Designing Infrastructure to Defeat Ransomware

With VMware Infrastructure & Security Products

Table of Contents

Introduction 3

Disclaimer 3

What is Ransomware? 3

What is Zero Trust? 4

Information Security Concepts 5

Implementation Introduction 7

- Consolidated Management & Workload Cluster 7
- Separated Management & Workload Clusters 8

Implementation Overview 9

- Infrastructure Management & Workload Separation 9
- Workload Network Isolation & Microsegmentation 9

Design Decisions 10

- Isolation, VLANs, and Separate Network Segments 10
- Perimeter Controls & Monitoring 11
- Storage Fabric Isolation 11
- Microsegmentation & Overlays 11
- Network Failover Techniques 12
- Trusted Platform Modules 12
- Authentication & Authorization 13
- System Dependencies & Placement 14
- Domain Name System (DNS) 14
- Network Time Protocol (NTP) 14
- Key Management Systems & Key Providers 14

Product Applicability 15

Conclusion 17

About the Authors 17

Introduction

In early 2022 a group of folks at VMware set out to install VMware vSphere. This time, though, our goal was a little different: configure the environment to deter attackers using all of the current best practices, keeping ransomware and zero trust in mind. The past few years have seen a massive rise in attacks, and as the industry has changed to cope, the tactics of the attackers have evolved, too. As organizations leaned into their backup and disaster recovery solutions to recover quickly from ransomware, attackers pivoted from ransom demands to focus more on intellectual property theft and extortion, often extorting both the victim and the victim's customers.

The answer to ransomware is not as simple as a backup solution, though. A proper defense requires both new tools and techniques as well as a return to security basics. Furthermore, the answer to ransomware also depends on where you are in the "stack." Tools and tactics to protect workloads are often different than the tools and tactics available for a storage array, firewall, and vSphere itself. That is what this effort is about, demonstrating good practices for building and protecting vSphere, aligned with current product guidance from both VMware and from the industry as a whole.

We also intend to document the processes of our design decisions. Most security guidance represents itself as the authoritative way to achieve a goal. This does the reader a disservice, though, because the reality of many decisions is much less clear. Security is always a tradeoff, and security always depends on context. A good example of this is authentication. Tying cloud infrastructure to centralized authentication can help an organization manage and monitor logins and privileges. However, tying cloud infrastructure to centralized authentication may also make it more susceptible to lateral movement by attackers. Why would you choose one way over another? Why did we choose the method we did? Exposing our thought processes for these types of decisions helps administrators better understand the choices available to them and help them make great decisions to secure their environments.

Disclaimer

This set of documents is intended to provide general guidance for organizations that are considering VMware solutions to help them address security and compliance requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided "AS IS." VMware makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of security and regulatory compliance requirements.

What is Ransomware?

Ransomware is a type of malware that denies access to a user's or organization's data, usually by encrypting the data with a cryptographic key known only to the hacker who deployed the malware. Ransomware is not a thing that can be patched for or defended against in a single way. It is a multifaceted attack by an entire ecosystem of clever and smart people. These criminals patiently invade and take over an organization's electronic assets with the intention of holding them hostage for money, stealing intellectual property, and extorting the primary victim AND that victim's customers.

Malware commonly enters through malicious downloads, email links, malicious advertisements, phishing attacks, social network messages, and websites. It also can enter through unpatched vulnerabilities and weaknesses in public-facing software and services. Once the malicious content has been executed the attackers gain a foothold into the organization from that endpoint and that user account, both compromised. The attackers "establish persistence" and "move laterally" to attack other targets from inside the organizational network's perimeter security defenses.

Ransomware itself is the end process of a breach. Once ransomware is deployed on systems to encrypt files the victim will be sure to notice! Ransomware itself blocks user access until requests for payments, which are often displayed in warning messages, are fulfilled. The ransom note usually threatens permanently losing access to their data, and publicly releasing intellectual property or embarrassing content. Before the encryption of files and systems these criminal enterprises also exfiltrate and steal data from their victims, to sell directly, and to extort the victim's customers, too. This "double extortion" threatens to publicly expose confidential details of the victim's customers unless another fee is paid. This type of threat is particularly effective against organizations whose customers have sensitive or confidential data, such as law firms, accounting firms, and so on.

Unfortunately, there is no guarantee that the cryptographic keys needed to break the encryption will be provided upon payment, or the decryption process will work correctly or promptly. Nor is there any guarantee that, if paid, they will not steal data or further extort the victims or the victims' customers. These are criminals and criminal enterprises, after all.

Ransomware targets all organizations, including for-profit companies, nonprofits, governmental agencies, health care services, and educational institutions of all size. While these criminal enterprises use various "strains" of ransomware, they have common attack vectors for compromise, such as brute force attempts at public-facing services including RDP, the exploitation of outdated public-facing web software, and known vulnerabilities that may have not been remediated. Defending against ransomware is a holistic effort, involving people, process, and technology to detect and contain attacks before they cause major harm and disruptions.

What is Zero Trust?

In the simplest terms, Zero Trust means "trust no device and trust no user." Access is constantly re-evaluated for every user and system, and all devices and user identities undergo continuous multifactor verification. Infrastructure services are often different, though, because they must run and connect to each other when no other services are available. Infrastructure software like VMware vSphere relies on features like Secure Boot, Trusted Platform Modules, VIB signing and verification, host attestation, and more, in order to build assurances in infrastructure that they can be trusted in their current configurations.

Zero Trust techniques can be applied to administration of infrastructure, though. Though grim, organizations need to assume that both a desktop and a user account is compromised. Organizations that adopt those assumptions have better mindsets for secure system design, rooted in Zero Trust, and are better able to detect and contain breaches when they occur.

Information Security Concepts

An understanding of information security concepts enables efficient communication within organizations, promotes understanding among different groups within an organization, and improves system design by highlighting areas of consideration.

