Ransomware Defense and Recovery Strategies

using VMware Infrastructure & Security Products

vmware®

April 2023

Table of Contents

Introduction

In 2022, a team at VMware published a paper on using VMware products to combat cyber attacks, with a focus on ransomware. In recent years, there has been a significant increase in such attacks; however, a well-designed IT infrastructure can effectively deter, detect, repel, and recover from breaches. It is essential to note that IT infrastructure is not an end in itself but serves to operate workloads and grant data access to organizations.

The 2022 paper determined that workload protections differ from infrastructure protections and primarily concentrated on the latter. This whitepaper explores the other direction, to investigate ransomware prevention in virtualized workloads. We aim to present best practices for operating workloads, in alignment with current guidance from both VMware and the industry, while also incorporating our own implementation and testing. Furthermore, we intend to chronicle our design decision-making processes so that others may learn from them.

Security guidance often purports to be "the authoritative way" to accomplish a goal. However, real-world scenarios are considerably more intricate and nuanced. Security involves trade-offs, and always depends on context. By examining these issues and discussing our choices we hope to help virtual and cloud administrators make better decisions for their workloads and data, even if their choices differ from ours.

Disclaimer

This document is intended to provide general guidance for organizations that are considering VMware solutions. 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 requirements and effectiveness of implementations.

What is Ransomware?

Ransomware is a type of malware that denies access to a user's or an organization's data, usually by encrypting it with a cryptographic key known only to the attacker. This multifaceted attack involves criminals patiently invading and taking over an organization's electronic assets with the intent of holding them hostage for money, stealing intellectual property, and extorting the primary victim and their customers.

Malware often enters through malicious downloads, email links, advertisements, phishing attacks, social network messages, and websites, as well as through unpatched vulnerabilities and weaknesses in public-facing software and services. Once executed, the attackers gain a foothold in the organization, compromising the endpoint and user account. They then "establish persistence" and "move laterally" to attack other targets within the organizational network.

Ransomware is the end process of a breach, blocking user access until payment demands are met. These demands usually include threats of permanent data loss and public exposure of sensitive content. Attackers also exfiltrate and steal data from victims to sell directly or extort their customers through "double extortion." This is particularly effective against organizations with clients who have sensitive data, such as law firms and accounting firms. Unfortunately, paying the ransom offers no guarantee that the attackers will provide the necessary decryption keys or that the decryption process will work correctly. Moreover, there is no assurance that they will not further exploit victims or their customers.

Ransomware targets all types of organizations, including for-profit companies, nonprofits, governmental agencies, health care services, and educational institutions. Attack vectors for compromise include brute force attempts on public-facing services like RDP, exploitation of outdated web software, and unremediated vulnerabilities. Defending against ransomware requires a holistic approach, involving people, processes, and technology to detect and contain attacks before they cause major harm and disruptions.

Information Security Concepts

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

Authentication

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

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

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

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

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

Authorization

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

Availability

Ensuring that data is available to authorized parties when needed.

CIA Triad

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

Compensating Control

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

Confidentiality

Ensuring that data is protected from access by unauthorized parties.

Data Breach

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

Defense-in-Depth

According to the US National Institute of Standards and Technology, defense-in-depth is "the application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering

heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another."

Identification

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

Incident

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

Integrity

Ensuring that data is protected against unauthorized modification.

Lateral Movement

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

Least Privilege

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

Recovery Point Objective (RPO)

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

Recovery Time Objective (RTO)

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

Security Control

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

Separation of Duties

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

Vulnerability

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

Identify Workloads, Policies, and Needs

The ability to detect, respond, and recover a workload from an incident such as ransomware starts with identifying systems, assets, and data, 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

RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are important metrics in ransomware recovery and business continuity planning. RTO indicates the targeted time to restore systems and applications after a ransomware attack, or the maximum amount of time that a business can afford to be without a critical system or application after a disruption occurs. RPO represents the acceptable data loss between the last backup and the attack.

RTO and RPO are business decisions and are crucial because they lay the foundation for developing effective protection strategies, allocating resources, and setting priorities and budgets. For example, an RPO of 5 minutes will require different data protections, like storage-level data replication, than an RPO of 24 hours where a daily backup may suffice.

With ransomware, recovery points and time may vary as data is restored and cleaned to prevent reinfection and further lateral movement by attackers. Achieving low RTO and RPO in these circumstances involves reliable backup and recovery processes, redundant infrastructure, ransomware protection measures, and robust 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 done through various means, such as restoring from a backup or using data replication technologies to recover data from another location. The goal of recovery is to minimize data loss and restore operations to normal as quickly as possible.

