BUILDING SECURITY INTO YOUR DATA CENTER MODERNIZATION STRATEGY

Every organization is exploring how technology can help it disrupt current operating models, enabling it to better serve customers and employees and to gain a competitive edge. IT teams choosing a software-defined data center (SDDC) model—featuring virtualized compute, networking, storage, and management—to accelerate their transformations are quickly discovering a digital foundation that provides the ultimate flexibility in how and where workloads run. At the same time, the SDDC provides an opportunity to create a zero-trust security model with comprehensive application visibility and consistent security controls across clouds. This model fully protects existing and new workloads in ways never before possible.

Threats From Anywhere Demand Security Everywhere

Security threats are growing in number and severity, and when intruders are successful enterprises experience decline in both brand loyalty and financial performance.

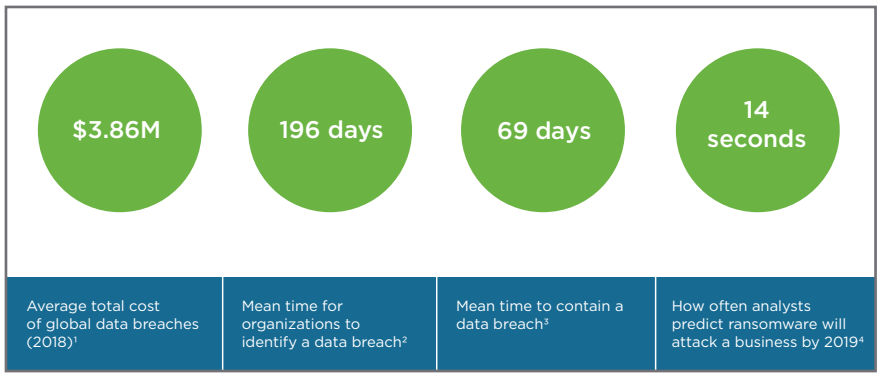

Figure 1. Ignoring security is expensive and time consuming.

With enterprises still searching for better threat protection, detection, and remediation models as regulators push for more risk control, cybercriminals continue to set their sights on new targets. Data centers that are still operating siloed with hardware-based infrastructure and running legacy applications are most vulnerable. Cybercriminals consistently seek weak links that enable them to penetrate perimeters and quickly move malware from server to server, application to application within the environment. There is no quick fix and adding complex security management with point tools can put organizations at greater risk. By ensuring security is built into all of the connected SDDC components, VMware helps enterprises safeguard all of their data and applications onsite and across clouds.

The VMware SDDC architecture provides the highest levels of protection because abstraction across compute, network, storage, and management creates an independent virtualization layer to secure infrastructure. VMware also provides deep visibility into interactions between users and applications, and the context to understand it. VMware's solution helps ensure enterprise IT teams align security to what matters most, the application. Finally, the location of VMware software within the compute platform provides the optimal control point to enforce policy and insert third-party services for additional layers of protection.

Enterprises deploying VMware SDDC architecture have an advantage battling security threats. Protections built into each component—virtualized compute, networking, storage, and management—and extending to hybrid cloud create a zero-trust security model. At the core of safeguarding workloads everywhere is VMware vSphere® Platinum, the purpose-built security solution protecting enterprise applications, infrastructure, data, and access.

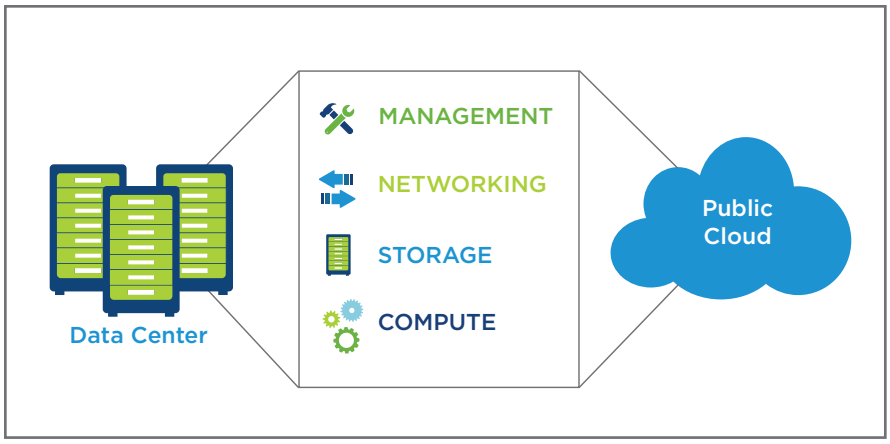

Figure 2. VMware delivers consistent SDDC infrastructure across data centers and clouds.

