ESG SHOWCASE

End-to-end Encryption for Efficient, Secure Storage from Thales and Pure Storage

Date: February 2020 **Author:** Doug Cahill, Senior Analyst

ABSTRACT: Data assets are at constant risk from both external cyber adversaries and malicious insiders, making strong data security critical to any organization's cybersecurity program. Front and center in all programs is encryption, a foundational best practice for protecting sensitive data sets. However, data security and storage efficiency have too often been mutually exclusive. More specifically, encrypting data at rest has, to date, negated important storage optimization technologies, namely data deduplication and compression. To eliminate the need to make such undesirable trade-offs, Thales and Pure Storage have collaborated on a solution that integrates encryption technologies to protect data while maintaining the efficiency customers expect from Pure Storage's all-flash storage array.

Cyber Threats and Growing Volumes of Data Challenge Data Security Initiatives

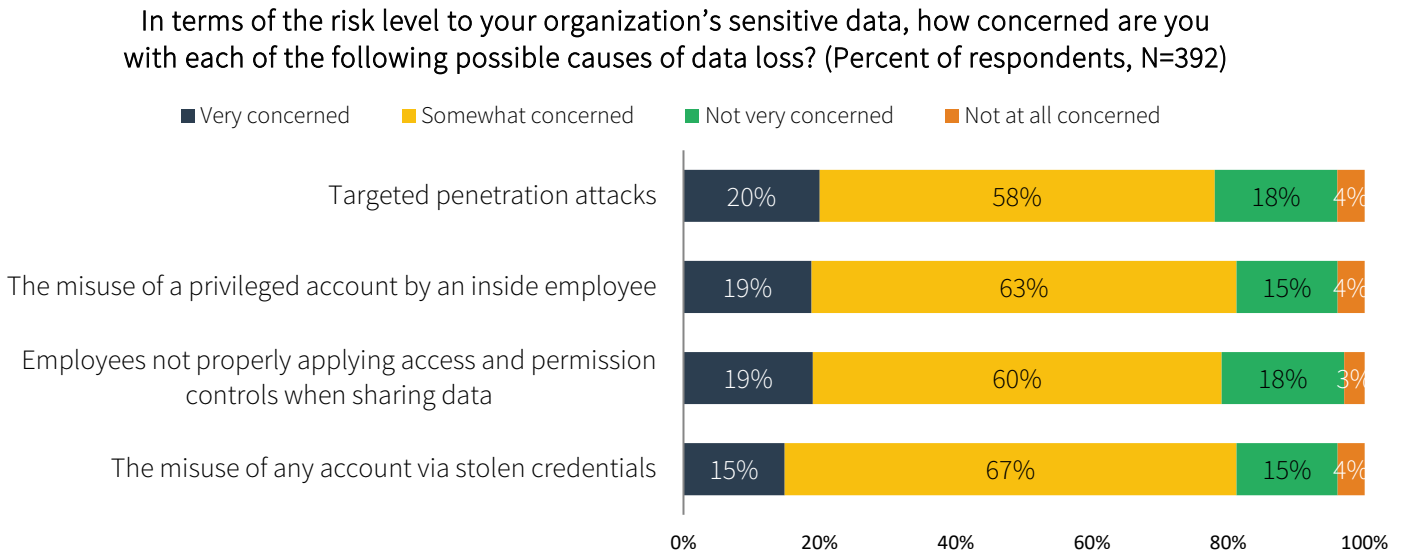
In today's economy, data is king as it continues to drive business decisions and customer experience. With such heavy reliance on sensitive data for business success, bad actors seek to leverage the value of this data by either holding it hostage as part of an extortion scheme or monetizing it on the dark web. These dynamics challenge both data security and regulatory compliance objectives.

A Diverse Threat Landscape Puts Data Assets at Risk

The sheer incident rate of cybersecurity attacks, including those that result in a data breach, continues unabated. Recent research conducted by ESG punctuates that reality with respect to the regularity and repeatability of cyber-attacks, with 60% of ESG research participants sharing their organization has experienced multiple ransomware attacks over the last 12 months, including 29% who have been attacked by ransomware on a weekly or daily basis.[1] ESG research also reveals strong concerns over a variety of possible causes of data loss, including data sharing policy violations and those associated with identity and access management issues such as the improper use of privileged accounts, and stolen credentials (see Figure 1).[2] These particular issues rooted in knowledge worker activity, identity, and level of privileges highlight the need for role-based access controls and establishing an audit trail of who accessed what data.

