vmware | Hewlett Packard Enterprise

Defeating Ransomware

With HPE ProLiant Compute
and VMware Infrastructure

Table of Contents

Introduction

Ransomware remains a predominant threat to organizations, even as attackers evolve their tactics. Its prominence is not without reason; ransomware attacks are both highly visible and potentially devastating. However, there isn't a single panacea to combat this threat. A comprehensive defense strategy combines innovative tools and techniques with foundational security principles. Additionally, the solutions for ransomware mitigation vary depending on the specific layer of IT infrastructure in focus. For instance, the methods used to safeguard workloads often differ from those deployed for storage arrays, firewalls, or VMware vSphere environments. This paper aims to outline best practices for securing VMware vSphere installations on HPE ProLiant server hardware, in line with current product and industry standards.

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 simply a thing that can be patched for or defended against in a single way. It is a multifaceted attack by an entire ecosystem filled with clever and determined 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 as well as 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 from 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 the loss of permanent access to their data, and the potential release of 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 that 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.

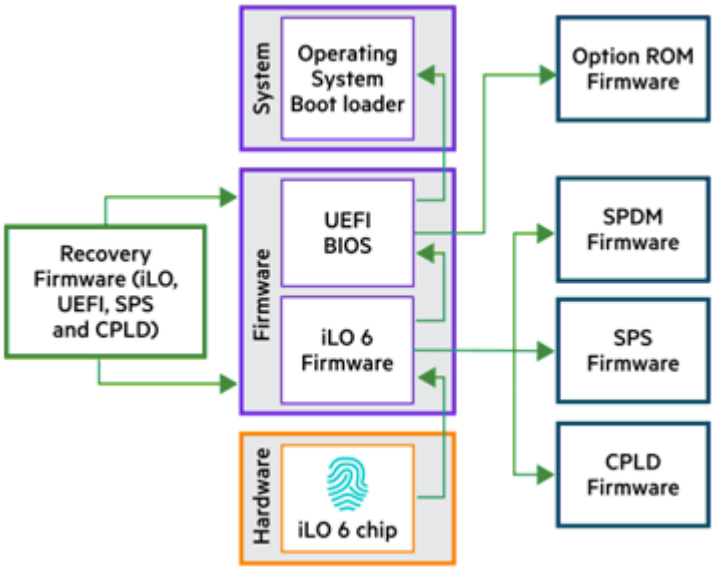
Ransomware targets all organizations, including for-profit companies, nonprofits, governmental agencies, health care services, and educational institutions of all sizes. While these criminal enterprises use various "strains" of ransomware, they have common attack vectors for compromise, such as brute force attempts at public-facing services including RDP, the

exploitation of outdated public-facing web software, and known vulnerabilities that might not have 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 verification. However, infrastructure services are often different, because they must run and connect to each other even when no other services are available. Infrastructure software, like VMware vSphere, relies on features such as Secure Boot, Trusted Platform Modules, VIB signing and verification, host attestation, and more, to build assurances in infrastructure that they can be trusted in their current configurations.

HPE Compute hardware extends these types of assurances deep into system firmware, with the iLO chip acting as a "silicon root of trust." A digital fingerprint of the iLO firmware is embedded in the iLO chip at a trusted chip fabrication facility. At startup, the iLO chip verifies the integrity of the iLO firmware and determines if it is allowed to run. This decision is based on whether the iLO firmware matches the digital fingerprint. If the iLO firmware fails validation, the system automatically restores the iLO firmware from the System Recovery Set.



When the iLO firmware runs, it verifies the UEFI BIOS, CPLD, Server Platform Services, Innovation Engine, and SPDM firmware. If these components fail validation, they can either be recovered automatically or through a manual process. However, system execution is blocked until the issue is resolved.

Beyond a defense-in-depth approach inside the infrastructure, Zero Trust techniques can be applied to the administration of infrastructure. Although grim, organizations that adopt the assumption that one of their desktops or user accounts is compromised have better mindsets for secure system design and are better able to detect and contain breaches when they occur.

Implementation Introduction

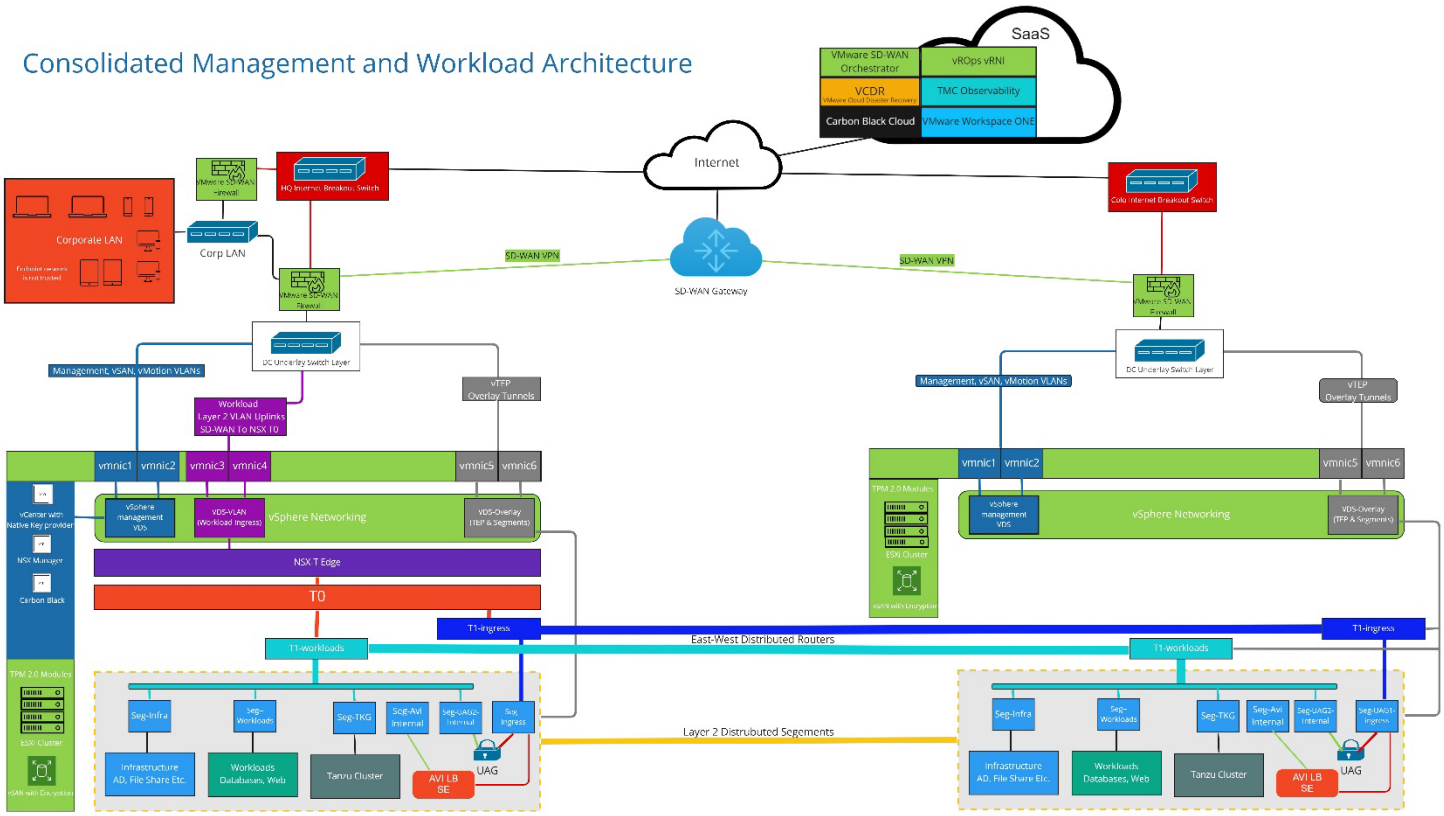


Figure 1: Consolidated Management & Workload Cluster Architecture

Consolidated Management & Workload Cluster

Figure 1 depicts a system design where the management systems (the "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 other components.

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 incur 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.