VMware's Holistic SDDC Security Advantage

A closer look at protections within each component—compute, networking, storage, and management—extending into hybrid cloud illustrates the holistic VMware SDDC architecture security advantage.

Compute: Advanced Infrastructure, Data, Access, and Application Security in the Compute Platform

In the VMware SDDC, software-defined compute establishes a foundation capable of addressing dynamic threats. VMware vSphere Platinum is a purpose-built security solution protecting enterprise applications, infrastructure, data, and access. It delivers key capabilities to reduce security risks:

- The industry-leading, efficient, and secure compute platform for all workloads, providing comprehensive, built-in security for the entire hybrid cloud environment.
- Native integration of VMware AppDefense® into core vSphere to provide visibility into virtual machine (VM) and application behavior with alerts for any deviations from the "known good" state, in addition to embedding threat detection and response into the virtualization layer, and data center endpoint security—all powered by machine learning and behavioral analytics.

Validation and Attestation Safeguards Infrastructure

Protecting workloads of any type, running on-premises and in hybrid clouds begins with securing the digital foundation, which in the VMware SDDC is the compute layer. Secure Boot for ESXi in vSphere Platinum ensures that only VMware and partner-signed code is running in the hypervisor. vSphere Platinum includes support for TPM 2.0 for ESXi hosts. This delivers hypervisor integrity by validating the Secure Boot for ESXi process and enables the ability to do remote host attestation. Secure Boot for Virtual Machines provides Guest OS support for the prevention of image tampering and unauthorized component loading.

vSphere Platinum includes role-based access controls, enhancing security by giving IT control over authorization of what can and can't be accessed. The solution also features support for Microsoft Virtualization-based Security (VBS), including Credential Guard for enterprises running Windows 10 and Windows Server 2016 security features on vSphere. Virtual TPM 2.0 allows for the introduction of in-guest security solutions while IT maintains full operational support for technologies such as VMware vSphere® vMotion® and VMware vSphere® Distributed Resource Scheduler™ (DRS).

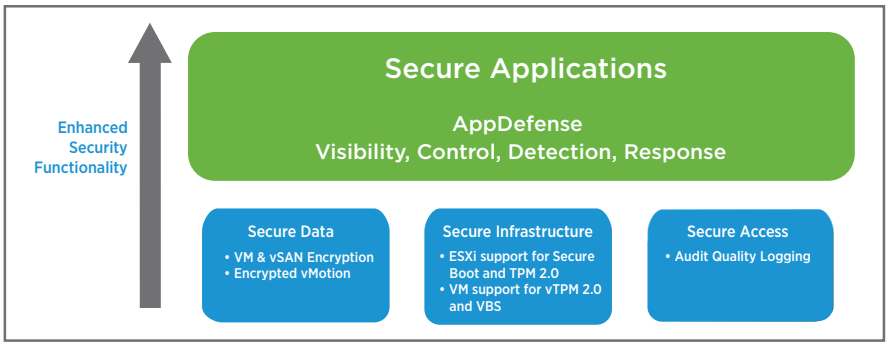

Figure 3. vSphere Platinum secures infrastructure, data, applications, and access.

Encryption Secures Data

Within the infrastructure, vSphere Platinum protects against unauthorized data access from the core to the cloud when data is in motion and at rest. It features FIPS 140-2 Validated cryptography that enables VM Encryption and Encrypted vMotion to provide easy-to-manage encryption with less hassle than legacy solutions.

