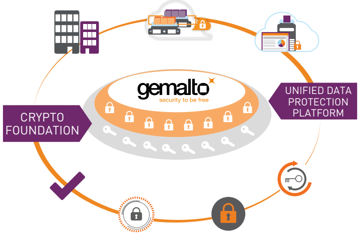


WHITE PAPER

Securing Data-at-Rest in Files, Folders and Shares:

Building a Sustainable Framework

Data growth is accelerating faster than ever before from the increasing prevalence of IoT devices, big data analytics and the general use of technology. As a result, more data is being produced, processed, and ultimately stored on file servers than ever before. This data can take many shapes from e-mail archives containing intellectual property to database files that hold payment cardholder information. Increasingly, this data lives dispersed in file servers across an organization and across locations rendering oversight difficult.

Growing volumes of valuable data motivate an increase in attacks that do not discriminate between businesses or government, or the size of the organization. These attacks target data and sensitive personal information or intellectual property and are becoming more prevalent and more severe.[1] Successful breaches are costly as fines, reimbursements and the damage to the victim's reputation can be significant. Today, data security is no longer optional for organizations, it's required.

What are the drivers for data security on file servers?

Organizations face threats ranging from privileged insiders abusing their position, to malicious outsiders infiltrating a network or nation states looking to steal IP. While attacks can have many goals, often the target of these attacks is information that resides in files living in a folder or on a network share.[2] Though organizations have a financial and existential interest in securing their data, for many, it's the specter of compliance that prompts the adoption of better security practices. Paradoxically, as the number of well publicized breaches increases so too does the pressure on lawmakers to tighten the very regulations that organizations dread in the first place.

The pervading assumption amongst security professionals is that strengthening the network perimeter is sufficient to keep data safe. Yet threats can appear in many forms and organizations must think beyond the perimeter and consider a wide range of vulnerabilities. Perimeters are an important part to the security strategy, but they are ineffective once an attacker is inside the network with access to many or even all of the files stored in its servers – as proven by the United States Office of Personnel Management (OPM) breach of 2015[3].

The vulnerabilities that organizations face include:

- External threats: Nation states, competitors, criminals and hacktivists are highly adept at evading organizations' perimeter defenses.
- Remote backups: Shipping data to offsite backup services or disaster recovery sites places it beyond the oversight of the administrator putting significant volumes of information at risk of loss or theft.
- Malicious employees: Employees can take advantage of broad access and steal sensitive data while on the job. For example, system administrators' access privileges put them in a position to use their technical expertise to access, steal or corrupt sensitive data throughout the organization.
- Inadvertent data leakage: Administrators and employees can make mistakes and expose data by storing it in the wrong location, accidentally bypassing manual security policies, or inconsistently adhering to existing policies.

[1] "While 2015 might not have had as many headline-grabbing data breaches as the previous year, it certainly saw a continuation of the large-scale assaults that have made cyber security a top priority for senior business executives and boards of directors at many companies– Breach Level Index Annual Report 2015

[2] "Third party evidence shows that the overwhelming focus on external attacks and insider abuse is to gain access to sensitive data stored on file and database servers." – Gartner, "Develop Encryption Strategies for the Server, Data Center and Cloud."

[3] http://arstechnica.com/security/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/

While none of these challenges are new to organizations, the speed at which attackers are able to target these vulnerabilities and circumvent traditional network and authentication technologies can no longer be ignored. Additionally, the advent of cloud services makes it easy for employees to reach into their own budgets for cheap sharing and storage services that, unfortunately, make it easy to move sensitive data offsite in unprotected formats. This evolution is simplifying work but also simplifies the process of data loss.

Another pain point for many organizations is that the roles and responsibilities of its administrators aren't coordinated enough to bring oversight to such gaps or keep up with the pace of technological innovation. For example, is the person responsible for storage also responsible for security? Since databases are also files does database security fall to the storage administrator or the database administrator? Who is responsible when these workloads are in the cloud? It's not an easy course to plot – even for the most forward thinking organizations.