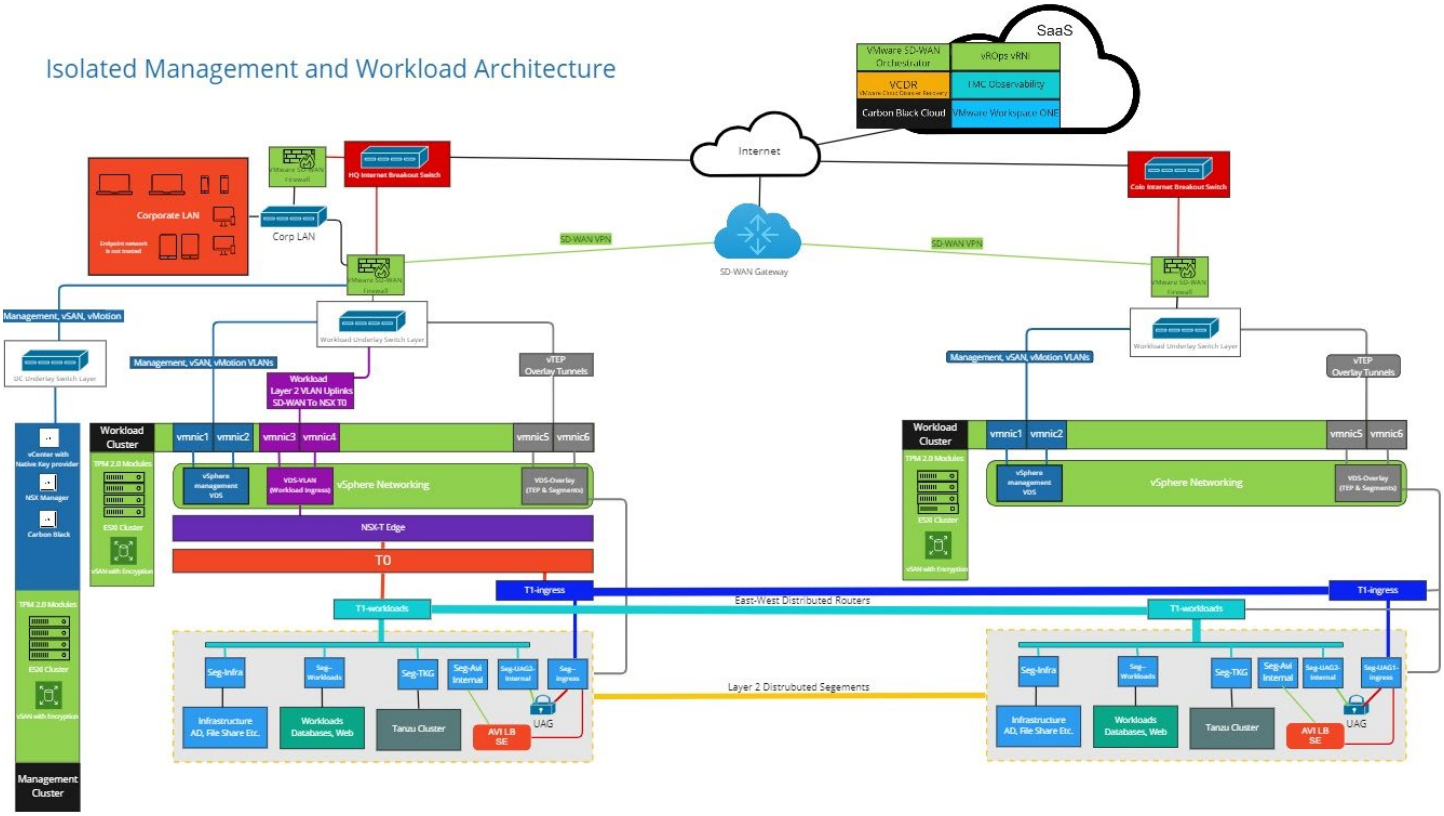


Figure 2: Separated Management & Workload Clusters

Separated Management & Workload Clusters

Figure 2 depicts a system design where the management systems (the "control plane") of the cluster are separated both physically and logically from the workloads they manage. The 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 the way VMware Cloud Foundation is deployed, with a "management domain" serving one or more "workload domains."

Physical isolation is present in this design, complementing the logical isolation provided by ESXi and NSX. The management domain can be secured separately, helping to further limit opportunities for attackers and 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 being amortized across all workload clusters.

Implementation Overview

These system designs rely on design decisions, which are further discussed in this paper. They all focus on defense-in-depth, a concept that involves the layering of security controls to ensure continued coverage if one is degraded or lost. This approach reflects the realities of how organizations are being compromised:

- Phishing and social engineering attacks that result in the compromise of a desktop.
- Compromised credentials, which stem from a pivot by the attackers from the compromised desktop to attacks on centralized identity management infrastructure.
- Insider threats and lax practices related to fundamental security concepts, such as least privilege.
- Configuration errors that might give opportunities to attackers.
- Software vulnerabilities and other mechanisms allowing lateral movement, even within a trusted environment.

One of the main objectives of this initiative is to demonstrate how to minimize these paths for attackers.

Separation of Infrastructure Management & Workloads

One of the primary features of these designs, as seen in the diagrams, is that management network traffic is isolated from workload traffic using NSX segments. These segments 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, while workload traffic ingress occurs over a Layer 2-only VLAN.

The datacenter underlay switches route only management traffic inside the datacenter and keep workload traffic isolated on the Layer 2 VLAN. This VLAN passes traffic from the SD-WAN appliance gateway to the NSX Tier 0 router gateway. Both the SD-WAN firewall and NSX Tier 0 router lack Layer 3 awareness of the datacenter switch fabric, ensuring all policies for management and workload traffic remain isolated at the firewall level. No shared routing tables exist within the direct datacenter fabric, separating the workload and management traffic.

Such a design significantly reduces the potential for lateral movement of an attack on the control plane managing workloads. It also offers options for managing dependencies within the infrastructure.

Workload Isolation & Microsegmentation

NSX microsegmentation is used for workload isolation inside 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. Therefore, 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 is granted based on rules and conditional checks from the 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, as 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 is described for UAG. With the NSX Advanced Load Balancer, web application firewall (iWAF) policies can be used to examine the 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. Furthermore, 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 remains 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, significantly reducing the attack surface of the management infrastructure from ransomware.

Specific Design Decisions

Why are these diagrams designed in this manner? Many decisions go into 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 promote ease of patching and maintenance of the infrastructure itself. This, in turn, ensures the preservation of confidentiality and availability at the infrastructure level. When patching is straightforward and does not result in outages for workloads, organizations are more likely to do it frequently. Regular patching removes opportunities for attackers and reinforces 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 occurring inside an organization. Networks can be configured to isolate discrete systems and provide checkpoints to validate and log network accesses.

Server Hardware Configuration

Modern server hardware, such as the HPE ProLiant compute family, has features that help VMware ESXi establish trust and continuously monitor system behavior.

HPE Trusted Supply Chain & HPE Server Security Optimized Service

The HPE Trusted Supply Chain provides a first line of defense against cyber attackers with supported servers built to heightened security standards in secured facilities. The HPE Trusted Supply Chain combines security, processes, and people to deliver protection for the most sensitive applications and data even before the server is deployed. By adding this service to supported servers, you can ensure that your system is built with the highest security standards in a secured facility in the USA. Additionally, the HPE Server Security Optimized Service can be added to enable advanced security by default, helping to ensure that its configuration is unable to be tampered with in transit from the factory.

Recommendation: These HPE offerings can help assure that your system hardware arrives in a state that is intended by HPE, based on your configuration specifications, and will also help save staff time while implementing new VMware vSphere environments.

Server Configuration Lock

Server Configuration Lock protects a server against tampering or compromise to the server composition. You can enable this feature when a server is in transit or use it all the time to monitor for configuration changes.

Server Configuration Lock monitors the server for DIMM changes, CPU changes, PCIe device changes, Security configuration changes, System firmware revisions, and Server Configuration Lock password authentication failures. If a configuration change

is detected during POST, an administrator must enter the Server Configuration Lock password to review the issue and continue the startup process. The configuration change is recorded in the Integrated Management Log (IML). A count of the detected issues is available in the Server Configuration Lock detection log in the UEFI System Utilities.

For more information visit: https://www.hpe.com/info/server-config-lock-UG-en

Recommendation: Once the server is configured appropriately, enable Server Configuration Lock to block VMware ESXi startup if there are changes to the system configuration. A security control of this type can be used as a denial-of-service attack, so ensure that there is adequate access to the system console and that the Server Configuration Lock password is a well-kept secret that remains available if all systems are down. To prevent inadvertent system lockouts to production environments, ensure that changes to system configurations are done in a test environment first.

Chassis Intrusion Detection Switch

Enabling the HPE ProLiant chassis intrusion detection switch allows for detection of any physical access inside the chassis. iLO logs an event when the access panel is opened or closed. Chassis intrusion monitoring and iLO reporting occur as long as the server is plugged in, regardless of the server power state. You can configure various alerting mechanisms (remote syslog, SNMP, or AlertMail) to notify you when a chassis intrusion event occurs.

Recommendation: Note that a loss of power to the server will prevent alerts of this type, but these security controls can still offer value (and the loss of power to a host may be monitored in an environment, too). Enable the chassis intrusion detection switch along with multiple alert mechanisms to allow both a timeline of events to be collected (such as through syslog) and timely alerts to notify you of an incident in progress.

Trusted Platform Modules

Trusted Platform Modules (TPMs) are inexpensive add-on components for server hardware, which serve three purposes for VMware ESXi:

1. Provide a secure enclave for storage of secrets.
2. Generate random numbers to seed PRNGs.
3. Facilitate host attestation, proving that the host is in a specific state to establish trust.

A TPM is cryptographically bound to the host in which it is first installed and configured, ensuring that it cannot be transferred to another host. VMware ESXi 7.0.2 and newer store the host configuration in an encrypted form on the ESXi boot volume. If the ESXi host is enabled with TPM 2.0, it will store the decryption key in the TPM, ensuring 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 they do make lifecycle, repurposing, and other operations easier and more secure. In turn, this liberates staff time and budget in organizations, allowing them to focus on other defenses.

Recommendation: Install and correctly configure TPMs as TPM 2.0 in your HPE ProLiant hosts prior to VMware ESXi installation. This ensures that ESXi will store its secrets there and that they are not written to boot media or elsewhere. This configuration will also enable advanced security inside the hypervisor itself, from system installation onward, helping to detect and prevent malware and other malicious activities. Ensure that your system recovery procedures are updated, as it is no longer possible to recover or change ESXi root passwords if lost. Ensure you back up your TPM Recovery Keys in a secure manner to ease restoration of systems that have undergone a system board change or inadvertent clearing of the TPM.

