SOLUTION BRIEF

Protecting Sensitive Data on Infinidat Storage
with Thales Data Protection Solutions

The modern IT landscape requires more attention than ever to the handling of customers' private data. A data breach, of any size, can result in a loss of trust, which results in a loss of business. To make matters worse, there is an increasing number of attack vectors being added to the landscape every day, with the growth of mobile apps, sensors, and data sharing arrangements. A common solution to this problem is end-to-end encryption. Unfortunately, this solution introduces a new set of infrastructure management challenges for encryption key management.

There are three driving forces behind this change:

- **Increase in economically-motivated breaches**
  In 2020, according to the 2021 Data Threat Report, 47% of global organizations report that they have been breached or failed a compliance audit in the past year. As reported in the 2021 Data Breach Investigations Report from Verizon, 64% of breaches were financially motivated and 9% were strategically motivated (espionage).
- **Increased privacy regulations**
  All over the world, regulators are raising the bar for the handling and protection of the private data of their citizens. Prominent examples are the GDPR in the EU, NYDFS Cybersecurity in the financial sector and Japan's APPI legislation.
- **Attacks growing in number and sophistication**
  As hacking toolsets have become a commodity sold off-the-shelf, their availability and sophistication have also increased. This has led to an increase both in the number of attackers as well as the complexity of identifying these attacks.

57%

According to an ESG/ISSA study, experienced security teams are in short supply; 57% of respondents indicated they have "felt the impact" and this is making many organizations more vulnerable to attack.

The impact of breaches includes financial losses, loss of IP, and increased business risk, with a potential for high fines when the organization fails to protect its customers' private data. On top of the fines, there's the risk of damaging the reputation of the organization as data breaches require notifying the data subjects. At the same time, studies such as the ESG/ISSA report titled, The Life and Times of Cybersecurity Professionals 2021, show that experienced security teams are in short supply. 57% of those respondents indicated that they have "felt the impact" and this skill shortage in the market is making many organizations more vulnerable to attacks.

However, realizing that no IT environment can be protected from all angles over time, some regulators have put in place a 'safe harbor' clause that covers the organization if they show that technological means and operational processes were put in place to prevent the data from being breached. Encryption is the most common and straightforward method of doing that, and is often clearly called for by the regulators (e.g. GDPR Article 34, NYDFS). Regulators have given businesses the means for protecting themselves both from a data breach and from its implications. This is important, as data can be intercepted both in flight and at rest.

VERIFIED SOLUTION
THALES

Protection guidelines

Encrypting data may take place at many levels across the IT stack, however there is one clear rule: As encryption moves higher up the IT stack (closer to the application), more layers are secured and as a result the attack surface becomes smaller and easier to protect.

For example: If the data leaves the already-encrypted VM, VM-level encryption is more robust as it encrypts everything and thus it can be moved from one location to another. vSAN on the other hand does not encrypt various system level decadency files. Making it more vulnerable than say VM, it remains encrypted as it travels down the stack through the network, storage, WAN links and Disaster Recovery (DR) site. This approach, known as End-to-End Encryption (E2EE) provides much wider coverage than data at rest encryption, which exposes the data in cleartext as soon as it leaves the storage (either towards the application or towards a DR system).

Where is Data Encrypted?	Attack Surface						
	App Admin	OS Admin	DBA	VM Admin	Network Admin	Storage Admin	Backup Admin
Application	⚠						
Volume or Filesystem	⚠	⚠					
Database	⚠	⚠	⚠				
VM Encryption	⚠	⚠	⚠	⚠			
Fabric (Data in flight)	⚠	⚠	⚠	⚠		⚠	⚠
Storage	⚠	⚠	⚠	⚠	⚠	⚠	⚠
Backup	⚠	⚠	⚠	⚠	⚠	⚠	⚠

Diagram 1: The impact of where data is encrypted on the resulting attack surface. E2EE remains encrypted as it travels down the stack through the network storage, WAN links and Disaster Recovery (DR) site, providing much wider security coverage than data at rest encryption, which exposes data in clear text as soon as it leaves storage.

Protection guidelines

As a rule of thumb, the higher up in the IT stack data gets encrypted, the more layers that are protected from data exfiltration in cleartext, the smaller the attack surface, and the easier it is to show the regulators in the event of an attack that data has not been compromised (which doesn't in itself mean that a data breach has not taken place, rather only that the data was not accessible). Here are the most common levels of protection available, and the threats that they protect against are:

- **Full disk encryption (FDE) and other disk level encryption solutions**
  Disk level encryption solutions only protect against physical loss or theft of a device. This is great for a laptop or desktop but does little to stop today's system level attacks on back-end data stores. While this is the most widely used option, the DBIR for recent years showed no successful data breaches this would protect against.
- **File system, volume or linked cloud storage encryption and access controls**
  These provide the next level up in data security by protecting at the system level. These solutions are quick to deploy and transparent to applications. No changes to operational processes or user workflows required, while system level threats from privileged users, compromised accounts, malicious insiders and others are excluded from access to data.
- **Transparent Database Encryption (TDE)**
  Adds protection from database administrators and internal users, but can bring scalability, compliance and best practice problems for encryption key management if not supported with complementary key management solutions.
- **Application layer encryption**
  Application layer encryption is, disruptive to existing processes but adds protection against internal application users, and is most frequently implemented when creating new applications, or during application refresh cycles.

