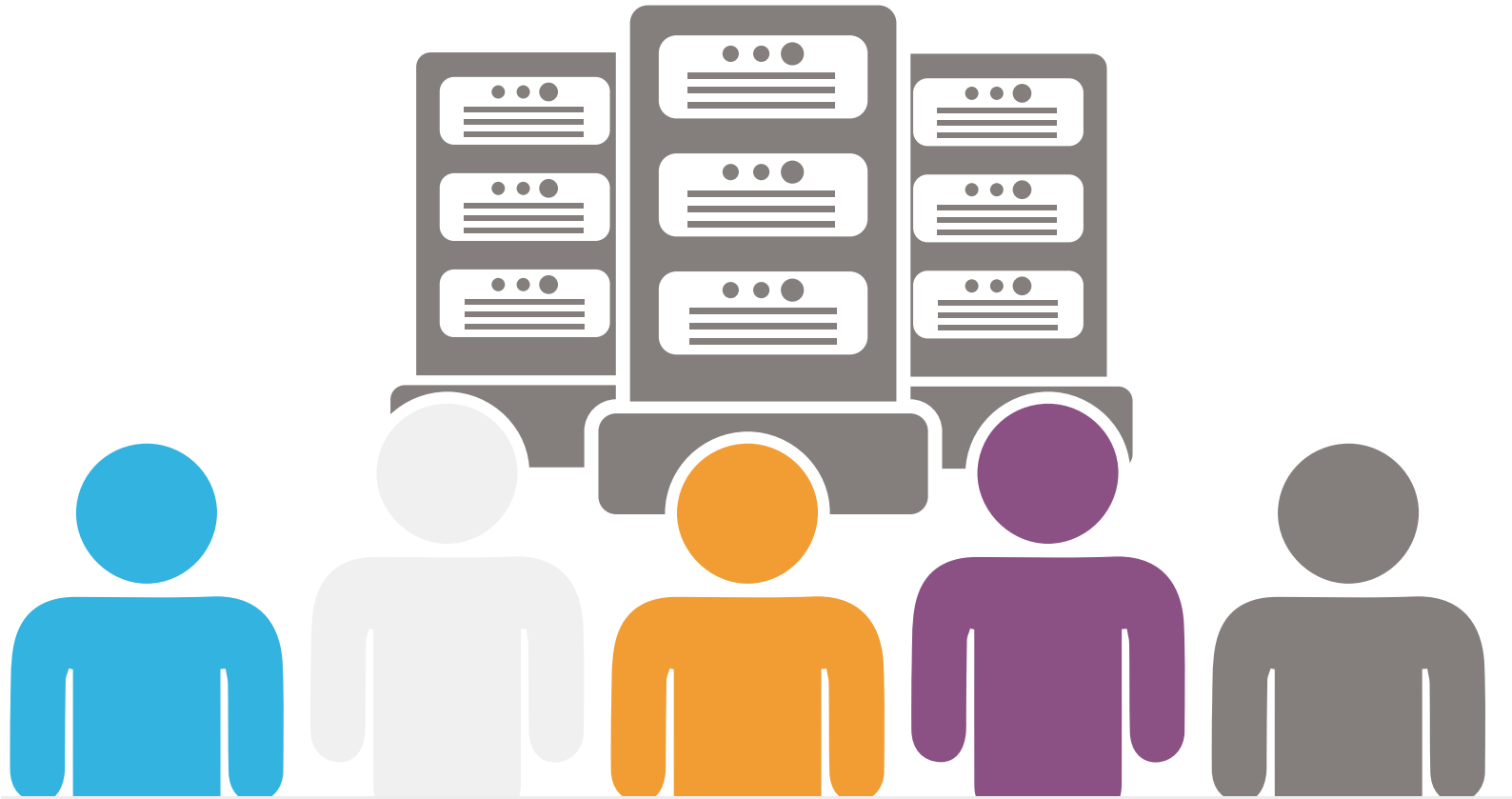
gemalto
security to be free

Encrypt Everything

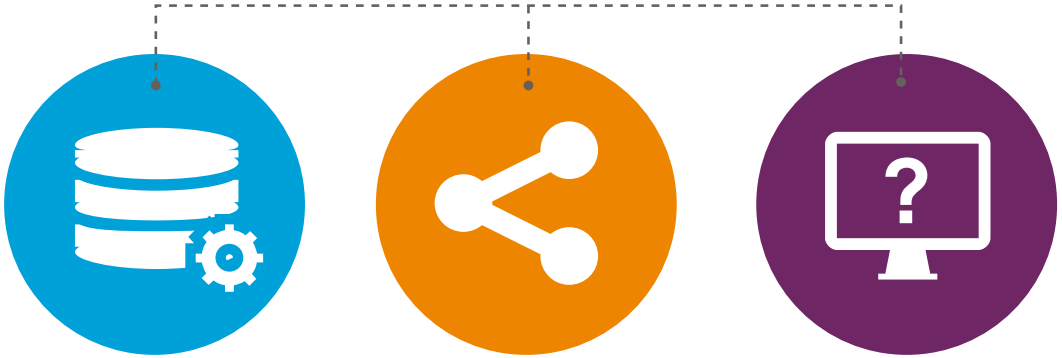
How to unshare and secure your sensitive data wherever it resides

The Data Protection Dilemma

Enterprises of every size and in every industry around the globe are producing more data than ever before. At the same time, there is a greater demand for access to this information.