BIOS and Other Platform Security Options

Modern server platforms offer a plethora of BIOS and firmware options that enable CPU features enhancing security. Many servers are shipped in a configuration that ensures broad compatibility. As a result, some features that could improve performance and security in vSphere might not be enabled by default. It's beneficial to spend some time on a new system going through the HPE UEFI System Utilities options, selecting the appropriate Workload Profile from the HPE Intelligent System Tuning options, and ensuring other pertinent system settings are in place.

HPE iLO provides various methods for configuring hosts, ranging from API access to configuration backup and restore, making it straightforward to apply the manual optimization performed on a single server to an entire fleet of new systems.

Recommendation: Use the HPE UEFI System Utilities to activate the "Virtualization – Power Efficient" system profile, and then make sure system configuration options align with your organization's preferences. Subsequently, you might select the "Custom" profile, which will retain all previously saved settings. It's crucial to ensure that security technologies, like Intel Trusted Execution Technology, are properly set up.

Turn off any boot options except for the primary VMware ESXi boot volume, giving special consideration to network boot options, which might be located separately in network interface settings.

Avoid using power-on passwords due to operational concerns related to patching and unattended system restarts. Consider the use of administrator passwords, either removing or altering the default password provided by HPE. Refer to the section on Physical Security for additional insights into power-on and administrator password security.

Integrated Lights-Out Management Controller (iLO)

The HPE Integrated Lights-Out (iLO) management controller is an autonomous, integrated component of HPE ProLiant servers, offering advanced management capabilities for enterprises. The iLO is often the primary means of console connectivity to a VMware ESXi host; it can configure and monitor the host hardware, and facilitates hardware firmware updates, all of which are important components of server security. It is imperative that the iLO management interface be well protected.

Recommendation: HPE provides a comprehensive whitepaper on the security of the iLO controller which should be reviewed. Services and functions that are unnecessary for the organization should be deactivated, including access methods like SSH, SNMP, and IPMI. iLO NTP and syslog services should be configured, and valid TLS certificates should be issued to these devices. Centralized corporate identity services are a major path for compromise of IT infrastructure. Thus, care should be taken to isolate the iLO management interfaces from a potential organizational identity provider compromise. Similar risk assessments should be made when enabling HPE SSO for the iLO.

The HPE Integrated Lights-Out Security Technology Brief can be found at: http://www.hpe.com/support/iLO4_security_en

Physical Security

Use of security features like the vSphere Native Key Provider and ESXi Key Persistence may cause security material to be stored locally on ESXi hosts, enabling attackers to boot and unlock otherwise protected clusters. Physical security considerations, such as theft, are crucial.

Beyond theft, being security-minded also means asking yourself and your organization "What could go wrong?" as well as "How would I know that something went wrong?", especially in unstaffed data center locations and colocation facilities.

Examine your data center and rack configuration. Do the data center doors automatically close and lock properly on their own? If they were left ajar, would there be a proactive alert? If your rack doors lock, is it still possible for someone to reach into the rack from the side or top and disconnect a cable? Or perhaps connect a cable of their own to a network switch? Is it possible for someone to remove a device, such as a storage device or even an entire server? What would they get if they did?

Could someone glean information about vSphere or your business from information displayed on the servers, such as LCD panels or consoles? If those information displays are inactive, could they be triggered with the use of a stiff metal wire from outside the rack? Are there other buttons, such as the power button, which could be pushed to create a service disruption for your company?

Are there other physical threats, such as the possibility of flooding, freezing, high heat, or dust & debris from the environment, which would impact availability?

Note that HPE servers and compute modules have hardware maintenance switches on the system board inside the server chassis. These switches can erase power-on and administrator passwords, enable system management functions that were previously deactivated, and more. This means that security controls, like the power-on password, which seem attractive for mitigating physical security concerns, are easily overridden by an attacker with physical access to the system. The HPE Integrated Lights-Out Security Technology Brief summarizes this in its first section as "It is assumed that anyone with access to the inside of a server chassis is a super-user or administrator."

Network & Communications Fabric Security

Isolation, VLANs, and Separate Network Segments

Among virtualization administrators there is a 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 and route discrete network segments, enabling perimeter controls and firewalls. However, the 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 it necessary to use separate VLANs 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 only for vSAN communications, might have management services enabled on it to circumvent perimeter security controls. Separation in this manner may also ease troubleshooting.

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.

Recommendation: It is recommended that multiple VLANs and IP ranges/network segments be employed for security isolation and for traffic management. A default or native VLAN should not be configured on the switch ports, and the switch ports configured statically as VLAN trunks.

Perimeter Controls & Monitoring

Isolation techniques alone are not very helpful without a checkpoint to limit access. From simple router ACLs to next-generation firewalls, there are methods to audit and restrict access into specific network segments. Isolating network traffic can simplify firewall rules in various environments.

Many virtualization administrators conceive of perimeter controls primarily in one direction: inbound or ingress. However, it's crucial to also limit outbound or egress connections. A pertinent example is the Log4j vulnerabilities from late 2021, where a compromised system initiated outgoing requests to malevolent LDAP servers. Environments that restricted outbound network traffic were shielded until they could enact mitigations or remediations.

Furthermore, environments that vigilantly monitor their traffic both entering and exiting these network segments can identify ongoing breaches. It's essential to configure perimeter firewalls to log denied traffic and set up alerts for such traffic as a method to detect intruders maneuvering within an environment.

It's vital to understand that systems linked to the same VLAN, or physical network segment, can freely communicate, bypassing any perimeter checkpoint (often termed "east-west" traffic). Consequently, it becomes imperative to group systems with analogous security and access needs on the same physical networks. If a system on the same physical network segment gets breached, attackers can scan and target other systems within that segment without sounding alarms. Microsegmentation via the VMware NSX distributed firewall addresses this issue for virtual workloads, but physical systems demand separate strategies.

VMware offers a portal at https://ports.vmware.com that assists customers in determining the optimal firewall rules for their environments.

Recommendation: Each network segment should have perimeter controls configured, including for infrastructure management interfaces, vMotion, vSAN, and NSX transport traffic. While vSAN traffic remains entirely isolated since it doesn't need to exit the site, vMotion features routable IP addresses to support cross-vCenter vMotion (xvMotion) for site-to-site and VMware Cloud migrations. Access to these interfaces should be regulated by the perimeter controls.

Storage Fabric Isolation

A major example of network traffic that is not widely encrypted is datastore communications. While vSAN offers full data-in-transit encryption capabilities, other storage types like Fibre Channel, iSCSI, or NFS do not. Isolating this traffic can be an acceptable compensating control for organizations using storage that lacks encryption support or where encryption results in a significant performance tradeoff.

Recommendation: Employ vSAN data-at-rest and data-in-transit encryption to safeguard storage traffic during transit. Incorporating a separate network segment provides an added layer of protection as a defense-in-depth strategy, beneficial if a misconfiguration leads to encryption being deactivated or if encryption must be intentionally deactivated for performance troubleshooting. Additionally, monitoring and diagnosing network traffic and storage performance is typically easier when such 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 packets, then transfers the encapsulated packets over the underlying transport network. This process allows all network traffic to be "software-defined," enabling security and policy to be applied directly to each workload. 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 utilize, and the vTEP is attached to that vDS.

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

Within a vSphere environment, NSX does not employ traditional VLANs. Instead, it facilitates the creation of separate network segments that offer enhanced options for routing and policies. These network segments connect to each other through the NSX overlay networking between the distributed routers on ESXi hosts, permitting "east-west" traffic to flow similarly to that of a traditional network switch. This approach is also how the NSX Distributed Firewall applies its rules and policies. NSX Distributed Firewall rules are evaluated at the virtual NIC level, ensuring that all traffic entering or exiting a virtual machine undergoes security policy enforcement. This approach contrasts with traditional firewalls that only enforce policies on north-south traffic crossing network segment boundaries.

North-South traffic is managed through edge nodes connected to the NSX Tier 0 router, which bridges the underlay network with the vTEP overlay networks. NSX routers can employ either static or BGP routing protocols and can also apply source or destination NAT to NSX segments and the virtual machines linked to them.

Recommendation: Employ an architecture that uses a dedicated vTEP vDS with distinct network interfaces. It's essential to avoid merging this vDS with underlay network VLANs. By ensuring this vDS caters to segment ports, a clear separation between the underlay and overlay vTEP traffic can be maintained. This not only boosts performance but also minimizes the chances of potential misconfigurations. Without such a distinction, there might be unintended direct access to the vTEP underlay VLAN from a workload VM, which could compromise datacenter security.

Network Failover Techniques

Network equipment requires maintenance, and addressing failures at the network level is crucial. VMware vSphere supports two major network failover techniques: 802.3ad Link Aggregation Control Protocol (LACP) and vSphere NIC Teaming and Failover. LACP is a prevalent method for network equipment that aggregates separate network connections, allowing for rapid failover and controlled degradation of service in various failure modes. LACP requires configurations on both the network equipment and on the ESXi host. However, LACP is sometimes incompatible with storage systems, which often employ different methods of handling failover in order to preserve the order of storage write instructions.

vSphere NIC Teaming and Failover does not require involvement from network switches and is straightforward to configure. A vSphere administrator adds two or more physical NICs to a virtual switch, specifying traffic distribution and failure detection and handling mechanisms. There are two methods of detecting failures: link status and beacon probing. Link status merely observes whether the NIC has a link, which might not identify instances where the Spanning Tree has blocked a port, the port has a misconfiguration, or the port produces errors. In contrast, Beacon Probing dispatches packets and listens for their return on other NICs, helping to pinpoint misconfigurations. However, it requires three or more NICs to function effectively. Similarly, in cluster design, having only two information sources eliminates the possibility of a “tiebreaker” during failures.

