White Paper

Building a Secure Private Cloud with VMware vSAN Hyperconverged Architecture

Securing Data at the Source

By Terri McClure, ESG Senior Analyst; Doug Cahill, ESG Senior Analyst; Leah Matuson, ESG Research Analyst

May 2017

This ESG White Paper was commissioned by VMware and is distributed under license from ESG.

Contents

Executive Summary: The Intersection of Hyperconverged Infrastructure and Cybersecurity

When discussing hyperconverged infrastructure (HCI), one rarely hears the subject of security being addressed. Rather, security discussions are typically centered around data security, network security, and authentication. One reason for this is that the HCI space has really been about operational benefits versus securing assets, therefore it has not seen much investment or innovation on the data security front. Yet increasing cybersecurity is top of mind for IT organizations across the board, and the business initiative that 39% of ESG research respondents believe will drive the most IT spending at their organizations in 2017 (see Figure 1).[1] At the end of the day, security is really about protecting data, and data now "lives" within the (software-defined) confines of HCI, so it makes sense that we are finally seeing some security investments and innovation from HCI vendors.

Figure 1. Business Initiatives Driving Most IT Technology Spend

Source: Enterprise Strategy Group, 2017

Let's face it: Data can be stolen in a number of ways—by external bad actors as well as insider threats. Ransomware attacks can lock data, putting sensitive and business-critical information at risk of being used for extortion. Additionally, cybersecurity attack behavior models, such as Lockheed Martin's Cyber Kill Chain (a framework for identifying and preventing cyber-attacks), illustrate that many attacks begin by compromising an endpoint, then move laterally across an organization's infrastructure to servers in order to gain access to corporate data assets—representing a grave risk to those assets stored on HCI systems.

[1] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, March 2017.

So it stands to reason that organizations would look to secure their data at the core, where it's stored—by encrypting it at rest.

Data Encryption at Rest

Encrypting data at rest is not a new concept, but it hasn't been executed broadly—or successfully, when it comes to HCI and the modern data center. Why? The easy answer is because IT felt secure within the four walls of the data center given the well understood and hardened perimeter security measures most organizations have in place. But with the Internet, as well as the rise in use of portable devices and software-defined architectures, perimeters are now less well defined and perimeter controls in and of themselves can no longer protect infrastructure and corporate data assets. That means data must be protected and encrypted anywhere and everywhere it is accessed or stored. The main impediment for broader use of encryption at rest inside the data center has been the lack of any means to effectively operationalize doing so, including following key management best practices. In previous iterations, encrypting data could hurt performance and organizations would have to accept a "performance penalty," especially noticeable when it came to reading encrypted files. Thankfully today, new technology and approaches are solving those operational issues.

Encrypting Data at the Source

Encrypting data at rest, at the physical storage layer, improves security on a number of fronts. Encrypted storage drives protect data from data leaks associated with the theft of drives, drives removed for upgrades or service, or misplaced drives. Several advantages of encrypting data at rest include the following:

- Added security for distributed organizations. Encrypting data at rest could be especially helpful for distributed IT organizations that depend on third parties for IT staff augmentation. For example, organizations with remote and branch offices that do not have access to local IT resources, and that depend on outsourcing, could benefit from the added security of encrypting their data at rest so that drive replacements don't introduce a risk of security breach by leaving readable data on a drive that is removed from the system.

- Simplified media disposal. Regulated or security-sensitive customers often need to physically destroy decommissioned media due to security risks. This requirement can be eliminated with native encryption.

- Data-format-agnostic. When encrypting data at rest, both structured and unstructured data will be encrypted. Without the time and labor needed to determine data types, organizations can conserve resources.

Self-encrypting Drives

Self-encrypting drives (SEDs) are a means used to mitigate risk and protect data by encrypting all data on a drive, where it is stored. This is one way HCI vendors could quickly and easily incorporate deeper security into their solutions.

One of the benefits to this technology is the fact that the encryption key is stored at a layer below the OS, so an attacker would need to employ a kernel-level attack to get to it. Though one might think this design would be less vulnerable to attack, certain assaults made on software-based encryption products can also affect SEDs. That said, organizations must explore these additional SED limitations before implementing this technology:

- High cost. Generally, organizations will pay a premium for SEDs, and given that hundreds or thousands of drives could pass through a large IT organization's data center over a few years, the costs would quickly add up.