[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.
[2] Source: ESG Master Survey Results, *Trends in Cloud Data Security*, January 2019. All ESG research references and charts in this showcase have been taken from this master survey results set unless otherwise noted.

Figure 1. Possible Causes of Data Loss of Concern



Source: Enterprise Strategy Group

Increased Data Volumes Increases Complexity

ESG research reveals that 37% of participating organizations cited higher volumes of data as a top contributing factor to increasing IT complexity, making it the most often cited response.[3] And when it comes to data security, 90% of participants agree that managing data security processes and technology is more difficult than it was two years ago. In today's data-oriented economy, storage and cybersecurity teams clearly need solutions that help them simplify and operationalize cybersecurity, including data encryption, to keep pace with the rate at which data is created.

Storage Efficiency and Data Security Often Compete

Cybersecurity considerations are at odds with other organizational objectives at times. To some, the deliberate nature of cybersecurity processes threatens to slow innovation. And when it comes to scaling for the rate at which data is created, performance and thus efficiency is paramount. Storage technologies, such as all-flash storage arrays, deduplication, and compression, provide requisite optimization capabilities. Unfortunately, for security-focused organizations, encrypting sensitive data at rest has historically negated storage efficiency gains since encrypted data cannot be deduped or compressed. In fact, encrypted data consumes more storage, creating a price penalty in addition to the storage utilization optimization considerations.

Unfortunately, for security-focused organizations, encrypting sensitive data in-motion has historically negated storage efficiency gains since encrypted data cannot be deduped or compressed.

The Strategic Imperative to Operationalize Data Security

The diverse threat landscape, ongoing acute shortage of cybersecurity skills, and increasing rate in the growth of data volumes demand a new approach to data security, namely one which can eliminate the typical "security versus efficiency" tradeoff. While much of the discussion related to cybersecurity is concerned with improving the detection and prevention

[3] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.

of threats, operational efficiency is another consideration which must be optimized if an organization is to thrive in a data-driven environment.

Increasing Investments in Data Security

The strategic imperative to protect data amidst a range of attack types has resulted in data security being a top area of incremental investment, with 40% of research respondents citing data security as an area in which their organization will substantially increase spending. But which type of data security controls will receive this investment? In addition to the 45% who already use third-party encryption, another 41% have plans to employ it. The focus on third-party encryption is driven by the need for more robust solutions than those provided natively within storage systems.

The focus on third-party encryption is driven by the need for more robust solutions than those provided natively within storage systems.

Requirements for Third-party Data Encryption

Encryption solutions native to storage systems have a limited, albeit important, purpose, which is to protect loss of data from physical media in the event storage drives wind up in the wrong hands. By definition, built-in encryption occurs on the device. Third-party encryption allows options to encrypt data on servers and over the network to deliver simple and efficient end-to-end encryption. In contrast to native encryption, third-party data encryption solutions provide additional capabilities:

- Key management including key expiration and rotation policies.
- High assurance with FIPS 140 validated key managers and agents for securing data at rest over the wire.
- Role-based access controls (RBACs) to restrict access by groups of users.
- Privileged user access control to restrict the abuse of root credentials.
- Access auditing to establish a record of data access.

Integrating Vormetric Transparent Encryption with Pure Storage Arrays to Unify Objectives

Thales and Pure Storage have collaborated on an integrated solution that addresses the security and efficiency tradeoff. Specifically, the Vormetric Transparent Encryption (VTE) solution from Thales has been integrated with the Pure Storage FlashArray EncryptReduce capability, offering a solution that maintains the full benefit of data reduction, even when encryption is enabled.