Recommendation: For optimal ease of use and broad compatibility with networking and storage, employ vSphere NIC Teaming & Failover as the failover mechanism across multiple network interfaces in the environment.

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. Securing infrastructure often hinges on separating infrastructure identity management from the identity systems used for the rest of the organization, such as desktops.

Attackers who compromise an identity provider can often add themselves to authorization groups, enabling them to log into systems they should not have access to. Moreover, reliance on central identity systems means that the administrators of these systems might also have infrastructure admin privileges, since they can add themselves to infrastructure access groups at will. Some regulatory compliance standards, such as PCI DSS and NIST 800-171, consider these identity management admins as “in scope” for audits and compliance actions. Organizations wishing to prevent their domain admins from becoming storage, firewall, vSphere, or other admins should reconsider the use of domain groups for authorization.

Most IT infrastructure, like vSphere, permits authentication and authorization to be conducted on the devices or systems themselves. This offers independence from other systems but poses challenges in monitoring, auditing, and management, and there is no assurance that administrators will not reuse passwords. vSphere supports the separation of authorization, allowing authentication against a central identity source such as Active Directory, with the authorization handled by a vSphere SSO group and not a domain group. This approach is both easily audited and easily implemented, making it harder for an attacker to gain access.

Many organizations are now establishing separate identity providers for their IT infrastructure systems, monitoring not only for failed logins but also for abnormal successful logins. Some organizations use ESXi Lockdown Mode to restrict access to hosts, directing daily authentication through vCenter Server and vSphere Identity Federation. Incorporating Active Directory Federation Services (ADFS) with Identity Federation enables multifactor authentication (MFA), with numerous third-party MFA plugins available, ranging from simple TOTP to comprehensive services like Duo, Okta, Ping, and others.

Recommendation: Implement good authentication practices by establishing distinct authentication for workloads and infrastructure. Support infrastructure authentication with Microsoft Active Directory (AD) and Active Directory Federation Services (ADFS). These should be deployed behind infrastructure perimeter controls. They should be used only for vSphere, NSX, and other infrastructure management interfaces, not for workloads or desktops, and not outside the perimeter controls protecting those management interfaces. Using both Active Directory and ADFS allows for broad support, utilizing AD over LDAPS as well as the direct ADFS federation capabilities in VMware vSphere. ADFS also permits other authentication sources to be connected, introducing multifactor authentication and other modern authentication technologies.

Consider adopting federated identity services such as Okta and Microsoft Azure ID. When implementing this, ensure that a separate tenant is used, distinct from workload and desktop authentication for the enterprise. Use a very limited set of administrators and enable security features such as conditional access, number matching, phishing-resistant MFA, and device hygiene tests.

Tightly restrict access to ESXi management interfaces. Drive all day-to-day administration through vCenter Server and the Role-Based Access Control (RBAC) model present there.

In all cases, move authorization to vSphere itself and avoid using authorization groups or other identity provider structures to authorize administrator access to vSphere. Add vSphere users and administrators to the vSphere SSO Administrators group directly.

System Dependencies & Placement

Ransomware attacks initiate business continuity processes and disaster recovery procedures. In turn, these procedures must be extended to address not just the loss of a site, but also the intentional corruption of the data that the site held. Previously, it was enough to have two sites and proper replication and backups between them. Now, however, 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 addressed 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, ensuring 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 serves as a method for establishing certificate-based trust between many of the components in a vSphere cluster. Some components can be used without DNS. For example, it is possible to add ESXi hosts to a vSphere cluster by IP address. However, this bypasses the primary historical purpose of DNS: to assist humans. In everyday operations, 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, it's essential to avoid helping attackers by giving them a map. Decisions here should be made with consideration for the administration staff and the tradeoffs between obscurity and human error.

Recommendation: Use DNS services, like those provided by an installation of Active Directory for infrastructure needs, which have appropriate redundancy and are protected against dependency loops. Restrict DNS traffic egress stringently so that unauthorized UDP traffic to the internet is curtailed.

Time Synchronization (NTP)

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

Recommendation: Configure systems with four NTP sources for redundancy, ideally using NTP services local to the systems. Restrict them heavily with perimeter firewalls to curtail unauthorized UDP traffic to the Internet. Use the Aria Operations system to monitor and raise alarms on time synchronization issues that may indicate a compromise.

Key Management Systems & Key Providers

vSphere offers 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 is compatible with any storage but can have a negative impact on storage array deduplication and compression. vSAN Data-at-Rest Encryption encrypts the disk groups that form the basis of the vSAN datastore and does so in a way that preserves deduplication and compression. The two technologies can work together, though VMware advises against "double encryption" due to complexity and performance concerns. However, features like vTPM depend on VM Encryption and function optimally when stored on vSAN.

In both cases, there are encryption keys involved, which are supplied 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 users 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 the KMS and will not be able to unlock encrypted vSAN volumes or VM objects.

The Native Key Provider aims to avoid dependencies and, as such, 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 the vCenter Server, which might be running inside the protected cluster. However, this also implies that vSphere clusters in locations without adequate physical security may be at risk, as an attacker who steals the entire cluster will have the capability to boot it.

Recommendation: Ensure that the cluster is located in a data center that boasts ample physical security protections. Opt for Native Key Provider because, barring additional regulatory requirements, it is extremely simple to configure and use with vSAN, VM Encryption, and vTPMs for workloads.

Design Workloads for Prevention & Recovery

Identify Workloads, Policies, and Needs

The ability to detect, respond to, and recover a workload from an incident such as ransomware starts with identifying systems, assets, and data, and then developing methods to help prevent a breach. This work happens at all layers of the stack, including the guest operating systems inside the virtual machines. Not all attacks are rapid; some have been measured in hundreds of days from beginning to end. This is an important fact to consider when determining how to protect workloads and data.

RTO & RPO

Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are essential metrics in ransomware recovery and business continuity planning. RTO represents the targeted duration within which systems and applications should be restored after a ransomware attack. It also indicates the maximum period a business can tolerate without a critical system or application after a disruption. On the other hand, RPO signifies the maximum acceptable data loss between the last backup and the attack.

RTO and RPO are business decisions and are vital because they establish the groundwork for devising effective protection strategies, allocating resources, and setting priorities and budgets. For instance, an RPO of 5 minutes necessitates different data protection measures, such as storage-level data replication, compared to an RPO of 24 hours, where a daily backup might be adequate.

In ransomware situations, recovery points and durations can fluctuate as data undergoes restoration and cleaning to ward off reinfection and restrict attackers' lateral movements. Ensuring low RTO and RPO in these situations hinges on dependable backup and recovery processes, redundant infrastructure, stringent ransomware protection protocols, and comprehensive recovery planning and testing.

Disaster Recovery

Recovery and disaster recovery are related concepts in the context of data protection and business continuity. Recovery refers to the process of restoring data or systems to a previous state after a disruption or outage. This can be accomplished through various means, such as restoring from a backup or using data replication technologies to retrieve data from another location. The goal of recovery is to minimize data loss and resume operations as swiftly as possible.

Disaster recovery is a broader process that entails preparing for and responding to potential disasters or disruptions that might affect an organization's operations. These disruptions can arise from natural disasters, cyber-attacks like ransomware, hardware failures, or other unexpected events. The aim of disaster recovery is to ensure that an organization can continue to function despite these disruptions and to reduce their impact on operations.

Disaster recovery planning typically involves identifying potential risks and vulnerabilities, formulating response plans, and devising strategies to lessen the impact of disruptions. Such strategies might encompass regular backups, data replication, failover systems, and other redundancy measures to guarantee that essential systems and data remain accessible.

Placement & Availability

The elasticity of services like VMware Cloud, and the ease of migrating workloads between sites using VMware vSphere vMotion and VMware HCX, provide more options for organizations. However, these options come with their own unique considerations for both incidents and long-term hybrid deployments. One of the key considerations to make is whether a workload or application service should have:

- A permanent, always-on cloud presence,
- Replicated copies ready to be powered up,

- Backups that can be restored,
- or some combination of these choices.

Most organizations employ a combination of tactics, depending on the type of workload or service, whether other workloads are dependent on it, and the time and effort it would take to reinstate the service in the new location.

Workload Dependencies

Not all workloads are the same; some are effectively standalone, while others have multiple tiers of dependencies. Other workloads, such as DNS and NTP, provide core services to all workloads and systems. Some types of workloads have other restrictions as well. For example, the historical guidance for Microsoft Active Directory has been to always build new domain controllers, as opposed to migrating them, to avoid database synchronization issues. Fundamental services used by all workloads are good candidates for a permanent, always-on presence at a secondary site or in the cloud to lower recovery times.

Dependencies come in many forms, including DNS, NTP, authentication, logging, network connectivity, storage, and more. There might also be hidden dependencies. For example, a query to a Microsoft SQL Server may also invoke calls to authentication sources and DNS. Tools such as VMware Aria Operations for Networks can help identify those dependencies, allowing you to plan for disruptions.

It is especially important to ensure that backup systems can restore data with a minimum of dependencies and that IT staff and virtualization administrators can gain access to the failover environment if the organization's primary site is offline.