- Implementation issues. Not all SEDs are created alike. Certain SEDs are not Opal-compliant (Opal is a storage device policy management standard). This issue may present major implementation, management, and troubleshooting challenges.

- **Costly updates (both time and resources).** If IT determines an SED encryption algorithm implementation is vulnerable to an attack, a simple patch might not fix the problem—in which case, the entire drive might need to be replaced. What's more, the way SEDs are designed (proprietary versus open source) could make it very difficult for IT to even examine a drive for encryption flaws.

- **Labor-intensive management.** Unlike software-based encryption methods (where encryption management is built into the deployment process), SED management could require a hands-on approach.

With the ever-increasing number of cyber-attacks being perpetrated on organizations across industries today, what can IT do to efficiently and cost-effectively protect their data at the source, on the disk, thwarting the efforts of bad actors to steal (and ransom) sensitive and business-critical information? Enter VMware's vSAN HCI solution.

VMware has taken a new approach to data-at-rest encryption, with its software-based native vSAN HCI encryption solution—offering native data-at-rest encryption, without the drawbacks of a self-encrypting drive approach.

Competing Priorities: Security and Cost Reduction

Improving Security and Driving Down Costs: IT's Top 2017 Initiatives

Given the rising numbers of high-profile security breaches across businesses in recent years, it should come as no surprise that cybersecurity is a top business-level initiative among IT organizations—and increasing cybersecurity is the most-cited IT initiative. In fact, based on a recent survey of IT professionals, ESG found that 39% of IT organizations state that improving cybersecurity is one of the business initiatives that will drive IT spending for them in 2017, while 32% said that cost reduction initiatives will drive their IT spending.[2]

While trying to thwart breaches and mitigate risk is top of mind in most every organization, it's that much harder because organizations are plagued with a problematic shortage of IT skills. In fact, almost one-half (45%) of IT organizations ESG surveyed said that cybersecurity was one of the areas in which their IT organization had a problematic shortage of existing skills, while more than one in five companies (22%) said cybersecurity was the area with the most significant shortage of skills.[3] The cybersecurity skill set shortage creates a need for operational efficiency—i.e., the ability to do more with less.

Organizations need to take a practical approach as cost is still a big consideration. Given that a majority of IT budgets may not increase on a yearly basis, organizations must become smarter about their investments. And that's where HCI makes sense—and security *plus* HCI makes even more cost-effective sense. Organizations looking to reduce costs and drive operational efficiency are deploying hyperconverged infrastructures because of the associated benefits of total cost of ownership (TCO). It's worth spending time to review HCI and examine cost efficiencies.

Hyperconvergence: TCO-optimized Infrastructure

Hyperconverged infrastructure (HCI) is a software-defined infrastructure (SDI) approach that seamlessly combines compute, storage, networking, and data services in a single solution running on industry-standard x86 system(s), with the intention of running virtualized and/or containerized workloads.

Enabled by a distributed architecture (file system and object store), clustering multiple systems within and between sites forms a shared resource pool and enables high availability, workload mobility, and efficient scaling of performance and capacity. Hyperconverged systems are typically managed through a single management framework or orchestration tool with policy definition and activity execution at the VM/container level.