Disaster recovery is a more comprehensive process that involves preparing for and responding to potential disasters or disruptions that could impact an organization's operations. This can include natural disasters, cyber-attacks like ransomware, hardware failures, or other unforeseen events. The goal of disaster recovery is to ensure that an organization can continue to operate despite these disruptions and minimize the impact on operations.

Disaster recovery planning typically involves identifying potential risks and vulnerabilities, developing response plans, and implementing strategies to mitigate the impact of disruptions. This can include measures such as regular backups, data replication, failover systems, and other redundancy measures to ensure that critical systems and data are always available.

Placement & Availability

The elasticity of services like VMware Cloud, and the ease of migrating workloads between sites using VMware vSphere vMotion and VMware HCX mean more options for organizations. However, these options come with some of their own 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,
- Replica 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.

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 was always to 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 may also be hidden dependencies as well. 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 (formerly vRealize Network Insight) 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.

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 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 VMware platforms. However, as mentioned earlier, dependencies and hidden dependencies may introduce additional latency into applications, not just between the clients and the 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. Also, consider that Transmission Control Protocol (TCP), used for most application network connections, has a three-way handshake process. This means that a site 2000 miles away (3200 kilometers, middle of the United States to the western coast) with a 40 millisecond (ms) network round-trip will incur a 60 ms 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 inform 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 ("split brain") DNS records, and more.

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

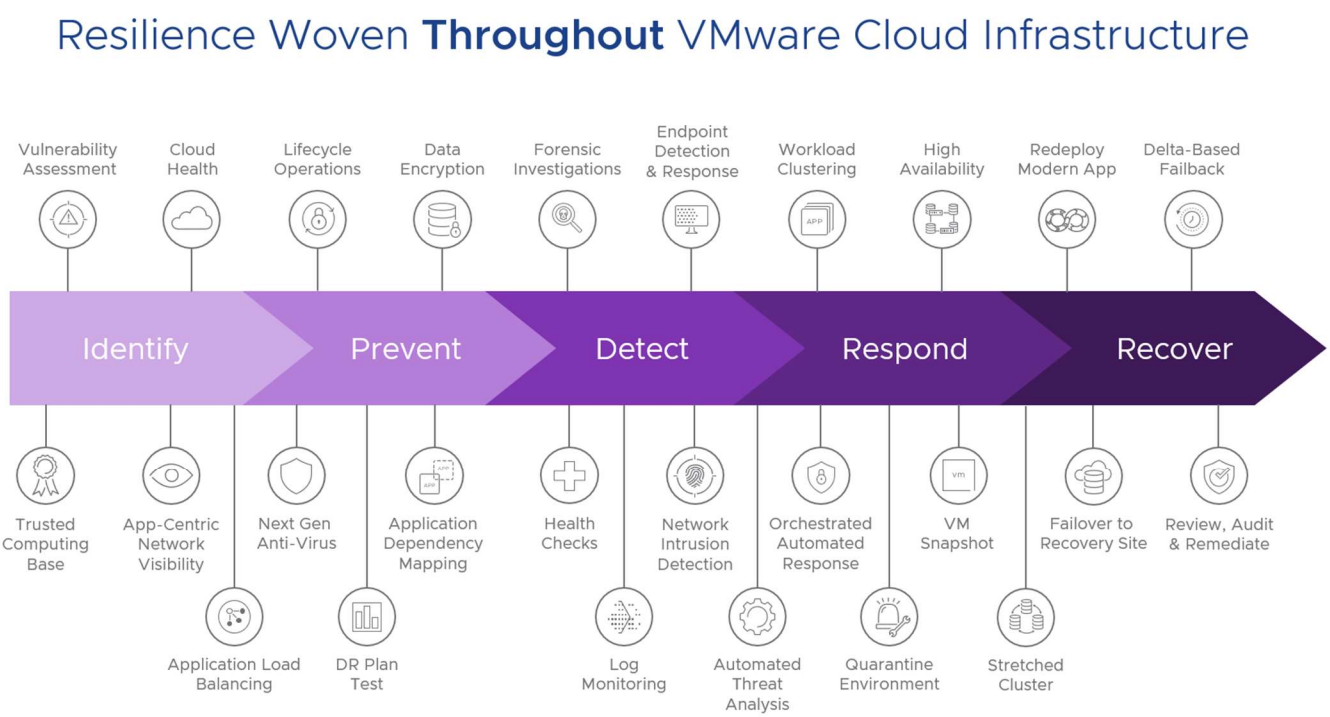
Air Gaps

Air gaps and ransomware are two concepts that are 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 may be vulnerable to attack.