Authentication

The ability to prove that a person or application is genuine, verifying the identity of that person or application. Authentication uses one or more of three primary methods, or factors: what you know, what you are, and what you have.

"What you know" encompasses passwords, personal identification numbers (PINs), passphrases, and other secrets. This type of authentication is not strong on its own and is typically paired with another authentication factor.

"What you are" involves biometric authentication methods, such as retinal scans, fingerprints, voice or signature recognition, and so on. These factors cannot be easily changed if compromised.

"What you have" entails objects or applications running on objects that you physically possess. Traditionally this involved keys, but modern forms may also involve USB tokens, smart cards, and one-time password applications on devices. This factor requires possession of the object at the time of use and may be hindered by intentional or unintentional loss of, or damage to, the object.

Multi-Factor Authentication is a method that uses authentication techniques from more than one factor. For example, combining a password with a one-time password application, or a facial scan with a PIN. This approach helps mitigate weaknesses in the use of each factor. Use of two techniques from the same factor, such as two passwords or two physical keys, is not considered multi-factor.

Authorization

The act of determining whether a user or application has the right to conduct particular activities in a system, relying on authentication to prove the identification of the user or application.

Availability

Ensuring that data is available to authorized parties when needed.

CIA Triad

An abbreviation for the core tenets of information security: confidentiality, integrity, and availability.

Compensating Control

Security and privacy controls implemented as an alternate solution to a requirement that is not workable for an organization to implement in its original form. The sum of the compensating controls must meet the intent and requirements of the original security control.

Confidentiality

Ensuring that data is protected from access by unauthorized parties.

Data Breach

An incident where data is accessed, copied, transmitted, viewed, or stolen by an unauthorized party. This term does not indicate intent; other terms such as "data leak" and "information leakage" help convey whether a data breach was intentional or not.

Defense-in-Depth

According to the US National Institute of Standards and Technology, defense-in-depth is "the application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another.”

Identification

The ability to uniquely prove who a user of a system or application is, to enforce access control and establish accountability.

Incident

The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations. Note that this is not limited to people, nor does it indicate intent; natural phenomena, disasters, and animals can also cause incidents, for example.

Integrity

Ensuring that data is protected against unauthorized modification.

Lateral Movement

A method of describing the techniques used by attackers, after breaching an endpoint or system, to “pivot” and extend access to other systems and applications in their target organization. This moves the attacker closer to their goals, such as accessing, changing, exfiltrating, or destroying sensitive information.

Least Privilege

Only assigning the minimum access rights that are necessary for staff or systems to perform their authorized tasks, for the minimum duration necessary.

Non-repudiation

The ability to associate messages, actions, and/or authentications with an individual in a way that cannot be denied by that individual.

Recovery Point Objective (RPO)

The largest amount of data that is acceptable to lose after recovering from an incident. This is measured in time, e.g. “one hour of customer data.”

Recovery Time Objective (RTO)

The largest amount of time that is acceptable for data to be unavailable due to an incident.

Security Control

A safeguard or countermeasure designed to protect the confidentiality, integrity, and availability of data.

Separation of Duties

Dividing critical functions among different staff to help ensure that no individual has enough information or access to conduct fraud.

Vulnerability

A weakness in an information security system, system security procedures, security controls, or implementations that could be exploited by a threat actor.

