WHITE PAPER

Understanding the Impact of **Comprehensive Data Security**

SCALE TO WIN

INFINIDAT

The Challenges

2017 and 2018 were not easy years to be a CIO or CISO, and 2019 isn't showing any signs of being easier. With so many career-ending-level data breaches in 2017 (e.g., Equifax, Uber, Yahoo, to name a few) and with the stronger regulatory requirements worldwide, CIOs/CISOs have a corporate responsibility to rethink their approach to data security. Regulatory compliance aside, companies have a responsibility to their customers and shareholders to protect data, and minimize its exposure not only to external attackers but also to employees. The most common method of data breach in 2017 was a phishing email sent to a company's internal employees (See 2017 Data Breach Investigation Report), This makes employees unwillingly complicit in the data breach. Over 80% of successful cyberattacks have a critical human element that enabled them. The average employee who opens the innocent-looking attachment or link, is unintentionally jeopardizing a company's data. While there is no 100% protection, there are common sense rules to decrease the attack surface of any company.

There are two terms we need to keep in mind when thinking about protecting data from hackers:

> ***"The attack surface of a software environment is the sum of the different points (the "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment. Keeping the attack surface as small as possible is a basic security measure."*** *(Wikipedia)*

A corporation that treats its data as the source of its business advantage, and understands how sensitive it is to its customers, should minimize the attack surface. Why are All-Flash-Arrays (AFAs) in the way of this?

When The Org Chart Dictates the Security Method

Conway's law has long taught us that the organizational structure directly impacts the results/design more than anything else. In the context of security, this is fairly simple: if the CISO and storage manager coordinate their duties, you are going to find your data encrypted in the storage layer, and the "encryption" box will be checked. Storage is also the "path of least resistance" as storage arrays can instantly enable encryption without any performance penalty. However, is storage level encryption helping to reduce your attack surface? A little, yes. It still leaves ALL other layers unencrypted, and that data traverses the network unprotected.

So Where Should We Encrypt the Data?

Think of it this way—the higher up the encryption of personal/sensitive data happens, the more layers remain protected. Each row in the table below represents your attack surface if you choose a specific layer to encrypt the data in.

Notice how little storage level encryption actually protects? And yet, this is a commonly used data security method.

Where is Encryption Used	✓ **Who Can See the Data?** ⚠ **Who Can Accidentally Cause a Breach?**						
	App Admin	OS Admin	DBA	VM Admin	Network Admin	Storage Admin	Backup Admin
Application	⚠	✓	✓	✓	✓	✓	✓
Application OS	⚠	⚠	✓	✓	✓	✓	✓
Database	⚠	⚠	⚠	✓	✓	✓	✓
VM Encryption	⚠	⚠	⚠	⚠	✓	✓	✓
Fabric (Data in flight)	⚠	⚠	⚠	⚠	✓	⚠	⚠
Storage	⚠	⚠	⚠	⚠	⚠	⚠	⚠
Backup	⚠	⚠	⚠	⚠	⚠	⚠	⚠

Why Are All-Flash-Arrays Increasing Your Attack Surface?

While most (if not all) AFAs offer disk level encryption, that is the only level of encryption they allow—data is encrypted anywhere else, the AFAs can't perform data reduction and the entire economics of AFAs break. AFAs must rely on data reduction (1:3 and 1:6) to minimize the price premium to a point where the customers can afford it.

This means customers choosing to base their production infrastructure on All-Flash-Arrays are effectively blocking themselves from implementing an end-to-end encryption policy, which all regulations of data privacy require (GDPR, SB-1386, HIPAA, PCI-DSS, NY-DFS and others).

When "Optimal" Meets Feasible

THIS OPTIMAL APPROACH FOR DATA SECURITY IS OFTEN LIMITED BY PRE-EXISTING REALITIES:

- The 10-year-old application that doesn't offer encryption and is no longer supported
- The business critical app that takes a year to receive maintenance for
- The application owner who won't invest the time to encrypt

When the rubber hits the road, compromises are often needed to accelerate your data security adoption. Many customers will opt to encrypt these environments in lower levels of the stack (DB/VM/OS) to be able to comply with corporate and regulatory requirements. This approach is often mandatory to meet compliance deadlines, however it's worth limiting the number of separate approaches the company uses to avoid a high overhead. It's worth noting (again) that all these alternatives have the same effect—limiting the data reduction of AFAs, and increasing their storage TCO.

Additional Benefits of Encrypting up the Stack

DISTRIBUTION/PERFORMANCE

With the exception of Self Encrypting Drives (SED), performance requires some CPU power. An IT stack always has more hosts than storage arrays, moving the task of data encryption to a higher level of the stack. This also means you get a wider distribution of the workload, while reducing the workload on the individual device and optimally distributing performance.

GRANULARITY

The higher up the stack we encrypt, the better our granularity:

An application can encrypt only the Personal Identifiable Information (PII) as it "understands" the context/meaning of the data. This will lead to lower overhead, too. If we go one level lower—the Database Administrator (DBA) can provide an encrypted table space and a non-encrypted table space and put the right data in the right place. While this is less granular, it is still better than encrypting an entire VM or LUN.

CLOUD READINESS

Moving the encryption up the stack is a prerequisite for any cloud migration if the data needs to maintain the same level of protection and stay protected over the network (WAN). Data that is already encrypted at the source (on-premises) doesn't require any additional security measures when bursting or migrating to a cloud provider. This enables a hybrid cloud strategy as well as a multi-cloud strategy, as the application is not tied to specific cloud provider's security mechanisms.

EASE OF INTEGRATION

Integrating encryption at the OS/DB/hypervisor levels has a benefit—there are very few flavors of each, while there are many applications in the environment. From an operations perspective, this can reduce complexity.

CALL TO ACTION

- Plan your organization's holistic data protection policy
- Set a cut-off date for new applications to be designed with encryption from day one
- Train in-house application developers on security-by-design methodologies
- Examine existing applications looking for the right way for your organization to protect data-in-flight
- Build a transition plan to encrypt legacy applications with private or sensitive data