Air gaps protect against ransomware attacks by preventing the spread of malware between systems, disabling 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, and the data on that system may remain safe.

However, air gaps are not foolproof, and there are still risks associated with relying solely on air gaps to protect against ransomware attacks. For example, if an attacker gains physical access to an air-gapped system, they may be able to infect it with malware or exfiltrate data from it. Additionally, human error or insider threats can also compromise the effectiveness of air gaps.

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



Design for Prevention & Recovery

Backup & Restore

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

- **Backup:** A backup is a copy of your data and applications that are stored separately from your primary systems. Backups can be created at regular intervals, such as daily or weekly, and can be stored on different types of media, including disk, tape, or cloud storage. In the case of a ransomware attack, having a recent backup can be the key to recovering your data without having to pay a ransom.
- **Restore:** Restoring data from a backup involves copying the data from the backup storage and returning it to its original location. This can be done using a variety of tools, depending on the type of backup and the systems being restored. It is important to test the restore process regularly to ensure that backups are working correctly and can be used in the event of a disaster.

In addition to traditional backup and restore solutions, there are also specialized tools and services available for ransomware recovery. These include:

- **Immutable storage:** Some backup solutions like VMware Cloud Disaster Recovery offer immutable storage, which means that once data is written to the backup, it cannot be modified or deleted. This can help protect against ransomware attacks that try to delete or encrypt backup data.
- **Snapshot-based backups:** Some backup solutions use snapshots like VMware Site Recovery Manager and VCDR to capture point-in-time copies of data. This can be helpful in recovering from ransomware attacks that affect a specific point in time.
- **Cloud-based recovery services:** VMware offers VMware Cloud Disaster Recovery, a cloud-based recovery service that can help recover data and systems quickly in the event of a ransomware attack. These services include features such as virtual machine replication and failover, so that critical systems can be restored quickly.

Regular testing of the restore process is essential. Specialized tools and services, such as immutable storage, snapshot-based backups, and cloud-based recovery services like VMware Cloud Disaster Recovery, can help provide additional protection against ransomware attacks. Through these solutions, organizations can enhance their data recovery efforts, restore critical systems quickly, and mitigate the impact of ransomware attacks without paying the ransom itself.

Snapshots & Clones

VMware vSphere Snapshots and Clones, as well as snapshots taken on storage arrays, can be helpful in mitigating certain types of risk. For example, failed application upgrades can be rolled back quickly if a snapshot was taken prior to the work. However, snapshots and clones do not automatically meet the criteria for a backup, as they are not stored separately from the primary copy of the workload.

Replication vs. Backups

Replication and backups are two different approaches to protecting data and ensuring business continuity.

Replication involves creating a copy of data and keeping it synchronized with the original data in real-time or near real-time. The primary use case for replication is to provide high availability (HA) and minimize downtime in case of hardware or software failures, network outages, or disasters. With replication, the replicated copy of data can be quickly activated and used in case of a failure, minimizing the impact on the business. However, the replicated copy will usually also contain malware, and possibly the effects of the ransomware attack, too, as the replication works to maintain nearly real-time copies of the data.

Backups involve creating periodic copies of data and storing them in a separate location, typically on a different storage medium. Backups are primarily used for data protection, data recovery, and long-term retention. Backups allow businesses to restore data to a specific point in time, which can be useful in case of data corruption, accidental deletion, and ransomware scenarios. Backups are not usually as close to real-time as replicated data.

Backup will be the most likely method of recovery from a ransomware attack, but more sophisticated ransomware can be present for an extended period, infecting backups before the ransomware attack occurs.

While replication and backups have different use cases, they can complement each other in a comprehensive data protection strategy. For instance, replication can provide near-zero RPO (recovery point objective) and RTO (recovery time objective) for mission-critical workloads, while backups can provide long-term retention and an additional layer of protection against data corruption, deletion, or ransomware attacks.

It is worth noting that replication and backups also differ in terms of cost, complexity, and scalability. Replication solutions are typically more expensive and require more infrastructure resources, while backup solutions can be more affordable and easier to manage. Additionally, while replication is well-suited for protecting active workloads, backups are useful for protecting both active and inactive workloads, such as archived data or applications that are no longer in use.

Immutable Backups

Immutable backup copies are backup copies of data that cannot be changed or modified in any way once they are created. This is achieved by using technologies such as Write Once Read Many (WORM) storage devices or immutability features in backup software.