Implementation Introduction

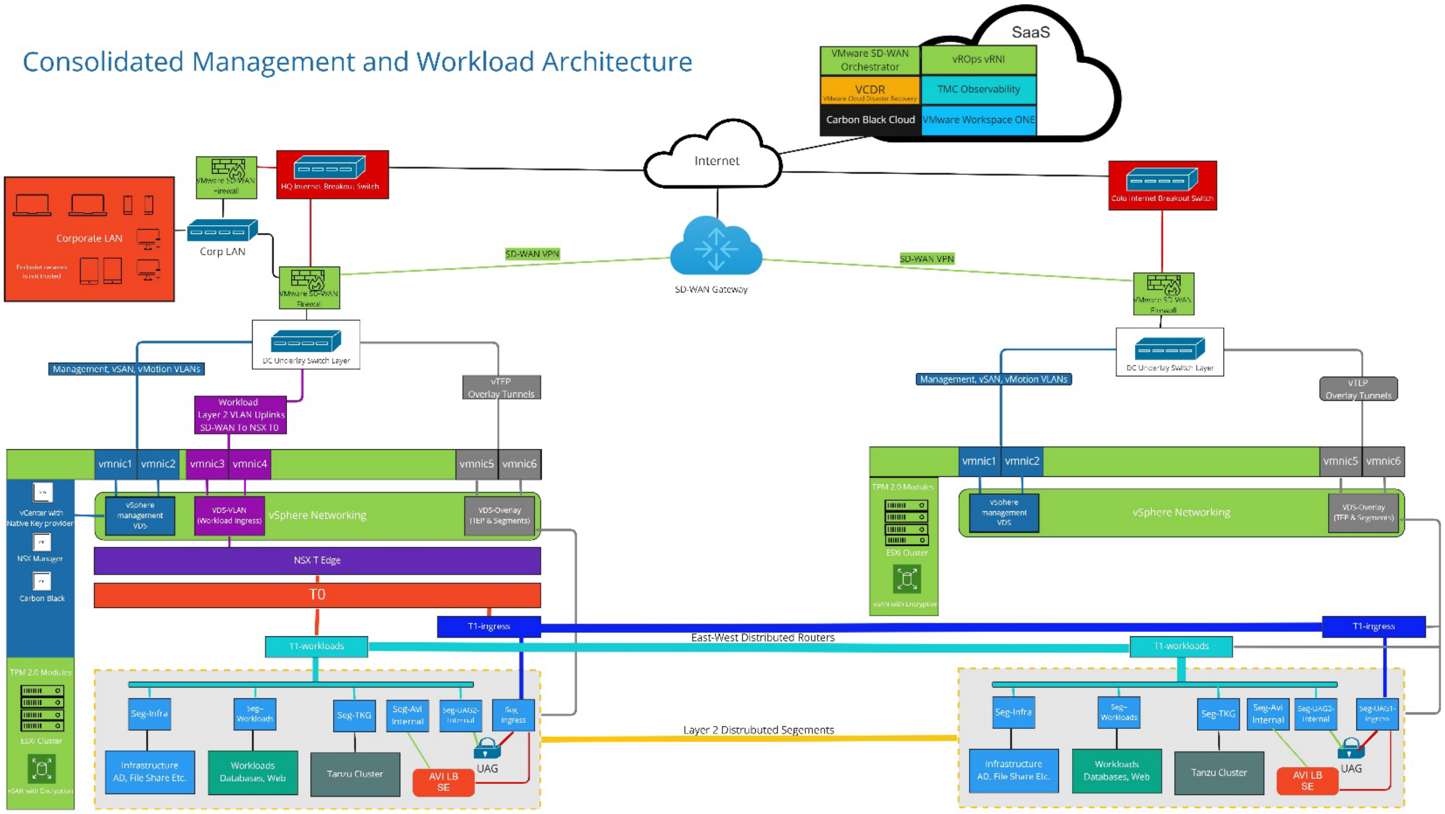


Figure 1

Consolidated Management & Workload Cluster

Figure 1 depicts a system design where the management systems ("control plane") of the cluster share the same underlying infrastructure. For example, vCenter Server, NSX Manager, and NSX Edges coexist in the cluster with workloads and share the same physical hardware, NICs, and so on.

Physical isolation is not possible in this scenario, but logical isolation is created and maintained using the isolation capabilities of VMware ESXi, as well as strict network policies and overlay networks through VMware NSX. This style of cluster deployment is common for smaller environments where a dedicated management cluster and infrastructure may be too much overhead. However, it does have implications for ransomware and other attack scenarios, with more opportunities for attackers to move laterally due to the consolidation.

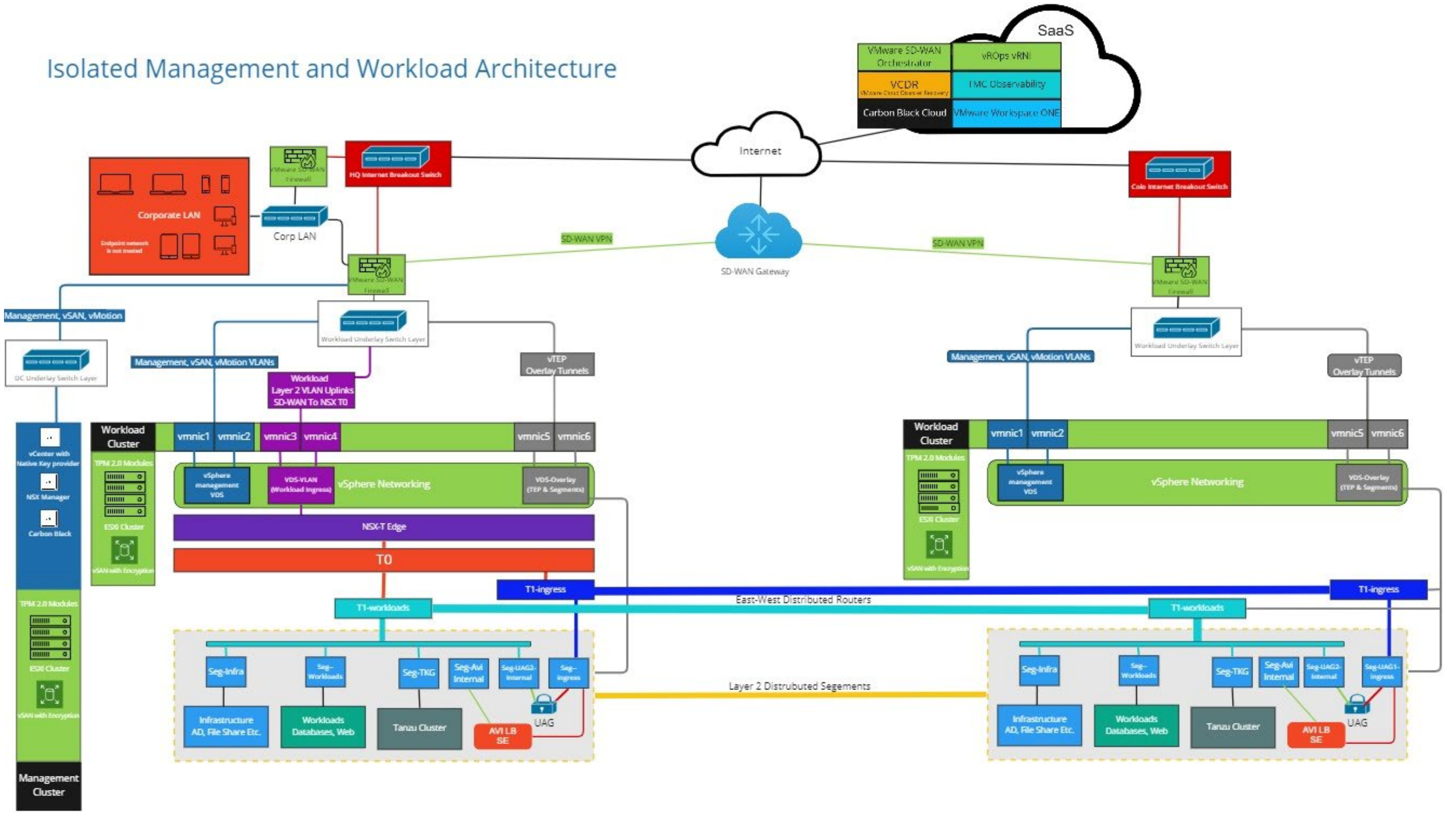


Figure 2

Separated Management & Workload Clusters

Figure 2 depicts a system design where the management systems ("control plane") of the cluster are separated both physically and logically from the workloads they manage. vCenter Server, NSX Manager, NSX Edges, and so on are part of a separate vSphere cluster dedicated to management functions. This style of cluster deployment is how VMware Cloud Foundation is deployed, with a "management domain" serving one or more "workload domains."

