Technical White Paper: **2023**

Addressing Key Security Concerns When Modernizing Data Center Infrastructure

vmware®

Table of contents

Addressing key security concerns when modernizing data center infrastructure

It is imperative that modern enterprises defend themselves against the staggering scale of cybersecurity threats. Any organization that is modernizing its cloud infrastructure views this as an opportunity to review security strategies and make adjustments to ensure alignment to corporate security mandates.

Cyberattacks threaten data centers by compromising sensitive information stored on these servers and disrupting critical business operations. Enterprises often store large amounts of confidential financial, personal and business data that can be accessed by unauthorized individuals and exploited for financial gain or to harm the organization. There are dozens of attack categories—from data breaches and theft of intellectual property, to extortion and ransomware. Ransomware is, by far, the most widely known. When an attacker denies access to things like fuel, food and health care services at a national level, it gets attention from governments, customers and shareholders alike.

Additionally, data centers often serve as a hub for an organization's IT infrastructure, and a successful attack on a data center can cause widespread operational disruption. This can result in lost productivity, revenue and damage to the organization's reputation.

Figure 1: Securing workloads is a matter of process, tools and strategy.

Cyberattacks are not just a threat to a company's infrastructure, but also to its cash flow management. The impact on both capital expenditure (CapEx) and operating expenditure (OpEx) can be significant when trying to mitigate potential threats, especially when these efforts are not part of an over-arching security strategy.

On the CapEx side, an organization may need to invest in new security technologies or equipment to mitigate the risks of future attacks and to comply with regulatory requirements. This can include firewalls, intrusion detection/prevention systems, encryption and other security tools. These directives can incur additional unplanned expenses when they are not executed as part of a budgeted exercise and a continuous proactive stance.

On the OpEx side, it may be necessary to increase IT and security staff to manage and maintain the new security technologies, and to train other employees in breach detection and response. The organization may also need to divert funds to incident response and forensic investigation in case of an attack, increasing their overall operating expenditure.

Cyber threat awareness is vital for an efficient security strategy

Not all cyberattacks are built the same way or have the same purpose. IT leaders and security architects need to be aware of the range in attacks, modus operandi and risk factor when designing an efficient security strategy. It's important to note that this is not an exhaustive list of all types of cybersecurity attacks, with new types of attacks constantly being developed. Therefore, it's important for organizations to have a comprehensive security strategy in place to detect and respond to security incidents in a timely manner.

The most common types of cyberattacks in today's landscape

Distributed Denial of Service (DDoS)
These attacks flood a data center's network with a large amount of traffic, overwhelming the network and rendering it unavailable to legitimate users.

Phishing
Attacks that use email or other forms of communication to trick users into providing an attacker with sensitive information, such as login credentials.

Ransomware
Attacks that encrypt the data on a data center's servers and demand payment from the organization in exchange for the decryption key.

Advanced Persistent Threats (APT)
Targeted attacks that are designed to gain access to a data center's network and steal sensitive information over an extended time period.

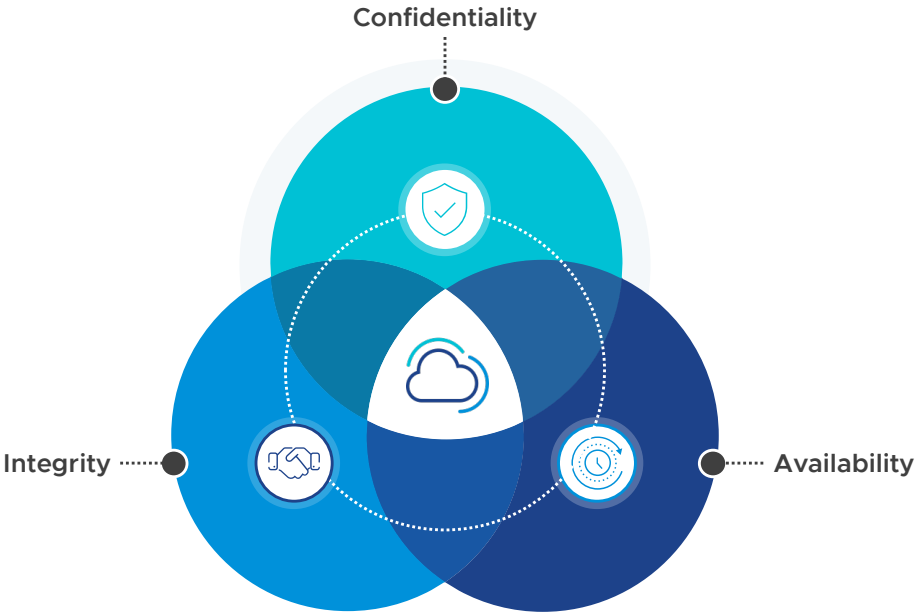
Malware
Malicious software that gains access to a data center's network, steals sensitive information or disrupts operations.