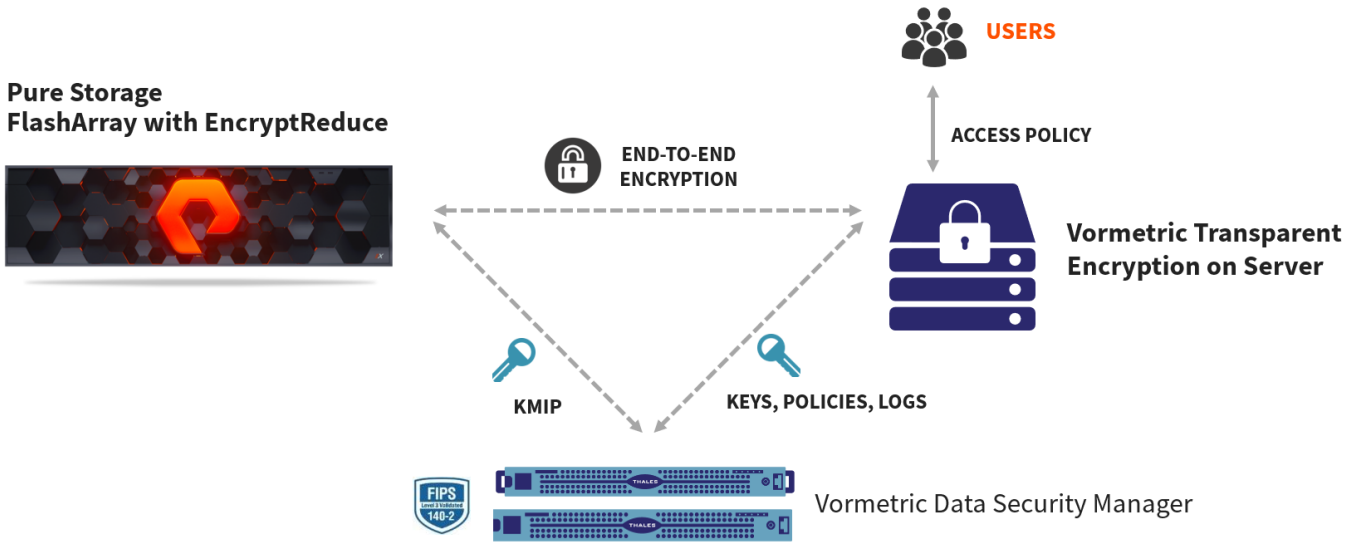
Secure Integrated Key Sharing

The Vormetric solution has been integrated with the Pure Storage FlashArray controller via Key Management Interoperability Protocol (KMIP), a protocol that allows for the secure sharing of encryption keys between the Vormetric Data Security Manager (DSM) and the Pure Storage FlashArray controller. It is important to note that sharing is trust-based

The result is managed end-to-end data encryption and access controls that don't sacrifice Pure's storage efficiency.

such that keys will only be shared with those Pure Storage FlashArray controllers with which the DSM has established a trusted connection. Key sharing via KMIP allows the Pure Storage FlashArray controller to decrypt encrypted data and perform deduplication (see Figure 2). The Pure Storage FlashArray then re-encrypts the data on the array with a storage-system-generated key. The result is managed end-to-end data encryption and access controls that don't sacrifice Pure's storage efficiency.

Figure 2. Key Sharing via the Key Management Interoperability Protocol (KMIP)



Source: Enterprise Strategy Group

Centralized Administration for Policy Management

The integrated solution utilizes the Vormetric Data Security Platform products. The Vormetric Data Security Manager (DSM) management console establishes trusted connections between hosts with VTE agent and Pure Storage FlashArray storage systems. With trust-based connections in place, the DSM console centralizes policy management across two important domains—key management and role-based access to establish a least-privileged posture.

Access Controls and Audit Trail

ESG research results show that 35% of respondents say actively monitoring user access to their most sensitive data is a top data security priority. To help meet this objective, VTE enforces the access control policies defined in the DSM and creates an audit log of permitted and denied access attempts. For auditing, the integrated solution offers two approaches:

- Natively in the DSM console. Collected at the system level, VTE logs report authorized and unauthorized access attempts to encrypted files and volumes—including user, time, process, and more.
- Third-party event management integration. Detailed data access audit logs delivered by VTE can be sent to security information and event management (SIEM) platforms and syslog servers. The VTE agent can also send logs to multiple locations simultaneously.

The Bigger Truth

Modern computing requirements demand that IT teams resolve competing objectives to enable business agility. Front and center is securing the speed at which organizations must move to capitalize on new market opportunities. Doing so requires optimizing the utilization of business-critical infrastructure such as high-performance flash storage arrays.

While employing end-to-end data encryption for array-resident sensitive data assets once meant forgoing the benefits of storage optimization technologies, Thales and Pure have partnered to remedy that tradeoff. The Pure Storage FlashArray with EncryptReduce data deduplication software combined with Vormetric Transparent Encryption creates an integrated data encryption workflow from the host to a Pure Storage FlashArray to leverage the data reduction technologies of the Purity Operating Environment. The integrated solution is rounded out with core data encryption policy management and auditing capabilities.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188