Physical isolation is present in this design, added to the logical isolation provided by ESXi and NSX. The management domain can be secured separately, helping to further limit opportunities for attackers, as well as supplying opportunities for attackers to expose themselves to monitoring systems as they attempt to move laterally. This model may also have positive implications for regulatory compliance, as individual workload clusters can adhere to separate regulatory compliance guidelines, with the capital and operational expenditures of a highly secured control plane amortized across all workload clusters.

Implementation Overview

These system designs rely on design decisions which we discuss further in this paper. They are all focused on defense-in-depth, which is the layering of security controls to ensure continued coverage if one is degraded or lost, and reflect the realities of how organizations are being compromised:

- Phishing and social engineering attacks resulting in the compromise of a desktop.
- Compromised credentials, stemming from a pivot of the attackers from the compromised desktop to attacks on centralized identity management infrastructure.
- Insider threats and lax practices around fundamental security concepts such as least privilege.
- Configuration mistakes that may provide opportunities to attackers.
- Software vulnerabilities and other mechanisms that permit lateral movement, even inside a trusted environment.

Working to demonstrate how to minimize these paths for attackers is a primary goal of this effort.

Separation of Infrastructure Management & Workloads

One of the primary features of these designs, as seen in these diagrams, is that management network traffic is isolated from workload traffic using NSX segments that have separate routes to the VMware SD-WAN firewall appliance. Management traffic uses a separate subnet VLAN and gateway on the SD-WAN appliance to enter the datacenter and workload traffic ingress is over a layer 2 only VLAN.

The datacenter underlay switch only routes management traffic inside the datacenter and keeps workload traffic isolated on the layer 2 VLAN that only passes traffic from the SD-WAN appliance gateway to the NSX Tier 0 router gateway. The SD-WAN firewall and NSX Tier 0 router do not have any layer 3 awareness of the datacenter switch fabric. This keeps all policies for management and workload traffic isolated at the firewall level. No shared routing tables exist inside of the direct datacenter fabric between the workload and management traffic.

This significantly reduces the ability of lateral movement of an attack on the control plane that manages workloads, as well as providing options for managing dependencies inside the infrastructure itself.

Workload Isolation & Microsegmentation

NSX microsegmentation is used for workload isolation inside of an the NSX overlay network with strict policies. By using NSX security tags, traffic is filtered between hosts at the network layer—even on the same network segment. NSX dynamically assesses this traffic and identifies its unique characteristics—a kind of fingerprint. Regardless of which port the traffic uses, its fingerprint determines which firewall rules apply to it. This firewall policy follows the workload VM instead of relying on MAC, port, or IP filtering, so even if the IP, service port or MAC address of the workload VM changes the firewall rules and filtering will still be applied.

A further layer of protection could be implemented using the VMware Unified Access Gateway (UAG) as an ingress point for workloads after the Tier 0 and Tier 1 routers, in a cross-segment or side-chained connection between an isolated segment and a workload Tier 1 attached segment. Conditional access through the UAG appliance would be granted based on rules and conditional checks from Workspace ONE Access cloud controller. UAG checks that the client is meeting user authentication with proper device posture or compliance before allowing access to the data center application. A client showing inconsistent behavior and incorrect security posture, such as what is often seen during breaches, will trigger alarms and deny traffic.

For non-managed endpoint traffic, the NSX Advanced Load Balancer (formerly AVI) can be used in a side-chained connection method similar to what was described for UAG. With the NSX Advanced Load Balancer, web application firewall (iWAF) policies can be used to look at behavioral characteristics of the traffic before passing it on to the destination. The NSX IDS/IPS functionality can also be enabled, helping to detect and prevent known attacks using signatures.

This setup is known as a positive security model because no entities are trusted until they are specifically assigned a positive measure of trust. And, because the iWAF is an intelligent firewall, it becomes smarter as it filters more traffic. While typical security policies are static, iWAF policies evolve as the firewall learns. With the iWAF constantly learning and training, it can protect applications from ransomware attacks by detecting the change in lateral movement in the traffic and blocking it from continuing.

With multiple datacenters as shown in the diagram the NSX overlay network can be stretched over the SD-WAN encrypted tunnel so that all east-west traffic maintains the same security between sites. At the second site there is no need for local ingress for workload traffic, and only SD-WAN and NSX vTEP encapsulated overlay traffic can access the workloads on the remote datacenter cluster. By using the VMware SD-WAN appliances as the main ingress point at each datacenter all traffic between the sites remain isolated in the SD-WAN tunnel between them. This also keeps all management and vMotion traffic encrypted in an isolated tunnel from the corporate underlay network as it moves between sites and significantly reducing the attack surface of the management infrastructure from ransomware.

Specific Design Decisions

Why are these diagrams the way they are? Many decisions go into a system design. Some security features and resilience techniques require changes to the underlying hardware, and it is important to consider those as part of the design process. These availability decisions lead to ease of patching and maintenance of the infrastructure itself, which in turn leads to preservation of confidentiality and availability at the infrastructure level. When patching is easy and does not cause outages for workloads organizations will do it more often. Patching removes opportunities for attackers and preserves defense-in-depth.

This paper assumes that infrastructure outside the direct control of a VMware vSphere, Cloud Foundation, or VMware Cloud deployment is secure. Network configuration is crucial as part of the effort to detect and contain breaches in progress inside an organization. Networks can be configured to isolate discrete systems and provide checkpoints to validate and log network accesses.