Cloud attacks
These attacks target the vulnerabilities in cloud infrastructure that can lead to unauthorized access, data breaches and other malicious activities.

IoT attacks
These attacks target vulnerabilities in Internet of Things (IoT) devices, such as security cameras and temperature sensors, that are connected to a data center's network.

Insider attacks
These attacks are conducted by an employee, contractor or other trusted user who has access to the data center's network.

What to look for when designing a future-proof security architecture



A good way to illustrate the required depth of security inside the platforms is to look through the lens of information security's three core tenets: confidentiality, availability and integrity.

1. **Data confidentiality** refers to the protection of sensitive information from being accessed or disclosed to unauthorized individuals or systems. Data confidentiality is important for organizations because sensitive information can be used for financial gain or to harm the organization if it is accessed or stolen by unauthorized individuals.

2. **Data integrity** refers to the accuracy and completeness of data and the assurance that data has not been tampered with, altered or destroyed in an unauthorized manner.Data integrity is important because it ensures that the data being used by an organization is accurate, reliable and can be trusted. Inaccurate or tampered data can lead to incorrect decisions, financial loss and damage to the organization's reputation.

3. **Data availability** refers to the ability of authorized individuals or systems to access data when they need it. Data availability is important for organizations because without access to data, business processes can be interrupted, leading to lost productivity, lost revenue and damage to the organization's reputation. It also is essential for continuity of operations, compliance with regulations and customer satisfaction.

Every infrastructure security feature can be mapped to one or more of these tenets. For example, encryption and data masking are data confidentiality features, while data integrity and hashing are part of the data integrity tenet.

That makes every single feature a security feature that is designed to help organizations reduce and eliminate risk. This is extremely powerful, and why security-conscious organizations choose VMware platforms.

Addressing key security strategy concerns

When planning a cloud infrastructure modernization program, it is critical that infrastructure and operations leaders understand and address key security requirements to protect the organization against attacks and establish an agile architecture to thwart future attacks.

Visibility and observability

Security starts with visibility. Enterprises cannot protect what they cannot see. However, simple visibility isn't sufficient. Observability is intelligent, contextual visibility. Complex modern infrastructures and applications make answering questions about what happened, who was affected and how it can be fixed more difficult than ever. Observability systems enable you to inspect and understand the application stack.

Observability is a key element in the end-to-end protection story. It goes beyond that ability to see and can bring contextual information to the user about what is going on in a dynamic system like today's software-defined data centers.

Visibility implies understanding what process assets are being utilized, by whom, for what reason and at what dimension of interest. System administrators can learn a lot about the infrastructure by looking at it from all aspects from within. While this might seem like an obvious requirement, it often gets forgotten in the policies and outdated processes of different enterprises. It is important to visualize and gain deep insights into all flows across the entire data center with stateful Layer 7 inspection and complete workload context, thereby eliminating security blind spots and accelerating incident remediation.

Policy-based security implementation

In software-defined infrastructures, policy-based security management or architecture is an ideal way to dynamically define and control the interaction between services and applications. Policy-based security management enables intelligent security capabilities and enhances fine-grained control over end-user behavior.