Multifactor Authentication

Multifactor authentication (MFA) serves as a powerful deterrent to cyberattacks by requiring users to provide multiple forms of verification before granting access to sensitive systems and data. By implementing MFA, organizations can significantly reduce the risk of unauthorized access due to compromised credentials, as attackers must overcome multiple layers of security to gain entry.

Some MFA providers restrict connectivity or use system identifiers that may change during a failover or recovery scenario, so it is important to test that functionality in advance. Additionally, any recovery data or "break glass" access mechanisms that exist should be examined in the context of failover and application migration.

Cloud DNS

Cloud DNS offerings are an attractive method to move an organization's DNS needs into a cloud service. These services can also help organizations separate their DNS infrastructure from their legacy Microsoft Active Directory installations, allowing for better security via separation of duties and least privilege configurations. However, these services can be vulnerable to ransomware attacks. A ransomware attack that targets DNS can lead to widespread disruption of internet services, both internally and externally, as well as the malicious rerouting of traffic. Some considerations to protect the use of cloud DNS include:

- Use Secure DNS Providers: Choose a DNS provider that has a strong security posture and is committed to protecting against ransomware attacks. Look for providers that have implemented best practices such as encryption, two-factor authentication, and regular security audits.
- Limit DNS Traffic: Implement a security policy that limits DNS traffic to known DNS servers within the enterprise. Only allow those known DNS servers to communicate outside the enterprise for DNS lookups. Ensure that all recursive DNS queries outside the enterprise are made to curated DNS services.
- Monitor DNS Traffic: Monitor DNS traffic for suspicious activity, such as large numbers of requests for non-existent domains, unusual patterns of DNS queries, and attempted queries to unapproved resolvers. This can help identify breaches and attacks early.

- Enable DNSSEC: Domain Name System Security Extensions (DNSSEC) is a protocol that adds an additional layer of security to DNS by verifying the authenticity of DNS responses. Implementing DNSSEC can help protect against DNS-based attacks, including ransomware attacks.
- Consider Time-to-Live (TTL) Settings Carefully: TTL informs DNS resolvers' caches about how long they can retain that information before looking it up again. Normally, a cache is a helpful performance boost, but in a situation where DNS records must be changed rapidly, it can be very detrimental, as millions of DNS resolvers across the world will not retrieve the new IP address until that TTL expires. Default TTLs can be 12 or 24 hours. The minimum TTL is 300 seconds, which offers rapid updating but will increase DNS resolver traffic, which may not be a concern for a large cloud DNS provider, but increases client latency, which would be a concern for your organization. You might consider an intermediate value such as 1 hour which offers reasonable caching opportunities without drastically limiting your options.
- Enable and Test Backups: Ensure that regular backups of DNS zone data are made, and regularly test those backups to ensure that DNS data can be restored in the event of an attack.

By taking advantage of the cloud's inherent scalability and global distribution, these services enable seamless workload migration and distribution across multiple regions, ensuring uninterrupted access to critical resources in the event of localized disruptions or system failures. Cloud DNS services also provide built-in redundancy and automatic failover mechanisms that contribute to enhanced service availability and resilience. Adopting cloud DNS services not only strengthens an organization's disaster recovery capabilities but also ensures that critical services remain accessible and operational, supporting overall business continuity.

Remote Access

Maintaining remote access to workloads during a disaster recovery or business continuity event can pose several challenges, especially in terms of managing firewall rules, VPNs, and access control mechanisms that rely on fixed IP addresses. Failover scenarios may involve the updating and modifying of firewall and other access control rules to accommodate changing network conditions and the need for secure remote access. VMware NSX offers security groups that can help organizations react quickly to both failover situations and application mobility needs, as well as day-to-day administration tasks.

Virtual Private Networks (VPNs) are commonly used to facilitate secure remote access to workloads during disaster recovery or business continuity events. It is essential to ensure that connectivity via a VPN does not depend on resources that could be unavailable, and that a secondary access method or secondary VPN configuration is granted access to workloads.

Time Synchronization

As with infrastructure components, time synchronization is important to workloads both for their regular operations and for cryptographic operations, as well as log capture and incident response forensics. Ensure that workloads have access to a reliable time source at the failover site.

Standalone vs. Interconnected Environments

It is important to remember that ransomware is the end state of a breach that may last for weeks or months. Over that time, systems that are interconnected and synchronizing data may replicate the compromise elsewhere. This can occur bidirectionally as well, with cloud-based workloads infecting on-premises deployments.

In many cases, it is possible to separate applications or services such that they appear identical to dependent workloads but they do not replicate data directly between the nodes of the service. However, care must be taken to maintain configurations and settings accurately between the sites. Automation can assist with this, but take care not to allow the automation to become an attack vector, as configuration management systems tend to have privileged access to environments.

Data Locality & Latency

The flexibility to migrate workloads repeatedly and rapidly between sites and clouds is a strength of the VMware platforms. However, as mentioned earlier, dependencies and hidden dependencies may introduce additional latency into applications, not just between clients and application servers.

Network connections between sites are subject to latency from intermediate network equipment, encryption, propagation delays of electrical signals, and the speed of light itself, at least until quantum-entangled network adapters are invented and commercialized. It's important to note that Transmission Control Protocol (TCP), used for most application network connections, has a three-way handshake process. This means that a site 2,000 miles away (3,200 kilometers, from the middle of the United States to the western coast) with a 40-millisecond network round-trip will incur a 60-millisecond connection latency for each connection startup. Multiply this by hidden calls to authentication systems, DNS, and other non-local systems, and application latency increases rapidly.

The net effect of latency is that incident response and recovery plans need to encompass entire applications, versus individual components, and may shape the architecture of dependencies. Systems can also be architected to abstract dependencies so that they can be redirected to site-local equivalents. For example, an application that is restored to an alternate site or cloud will still be configured for DNS at the original site. However, technologies such as anycast DNS might be employed to automatically route those requests to the nearest available DNS server without having to change the workload's network configuration. Similar abstractions can be used for other services, such as site-specific DNS records (often referred to as "split brain") and more.

Lastly, network traffic that remains local to a cloud deployment may also avoid network ingress/egress charges.

Air Gaps

Air gaps and ransomware are two concepts often discussed together in the context of cybersecurity. An air gap is a physical or logical isolation between two systems or networks that prevents data from flowing between them. In the context of cybersecurity, an air gap can be used to protect critical systems or data from cyber-attacks by isolating them from the internet or other networks that might be vulnerable to attack.

Air gaps protect against ransomware attacks by preventing the spread of malware between systems and eliminating the ability for lateral movement of the ransomware. If a system is air-gapped from other systems infected with ransomware, the malware cannot spread to the isolated system, ensuring the data on that system remains safe.

However, air gaps are not foolproof, and risks remain when relying solely on them to protect against ransomware attacks. For instance, if an attacker gains physical access to an air-gapped system, they might be able to infect it with malware or exfiltrate data. Human error or insider threats can also diminish the effectiveness of air gaps.

Therefore, while air gaps can serve as an effective component of a cybersecurity strategy, they should not be viewed as the only defense against ransomware attacks. Other security measures, such as regular backups, network segmentation with products like VMware NSX, and user training, should be implemented to reduce the risk of a successful ransomware attack.

Backup & Restore

Proper backups and restore capabilities are critical when recovering from ransomware attacks.

- Backup: A backup is a copy of data and applications stored separately from primary systems. Backups can be created at regular intervals, such as daily or weekly, and stored on different types of media, including disk, tape, or cloud storage. In the event of a ransomware attack, a recent backup can be the key to recovering data without paying a ransom.
- Restore: Restoring data from a backup involves copying it from the backup storage and returning it to its original location. This action can be performed using various tools, depending on the backup type and the systems being restored. Testing the restore process regularly is vital to ensure that backups are functional and available during a disaster.

Besides traditional backup and restore solutions, specialized tools and services for ransomware recovery are also available:

- Immutable storage: Some backup solutions, such as VMware Cloud Disaster Recovery, offer immutable storage. Once data is written to the backup, it cannot be modified or deleted, safeguarding against ransomware attacks that attempt to delete or encrypt backup data.
- Snapshot-based backups: Certain backup solutions utilize snapshots, such as VMware Site Recovery Manager and VCDR, to capture point-in-time data copies. This strategy can aid in recovering from ransomware attacks that target a specific moment.
- Cloud-based recovery services: VMware provides VMware Cloud Disaster Recovery, a cloud service designed to expedite data and system recovery after a ransomware attack. These services boast features like virtual machine replication and failover, enabling rapid restoration of crucial systems.

It's imperative to regularly test the restore process. Tools and services like immutable storage, snapshot-based backups, and cloud-based recovery services, including VMware Cloud Disaster Recovery, bolster defense against ransomware attacks. Leveraging these solutions, organizations can amplify their data recovery strategies, promptly restore essential systems, and counteract the repercussions of ransomware attacks without succumbing to ransom demands.

Snapshots & Clones

VMware vSphere Snapshots and Clones, as well as snapshots taken on storage arrays, can be beneficial in mitigating certain types of risks. For instance, failed application upgrades can be swiftly rolled back if a snapshot was captured before the work commenced. Nevertheless, snapshots and clones do not inherently qualify as a backup, as they are not housed separately from the primary copy of the workload.

Replication vs. Backups

Replication and backups serve distinct roles in data protection and business continuity.