Isolation, VLANs, and Separate Network Segments

Among the tribe of virtualization administrators is knowledge that a VMware vSphere deployment should isolate management traffic, vMotion traffic, vSAN and storage traffic, NSX overlay traffic, and so on. This can certainly be done in vSphere using individual physical network interfaces (NICs) but is often done using 802.1q VLAN tagging, which simplifies server configurations, cabling, and reduces physical network switch port usage. VLANs are typically used to contain & route discrete network segments, enabling perimeter controls and firewalls. However, routing of certain types of traffic is not always a requirement. Traffic that is purely local to a vSphere implementation could be given local, unrouted addresses on an isolated network segment.

Is using separate VLANs necessary when most network traffic is encrypted nowadays? Not strictly necessary, but helpful. Putting more boundaries between different types of network traffic is a form of defense-in-depth, helping to prevent the exploitation of minor misconfigurations during a breach, and making life more difficult for an attacker who may have gained administrative access to a system. One example of this is where an ESXi VMkernel network interface, normally used for only vSAN communications, might have management services enabled on it to circumvent perimeter security controls. Separation in this manner may also ease troubleshooting, too.

VLANs are not a perfect solution for network isolation. As with any logical construct they can be attacked or misconfigured, especially in situations where VLAN trunks are created dynamically. Similarly, many networks have a “default” VLAN configured on them, often VLAN 1, which may offer opportunities for attackers to communicate by crafting their own tagged packets.

Our Environment: We employed multiple VLANs and IP ranges/network segments for security isolation and for traffic management. A default or native VLAN is not configured on the switch ports. The switch ports are configured statically as VLAN trunks.

Perimeter Controls & Monitoring

Isolation techniques not very helpful without a checkpoint to limit access. Simple use of router ACLs all the way to next-generation firewalls are ways that access into a particular network segment might be audited and limited. Separation of network traffic can help simplify firewall rules for environments.

Most virtualization administrators think of perimeter controls in one direction: inbound or ingress.It is very important to also limit outbound or egress connections, too. A good example of this is the Log4j vulnerabilities from late 2021, where a vulnerable system would make outgoing requests to malicious LDAP servers. Environments that curtailed outgoing network traffic were protected until they could implement mitigations or remediations.

Even better, environments that monitor their traffic into and out of these network segments are able to notice breaches in progress. Configuring perimeter firewalls to log denied traffic, and alerting on denied traffic, is an important way to detect attackers moving inside an environment.

Please note that systems connected to the same VLAN or physical network segment can communicate with each other at will, without passing through a perimeter checkpoint (commonly referred to as “east-west” traffic). This means it is important to group systems with similar security and access requirements together on physical networks. If another system attached to the same physical network segment is compromised the attackers will be able to scan and attack other systems on that segment without triggering alarms. Microsegmentation with the VMware NSX distributed firewall solves this problem for workloads, but physical systems need other considerations.

VMware provides https://ports.vmware.com which helps customers find the right firewall rules for their environments.

Our Environment: Perimeter controls are configured on each network segment, for infrastructure management interfaces, vMotion, vSAN, and NSX transport traffic. vSAN traffic is fully isolated, as it does not need to leave the site, but vMotion has routable IP addresses to support cross-vCenter vMotion (xvMotion) for migration between sites and the VMware Cloud. Access to these interfaces is controlled with the perimeter controls.

Storage Fabric Isolation

One major example of network traffic that is not widely encrypted is datastore communications. While vSAN has full data-in-transit encryption capabilities, other types of storage like Fibre Channel, iSCSI, or NFS do not. Isolating this traffic is often an acceptable compensating control for organizations who employ storage that does not support encryption, or where the encryption imposes an unacceptable performance tradeoff.

Our Environment: Our architecture uses vSAN data-at-rest and data-in-transit encryption, which serves to protect storage traffic in transit. The use of a separate network segment adds a layer of protection as defense-in-depth, useful if a misconfiguration occurs and encryption is disabled. Or if encryption needs to be intentionally disabled to troubleshoot performance. Additionally, network traffic and storage performance may be easier to monitor and troubleshoot if that traffic is isolated.

Microsegmentation & Overlays

At its core, VMware NSX is an overlay network technology, creating encrypted tunnels that run across an existing physical network fabric. NSX encapsulates frames inside of packets, then transfers the encapsulated packets over the underlying transport network. This allows all network traffic to be “software-defined,” allowing security and policy to be wrapped around each workload directly. The NSX virtual tunnel endpoint (vTEP) connections are interfaces that the overlay network uses for communication between hosts and the edge VMs. A virtual distributed switch (vDS) is created for these connections to use, and the vTEP is attached to that vDS.

NSX is deeply integrated with vSphere, through both integration of the management consoles between vCenter Server and NSX Manager, as well as at the network level. In addition to the traditional firewalling based on protocols, IP, and MAC addresses, NSX Distributed Firewall rules can be defined on virtual machines and virtual machine tags. This allows more flexibility in assigning and maintaining security policies.

Inside a vSphere environment, NSX does not use traditional VLANs, but instead allows the creation of separate network segments that offer more options for routing and policies. These network segments are connected to each other through the NSX overlay networking between the distributed routers on ESXi hosts, allowing “east-west” traffic to move in a fashion like a traditional network switch. This is also how the NSX Distributed Firewall applies rules and policies. NSX Distributed Firewall rules are assessed at the virtual NIC level, meaning that all traffic in or out of a virtual machine is subject to security policy enforcement. This differs from traditional firewalls which only enforce policies with north-south traffic which crosses network segment boundaries.

North-South traffic is handled through edge nodes connected to the NSX Tier 0 router, bridging the underlay network with the vTEP overlay networks. NSX routers can use static or BGP routing protocols, as well as apply source or destination NAT to NSX segments and virtual machines connected to them.

Our Environment: This architecture uses a dedicated vTEP vDS with separate network interfaces and does not share this VDS with underlay network VLANs. Since this vDS is used for segment ports, this isolation of underlay from the overlay vTEP traffic not only optimizes performance but avoids possible misconfigurations that could allow direct access to the vTEP underlay VLAN directly from a workload VM compromising the security of the datacenter.