VM Encryption introduces encryption solutions for every workload type and protects VMs against unauthorized data access. Encrypted vMotion ensures the secure live migration of running VMs from one physical server to another with zero downtime, ensuring continuous service availability and complete transaction integrity with no modification to existing network infrastructure.

Purpose-Built VMs Protect Applications

vSphere Platinum starts with protecting VMs at the infrastructure level and then extends its protection, via AppDefense, to the application level. It does so by ensuring "known good" behaviors rather than relying on updates of "known bad" behaviors. This approach addresses zero-day threats for which there is no known signature of bad behaviors.

Embedded machine learning helps vSphere Platinum secure infrastructure and applications in a way that is operationally simple with minimal overhead and impact on performance. Administrators easily address in-guest threats and eliminate risks by delivering secure infrastructure and applications with VMs running in their "known good" states. Ensuring good is possible because AppDefense understands an application's intended state and behavior and monitors it for changes. Any change from a "known good" state signals a threat for which a number of automatic remediation actions are available. VMs continue to run optimally without burdening administrators to detect threats that may not fit a known signature. Known-good state VMs, in turn, support robust micro-segmentation in the VMware SDDC networking layer.

Greater Visibility Limits Access

Because users can inadvertently cause harm to organizational security postures, vSphere Platinum's audit quality logging capability promotes authorized administration and control through high-fidelity visibility into user activity. It maximizes the efficiency and effectiveness of virtualization and security operations while streamlining the application security readiness review process. Easy to use and install, vSphere Platinum simplifies workflows and boosts collaboration among vSphere administrators and security, compliance, and application teams while streamlining security incident response and remediation.

Network: Advanced Traffic, App, and Data Protection

A software-defined network as part of the VMware SDDC maximizes IT security and agility. Organizations trust VMware NSX® to automate network and security provisioning so that as new compute resources are created, they are secured by default. Using policy-based security automation and micro-segmentation, IT teams prevent intrusion and secure network traffic inside enterprise environments, such that malware cannot move laterally.

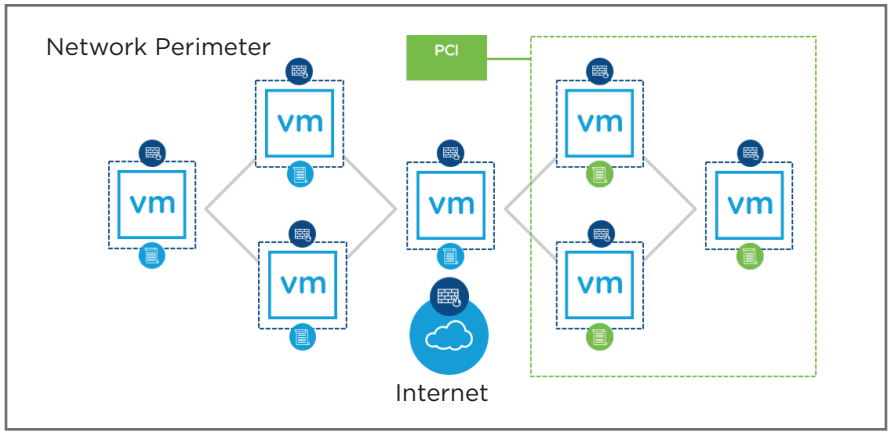

Figure 4. VMware NSX enables security through micro-segmentation.

Micro-segmentation limits a threat's ability to propagate across the environment by enforcing network security policies at the most granular level of an application, the individual data center endpoint. Organizations then segment workloads residing on the same physical host without hair-pinning traffic out through an external physical or virtual firewall. With VMware NSX, IT organizations enforce a least-privilege model, limiting access by user or role and preventing system components from interacting unnecessarily.

Storage: Hyperconverged Infrastructure and Encryption for Data Safety

Software-defined storage, standalone or as part of hyper-converged infrastructure (HCI) in the VMware SDDC, extends security built into the foundation. VMware vSAN™ helps IT organizations evolve to flash-optimized shared storage across virtualized workloads. Native integration with vSphere removes dependency on external shared storage appliances, offering a secure and consistent operating environment every day.