Replication entails generating a copy of data and synchronizing it with the original source either in real-time or near real-time. Its primary function is to ensure high availability (HA) and curtail downtime due to hardware or software failures, network interruptions, or disasters. Using replication, the copied data can be activated promptly in the event of a failure, reducing business disruption. Nonetheless, the replicated copy often contains malware and might also reflect the consequences of a ransomware attack since replication aims to preserve nearly real-time copies.

Backups, on the other hand, revolve around making periodic data copies and housing them in a distinct location, often on varied storage media. The main purposes of backups are data safeguarding, data recovery, and prolonged retention. They enable businesses to revert data to a specific moment, proving invaluable in situations like data corruption, unintended deletions, or ransomware incidents. Generally, backups aren't as up to date as replicated data.

Backup remains the most probable recovery method after a ransomware attack. However, advanced ransomware might linger for a protracted duration, compromising backups before the ransomware assault is evident.

While replication and backups cater to different needs, they synergize in a holistic data protection strategy. For example, replication can offer near-zero recovery point objective (RPO) and recovery time objective (RTO) for essential workloads. In contrast, backups provide extended retention and an extra defense layer against data corruption, deletion, or ransomware invasions.

It's pertinent to mention that replication and backups also vary in aspects like cost, intricacy, and expandability. Replication systems generally carry a steeper price tag and demand more infrastructure assets, whereas backup solutions tend to be cost-effective and more straightforward to oversee. Moreover, while replication excels in shielding active workloads, backups excel at safeguarding both active and dormant workloads, including archived information or applications that have been phased out.

Immutable Backups

Immutable backup copies represent data backups that, once generated, remain unalterable and impervious to modifications. Such integrity is realized through technologies like Write Once Read Many (WORM) storage mechanisms or immutability functionalities in backup software.

They play a pivotal role in defending against data compromise or corruption due to malware, ransomware, or assorted cyber threats. By ensuring backups remain immutable, entities can retain a pristine and safeguarded data replica, poised for system restoration following a cyber onslaught.

Beyond serving as a shield against adversities, immutable backup copies also facilitate compliance with data retention mandates and standards. By guaranteeing the immutability of backups, institutions can attest to possessing an intact and untouched data record throughout the stipulated retention span.

Immutable backup copies stand as a crucial element within a robust data protection and ransomware recovery blueprint. It's imperative for establishments to incorporate them within their backup and recuperation strategies.

Content Libraries & Templates

An often-overlooked area of incident response and system recovery is the ability to deploy new virtual machines and perform "rescue boots" from operating system media. Activities such as downloading specific operating system media, transferring them to remote sites, mounting ISO images remotely across WAN links, and more can be time-consuming, extending recovery times. VMware vSphere offers Content Libraries as a way to organize and manage media and virtual machine templates. Content Libraries can be subscribed to one another, meaning that a central copy can be maintained with updates that automatically propagate to other sites and vSphere environments in the cloud.

Secure Boot

UEFI Secure Boot is a security feature of the Unified Extensible Firmware Interface (UEFI) designed to safeguard a computer's boot process from malware and unauthorized interference. It achieves this by mandating that all firmware components and operating system bootloaders are digitally signed with a trusted certificate. During the boot process, the UEFI firmware checks the signatures of these components against a built-in database of trusted certificates to confirm their authenticity. If any component does not pass this verification, the boot process is halted, stopping potentially harmful software from running. UEFI Secure Boot is valuable because it offers an essential layer of defense against low-level threats that might otherwise jeopardize the system from the outset, enhancing the overall security and stability of the computing environment.

vTPM & Security Devices

A Trusted Platform Module (TPM) is a specialized hardware component designed to enhance the security of a computer system. It provides a secure environment for cryptographic operations and the safe storage of sensitive information, such as encryption keys, passwords, and digital certificates. TPMs are typically embedded as dedicated microcontrollers on the motherboard or integrated within the processor. They offer various security features, including hardware-based encryption, secure key generation, and system integrity attestation. The primary benefit of a TPM is its ability to protect sensitive data and cryptographic operations from software-based threats, as the data never exits the secure confines of the TPM. This ensures the confidentiality and integrity of vital information, making it challenging for unauthorized parties to access or alter the data. Moreover, TPMs can support secure boot processes, remote attestation, and platform authentication, enhancing overall system security.

VMware vSphere provides virtual TPMs (vTPMs) to workloads, supported by VM Encryption for data-at-rest security. These virtual TPMs activate guest OS features such as Microsoft Device Guard, Credential Guard, BitLocker, Windows Hello, Measured Boot, and more. They are often necessary for advanced security measures and regulatory compliance needs. It's essential to confirm that the recovery target environments can handle these workloads and that the key provider for VM Encryption is set up and ready for use.

Service Startup

Where possible, workload services should be configured to start automatically. This benefits recovery times, allowing application administrators to focus on more complex workloads during the recovery process. It also aids many day-to-day operations. VMware vSphere High Availability events are less impactful when workload services automatically and smoothly restart, as are automated operating system patches. When everything restarts automatically and efficiently there is much less friction in updating workloads, which in turn reduces vulnerabilities and helps deter attacks.

Additionally, periodic reboots from patching processes ensure that Secure Boot can identify and prevent the loading of malware on workload operating systems. As its name suggests, Secure Boot only runs at boot, so a periodic restart can be very helpful in proactively detecting breaches before a full ransomware attack.

Data Volumes vs. Operating System Volumes

Breaches often involve the introduction of malware and compromise of workload operating systems and may require restoring a workload twice: once to obtain a clean operating system version, and another time to restore data according to the RPO. Organizations that differentiate their workload data from operating system data by using additional virtual hard disks (VMDKs) experience an easier time remounting discrete volumes during the recovery process.

IP Addressing & Connectivity Strategies

There are numerous IP addressing strategies and considerations to make when designing applications to resist attacks, recover quickly, and promote application mobility:

- Segmentation: Dividing the network into smaller subnets can help contain the spread of ransomware in the event of an attack. By isolating critical applications and their associated infrastructure, it becomes more challenging for ransomware to propagate throughout the network. This can be achieved by employing technologies such as VLANs or software-defined networks like VMware NSX micro-segmentation technologies.
- Load Balancing: The VMware NSX Advanced Load Balancer can protect the application from ransomware attacks by implementing application layer security with WAF, SSL/TLS encryption, access control lists, as well as monitoring traffic patterns, sending alerts, and notifications for unusual traffic patterns. Load balancers can also protect applications by using pools that only the load balancer should communicate with, limiting direct access to the application. IP pools also let backend applications move without disrupting services.
- Network Access Control (NAC): NAC solutions can enforce policies around network access and ensure that only authorized devices connect to the network. This can help curb the spread of ransomware by limiting the number of devices that can access critical applications and infrastructure.
- Virtual Private Network (VPN): Using a VPN can shield applications from ransomware attacks by ensuring that all traffic between sites is encrypted. VPNs can also be employed within a private network to restrict access between critical infrastructures.
- IP Address Management (IPAM): Adopting a centralized IPAM solution can curb ransomware attacks by ensuring all IP addresses are tracked and managed correctly. With centralized IPAM, administrators can promptly identify rogue devices and IP addresses that are not authorized, which might indicate a ransomware attack.

A robust IP addressing strategy is essential for ensuring failover and business continuity in the face of unforeseen network disruptions or system outages. By adopting a well-conceived IP addressing scheme, administrators can establish seamless failover mechanisms, allowing rapid transfer of network services to redundant systems, thus reducing downtime. A strategic IP addressing method also streamlines network management and fosters efficient resource allocation, subsequently improving overall network performance and resilience. Moreover, a sound IP addressing strategy supports business continuity by facilitating rapid recovery and maintaining the availability of critical services, ensuring organizations operate with minimal disruption and protect their long-term viability.

Network Segment Design & Firewalling

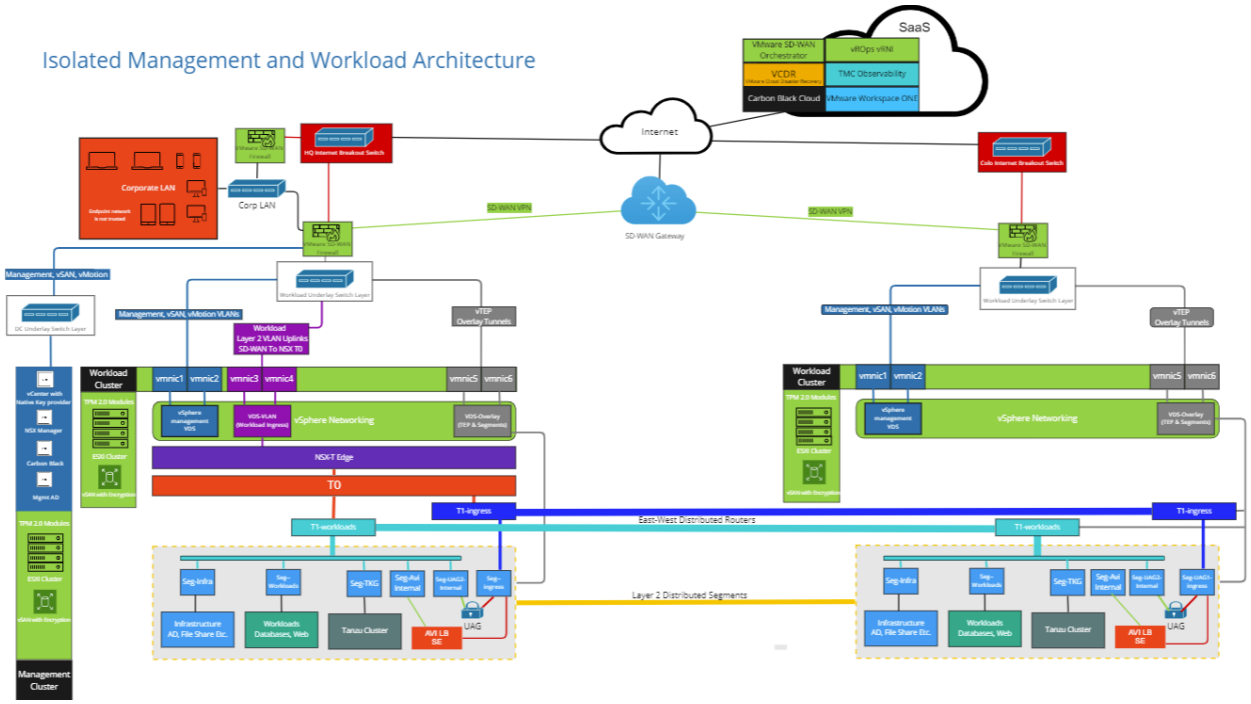
VMware NSX is a robust network virtualization and security platform designed specifically to protect virtual machines from cyber threats, including ransomware attacks. By employing micro-segmentation, NSX effectively isolates workloads and restricts network traffic, impeding lateral ransomware movement across the network.