Network Failover Techniques

Network equipment requires maintenance, too, and coping with failures at the network level is very important. VMware vSphere supports two major network failover techniques: 802.3ad Link Aggregation Control Protocol (LACP) and vSphere NIC Teaming and Failover. LACP is a common method for network equipment to aggregate separate network connections, allowing for rapid failover and controlled degradation of service throughout a wide variety of failure modes. LACP requires participation to be configured on both the network equipment and on ESXi. LACP is sometimes incompatible with storage systems which often have other methods of handling failover in a time-bounded way.

vSphere NIC Teaming and Failover does not require participation from network switches and is simple to configure. A vSphere administrator adds two or more physical NICs to a virtual switch, specifying how traffic is to be distributed, and how failures are to be detected and handled. There are two methods of detecting failures: link status and beacon probing. Link status simply observes whether the NIC has a link, which may not detect situations where Spanning Tree has blocked a port, the port is misconfigured, the port is generating errors, and so on. Beacon Probing sends packets out and listens for them on other NICs, which helps it detect misconfigurations, but requires three or more NICs to be effective. Just as with cluster design, two sources of information mean that you cannot have a “tiebreaker” when failures occur.

Our Environment: Because of its ease of use and wide compatibility with networking and storage we employ vSphere NIC Teaming & Failover as the failover mechanism across the multiple network interfaces in the environment.

Trusted Platform Modules

Trusted Platform Modules (TPMs) are inexpensive add-on components for server hardware, and serve three purposes for an operating system like ESXi:

1. Supply a secure enclave for storage of secrets.

2. Generate random numbers to seed PRNGs.
3. Host attestation, proving that the host is in a specific state to establish trust.

A TPM is cryptographically bound to the host it is first installed and configured in, so that it cannot be transferred to another host. Beginning in ESXi 7 Update 2 the host configuration is encrypted when stored on the ESXi boot volume. If the ESXi host is enabled with a TPM 2.0 it will store the decryption key in the TPM, helping ensure that no sensitive information is stored in the clear on the boot volume. Other features such as vSphere Native Key Provider, vSAN, and ESXi Key Persistence will also store their secrets in the TPM if available.

TPMs do not address attacks such as ransomware directly but do make lifecycle, repurposing, and other operations easier and more secure. In turn, this frees staff time and budget in organizations, allowing them to focus on other defenses.

Our Environment: the hardware we selected did not arrive with TPMs installed, as is often the case with server hardware. The hosts were retrofitted before ESXi installation so that ESXi could always take advantage of the security from the beginning and ensuring that secrets have never been written to boot media in the clear.

Authentication & Authorization

One of the most common methods of compromise for infrastructure is through stolen credentials. Many organizations tie their infrastructure's authentication and authorization to a central identity provider, such as Microsoft Active Directory. Denying an attacker access to infrastructure often hinges on separating infrastructure identity management from the identity systems used for the rest of the organization (desktops and such).

Attackers who compromise an identity provider can often add themselves to authorization groups, and simply log into systems they should not otherwise have access to. Additionally, reliance on central identity systems means that the administrators of those systems are potentially infrastructure administrators, too, as they can add themselves to infrastructure access groups at will. Some regulatory compliance efforts, such as for PCI DSS and NIST 800-171, flag those identity management admins as "in scope" for audits and compliance actions. Organizations that do not wish their domain admins to be storage, firewall, vSphere, or other admins should reconsider the use of domain groups for authorization.

Most IT infrastructure, including vSphere, allows authentication and authorization to be done on the devices or systems themselves. This has the advantage of no dependencies on other systems, but is hard to monitor and audit, could be tedious to manage, and doesn't guarantee that an administrator will not reuse passwords. vSphere allows the separation of authorization, where the authentication can be done against a central identity source like Active Directory, but the authorization is done with a vSphere SSO group and not a domain group. This has the advantage of being easily audited, and often easily implemented, while making it incrementally harder for an attacker to gain access.

Many organizations have begun to build separate identity providers for their IT infrastructure systems, monitoring it closely for failed logins, but also successful logins that are abnormal. Some organizations employ ESXi Lockdown Mode to limit all access to hosts, driving all day-to-day authentication through vCenter Server and vSphere Identity Federation. Use of Active Directory Federation Services (ADFS) with Identity Federation allows for multifactor authentication (MFA) to be used, with many third-party MFA plugins readily available (from simple TOTP to full services like Duo, Okta, Ping, and the like).

Our Environment: we chose to model good authentication practices by having separate authentication for workloads and for infrastructure. Infrastructure authentication is supported by Microsoft Active Directory, deployed behind the infrastructure perimeter controls, and used only for vSphere, NSX, and other management interfaces (and not for workloads). The authentication source is configured simply as Active Directory over LDAPS, because of its support across all devices. A future improvement will be to employ federated identity and MFA.

System Dependencies & Placement

Ransomware attacks trigger business continuity processes and disaster recovery procedures. In turn, those procedures must be extended to cover not just the loss of a site, but the intentional corruption of the data that site held. It used to be enough to have two sites and proper replication and backups between them. Now all connections between the sites and between backup systems need to be hardened. For the purposes of this paper, a single site is considered.

At an individual site, dependencies can often be handled either with dedicated physical servers, or with a separate, unclustered ESXi host that holds primary copies of DNS, NTP, KMS, and authentication systems. By clustering the services on that host with sibling instances of DNS, NTP, KMS, etc. that exist in the local vSphere cluster (using Windows Server Failover Clusters or keepalived) this unclustered host and its workloads can also be patched and serviced without causing issues. The unclustered host can also be configured to start the DNS, NTP, KMS, etc. virtual machines automatically on reboot, so that response time after a power outage or other failure is minimized.