In parallel, organizations face rules and regulations that outline their obligations in collecting, storing and sharing data. These compliance concerns span industries and affect every level of the organization from finance to HR to health professionals on the ground and executives in the C-suite. Most significantly, they can take precedence in charting a data security path because fines are easily quantifiable whereas the impact of a security breach may seem more nebulous. When making a case for budget, fines make for clear metrics. This drives a piecemeal approach to security that may not address the most strategic and persistent needs.

Realistically, securing data from so many complicated risks is a difficult task, but it's one that must be done. Without proper security, organizations leave themselves open to attack and the ire of the regulatory structures under which they find themselves.

Required Elements of an Enterprise-ready Data Protection Solution

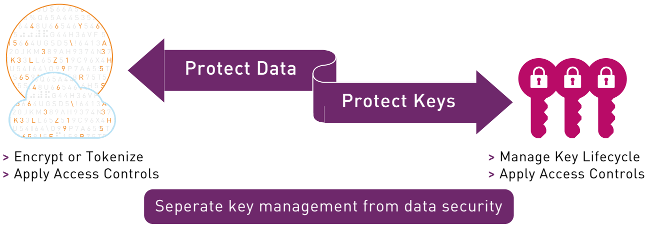
In meeting these challenges, organizations risk adopting a project by project approach that addresses individual security concerns, but becomes untenable when all put together. Growth will happen and security will need to scale to meet future needs. To be ready organizations must think beyond individual projects and choose solutions today that will continue to be relevant tomorrow.

A strategic thinker would build a framework for the long term that would be easy to manage, scalable, and relevant even as technology evolved. To be effective in the short and long term, a solution should be easy to deploy, have minimal impact on performance, and provide auditing and reporting capabilities. To remain relevant, the solution should also work across traditional data centers, multiple clouds, virtual environments, and hybrid infrastructures.

The best, proven, fundamentally sound way to achieve these short and long term strategic goals is to use encryption to attach security to the data itself unified behind a single, comprehensive key management system.

With encryption, users must have the appropriate key to access data in clear-text. Without the appropriate key, stolen encrypted data is unreadable, and remains useless to the thief. Because it affects the data itself, encryption follows the data as it travels to offsite back-up environments or into cloud servers. Even when the data stays on-site, encryption keeps it secure when attackers find ways to bypass the perimeter.

Uniting encryption solutions makes management easier across layers of the datacenter stack. This means centralizing encryption key and policy management behind a single key management platform. A single management point opens up the possibility of nuanced access controls, better automation, and demonstrably better logging and oversight. When centralized, encryption is no longer a limiting factor to growth - future requirements are less likely to outstrip the capacity to manage infrastructure.