Non-Technological Aspects

Another consideration for organizations is the skill shortage in cybersecurity, making both recruitment and security solution implementation longer, and leading organizations to look for solutions that can be integrated across multiple platforms to minimize the number of integration points required.

Operational Implications of Encryption on the IT Stack

What to Encrypt?

When determining where data encryption should be implemented to best meet your requirements, there are several tradeoffs to consider. Some organizations choose selective encryption (e.g. application layer encryption), leading to a complex data classification process that leaves a lot of room for human errors, most commonly as database schemas change. In addition, existing applications often require changes and rewrites to accommodate such selective encryption. Another option, wider "blanket" encryption at the file system or volume level, eliminates these problems by allowing the entire dataset to start out encrypted from the moment the application writes data to persistent memory, and to stay encrypted from that point on, including in the storage array. This has the advantage of easily and transparently protecting the dataset at the system level, while leaving a small, easier to defend attack surface.

Key Management

Regardless of the encryption solution chosen, compliance requirements, regulations and best practices all require strong encryption key lifecycle management. The strongest and most flexible protection will come with solutions that have been validated by third parties and provide interoperability with a wide range of other security solutions, whether or not compliance is required. Thales provides multiple solutions to these problems. CipherTrust Manager is the central management point for all CipherTrust Data Security Platform products. CipherTrust Manager enables centralized management of data security policies and key management, simplifying training, deployment and operations. CipherTrust Manager is available in different form factors and FIPS 140-2 levels (1, 2, or 3 validated).

The CipherTrust Data Security Platform makes it easy and efficient to manage data-at-rest security across your entire organization. Built on an extensible infrastructure, the data security protection platform features multiple data security products that can be deployed individually or in combination to deliver advanced encryption, tokenization and centralized key management. This data security solution prepares your organization for the next security challenge and new compliance requirement at the lowest TCO.
For organizations that require the highest level of assurance, customization, and trust in key management, Thales provides Hardware Security Modules (HSMs). Thales Luna Network HSM provide a hardened, tamper-resistant environment and are available in three certified form factors to support a variety of deployment scenarios including highly secure encryption operations, certificate authority support, secure code signing, IoT identification, and other custom PKI applications.

Infrastructure Implications

CPU Utilization

The overhead from encryption is minimized using the encryption capabilities available in modern CPUs. Modern CPUs from Intel and AMD include hardware encryption libraries that accelerate encryption operations to in-line speeds, eliminating the overhead of legacy software encryption solutions. With this change, and the move to a predominantly virtualized environment where the number of CPU cores available is the highest in the IT stack, and easily scales, this is no longer a real challenge.

Where to Encrypt

The solution that is quickest to deploy, with the lowest operation impacts, and that meets the highest number of compliance and best practices with a single deployment, are file and volume level encryption. These security controls require no changes to how applications are used or managed, but immediately help organizations meet compliance and best practice requirements by eliminating system level threats. System level privileged users can do their work (backups, systems management, patching and updating and so on) without being exposed to sensitive data in cleartext, while applications and application users continue to work with no changes.

CipherTrust Transparent Encryption enterprise software from Thales delivers data-at-rest and in-flight encryption with centralized key management, privileged user access control and detailed data access audit logging. This protects data wherever it resides, on-premises, across multiple clouds and within big data, and container environments.

The deployment is simple, scalable and fast, with agents installed at operating file system or device layer, and encryption and decryption is transparent to all applications that run above it. CipherTrust Transparent Encryption is designed to meet data security compliance and best practice requirements with minimal disruption, effort, and cost. Implementation of the server encryption software is seamless keeping both business and operational processes working without changes even during deployment and roll out.

Application layer data security occurs at the earliest stages in the data flow and represents the strongest option for protecting sensitive information. Solutions in this area provide protection against threats originating both within the application environment, at the DBA or Application Administrator level, as well as against lower level threats such as those resulting from system level privileged users and accounts.

Application encryption enables organizations to encrypt specific fields at the top of the technology stack, securing sensitive data before it is stored, and enabling application developers to control which users and roles have access to sensitive data.

CipherTrust Tokenization with Dynamic Data Masking dramatically reduces the cost and effort required to comply with security policies and regulatory mandates like PCI DSS while also making it simple to protect other sensitive data including Personally Identifiable Information (PII). Dynamic Data Masking protects data in use while tokenization is protecting data at rest. You can efficiently address your objectives for securing and anonymizing sensitive assets — whether they reside in data center, big data, container or cloud environments. Beyond performing data tokenization, the Tokenization Server centralizes all tokenization configuration with a graphical user interface for creating templates for both tokenization and data masking. Simplicity results from the ability, with as few as just one line of code inserted into applications, to tokenize or detokenize with dynamic data masking. For instance, replacing a U.S. Social Security Number, or U.K. National Insurance ID with a token.