Domain Name System (DNS)

DNS is one of the core dependencies for vSphere and is used as a method for establishing certificate-based trust between many of the components in a vSphere cluster. Some components can be used without DNS, though. For example, it is possible to add ESXi hosts to a vSphere cluster by IP address. However, this overlooks the primary historical purpose of DNS: to help humans. Indeed, on a day-to-day basis it is much easier to interact with systems that have names, even if those names are arcane.

Cloud-based DNS services can be helpful for ensuring that DNS is available to all sites but may also expose internal system names publicly. The idea of hiding services to secure them – often described as “security through obscurity” – is not considered a valid security technique. However, nobody wants to help attackers by giving them a map. Decisions here should be respectful of the administration staff and the tradeoffs between obscurity and human error.

Our Environment: we use DNS services provided by the installation of Active Directory that is dedicated to infrastructure, with one domain controller and DNS server assigned to a particular ESXi host using DRS “should” rules so that the host can be powered on first in case of an outage. This helps resolve dependency issues between vCenter Server and NSX Manager’s use of DNS.

Network Time Protocol (NTP)

Time services are crucial to proper vSphere and vSAN cluster operation, as well as generation of audit logs for forensics and incident response. A process called “timestomping” where system times are changed helps attackers modify file creation and modification attributes on systems to hide their activities.

Our Environment: we configure our systems with four NTP servers for redundancy ({0-3}.vmware.pool.ntp.org), and use vRealize Operations Manager to monitor and alarm on time synchronization issues that may indicate a compromise.

Key Management Systems & Key Providers

vSphere has two major forms of data-at-rest encryption: VM Encryption and vSAN Data-at-Rest Encryption. VM Encryption protects virtual machines by encrypting the VM object files. This means it can work on any storage but has a negative impact on storage array deduplication and compression. vSAN Data-at-Rest Encryption encrypts the disk groups underpinning the vSAN datastore and does so in a way that preserves deduplication and compression. The two technologies can work together, though VMware does not recommend “double encryption” for complexity and performance reasons. However, features like vTPM rely on VM Encryption, and work well when stored on vSAN.

In both cases there are encryption keys involved, which are suppled by the key provider. vSphere supports three types of key providers:

- Standard Key Provider, the traditional method of storing encryption keys using an external, KMIP-compliant Key Management System (KMS).
- Trusted Key Provider, where the Standard Key Provider is proxied through vSphere Trust Authority, and access to cryptographic keys is limited to hosts that pass remote attestation.
- Native Key Provider, where vSphere can generate and store its own cryptographic keys for encryption.

The primary consideration between the Standard Key Provider and the Native Key Provider is physical security. The Standard Key Provider does not cache keys persistently on hosts (unless you use ESXi Key Persistence, which is not the default, and will not be considered further in this paper). When a host using the Standard Key Provider restarts it will need to retrieve all encryption keys from the provider and assumes the KMS is available to do so. This is an important dependency consideration. It also means that a stolen host will not have access to a KMS, so will not be able to unlock encrypted vSAN volumes or VM objects.

Native Key Provider must avoid dependencies, and so it persistently stores the decryption keys on the ESXi hosts, using a TPM if one is available. This allows a cluster to restart properly without access to vCenter Server, which may be running inside the protected cluster. This also means that vSphere clusters in locations without adequate physical security may be at risk because an attacker who steals the entire cluster will be able to boot it.

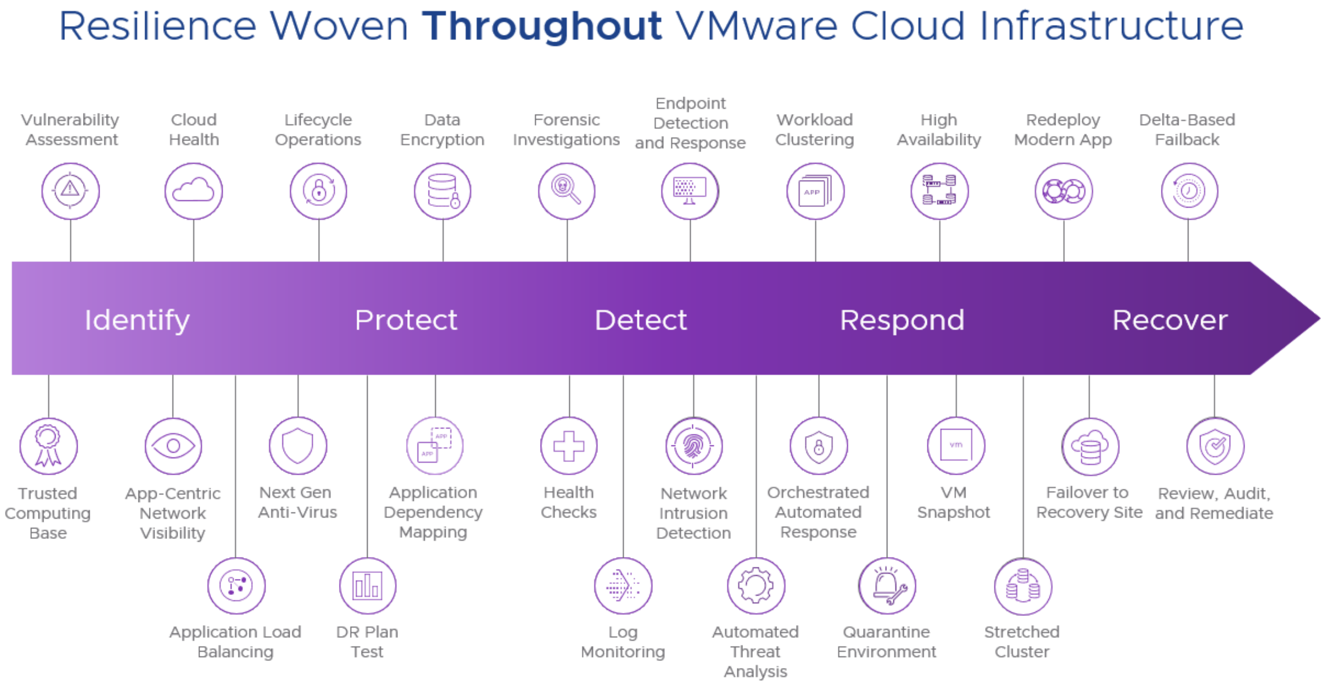
Our Environment: Our cluster is in a data center that has ample physical security protections. We chose to use Native Key Provider as it is extremely simple to configure and use with both vSAN, VM Encryption, and vTPMs for workloads.