Immutable backup copies are essential to protect against data loss or corruption caused by malware, ransomware, or other cyber threats. By making sure that backup copies cannot be modified, organizations can ensure that they have a clean and secure copy of their data that can be used to restore systems in the event of an attack.

In addition to protecting against cyber threats, immutable backup copies can also help organizations comply with data retention policies and regulations. By ensuring that backup copies cannot be deleted or modified, organizations can demonstrate that they have a complete and unaltered copy of their data for the required retention period.

Immutable backup copies are an important component of a comprehensive data protection and ransomware recovery strategy. Organizations should implement them as part of their backup and recovery plans.

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 like downloading specific operating system media, transferring it 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 media and virtual machine templates. Content Libraries can be subscribed to each other, meaning that a primary 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 protect a computer's boot process from malware and unauthorized tampering. It achieves this by requiring all firmware components and operating system bootloaders to be digitally signed with a trusted certificate. During the boot process, the UEFI firmware verifies the signatures of these components against a built-in database of trusted certificates to ensure their authenticity. If any component fails this verification, the boot process is halted, preventing potentially harmful software from executing. UEFI Secure Boot is beneficial because it provides a crucial layer of protection against low-level threats that could otherwise compromise the system from the very beginning, thereby improving the overall security and integrity of the computing environment. As for ESXi, it can be easily enabled for a virtual machine through the VM settings.

vTPM & Security Devices

A Trusted Platform Module (TPM) is a specialized hardware component designed to enhance the security of a computer system by providing a secure environment for cryptographic operations and secure storage of sensitive information, such as encryption keys, passwords, and digital certificates. TPMs are usually embedded as dedicated microcontrollers on the motherboard or integrated into the processor itself. They offer a range of security features, including hardware-based encryption, secure key generation, and attestation of system integrity. The primary advantage of using a TPM is that it protects sensitive data and cryptographic operations from software-based attacks, as the data never leaves the secure confines of the TPM. This helps ensure the confidentiality and integrity of critical information, making it more difficult for unauthorized parties to access or tamper with the data. Additionally, TPMs can facilitate secure boot processes, remote attestation, and platform authentication, further enhancing overall system security.

VMware vSphere offers virtual TPMs (vTPMs) to workloads, backed by VM Encryption for data-at-rest security. These virtual TPMs enable guest OS features such as Microsoft Device Guard, Credential Guard, BitLocker, Windows Hello, Measured Boot, and more, and are often required as part of advanced security and regulatory compliance efforts. Ensure that your restore target environments support restoring these types of workloads, and that the key provider for VM Encryption is available and configured for use.

Service Startup

Where possible, workloads' services should be configured to start automatically. This has positive effects on recovery times, allowing application administrators to focus on more complex workloads during the recovery process. It also aids many day-to-day operations, too. VMware vSphere High Availability events are less impactful when workload services automatically restart, as is automated patching of operating systems. When everything restarts automatically and gracefully, there is much less friction in updating workloads, which in turn removes vulnerabilities and helps deter attacks.

Additionally, periodic reboots from patching processes ensure that Secure Boot can detect 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 prior to a full ransomware attack.

Data Volumes vs. Operating System Volumes

Breaches often involve the installation of malware and corruption of workload operating systems and may require restoring a workload twice: once to get a clean operating system version, and another time to restore data according to the RPO. Organizations that separate their workload data from operating system data using additional virtual hard disks (VMDKs) have 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 enable application mobility:

- **Segmentation:** Segmenting the network into smaller subnets can help contain the spread of ransomware in case of an attack. By isolating critical applications and their associated infrastructure, it becomes more difficult for ransomware to spread throughout the network. This can be achieved by using technologies such as VLANs or software defined networks like VMware NSX micro-segmentations technologies.
- **Load Balancer:** The VMware NSX Advanced Load Balancer can isolate 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 isolate applications with the use of pools that only the load balancer should communicate with, limiting direct access to the application. IP pools also allow the backend applications to be moved without disrupting services.

- **Network Access Control (NAC):** NAC solutions can be used to enforce policies around network access and ensure that only authorized devices are allowed on the network. This can help prevent ransomware from spreading by limiting the number of devices that can access critical applications and infrastructure.
- **Virtual Private Network (VPN):** Implementing a VPN can help protect applications from ransomware attacks by ensuring that all traffic between sites is encrypted. VPNs can also be used within a private network to limit access between critical infrastructure.
- **IP Address Management (IPAM):** Implementing a centralized IPAM solution can help prevent ransomware attacks by ensuring that all IP addresses are tracked and managed properly. With centralized IPAM, administrators can quickly identify rogue devices and IP addresses that are not authorized, which can be an indicator of a ransomware attack.