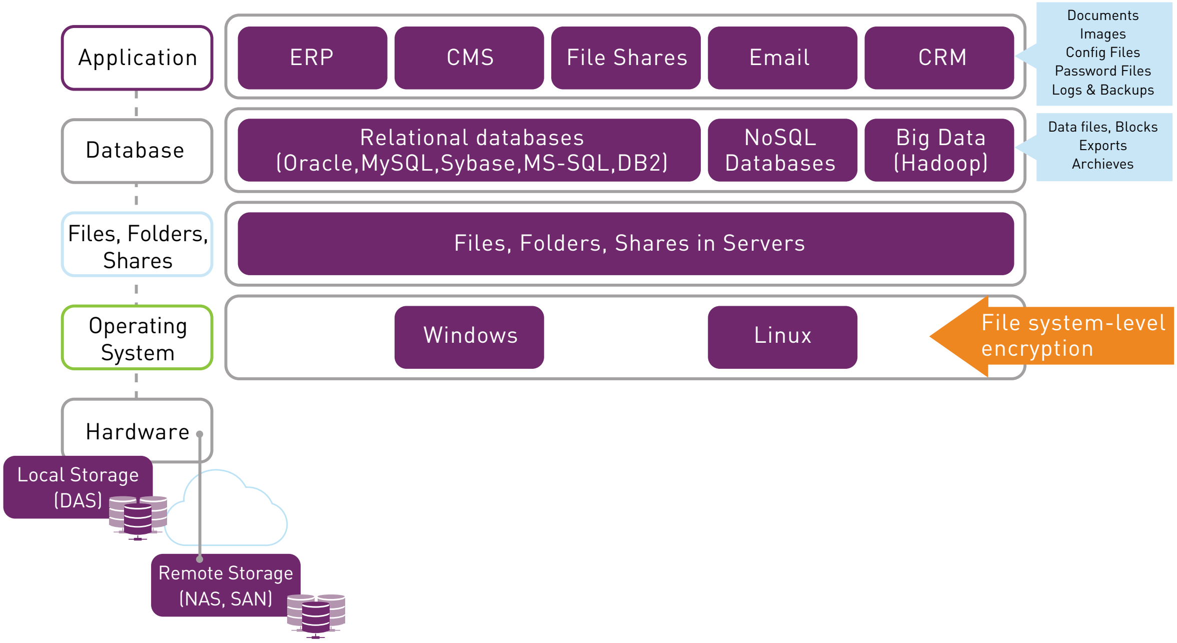


The key and policy management that accompanies encryption is where customers establish control and security to thwart or deter potential attacks. Not all key management is created equal; strong key management is fundamental to strong encryption security. Keys should always be stored separately and securely to preserve encryption's barrier to access. Restricting access to encryption keys by using policies gives administrators finely tuned control over who can access sensitive data. Now organizations can limit data access to what is needed to complete a job function.

File Encryption: The Swiss Army Knife Approach to Data Protection

Implementing encryption at the file, folder, or network share level can secure a wide range of data as it is written to disk. Securing an entire file or folder protects data against risks on-premises, in the cloud, or as it travels off site to replication centers. At this layer, encryption is a versatile approach to security.

Because it secures the entire file, it can be applied to any database, image, log, configuration, ERP or CMS file that may contain valuable intellectual property or customer information. Often, of the encryption approaches, adopting file-level protection requires the smallest investment of time and money because it does not require any changes to your applications or databases. Yet, despite the small investments, file-encryption can yield big results in protecting data at rest.



The uses can be wide ranging. File encryption can secure data in Hadoop and other big data implementations. Additionally, it can be cloud agnostic, letting you take advantage of opportunities in the cloud while staying in full control. When the objective is securing data while it is at rest, file-level encryption is a powerful solution with few barriers to entry.

Improved Security through Encryption and Key Management

Better Security through Simplification

Encryption and key management concepts are relatively straight forward, but in practice implementation can quickly become complicated. As files and their storage are distributed around an enterprise – sometimes even offsite, in the cloud – encryption can become unwieldy. A key per folder or server or node can quickly add up in large datacenters to make effective management impossible. When unaligned database or application encryption solutions are added to the mix, organizations can be faced with a large number of silos, each with its own set of management requirements. More often than not organizations will meet their encryption needs by deploying solutions from multiple vendors ultimately deepening the problem of silos and complicating key management.

Although it may seem like only a scalability issue, complexity is fundamentally a challenge to security. The more complicated security becomes the more likely administrators will begin to look for ways to cut corners. Diverse encryption silos weaken security because it increases the likelihood that gaps will go overlooked as administrators struggle to keep track of the moving parts.