However, dynamic variations in network, rapid increases in security attacks, geographical distribution of nodes, and complex heterogeneous networks can have serious effects on the performance of policies. The more intelligent the policy definition, the more likely it is to withstand evolutions in security breaches. Therefore, as soon as IT leaders understand the flow of infrastructure applications, engineers can define a better way to protect applications and core assets. Introducing a system that requires as little human intervention as possible means it becomes more flexible, more scalable and less error-prone.

Ensuring policy execution

Security policies play an important part in the overall enterprise security model. However, in many organizations the challenges are split in three parts:

1. The challenge of understanding the scope of the policy (which we tackle with observability)
2. The challenge of defining a comprehensible security policy that takes everything into account
3. The challenge of initial implementation and execution

Organizations should ensure that there are robust processes supporting security policy requirements. Automation and intelligent systems, such as those provided by VMware NSX® or the Advance Threat Analyzer product, help execute these processes consistently and more reliably than human intervention, which has a higher probability of execution failure.

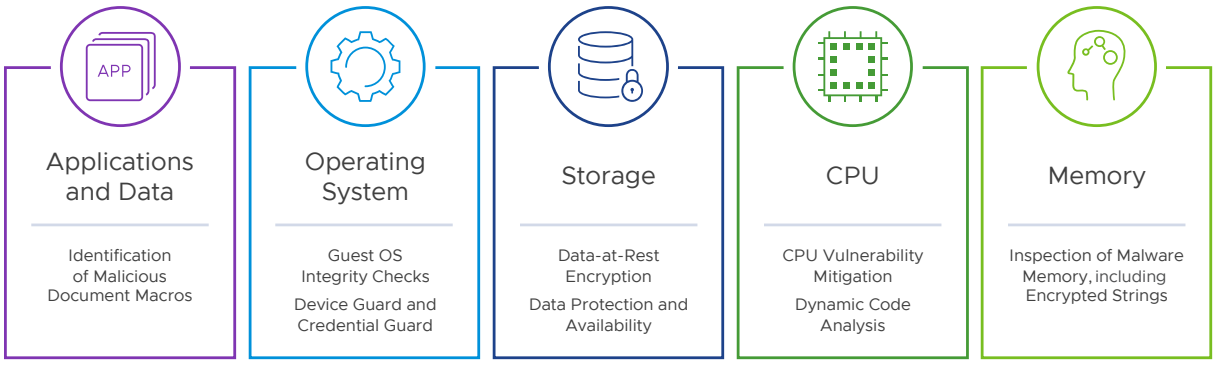
Implementing modern security architectures with VMware Cloud Foundation

Security in VMware Cloud Foundation™ (VCF) is more than just virtualized routers and switches.

Network and security services are programmatically distributed to each virtual machine, independent of the underlying network hardware or topology, so workloads can be dynamically added or moved and all the network and security services attached to the virtual machine move with it, anywhere in the data center.

Using NSX, VCF reproduces the entire networking stack in software within each virtual network. It offers a distributed logical architecture for L2-7 services, including logical switch, router, firewall, load balancer and VPN.

Security in VMware Cloud — more than just firewalling



On top of classic networking services, engineers can leverage deep security features:

At the application layer:
Identification of malicious document macros.

At the operating system layer:
Operating systems are running everywhere, so you want to make sure they are as secure as possible. That means not just relying on machine-level firewalling, but also relying on your infrastructure to protect against attacks.