{MORE SENSITIVE DATA}



Produced, processed and stored in **more places**

Shared more

Distributed to **more locations** outside of your control

From business intelligence and marketing teams, to partners and third party vendors, everyone wants their eyes on the data to reduce costs, improve efficiency, develop new products, optimize offerings, and to make smarter, data-driven business decisions. To meet these demands, data will need be produced in more places, stored in more places, processed in more places, and ultimately, shared and distributed to more places.

As an IT professional, this isn't new news. You're living it – and it's quite the data protection dilemma. The thought of sharing your organization's sensitive data outside of your brick and mortar location (and outside of your watchful eye) is a growing concern. So how do you find a way to balance critical business needs and requirements, while protecting your data from malicious threats?

→ **Let's explore how to address this data protection dilemma.**

Unsharing Your Data

We live in a world of sharing, and sometimes we share a little more than we should. Of course, we're not only referring to social media posts here; this also includes what is happening with your corporate data assets too.

With your organization's sensitive data being stored, sliced and diced, and shared more than ever before, you must have a way to keep it safe, especially in cloud and multi-tenant environments. Approved users and processes need to be able to leverage the data that's available, while you ensure any high-value, sensitive information, such as intellectual property, personally identifiable information, and company financials, remains on lock down wherever it resides.

We call this unsharing your data.

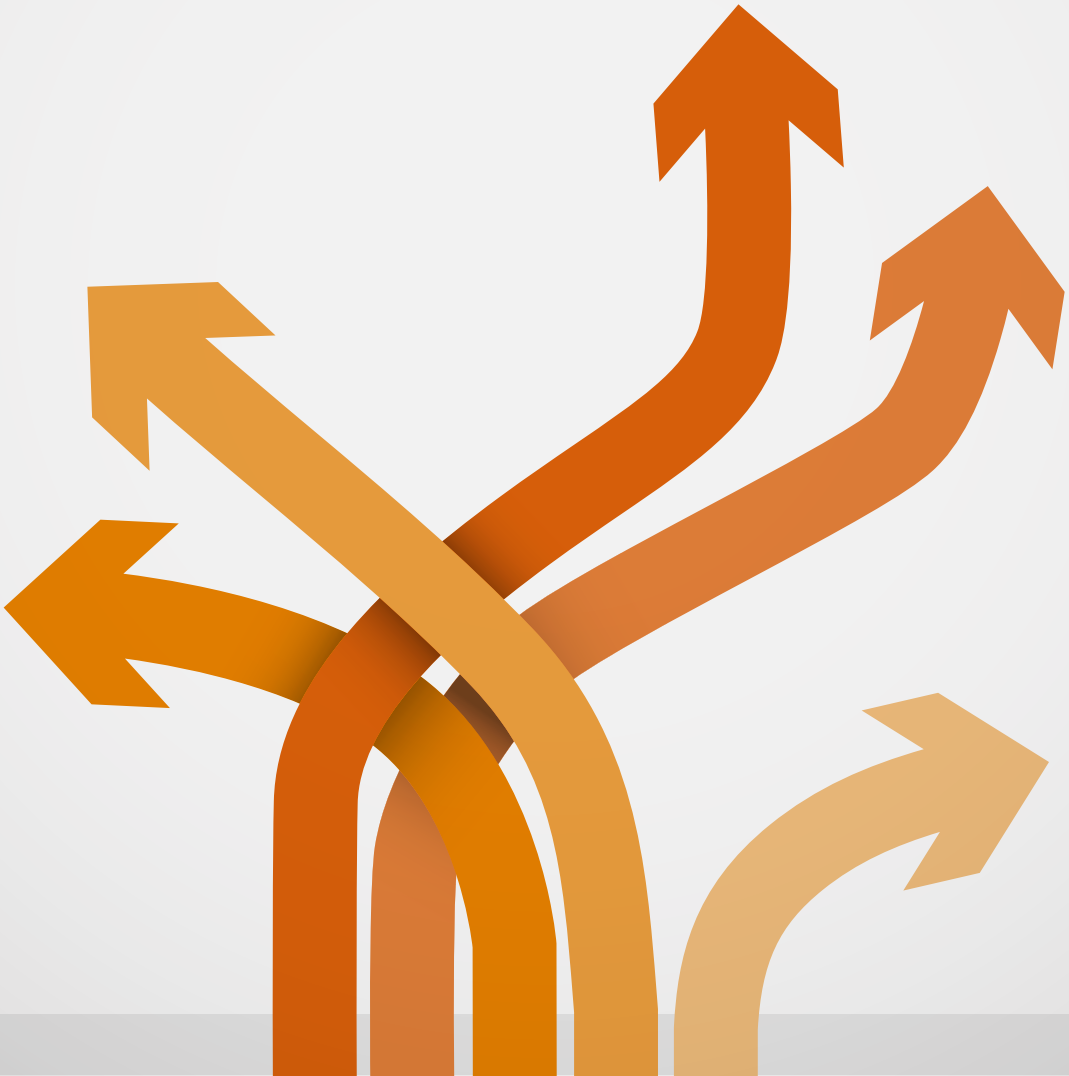
Here are a few trending reasons your business may need to unshare sensitive data:

Migrating data to the cloud to take advantage of the efficiency and scalability available, while still maintaining complete ownership and control of your data and encryption keys in a shared environment.