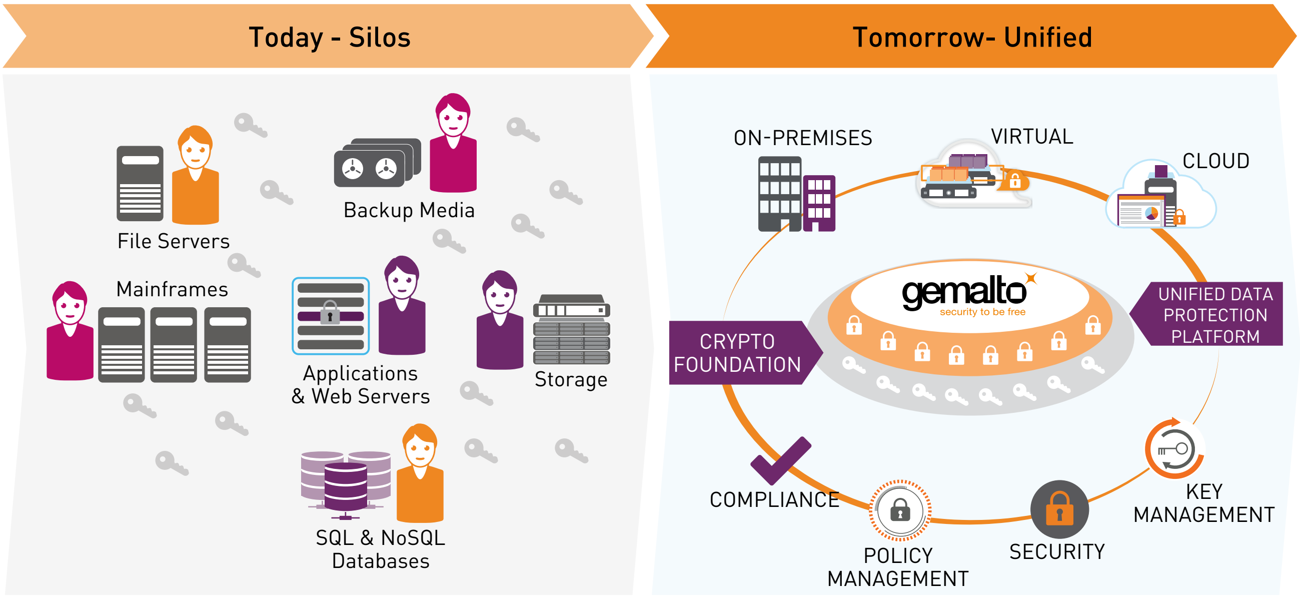
Segregate Data and Shared Servers

Organizations can use file encryption to ensure that data remains isolated in virtual and multi-tenant environments. With file encryption, administrators have the ability to use different encryption keys for each file or folder to restrict data access without fully restricting user access to the file share. Such a fine level of control gives security teams the flexibility to set up a framework of policy-based access controls according on user privileges, job responsibilities, and data location without seriously impacting ongoing operations or reducing information availability.

Nuanced Control through Access Policy and Key Management

Controlling access to encryption keys lets organizations mitigate risks posed by privileged users and administrators. For instance, an organization can assign key management responsibilities to one administrator and then assign storage infrastructure management to a colleague. While the key administrator has access to the clear-text data, she would not be able to manage the storage infrastructure. Conversely, the storage administrator can continue to manage the file server infrastructure – and all of the corresponding back up and replication sites – without ever earning access to the clear text data. Suddenly, the organization's data is secured from external attacks as well as the vulnerabilities that exist from privileged users within the organization.

Enterprise Data Protection as Centralized Service



Other options for securing data in files, folders, and shares

The security conversation for data-at-rest doesn't have to be limited to file encryption. While it is an incredibly powerful yet easy to implement solution, customers have several encryption options that can address ancillary concerns. Each of the following methods has its advantages, but customers would have to balance their needs and resources with their desired level of security.[4] As security gets implemented closer to the source where data is created, implementation effort increases and performance is affected. Implementing closer to the source reduces the amount of time data travels in the clear but, in return, it consumes more compute resources and can require meaningful effort to setup and manage.

Application-level Encryption

Encryption incorporated directly into the application secures data as it is generated. The benefit is that data is secured earlier in its flow to rest. If malicious outsiders attempt to steal it while it is in transit from the application to the file server, it will be unreadable to the attacker.

Application-level encryption solutions can leave data transparent to the application and end-user, so as authorized users access data as part of their normal job responsibilities, they can access it without altering their experience. Much like file encryption, application encryption secures a broad spectrum of file types – from CRM data to database files. Unlike file encryption, however, incorporating encryption into an application requires development effort – often small - and may not always be possible.