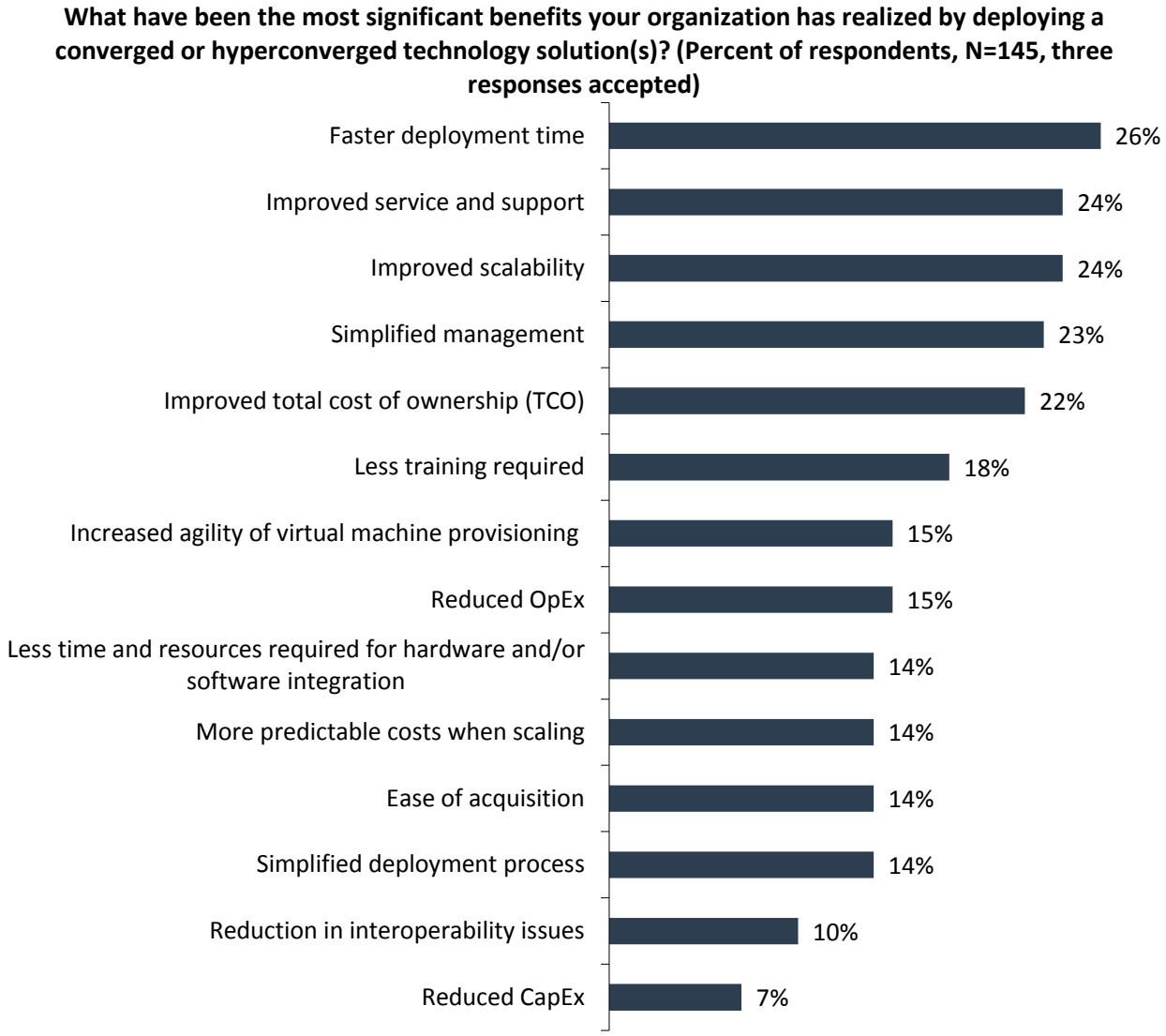
[2] ibid
[3] ibid.

Choice, Cost Savings, and Simplicity

HCI is operationally efficient: It is less complex than traditional types of systems, with less to manage and fewer components involved. HCI offers organizations choice, cost savings, and simplicity with the ability to easily scale with the needs of the business. Perhaps the biggest benefit of HCI is derived from the fact that storage subject matter expertise is not required. The days of carving out volumes, LUNs, and managing Fibre Channel fabrics are gone. HCI is managed within the virtual server context of virtual volumes required to support virtual machines. Essentially this means that IT generalists are well equipped to deal with HCI systems.

A number of organizations that have deployed HCI solutions report wide-ranging benefits. According to ESG research, 22% of organizations reported lower TCO as a primary benefit of deploying a converged or hyperconverged solution. Other benefits reported by respondents included reduced operating costs and IT agility. Additionally, 26% of respondents cited faster time to deploy; 24% respectively cited improved service and support, and improved scalability; and 23% cited simplified management as benefits (see Figure 2).[4]

Figure 2. Most Significant Benefits of Infrastructure Convergence



Source: Enterprise Strategy Group, 2017

[4] Source: ESG Brief, *Convergence Continues to Gain IT Traction*, June 2016.