Enabling big data analysis without exposing sensitive information to external and internal threats that could result in a breach.

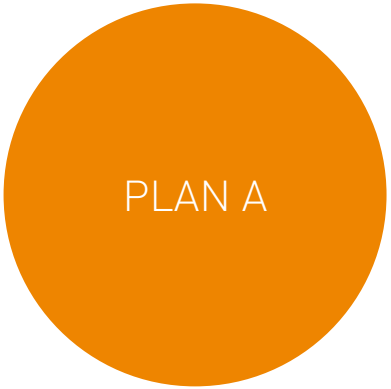
Granting access to available data while keeping intellectual property or personally identifiable information secure through the authentication of users and services to ensure they are who and what they say they are.

How to build a strategy for unsharing your data.



Have a Plan

In order to unshare your sensitive data, you need a plan. Actually, you need two plans.



First, there's a **Plan A**. A few years back this would likely be the only plan you had – perimeter protection. Here's the thing. That line of defense is too late. While there is nothing wrong with network perimeter security technologies as an added layer of protection, you cannot rely on them as the foundation of your data security strategy. A breach will happen and you need to accept it. Traditional perimeter security is no longer enough and your data is the new perimeter.

And that's why you need **Plan B**.

Remember the adage, keep your friends close and your enemies closer? Adversaries are after your sensitive data. Take the time to identify all potential and emerging threats, both external and internal to your organization. Then apply protection to the data itself to ensure that even after the perimeter is breached, your data assets remain secure.

Sounds like a pretty solid plan, right?

Here's what you need to develop your **Plan B** and lock down your data.