VMware vSAN is the first HCI solution to offer native, software-based FIPS 140-2 Validated data-at-rest encryption. vSAN Encryption provides data-at-rest security at the cluster level and offers simple key management with support for KMIP-compliant key managers. It meets rigorous enterprise and government agency compliance requirements while supporting choice of standard drives (SSDs and HDDs) and avoiding the limited options, configuration challenges, and pricing premium of self-encrypting drives (SEDs).

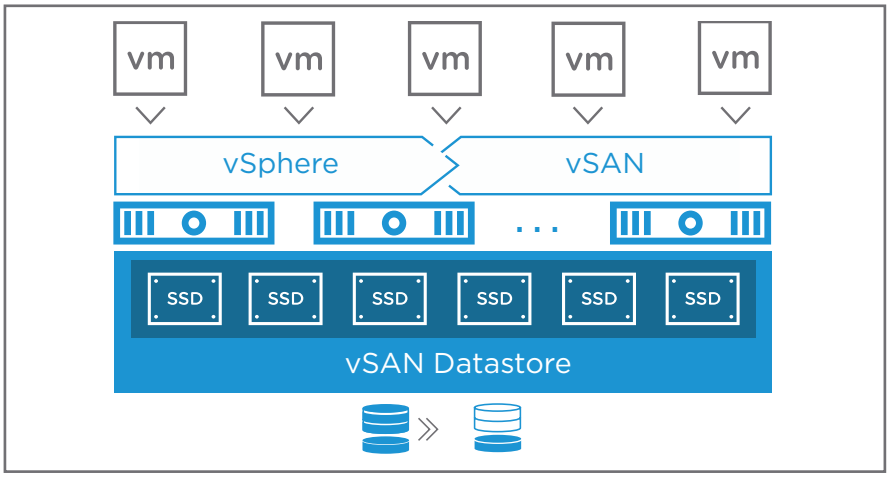

Figure 5. VMware vSAN Encryption provides data-at-rest security.

Unlike other software-defined storage solutions, vSAN features security, as well as cost and agility benefits. vSAN is built into the vSphere kernel. This tight integration optimizes the data I/O path and provides the highest levels of performance with minimal impact on CPU and memory.

Data Center Management: Policy-Based Protection

The VMware modern SDDC consolidates, standardizes, and automates operations as it breaks down silos and reduces risk. It uniquely delivers secure, consistent infrastructure and VM-centric operations—all managed by VMware vRealize® Suite, the enterprise-ready cloud management platform purpose-built for the hybrid cloud. vRealize Suite reduces risk by ensuring hardening for vSphere and all VMware SDDC components. It includes intelligent operations such as Smart Alerts and predictive analytics to proactively identify and solve emerging operational and security issues before they negatively impact user experiences. vRealize Suite empowers consistent deployment models, security policies, visibility, and governance for all applications—whether they are running in an on-premises SDDC, in VMware Cloud™ on AWS, in other public clouds, or in any combination of those.

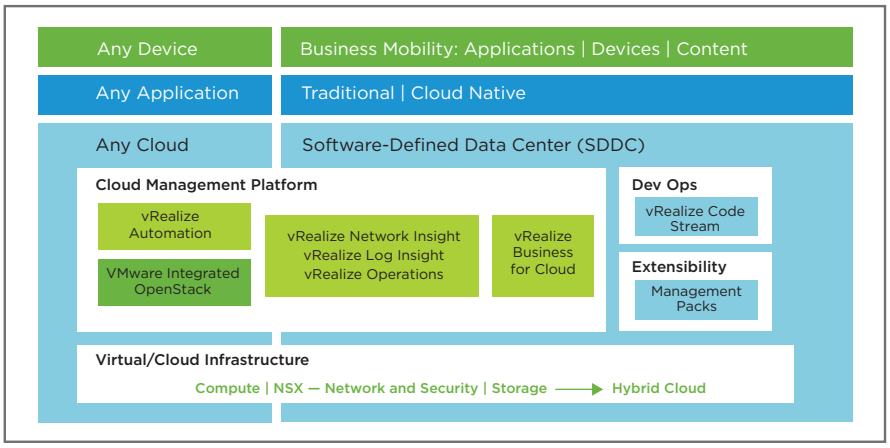

Figure 6. vRealize Suite delivers intelligent operations and consistent policy-based security.