Hyperconvergence is core to IT transformation and data center modernization exercises. In fact, according to ESG research, among organizations prioritizing data center modernization in 2017, one in four expect to invest in HCI as part of these efforts.[5]

The VMware Approach to HCI Security: vSAN with Native, Software-based Encryption

As the benefits of HCI fuel rapid adoption rates, organizations require a secure, agile, and cost-efficient way to protect their data assets stored on HCI, while being agile enough to scale as needs of the business dictate. Comprising a single integrated platform for storage, compute, and networking, VMware HCI solutions offer organizations a secure, cost-effective means to more easily update and manage their data centers, without sacrificing agility or performance.

VMware vSAN, VMware's software-defined HCI solution, offers native encryption that is both VM- and hardware-agnostic (no specialized SEDs needed) and can be deployed on existing or new storage devices. Native HCI security is provided with encryption built in at the software layer—offering a future-proof platform for hardware, applications, and cloud strategies. With vSAN, this means security is built into the hypervisor level, and not within the VM or hardware. Management is simplified since virtualization allows several applications, as well as operating systems, to run on a single server or "host." Data is managed and secured via policy, regardless of any guest operating systems.

Available for all-flash as well as hybrid configurations, vSAN encryption fits neatly within existing security frameworks. It integrates with industry-standard Key Management Interoperability Protocol (KMIP) 1.1 compliant key management technologies. Keys can be effectively managed using hardware security module (HSM) solutions, which protect and manage digital keys for strong authentication, and enable organizations to meet compliance by employing key management best practices such as the separation of keys and data, key rotation, and maintenance of an audit trail of access.

Why Native Software

Using a native software approach, organizations can enjoy benefits that include:

- Hardware independence. Deploy on any certified hardware, and enjoy freedom to deploy in brownfield environments (i.e., rebuild a project based on an existing one) and greenfield environments (build from the ground up).
- Lower cost. Unlike premium charges for SEDs, native software offers many choices, which leads to greater flexibility in pricing.
- Management. A single key is used for an entire cluster. There are no per-drive PINS or keys to manage and track. Complicated media disposal processes can also be eliminated with encrypted data.

Standalone, vSAN HCI encryption is effective and, combined with the broader VMware portfolio, can further help IT organizations significantly improve their security posture without adding extra labor and resource requirements.

Currently, the VMware Cryptographic Module used by vSAN is pending FIPS 140 certification.[6] vSAN encryption supports 2-factor authentication, including SecurID and Common Access Card (CAC). Additionally, vSAN is at the core of VMware's vSphere server security technical implementation guide (STIG) that defines its best practices.

[5] Source: ESG Research Report, *2017 IT Spending Intentions Survey,* March 2017.
[6] Source: NIST, *Cryptographic Module Validation Program FIPS 140-2 Implementation Under Test List*.

Better Together: VMware End-to-end Security

This paper touches on just one aspect of security—encrypting data at rest. While the VMware vSAN encrypted HCI solution can help IT organizations improve their security posture by protecting data where it is stored, VMware's security investments span the portfolio, assisting IT organizations in securing data at every level of the stack.

Organizations deploying vSAN can ensure that data is encrypted at the storage layer. Networks are secured through microsegmentation, which means access is thoroughly secured via multi-factor authentication, as well as through role-based access controls. Data in use can be secured though encrypted virtual machines (VMs) and Encrypted vSphere vMotion, VMware's solution for live VM migration, performed at the VM level using a one-time key. Additionally, data in the cloud is protected with security policies that extend across hybrid clouds. IT organizations looking to drive agility through cloud adoption and improve their IT security posture across the board would do well to consider the strength of an integrated, secure VMware portfolio that spans on-premises and cloud.

The Bigger Truth

Given the current threat landscape, all IT organizations, and especially those within regulated environments (think banking, financial services, and health care, for starters), must do more to improve their security postures. Security steps must be taken at every layer of the infrastructure. And because protecting data is one of the top goals of IT, it is logical to start with protecting data at the source by using encryption at rest.

Security can be approached in a practical, efficient, and cost-effective manner—and VMware has done just that by layering security into HCI. VMware vSAN adds value to HCI (including server, storage, and security) implementations by further collapsing the stack, enabling IT organizations to drive operational efficiency with integrated systems that also include a secure data layer. Organizations looking for a means to grow a more secure, faster performing, and easy-to-manage data center should explore the possibilities with VMware vSAN.

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

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188