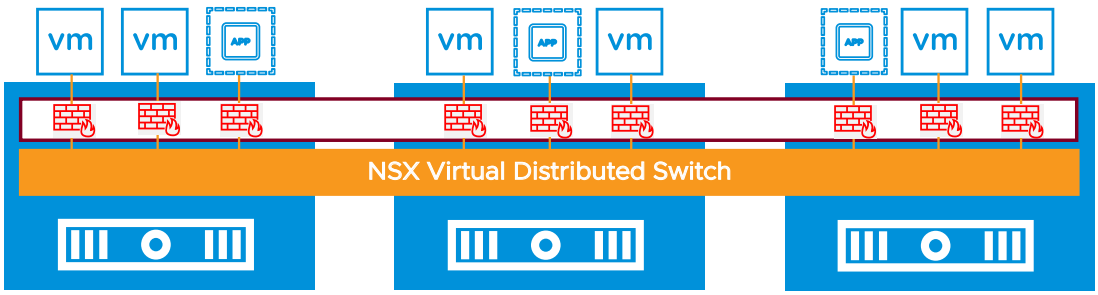
At the storage layer:
VMware Cloud Foundation leverages VMware vSAN™ to store customer data and, in the process of storing it, also secure and encrypt it, thereby making sure that enhanced data protection policies are consistently updated for today's threats.

At the hardware layer:
VMware Cloud Foundation can help with issues in hardware, too. Not only are there options for dynamic code analysis in workloads, but also options for smoothly handing issues like CPU vulnerabilities, offering choice so that an organization can match its response to its business requirements.

Memory:
VMware Cloud Foundation NSX Advanced Threat Analyzer finds malware processes and snippets of malware trying to hide in memory and immediately takes action to protect infrastructures.

Next-generation firewalling in VMware Cloud Foundation

Perimeter firewalling, also known as network firewalling, is a traditional security measure that is used to control the flow of network traffic between internal and external networks. While perimeter firewalls can provide a valuable layer of security, they also have certain limitations: from limited visibility into internal network traffic, to limited protection against advanced threats to limited protection for mobile and remote users.



The Distributed Firewall (DFW) is a stateful firewall, meaning it monitors the state of active connections and uses this information to determine which network packets to allow through the firewall. DFW is implemented in the hypervisor and applied to virtual machines on a per-vNIC basis. That is, the firewall rules are enforced at the vNIC of each virtual machine. Inspection of traffic happens at the vNIC of a VM just as the traffic is about to exit the VM and enter the virtual switch (egress). Inspection also happens at the vNIC just as the traffic leaves the switch but before entering the VM (ingress).

Each VM has its own firewall policy rules and context. During vMotion, when VMs move from one ESXi host to another host, the DFW context (Rules table, Connection Tracker table) moves with the VM. In addition, all active connections remain intact during vMotion. In other words, DFW security policy is independent of VM location.

Conclusions

Security is an important aspect of data center modernization that helps protect an organization's valuable data and applications from cyber attacks. To protect sensitive data, is important to implement robust security measures such as network segmentation, firewalls, intrusion detection and prevention systems, and encryption. Modernizing overall data center infrastructure enables better security, and a more granular approach to threat prevention.

- **Leveraging a Software-Defined Data Center (SDDC) architecture** such as VMware Cloud Foundation allows for the automation and orchestration of infrastructure and security. This makes it easier to apply and enforce security policies consistently across the entire data center, and to quickly respond to security incidents.
- **Implementing network virtualization** such as VMware NSX, as part of VMware Cloud Foundation, allows for the creation of multiple virtual networks within a single physical network. This allows for granular network traffic control and enables micro-segmentation, which helps to reduce the attack surface and isolate different workloads and applications from one another, making it harder for attackers to move laterally through the network.
- **Deploying improved threat analysis** by leveraging tools such as Advanced Threat Protection can provide organizations with additional visibility and insight into security threats, as well as the ability to respond to them more quickly and effectively.
- **Automation and orchestration** enable rapid identification and response to security incidents, using security tools that can detect and respond automatically to security threats.
- **Improving compliance:** Data center modernization and security optimization can help organizations comply with various regulatory and compliance requirements, such as HIPAA, PCI-DSS and SOC 2, by providing a secure and compliant infrastructure.

Deploying VMware Cloud Foundation integrates all of these modern technologies and security features within a data center modernization platform that is secure, compliant and agile.

Item No: Addressing Key Security Concerns in the Modern Enterprise Data Center 2/23