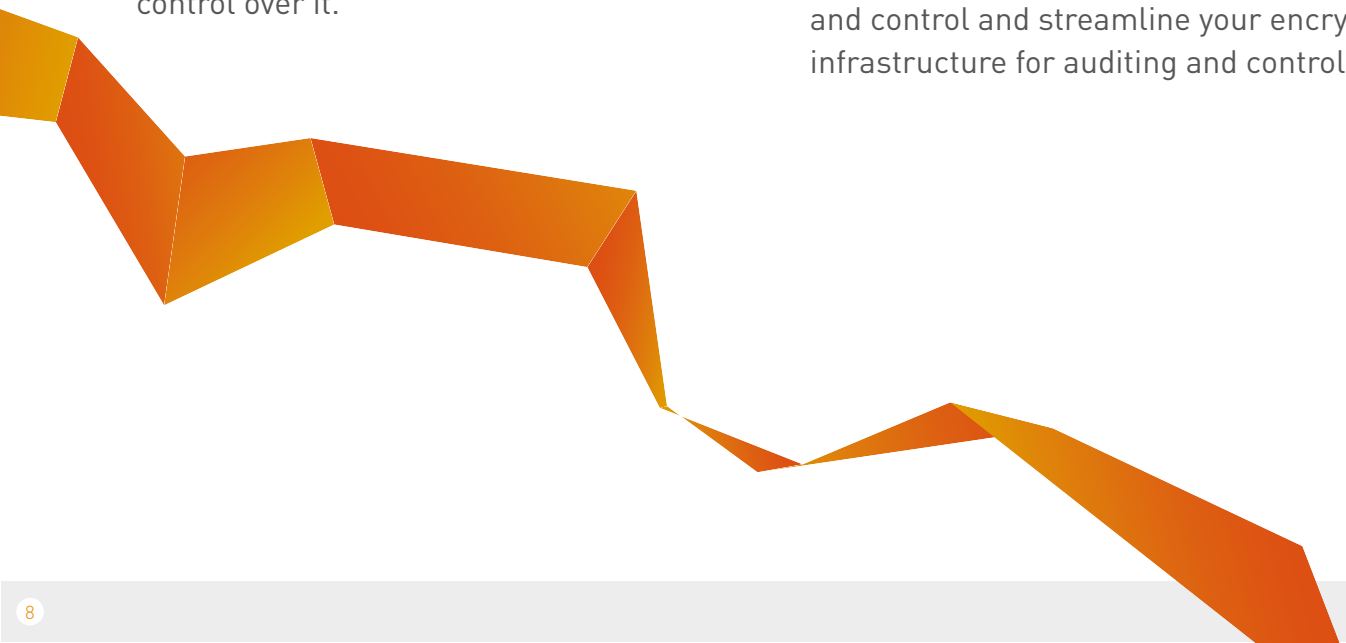
Encrypt Everything

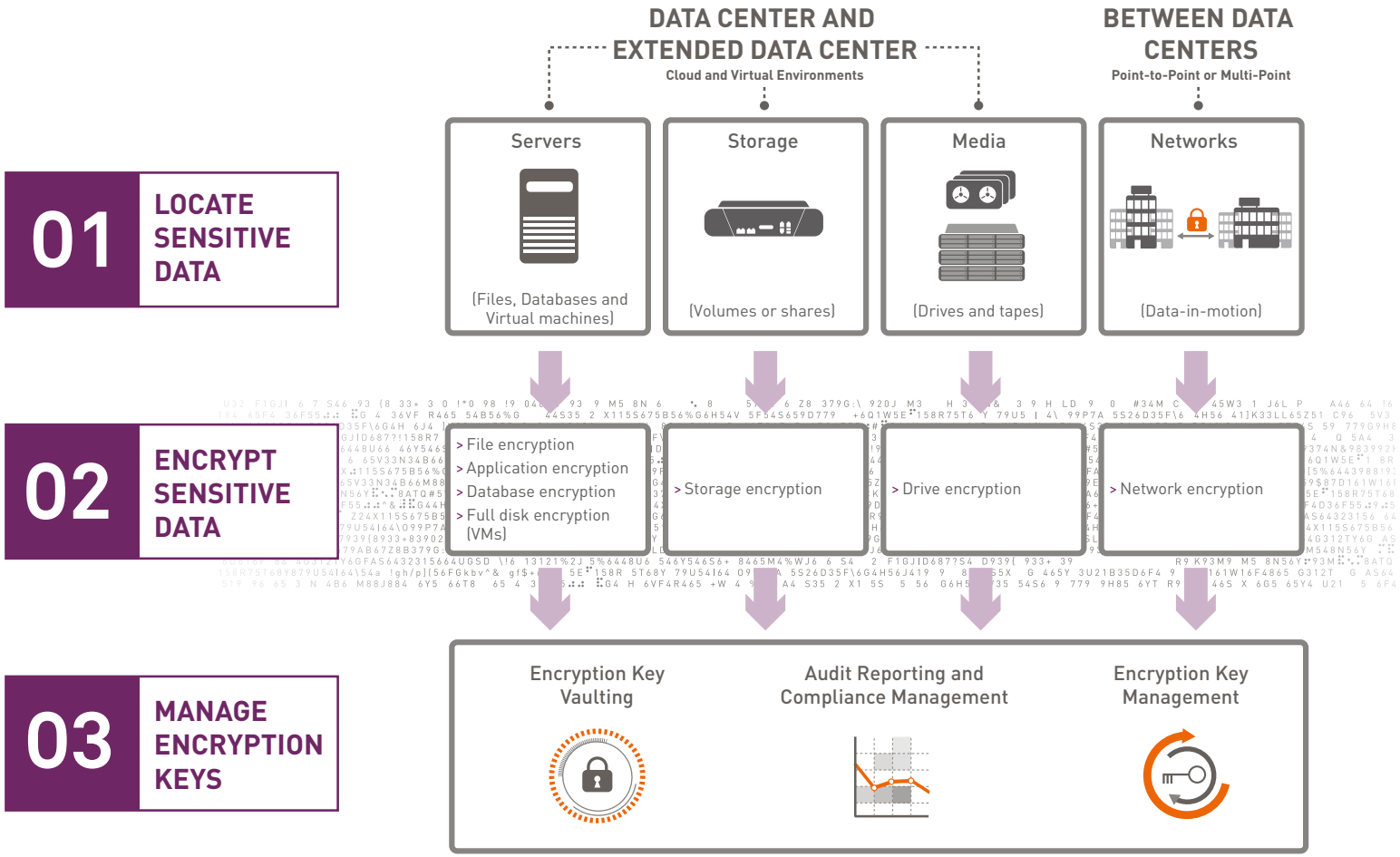
Follow these steps to unshare and protect your sensitive data

Start by identifying where your most sensitive data assets reside in your on-premises data center and then move to your extended data center (cloud and virtual environments). Search your storage and file servers, applications, databases and virtual machines. Don't overlook the traffic flowing across your network and between data centers. Once this data leaves the confines of your organization, you no longer have control over it.

Next, encrypt it. The promise of data encryption is probably familiar territory for you. However, the technological capability to encrypt data at scale, and in a centralized way that does not disrupt the flow of business, is a reality with today's enterprise-ready solutions.

And don't forget the keys. By managing and storing your keys centrally, yet separate from the data, you can maintain ownership and control and streamline your encryption infrastructure for auditing and control.