Hybrid Cloud: Extending Security Off-Site

VMware Cloud on AWS takes the benefits of the VMware SDDC to the hybrid cloud. As more products and services move online, opportunities increase for cybercriminals. Successful businesses protect distributed modern applications by ensuring dynamic security is an intrinsic feature of the infrastructure across both private and public clouds.

vSphere and VMware Cloud on AWS deliver a consistent and intrinsic security architecture from the data center to the cloud. VMware Cloud on AWS provides a robust and hardened cloud infrastructure with rich security features built in. From an operations standpoint, VMware protects the information systems used to deliver VMware Cloud on AWS. The service is also monitored for security events involving the underlying servers, storage, networks, and information systems used in the delivery of this service. Moreover, VMware performs routine vulnerability scans to surface critical risk areas and addresses them in a timely manner. Security configurations and operational procedures have been audited, resulting in VMware Cloud on AWS obtaining industry certifications, such as SOC and ISO.

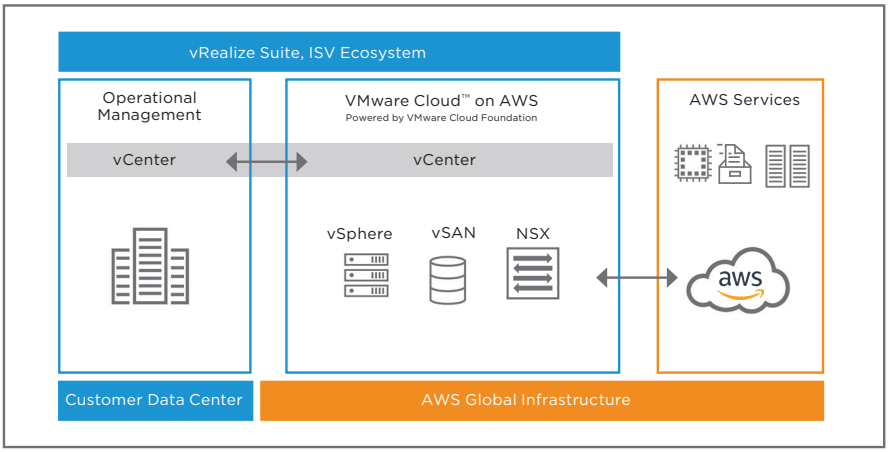

Figure 7. vSphere and VMware Cloud on AWS deliver a consistent and intrinsic security architecture from the data center to the cloud.

Take Your Security to the Next Level with the VMware SDDC; Start with vSphere Platinum

The VMware SDDC features a comprehensive, zero-trust security approach that addresses enterprises' most stringent protection requirements without sacrificing agility.

As the ideal, efficient, secure universal platform for hybrid cloud supporting new and existing applications as well as serving the needs of IT and the business, vSphere reinforces enterprise investment in VMware. It is a core component of the VMware SDDC and a fundamental building block of cloud strategy. With vSphere, enterprises can run, manage, connect, and secure their applications in a common operating environment, across hybrid cloud.

Figure 8. Comprehensive built-in security for your data center with vSphere Platinum.

By building security into the core compute platform instead of as a bolted-on afterthought, VMware ensures threats from anywhere are met by security everywhere. vSphere Platinum, the foundation of the VMware SDDC, mitigates risks with purpose-built safeguards across the entire IT environment so enterprise IT teams can focus more on the innovation that drives competitive advantage.

Discover vSphere Platinum.

1-3 Ponemon Institute. "2018 Cost of a Data Breach Study," July 2018.

4 Cybersecurity Ventures. "Global Ransomware Damage Costs Predicted to Exceed $5 Billion in 2017," May 18, 2017.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com