Virtual Machine Encryption

As files reside on a virtual machine, it is possible to secure the entire virtual machine instance as a blanket form of security for everything contained within. This could be considered as similar to Full Disk Encryption, except of a virtual machine. This ensures that a virtual instance cannot be copied and replicated in an unauthorized environment to yield the sensitive data. It is an effective form of security for virtual machines used primarily for backup and storage. When the virtual machine is running, the data passes in and out of the instance in clear-text. Some virtual machine encryption solutions will only decrypt files when they are open, keeping unopen files secure even as the virtual machine runs. This option offers more flexible security than a traditional full disk encryption approach. Much like file level encryption, using virtual machine encryption requires a smaller investment of time and energy in deploying the solution. Virtual machine encryption can be easier to deploy than file system-level data protection solutions, but may not offer granular controls to secure data at the folder level.

The Gemalto Approach: SafeNet Data Protection Solutions

Gemalto's SafeNet data protection portfolio offers a comprehensive range of data protection and key management solutions to secure data-at-rest, as well as data-in-motion across the enterprise. The SafeNet data protection portfolio is cloud agnostic and uses the SafeNet KeySecure key management appliance to run cryptographic operations and ensure efficient centralized key management for encryption deployments on-premises or in the cloud. The following solutions are most appropriate for protecting data-at-rest.

SafeNet ProtectFile: Transparent File Encryption

SafeNet ProtectFile provides transparent and automated file system-level encryption of server data at rest in the distributed enterprise. SafeNet ProtectFile supports Common Internet File System (CIFS) and Network File System (NFS) file sharing protocols to secure files that reside on direct-attached storage (DAS), storage area network (SAN), and network-attached storage (NAS) server environments.

SafeNet ProtectFile includes policy-based access controls to mitigate the risks posed by malicious insiders. Additionally automated key rotation and data re-keying, and comprehensive logging and reporting are built-in to enhance data protection.

[4] "CISOs will need to detail and document the variety of use cases for encryption tailored to each environment and compliance requirement through prioritization of protection against risks and threats. The risks posed by data residency and hacking must be addressed." Gartner, "Develop Encryption Strategies for the Server, Data Center and Cloud."

SafeNet ProtectFile represents an optimal solution for securing files whether they stay on-premises or are backed-up offsite. The solution also offers effective security across cloud environments and in big data implementations, including those running on Apache Hadoop and IBM InfoSphere BigInsights.

SafeNet ProtectApp: Application-level Encryption

SafeNet ProtectApp encrypts data at the application level to secure sensitive data—such as intellectual property or personally identifiable information (PII)—as it is created. It protects both structured and unstructured data making it a comprehensive solution to the data security challenge.

SafeNet ProtectApp is an API based solution that is easy to incorporate into enterprise-grade applications. Like SafeNet ProtectFile, SafeNet ProtectApp also includes, comprehensive auditing and logging features, built-in automated key rotation and data re-keying, as well as granular access controls that restrict data access to authorized users and applications.

SafeNet ProtectV: Virtual Machine Encryption

SafeNet ProtectV empowers you to secure your data and prove compliance in cloud-enabled environments. SafeNet ProtectV encrypts virtual machines and their associated storage volumes, instance snapshots and backups, and partitions. SafeNet ProtectV secures data in virtualized and cloud environments while letting organizations maintain ownership and control of their data and encryption keys at all times. Its pre-boot authentication requirement restricts the launch of virtual machine instances while the SafeNet ProtectV manager lets customers audit and report on all key access, or revoke that access in the event of a breach.

Robust, Centralized Enterprise Key Management

SafeNet KeySecure

SafeNet KeySecure is a FIPS 140-2 validated centralized encryption and key management appliance that streamlines encryption deployments across the enterprise. It seamlessly integrates with the SafeNet data protection portfolio as well as a broad portfolio of third-party partners via the Key Management Interoperability Protocol (KMIP) standard to eliminate the encryption silos that exist within organizations today. SafeNet KeySecure's efficient centralization is the perfect solution for strategic thinking administrators planning for the future growth of their data protection implementation.

Conclusion

Protecting the valuable information that currently resides in files across the organization will only grow as a concern. Fortunately, Gemalto's portfolio of SafeNet Data Protection solutions addresses the challenges organizations face in forming a durable, cohesive approach. Putting unified key and policy management at the center of the strategy not only makes data protection easier, it eliminates blind-spots, and through the encryption it supports, keeps data safe wherever it travels.

About Gemalto

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.

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

Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free