Product Applicability

The NIST Cybersecurity Framework defines five functions as part of a comprehensive view of the cybersecurity lifecycle. NIST Special Publication 1271 describes these functions well:

- Identify: Develop an organizational understanding to manage risk to systems, assets, data, and capabilities.
- Protect: Develop and implement the proper safeguards to ensure delivery of services.
- Detect: Develop and implement the proper activities to identify the occurrence of a cybersecurity event.
- Respond: Develop and implement the proper activities to act on a detected cybersecurity event.
- Recover: Develop and implement the proper activities to support plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Seen through these lenses, and the lenses of common information security tenets like the CIA Triad, all features in all VMware products mitigate risk in some manner and can be mapped to one or more of these functions.



VMware vSphere

VMware vSphere is the foundation of software-defined data centers and has direct applicability to multiple components in the Framework, as well as enabling other functions through integrations with tools like Carbon Black Workload, NSX, and so on. Features like VM Encryption, vMotion, DRS, snapshots, Replication, high availability, and clones speak directly to Protect, Respond, and Recover.

VMware NSX

VMware NSX provides overlay software defined networking with advanced micro-segmentation firewall technology, called the NSX Distributed Firewall. With the ability isolate workloads and data using security tags and layer 7 filtering based on application fingerprint reduces ransomware lateral movement protecting assets from attacks. The VMware NSX suite of tools also includes VPN connectivity, IDS/IPS capabilities, container observability and security, and integrations with tools like Carbon Black. NSX itself spans Identify, Protect, Detect, and Respond.

VMware SASE & SD-WAN

The VMware Secure Access Service Edge (SASE) suite of tools includes SD-WAN capabilities, providing a SaaS control plane orchestrator to allow central configuration management across all regions and deployments. The SD-WAN device can be standalone physical hardware or a virtual machine running on a hypervisor. Since management and configuration of this device is all provided from the cloud orchestrator there is no local configuration once the device has been registered with the cloud controller. This significantly reduces the attack surface for local attacks, and also decreases the chance of policy errors that attackers can take advantage of. With the addition of VMware vRealize Network Insight, the VMware SD-WAN appliance can report in real time details of all traffic moving through each SD-WAN appliance. VMware SASE tools span Identify, Protect, and Detect.

Carbon Black & Carbon Black Workload

The VMware Carbon Black suite of tools provides comprehensive security to workload and endpoints, providing better understanding of security posture with workload behavior monitoring. Carbon Black Workload integrates with vSphere allowing a centralized and comprehensive view of the security state of workloads. Together, these tools provide risk assessments of possible exploits and malicious activity for quick response to ransomware attacks, including integrations with VMware Cloud Disaster Recovery for analysis and flexible recovery. These tools span the entire NIST Cybersecurity framework.

VMware vRealize Suite

The VMware vRealize suite of tools includes:

- Operations Manager, a tool that enables IT to monitor break-fix types of issues in an environment, trend capacity and performance, and continuously monitor security and compliance through the use of pre-built compliance and security packs available through the VMware Solutions Exchange. Operations Manager helps address Identify and Detect on the Cybersecurity Framework.
- Network Insight, a tool that closely monitors network activity and workload configurations, allowing admins and security staff to visualize and report on traffic. Network Insight also integrates with NSX and can help manage and automate very granular distributed firewall rules. Network Insight addresses Identify, Detect, and Respond.
- Log Insight, a tool that accepts logging traffic in standard syslog and syslog-like formats, aggregating event monitoring traffic into a common timeline on which alerts can be generated. Log Insight addresses Identify, Detect, and Respond.

VMware Cloud Disaster Recovery

VMware Cloud Disaster Recovery is a product that works in conjunction with VMware Cloud on AWS, allowing organizations to flexibly protect themselves in case of disaster, while using the elastic properties of the public cloud to save money and time in operating disaster recovery and failover sites. New features in VMware Cloud Disaster Recovery include Ransomware Recovery, which use direct integrations with Carbon Black to respond to attacks in progress and automate recovery. Cloud Disaster Recovery with Ransomware Recovery addresses Protect, Detect, and Recover.

Conclusion

Ransomware is a scourge that no single approach solves. Adding to the complexity, the approaches for workloads differ from the approaches for IT infrastructure components. Where workloads can take advantage of integrated protections the infrastructure provides, infrastructure has to be self-sufficient. To defeat ransomware and other attacks in infrastructure we must begin architecting environments to be flexible, resilient, isolated, and non-permissive.

About the Authors

Jerry Haskins is a Solutions Architect responsible for collaboration of products on the VMware Partner Solutions Engineering Team in VMware's Office of the CTO. With 20 years+ of experience in the IT Industry he has spent his career in innovative roles managing enterprise networks and datacenters, working with virtualization technologies, micro services, CI/CD workflows and HPC solutions.

Bob Plankers works in the Cloud Platforms group at VMware, focusing on all forms of security and compliance from VMware Cloud to on-premises vSphere. Prior to joining VMware, he spent more than two decades leading cross-organizational teams that designed, built, and operated reliable, secure, and compliance-oriented IT infrastructures worldwide, focusing not just on technological solutions, but also the people and process aspects, too.

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

Item No: vmw-wp-tech-temp-uslet-word-2021 8/21