CipherTrust enterprise key management offerings from Thales extend CipherTrust Data Security Platform solutions to enable organizations to centrally manage and control encryption keys for third party devices including Microsoft SQL TDE, Oracle TDE, external environments and native database encryption in conjunction with other platform products for simplicity, efficiency and lower cost of ownership.

Storage Layer

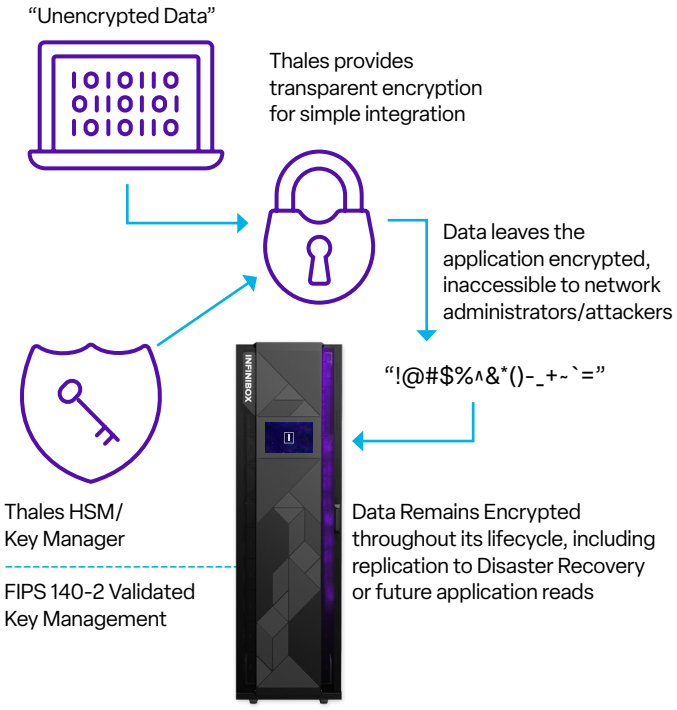
The storage layer has the potential to be impacted the most by end-to-end encryption, as many storage solutions rely heavily on data reduction technologies (deduplication, compression, pattern removal etc.) to offset the high cost of the flash hardware used to store data. Data reduction technologies do not work on encrypted data, and as a result, effective storage prices can increase between threefold and fivefold (depending on the current data reduction rate).

Not all storage solutions rely on data reduction features such as deduplication to reduce cost. InfiniBox relies on a hierarchy of memory types and leverages Neural Cache, a learning algorithm that enables 100% of writes and almost all reads to come from RAM instead of Flash. By avoiding the dependency on deduplication of data to achieve cost-efficient storage InfiniBox is the only solution to enable cost-effective storage for encrypted data. At the same time, InfiniBox still offers the non-encrypted datasets the modern data reduction capabilities to reduce costs further.

Storage Performance Considerations

Being able to complete an IO or a complex transaction quickly is key to user experience, and usually has direct implications on revenue. The small increase in latency due to the need to encrypt data can be minimized by committing new data to RAM (instead of slower media such as Flash) and by avoiding the need to decrypt the data again in the storage layer. This will also impact reads positively as data read from the storage will not require encryption before being sent over the wire followed by a decryption once it arrives at the host or application.

Avoiding another encryption and decryption of data in the storage layers just to enable it to traverse securely over the data fabric will also result in lower CPU load in the storage array, allowing it to consistently drive high IOPS at a low latency.



Conclusion

As Digital Transformation initiatives increase data value and sensitivity, privacy regulations like NYDFS Cybersecurity and GDPR will continue to expand both in requirements and in their global reach, and attacks will become increasingly sophisticated, posing ever-present threats and increased business risks. Organizations moving to E2EE will enjoy a reduced exposure to fines and negative press, while simplifying data security operations. The combination of InfiniBox for efficient storage of encrypted data and Thales products for data encryption and key management offer more comprehensive and cost-efficient protection to your data.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

About Infinidat

Infinidat is the most innovative enterprise storage company at scale today delivering a fully automated and autonomous set-it-and-forget-it approach with unprecedented 100% availability, unmatched real-world application performance, and a substantially lower total cost of ownership with significant savings in CAPEX and OPEX. The company's software-defined, storage-based portfolio provides enterprises and service providers with best-in-class solutions for primary storage, modern data protection, disaster recovery and business continuity, and cyber resilience.

InfiniBox provides multi-petabyte enterprise storage with scalability exceeding 8PB in a single 42U rack, unparalleled real-world workload performance, 100% availability guaranteed, and multi-protocol support with our automated set-it-and-forget-it ease of use. With a disruptive price point, InfiniBox also provides unprecedented business and technical value for modern enterprise storage.

InfiniBox™ SSA consistently delivers unmatched performance for the most extreme workloads— those that require ultra-low, micro-second latency for every I/O. InfiniBox SSA delivers the same proven reliability, 100% guaranteed availability, incredible ease-of-use and customer experience that enterprise IT organizations and cloud service providers have come to expect from the industry-acclaimed Infinidat family of enterprise storage solutions.

sales@infinidat.com | +1.855.900.4634

INFINIDAT