The NSX Distributed Firewall (DFW) supports both Macro-Segmentation (Security Zones) and Micro-Segmentation, delivering comprehensive L2-L7 East-West visibility and enforcement with automated policy formation. Various segmentation strategies, including Zone Segmentation, VLAN Segmentation, Application Segmentation, and Micro-Segmentation, can coexist, each applied to different sections of the environment to suit the organization's requirements.

The distributed firewall within NSX enforces stringent security policies across both virtual and physical workloads, ensuring continuous protection even when workloads are moving. Using NSX Security Groups can make changes to security policies easy and quick. Moreover, NSX boasts intrusion detection and prevention capabilities that actively counter ransomware threats not just from outside of your organization, but also attacks between systems as attackers move laterally. For added security, the NSX Advanced Load Balancer (previously known as AVI) incorporates web application firewall policies to inspect traffic behavior before directing it to the intended destination. This feature further enhances the platform's defensive capabilities.

NSX's distributed architecture integrates security enforcement controls at the virtual network interface of each workload, enabling granular traffic flow management without the need for a centralized appliance or routing of network traffic through a network security stack. As NSX is integrated into the virtualization infrastructure, it provides visibility into all applications and workloads, using this insight to generate rich application context, monitor workload life cycles, and automate security policy management.

The example architecture outlined below demonstrates the use of NSX micro-segmentation, perimeter isolation with SD-WAN, and iWAF ingress packet inspection in conjunction with NSX tags to minimize lateral movement and defend against ransomware attacks. It is important to note that the management control plane and workloads do not have any common infrastructure or networks, further bolstering security measures.



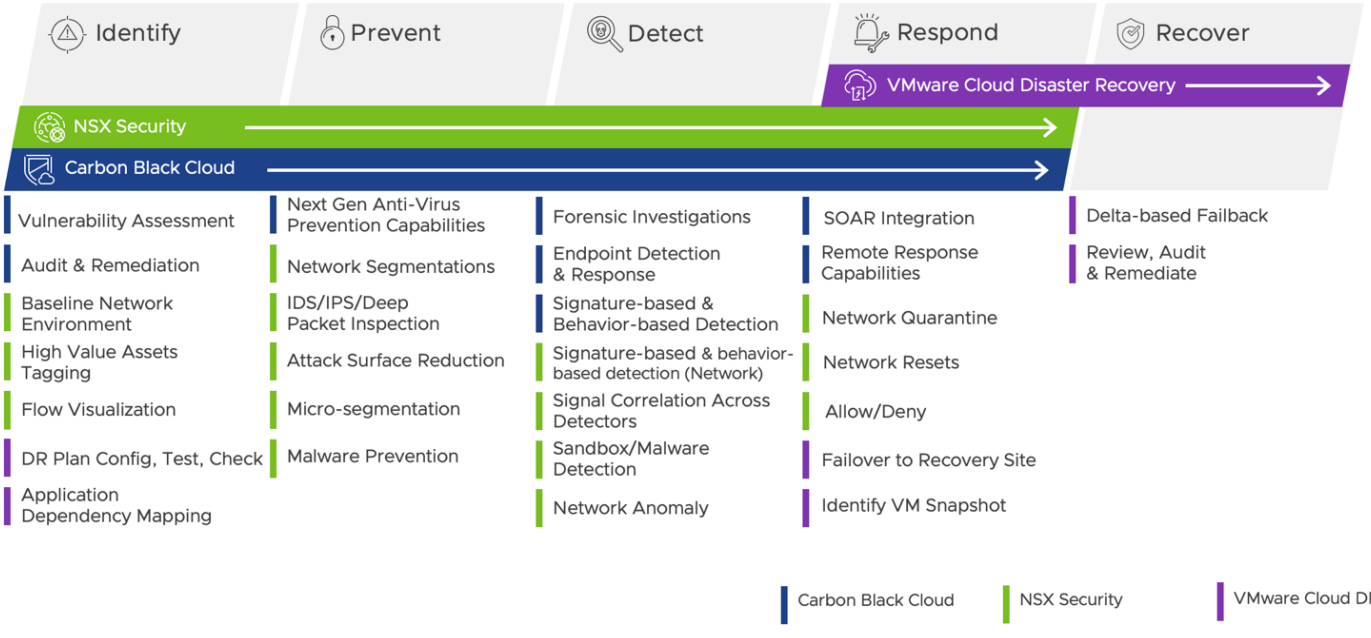
Detection & Response

Detection, response, and recovery capabilities for workloads inside a VMware environment are robust, ranging from simple reversal of snapshots to elaborate orchestrated failover to alternate sites. A variety of tools are available to VMware customers to address these scenarios, such as VMware Cloud Disaster Recovery, VMware Site Recovery, VMware Carbon Black, and more.

From a ransomware detection perspective, the goal is to assist organizations in detecting ransomware early, minimizing the damage caused by an attack, and recovering from the attack as swiftly as possible. The key components of a ransomware detection and recovery strategy include:

- Prevention: The initial line of defense against ransomware is prevention. This encompasses measures such as keeping systems and software up to date, following security best practices, and training employees on how to recognize and avoid phishing attacks.
- Detection: Ransomware detection and recovery depend on advanced detection tools to identify ransomware attacks. This encompasses endpoint protection solutions that employ behavioral analysis and machine learning algorithms to detect anomalous behavior and halt the spread of ransomware, like VMware Carbon Black and Workspace ONE.
- Response: Once ransomware is detected, a prompt and effective response is vital to minimize the damage. This encompasses isolating infected systems, quarantining affected files, and implementing steps to prevent the ransomware from spreading to other systems.

VMware offers a comprehensive software stack for ransomware detection and recovery, covering virtualization, backup and recovery, monitoring, detection, network isolation protection, as well as detection and remediation solutions.



Endpoint Detection & Response

VMware Carbon Black Cloud, a cloud-native endpoint protection platform (EPP), delivers intelligent system hardening and behavioral prevention capabilities to counter emerging threats. It employs a single lightweight sensor and an intuitive console to interpret attackers' behavior patterns, enabling real-time detection and prevention of unprecedented attacks and promptly alerting IT staff to unusual behavior.

Behavioral analysis forms the foundation of VMware Carbon Black Cloud, ensuring optimal security by grasping how attackers operate. Many endpoint security solutions only record data when they consider an activity suspicious, often overlooking earlier activities crucial for determining the root cause. Conversely, VMware Carbon Black Cloud persistently monitors and scrutinizes endpoint activity, regardless of its perceived intent.

Besides its superior detection and prevention features, VMware Carbon Black Cloud integrates response capabilities within the console, markedly shortening the time to resolution. The platform empowers administrators to search and sift through events across the environment over the past 30 days, furnishing the vital data for exhaustive investigation. Moreover, the alert visualization tool offers a clear view of events transpiring during an attack, equipping security teams to swiftly evaluate the situation and respond accordingly.

VMware Carbon Black Cloud addresses diverse requirements, providing plug-and-play protection for those favoring a hands-off approach, alongside tailored policies. Accommodating a broad spectrum of endpoint and workload operating systems in various settings, VMware Carbon Black Cloud emerges as a holistic and anticipatory defense tool, shielding organizations' pivotal data and systems from evolving cyber threats.

Intrusion Detection & Protection

Intrusion detection and prevention systems (IDS/IPS), such as the NSX Distributed IDS/IPS, play a critical role in detecting ongoing attacks. These systems continuously monitor network traffic and activities for malicious patterns, anomalous behavior, or known attack signatures. This monitoring enables the early detection of potential threats. By identifying and containing breaches in their early stages, IDS/IPS can significantly reduce the potential impact of an attack and limit the spread of malware across the network.

During the recovery process from a ransomware attack, an effective IDS/IPS acts as a valuable tool in mitigating further damage and promoting swift remediation. By providing real-time threat intelligence and comprehensive visibility into the attack, an IDS/IPS helps security teams in tracing the source of the infection, pinpointing vulnerabilities, and implementing suitable countermeasures. Furthermore, intrusion prevention capabilities can block ongoing attempts to exploit these vulnerabilities, ensuring that the organization can recover from the attack with minimal disruption and lessen the likelihood of future ransomware incidents. An IDS/IPS provides a proactive and robust defense mechanism that is essential for maintaining the security and resilience of an organization's digital assets.