01
LOCATE SENSITIVE DATA
02
ENCRYPT SENSITIVE DATA
03
MANAGE ENCRYPTION KEYS
DATA CENTER AND EXTENDED DATA CENTER
Cloud and Virtual Environments
BETWEEN DATA CENTERS
Point-to-Point or Multi-Point
Servers
(Files, Databases and Virtual machines)
Storage
(Volumes or shares)
Media
(Drives and tapes)
Networks
(Data-in-motion)
> File encryption
> Application encryption
> Database encryption
> Full disk encryption (VMs)
> Storage encryption
> Drive encryption
> Network encryption
Encryption Key Vaulting
Audit Reporting and Compliance Management
Encryption Key Management

Encrypt Your Sensitive Data Wherever It Resides

Your encryption strategy and the solution you choose to deploy should meet two core requirements:

> **Provide access controls**
Define who and what can access your data

> **Protect the data directly**
Apply protection and controls that sit with the data itself

In addition to strong, centralized key management, ensure your data protection solution can also encrypt your sensitive data wherever it resides both at-rest and in-motion, including:

Application-Level Encryption

With application-level encryption, protection can be applied to multiple data types, from unstructured data, including Excel and PDF files, to structured data, such as credit card numbers, social security numbers, national ID numbers, and passwords. Encrypting this data as soon as it is generated or first processed by a web or application server keeps it secure across its entire lifecycle no matter how many times it is transferred, backed up, copied, or migrated from one environment to another.

Column-Level Database Encryption

From credit card information, patient data, and social security numbers to customer email addresses, you're likely storing some of your most valuable information assets in databases. A column-level encryption solution will enable you to move large amounts of sensitive, structured data in and out of the data stores rapidly by efficiently encrypting and decrypting the specific fields containing sensitive data. Encrypting this column-level data in your on-premises, cloud, and virtualized environments can prevent exposure in the event of a data breach, as well as ensure your organization maintains compliance with various regulations and mandates.

File and Folder Level Encryption

Due to its volume and relevance, high value data on network drives and file servers in on-premises, virtual, and cloud environments is often the most attractive and easily targeted. Examples include sensitive data, such as credit card numbers, personal information, logs, passwords, configurations, and more in a broad range of flat files, including word processing documents, spreadsheets, images, designs, database files, exports, archives, and backups. A file-level encryption solution will enable you to provide automated and transparent encryption of this sensitive data in local and mapped network files and folders based on policies you have established. In the event of a breach, misuse or hijacking of privileged accounts, physical theft of servers, and other potential threats, a file encryption solution will render sensitive data useless.

Full Disk Encryption of Virtual Machines

Migrating business applications and storing sensitive data in cloud environments is risky without the proper levels of encryption for the cloud storage environment. With your data residing in environments hosted by independent cloud service providers, it is important a high-availability solution is in place that provides full disk encryption of the entire virtual machine, as well as attached storage volumes. Encrypting the entire virtual machine will ensure you maintain complete control of your sensitive data in the cloud, while enabling you to address a number of industry security standards and government regulations, such as PCI DSS and HIPAA HITECH.

Network Storage Encryption

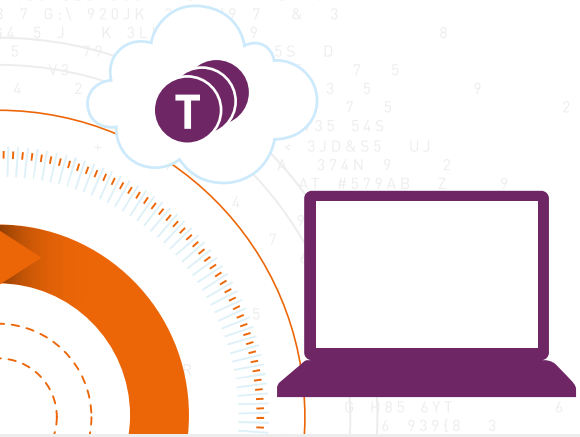
Increasingly sophisticated security breaches and more stringent government regulations, combined with explosive data growth, virtualization, and consolidation create new challenges for storage security. Network storage encryption secures file data connected to Ethernet networks — securing NAS storage using SMB(CIFS)/NFS file sharing protocols. Once sensitive data is encrypted on your network storage, it remains encrypted through its lifecycle, regardless of the media on which it is stored. Even backups and archives are secure, without any additional actions. Network storage encrypts data based on customizable business policies, enhances current authentication services and ensures data segregation — even in multi-tenant environments. The data is only accessible in clear text to authorized users.

Tokenization

As the amount of personal, sensitive data an organization collects grows, so does the risk of data exposure. Tokenization is another data protection solution that secures sensitive data, such as primary account numbers, social security numbers, phone numbers, passwords, email addresses, etc., by replacing it with a unique token that is stored, processed or transmitted in place of the clear data. Format Preserving Tokenization (FPT) preserves the length and format of the sensitive data with no changes needed to databases and applications—making it extremely scalable across multiple datacenters in on-premises, cloud, and virtual environments.

High Speed Encryption

In addition to data-at-rest solutions, you also want to protect data flowing across your network and/or between data centers. Networks are under constant attack and sensitive assets continue to be exposed. More than ever, leveraging encryption is a vital mandate for addressing threats to data as it traverses networks. Layer 2 High Speed Encryption can help organizations ensure that network traffic— sensitive data, video and voice, and even metadata — is secure. At the same time, the solution offers capabilities that help maximize network performance and operational efficiency to provide security without compromise, as well as maximum throughput and zero to minimal latency.