Log Monitoring and Alerting

VMware Aria Operations for Logs is a powerful log management and analysis solution that provides organizations real-time visibility into their infrastructure, applications, and security events. By collecting, centralizing, and analyzing log data from various sources across the IT environment, VMware Aria Operations for Logs assists security teams in proactively detecting potential attacks and breaches in workloads. Its advanced analytics and machine learning capabilities can identify patterns and anomalies that may indicate malicious activities, allowing security staff to quickly respond to emerging threats.

In addition to its detection capabilities, VMware Aria Operations for Logs also features customizable alerting, ensuring that security teams are promptly notified of critical issues and potential breaches. By creating custom alerts based on specific events, patterns, or thresholds, security personnel can focus on the most relevant incidents, reducing the chance of overlooking critical security events. Furthermore, VMware Aria Operations for Logs' integration with other VMware solutions, such as NSX and Aria Suite, simplifies the monitoring and management process, enabling organizations to maintain a comprehensive security posture for their workloads.

To guarantee that workloads have log forwarding agents installed and operating, and that they have access to log collectors in both their primary and backup locations, organizations should implement a robust log management strategy. Additionally, log management systems should be strengthened, isolated, and highly available to ensure that they themselves are not subject to ransomware attacks.

Recovery

What Backup Copy Do You Trust?

With ransomware, it's essential to have a backup strategy that ensures data recovery in the event of an attack. However, not all backup copies can be trusted in the event of ransomware.

Typically, ransomware targets the most recent backups first, so having multiple backup copies, including older ones taken prior to the ransomware attack, is crucial. It's also vital to store backup copies in a separate location from the production environment to prevent them from being encrypted by the ransomware.

A consistent process should be in place to regularly test backup and restoration procedures, ensuring that the backups are dependable for successful data recovery. Adopting a backup strategy with immutable backups ensures that backup data cannot be altered or removed, offering an extra layer of defense against ransomware attacks.

When restoring data and services following a ransomware attack, it's advisable to first use an isolated environment to test the recovery and to scan for ransomware before reintroducing data, applications, and services into production.

Failover vs. Restore

Failover and restoration are two concepts used in data protection and disaster recovery. Failover switches from a primary to a secondary system in the event of a failure, while restoration recovers data or systems from a backup after an unexpected event. Failover aims to minimize downtime, while restoration is a reactive approach to return affected systems to their original state. Both are essential in minimizing the impact of unexpected events on operations, such as a ransomware attack. During an incident, an organization may need to decide which path to take.

Tools For Recovery

vSphere Replication

VMware vSphere incorporates VMware vSphere Replication, which allows organizations to replicate workloads to an alternate site or cluster, managed directly from the VMware vSphere Client. These capabilities require manual management and do not encompass the advanced orchestration features found in VMware Site Recovery and VMware Cloud Disaster Recovery.

VMware Site Recovery Manager

VMware Site Recovery Manager (SRM) is a disaster recovery solution for VMware vSphere environments that automates the disaster recovery process and aims to minimize downtime and data loss due to disasters. It provides automated orchestration of failover and failback operations and replicates virtual machines to a secondary site. With SRM, administrators can create and test disaster recovery plans, perform non-disruptive testing of plans, and monitor and report on replication and recovery status.

VMware Site Recovery Manager (SRM) can offer protection from ransomware by allowing administrators to create and test disaster recovery plans that include automated failover and failback operations. In the event of a ransomware attack, administrators can use SRM to promptly failover to a secondary site, minimizing downtime and data loss.

By replicating virtual machines to a secondary site, SRM can help ensure that data is protected and available in the event of a ransomware attack. SRM also provides monitoring and reporting capabilities that can help administrators proactively identify potential issues and implement corrective actions to mitigate the impact of a ransomware attack.

Using SRM, a customer can perform non-disruptive testing of disaster recovery plans, allowing administrators to validate the effectiveness of their plans without impacting production environments. This can help ensure that recovery plans are up to date and effective in the event of a ransomware attack.

There are several failover strategies that organizations can adopt to ensure business continuity in case of a disaster or ransomware attack:

- Hot/Hot Failover: In this strategy, there are two active production environments that are fully synchronized and ready to take over in the event of a disaster. This approach provides the fastest recovery time and ensures minimal data loss, but it can be expensive to maintain and requires a robust infrastructure. However, it might not offer protection from ransomware attacks, as the replication can facilitate the spread of ransomware to the secondary site.
- Hot/Cold Failover: In this strategy, there is a primary active production environment that is fully operational, and a secondary environment that is maintained in a dormant state. In the event of a disaster, the secondary environment is activated, and production is transferred to it. This approach is less expensive than Hot/Hot but requires manual intervention to switch to the secondary environment. This can be an effective ransomware recovery strategy as the secondary environment can be kept in a clean state and snapshots can be applied to access different versions of the recovery state to reach a clean running version. The environment will likely be out of date so another backup and recovery method should also be in place to clean and recover mission critical data.
- Warm Failover: This strategy involves maintaining a partially operational secondary environment that is up to date but not fully synchronized. In the event of a disaster, the secondary environment can be quickly updated and used for recovery. This approach provides a balance between cost and recovery time but may result in data loss. This can be an effective ransomware recovery strategy if the last synchronization was not infected with the ransomware attack.
- Cold Failover: In this strategy, there is a secondary environment that is fully configured but not running. In the event of a disaster, the secondary environment is activated, and the primary environment is reconstructed. This approach is the most cost-effective but has the longest recovery time and can result in significant data loss. This can be highly effective for ransomware recovery as the cold environment can be tested and maintained in a known clean state. Data will not be up to date and will need to be recovered, but this environment can bring mission critical services back up while clean and recovery actions are underway.
- Migration: This approach involves moving production workloads and data to a different location before a disaster occurs. This approach can be expensive and time-consuming but provides the most control over the recovery process and can minimize data loss. This approach is not an effective ransomware recovery method since a business is unlikely to detect an attack before it happens.

Organizations should choose the appropriate failover strategy based on their specific requirements, budget, and recovery time objectives. It is important to understand that disaster recovery and ransomware recovery are not the same thing. They may use similar overlapping strategies, but each scenario should be planned and addressed separately to ensure a comprehensive strategy for each situation.

VMware Cloud Disaster Recovery

VMware Cloud Disaster Recovery (VCDR) is a disaster recovery solution provided by VMware that offers cloud-based disaster recovery for VMware environments. With VMware Cloud Disaster Recovery, customers can replicate their virtual machines and data to a secondary site in Amazon Web Services (AWS), ensuring that critical systems and data are consistently available, even if a disaster occurs.

The solution provides continuous replication and snapshots of the replicated backups, allowing customers to select from numerous recovery points in the case of a ransomware attack. Customers can also design and test recovery plans, and fail over to the cloud with just a few clicks, offering a rapid and dependable method to recover after a disaster.

With the incorporation of VMware Carbon Black Cloud, VCDR can tap into intelligence in an air-gapped recovery environment to clean and reconstruct VMs from multiple recovery points, eliminating ransomware before returning the VM to production.

VMware Cloud Disaster Recovery is available as a subscription-based service and necessitates a VMware Cloud on AWS subscription. The solution is crafted to be straightforward to establish and oversee and can be integrated with other VMware products and services.

VMware Cloud Disaster Recovery Pilot Light

VMware Cloud Disaster Recovery Pilot Light is a disaster recovery strategy that uses cloud-based infrastructure to ensure rapid recovery of critical IT services in the event of a disaster. The Pilot Light approach keeps a minimal set of infrastructure and resources running in the cloud, ready to be engaged in the event of a disaster.

In the context of VCDR, the Pilot Light approach means maintaining a small, but critical, set of virtual machines (VMs) in the cloud that are configured and ready to be powered on and used for disaster recovery. These VMs typically include critical infrastructure components such as domain controllers, DNS servers, and other core services required to support the failover of other VMs and applications in the event of a disaster.

During normal operation, these VMs are kept in a "powered off" or "hibernated" state, consuming minimal resources and incurring minimal costs. However, in the event of a disaster, the Pilot Light VMs can be quickly engaged, providing a base infrastructure for failover and recovery of other critical services and applications. Depending on the last recovery point state, these Pilot Light services can assist in the recovery of basic critical services in the event of a ransomware attack.

The Pilot Light approach provides a cost-effective and efficient way to maintain disaster recovery capabilities in the cloud, without the need for a fully equipped and constantly running environment. It also ensures rapid recovery of critical IT services, minimizing downtime and reducing the impact of a disaster on business operations.

Conclusion

Protecting workloads from ransomware requires a comprehensive and multi-layered approach that encompasses prevention, detection, and recovery. By leveraging the advanced features and security capabilities of VMware NSX, VMware Carbon Black, and backup and recovery solutions such as VMware Cloud Disaster Recovery (VCDR), organizations can establish a strong defense against ransomware threats. It is also vital to maintain up-to-date backups, implement micro-segmentation, and employ advanced threat prevention techniques to secure the virtual environment. By adopting these strategies, organizations can not only protect their critical workloads on VMware vSphere but also ensure business continuity and resilience in the face of evolving ransomware threats.