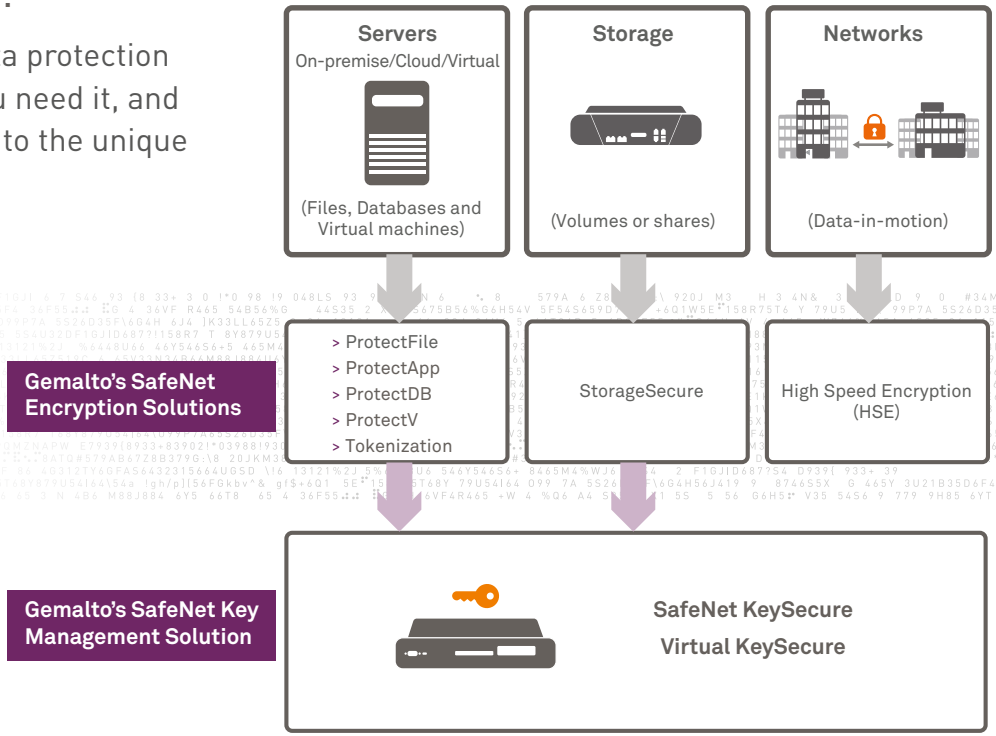



YOUR DATA
EVERYONE ELSE

When You're in the **Spotlight**, We've Got Your Back

With data security in the headlines, your executive team is probably taking notice and turning to you to ease their concerns. You're in the spotlight, but don't worry. We have your back, and the solutions you need to keep sensitive data at rest and data in motion safe, even in the event of a breach.

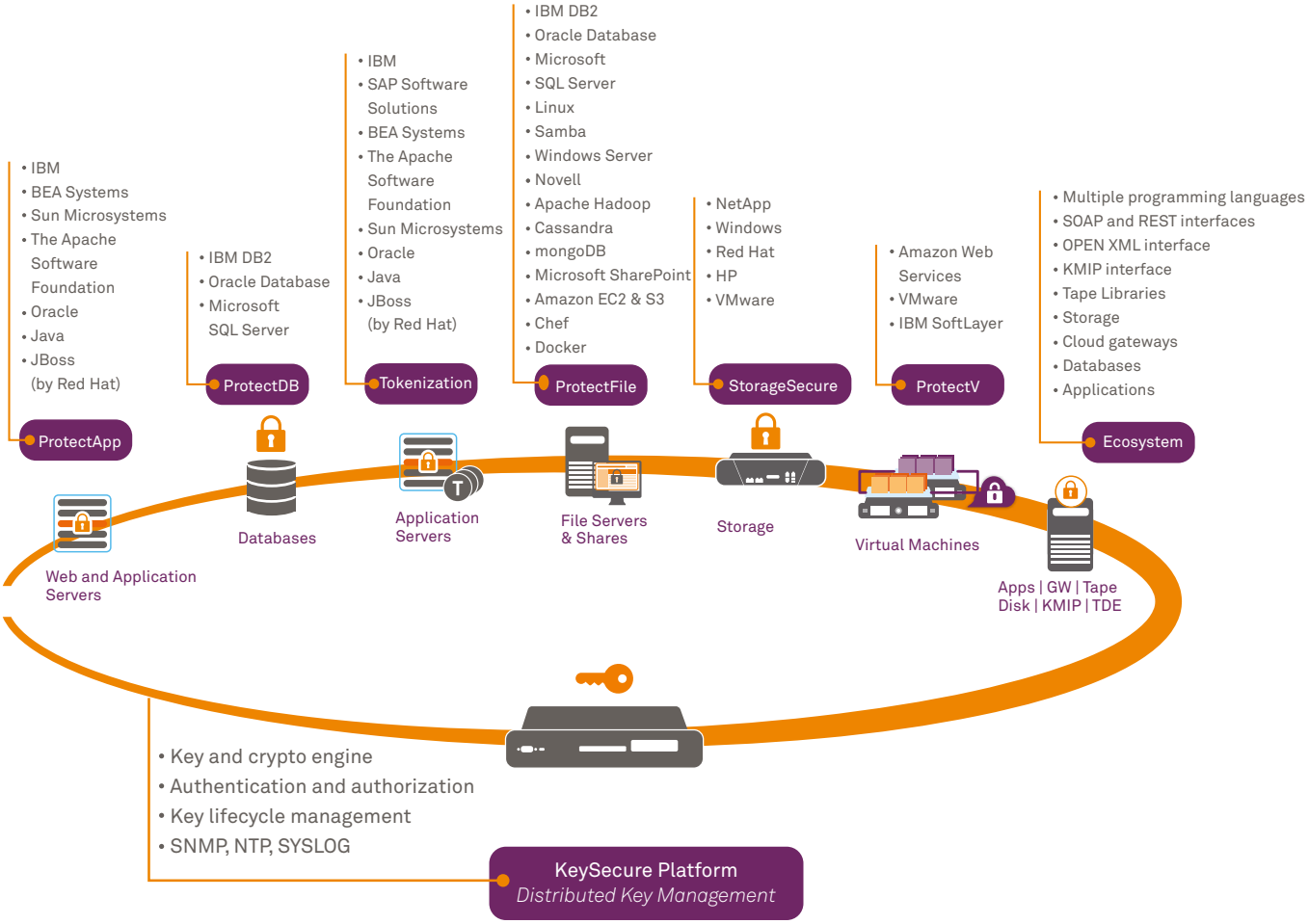
With Gemalto, you apply data protection where you need it, when you need it, and how you need it—according to the unique needs of your business.



Data-at-Rest Encryption Solutions

You know your data and infrastructure better than anyone. Gemalto's portfolio of data-at-rest encryption solutions delivers unmatched protection—securing databases, applications, file servers, and storage in your on-premises, cloud, and virtual environments. They seamlessly integrate with SafeNet KeySecure, Gemalto's FIPS 140-2 up to Level 3 validated enterprise key manager for centralized key and policy management.

This holistic approach means you can meet your immediate data protection needs now, while investing in a solution that provides robust security, a growing ecosystem, and the scalability you need to build a trusted framework for the future.


• IBM
• BEA Systems
• Sun Microsystems
• The Apache Software Foundation
• Oracle
• Java
• JBoss (by Red Hat)
ProtectApp
• IBM DB2
• Oracle Database
• Microsoft SQL Server
ProtectDB
• IBM
• SAP Software Solutions
• BEA Systems
• The Apache Software Foundation
• Sun Microsystems
• Oracle
• Java
• JBoss (by Red Hat)
Tokenization
• IBM DB2
• Oracle Database
• Microsoft
• SQL Server
• Linux
• Samba
• Windows Server
• Novell
• Apache Hadoop
• Cassandra
• mongoDB
• Microsoft SharePoint
• Amazon EC2 & S3
• Chef
• Docker
ProtectFile
• NetApp
• Windows
• Red Hat
• HP
• VMware
StorageSecure
• Amazon Web Services
• VMware
• IBM SoftLayer
ProtectV
• Multiple programming languages
• SOAP and REST interfaces
• OPEN XML interface
• KMIP interface
• Tape Libraries
• Storage
• Cloud gateways
• Databases
• Applications
Ecosystem
Web and Application Servers
Databases
Application Servers
File Servers & Shares
Storage
Virtual Machines
Apps | GW | Tape Disk | KMIP | TDE
• Key and crypto engine
• Authentication and authorization
• Key lifecycle management
• SNMP, NTP, SYSLOG
KeySecure Platform
Distributed Key Management

Data-in-Motion Encryption

In addition to its data-at-rest solutions, Gemalto delivers the world's leading certified **high speed encryptors** to secure data in motion. Gemalto ensures the most secure data-in-motion protection, maximum performance, near-zero overhead with "set and forget" management, and lowest total cost of ownership for speeds up to 10 Gbps. The first choice for Layer 2 encryption, our solutions are field-proven to secure data in transit for governments, defense agencies, global financial transactions networks, and the world's biggest cloud services providers. Gemalto high speed encryption solutions protect data in motion, including time-sensitive voice and video streams, as well as metadata for enterprise and government organizations.

Gemalto's SafeNet Encryption Solutions in Action

Let's take a closer look at how organizations are deploying our solutions to ensure their data at rest and data in motion remains secure:

> Enable secure cloud bursting

> Meet compliance and regulatory mandates

> Protect intellectual property

> Secure data, voice, and video in motion

> Deploy encryption as an IT service

Use Case: Enable Secure Cloud Bursting

Global Financial Services Firm Secures Data in the Cloud

Customer Problem

A leading global financial services firm wanted to deploy a single, third-party data security solution that included both encryption and key management to protect sensitive financial information – both internal organization data and customer data. The solution needed to run not only Amazon Web Services, but offer the flexibility to support future cloud service providers. They also wanted to be more elastic with their resources and test secure cloudbursting, or the ability to leverage the public cloud when an on-premises datacenter required additional compute power to support spikes in demand during the business day. A final requirement was the ability to deploy a single solution that would also support future cloud service providers and additional users, as needed.

Gemalto Solution

Gemalto SafeNet ProtectV and Virtual KeySecure was deployed to provide strong encryption and key management and support secure cloudbursting. As a security-conscious company, the organization did not want to rely on Amazon's key management and encryption solutions. They selected the Gemalto solution as it was independent from the cloud service provider and enabled them to maintain complete ownership and control of their data and encryption keys at all times. SafeNet ProtectV was also able to meet the organization's requirements to encrypt the entire virtual machine instance, including attached storage volumes, as well as require authorization of a user before launching a virtual machine.

Use Case: Meet Compliance and Regulatory Mandates

Leading Insurance Provider Ensures PCI DSS Compliance

Customer Problem

A leading insurance provider wanted to deploy a strong data protection strategy to comply with PCI DSS requirements and safeguard customer data, such as credit card numbers, telephone numbers, and other structured data residing in databases.

Gemalto Solution

To meet the PCI DSS requirement, the company selected SafeNet ProtectDB and SafeNet KeySecure, Gemalto's industry-leading enterprise key manager that delivers centralized key and policy management. SafeNet ProtectDB enables column-level encryption of the company's sensitive company data and ensures separation of duties by preventing database administrators (DBAs) from impersonating other database users to access sensitive data.

In addition, SafeNet KeySecure provides a unified data protection platform that can be extended to applications, files and folders, and mainframe environments to enable the organization to address their current data security needs, while providing a foundation for supporting future risk and compliance challenges.

Use Case: Protect Intellectual Property

Well-known Consumer Electronics Brand Keeps Intellectual Property on Lock Down

Customer Problem

A well-known manufacturer of consumer electronics required a solution to secure design work and other intellectual property. The company desired a solution that was able to encrypt unstructured data files, such as word processing documents, spreadsheets, images, designs, and more, while applying policies to ensure only authorized users could access this critical information.

Gemalto Solution

The company deployed Gemalto SafeNet ProtectFile to encrypt its highly sought-after intellectual property in combination with SafeNet KeySecure for centralized key and policy management. SafeNet ProtectFile ensures the teams working on these sensitive and confidential projects can collaborate productively with the confidence that their files remain secure. When designers or product architects create a design document, it is first encrypted by SafeNet ProtectFile and stored. The file can only be accessed by authorized users or applications based on policies set by administrators.

Use Case: Secure Data, Voice and Video in Motion

Multinational Telco Secures Customers' Data in Motion

Customer Problem

A multinational telecommunications company provides telecommunications and IT services to corporate clients (commercial and government) across the globe. These clients require that their information in transit, including high bandwidth live video streaming, remains secure. Types of applications that require this include: legal proceedings via video link, confidential internal organization meetings such as earnings calls for global companies, and live remote supervision of border controls. Network data quality is a central factor in customers' relationships with service providers, and security needs to be seamless, so as not to negatively affect the entire user experience. Video in particular places significant demands on networks, and customers are unable to compromise on quality issues such as latency, jitter or packet loss.

Gemalto Solution

Gemalto's broad range of SafeNet High Speed Encryptors (HSE) suited the telco's different customer requirements, such as certifications and attractive pricing for large scale deployments. SafeNet HSEs deliver high speed Layer 2 encryption while meeting the most demanding requirements for secure network performance for data, voice, and video in large scale deployments. The solution is ideal for real time applications, providing very low latency and near zero overheads. Easy to deploy, SafeNet HSEs offered a much better return than alternate solutions the telco considered such as Layer 3 that include encryption but with very high overheads or MACsec which was only designed for LAN-based "hop-by-hop" network connections. Neither solution scales to meet the telco's requirements today, or into the future. With Gemalto's Layer 2 encryption, the telco's customers get what they pay for from their networks, and the company can deliver the value-added services that help fuel improved customer satisfaction, reduce churn, and enhance retention.

Use Case: Deploy Encryption as an IT Service

Financial Giant Pioneers Encryption as an IT Service with Gemalto's SafeNet Encryption Solutions

Customer problem

A leading provider of consumer and business financial management solutions had sensitive data residing in on-premises and public cloud environments that needed to be secured to meet PCI DSS requirements and protect it from potential threats. Instead of addressing this need on project-by-project basis by department, the company wanted to centralize and unify its data protection approach by utilizing solutions from a single vendor. This approach would place all security ownership and decision-making to a select group in IT to reduce costs and centralize control of its data security solutions.

Gemalto Solution

The company chose Gemalto's portfolio of SafeNet data protection solutions, including SafeNet KeySecure for centralized key and policy management, as well as SafeNet ProtectApp, SafeNet ProtectDB, SafeNet ProtectFile, SafeNet ProtectV, SafeNet StorageSecure, and SafeNet Tokenization to encrypt and secure sensitive information across on-premises and cloud environments at all levels of the enterprise data stack. As a result, the company was able to meet their immediate compliance and data protection needs, while building a flexible, scalable framework for the future. In addition, by instituting an Encryption as an IT Service model, the organization was able to centrally deploy and manage data protection, while increasing overall security, administrative efficiency, and business agility.

Ready to Unshare Your Sensitive Data?

With threats to your sensitive data increasing and becoming more complex, it's important to take the steps to protect it now.

Contact us today or **learn more** about how Gemalto can help you unshare your data.

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: **data-protection.safenet-inc.com**

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

gemalto
security to be free