An effective IP addressing strategy is crucial for ensuring failover and business continuity in the event of unforeseen network disruptions or system failures. By employing a well-planned IP addressing scheme, administrators can facilitate seamless failover mechanisms, enabling rapid transfer of network services to redundant systems and minimizing downtime. A strategic IP addressing approach also simplifies network management and supports efficient allocation of resources, which in turn enhances overall network performance and resilience. Furthermore, a robust IP addressing strategy promotes business continuity by enabling quick recovery and maintaining the availability of critical services, ensuring that organizations can continue to operate with minimal disruption and safeguard their long-term success.

Remote Access

Maintaining remote access to workloads during a disaster recovery or business continuity event can pose several challenges, particularly in terms of managing firewall rules, VPNs, and access control mechanisms that rely on fixed IP addresses. Failover scenarios may involve updating and modifying 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, application mobility needs, and 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. 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 allowed access to workloads.

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 may exist should be examined in the context of failover and application migration.

Cloud DNS

Cloud DNS offerings are attractive as a 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, they, too, 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 as to 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, and increase 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.

Network Segment Design & Firewalling

VMware NSX is a robust network virtualization and security platform specifically designed 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.

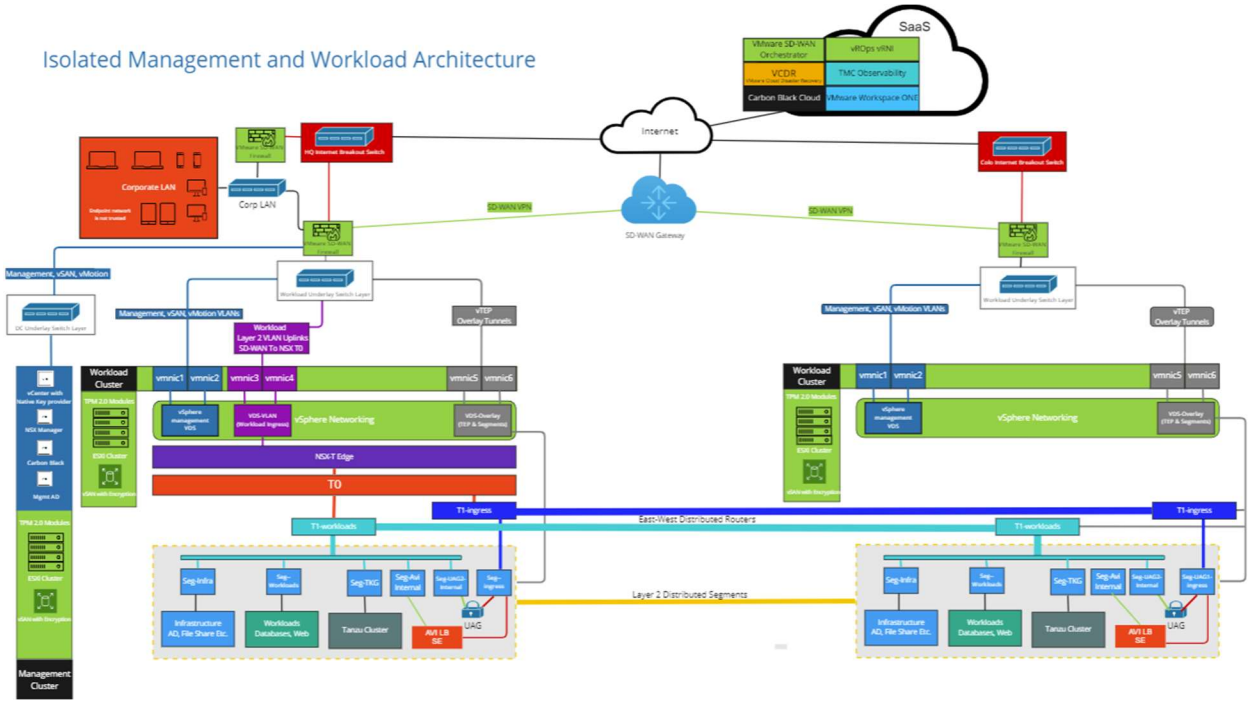
The NSX Distributed Firewall (DFW) facilitates both Macro-Segmentation (Security Zones) and Micro-Segmentation, delivering comprehensive L2-L7 East-West visibility and enforcement with automated policy formulation. Various segmentation strategies, including Zone Segmentation, VLAN Segmentation, Application 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 in transit. The use of 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 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 network traffic through a network security stack. As NSX is incorporated 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 share any common infrastructure or networks, further bolstering security measures.



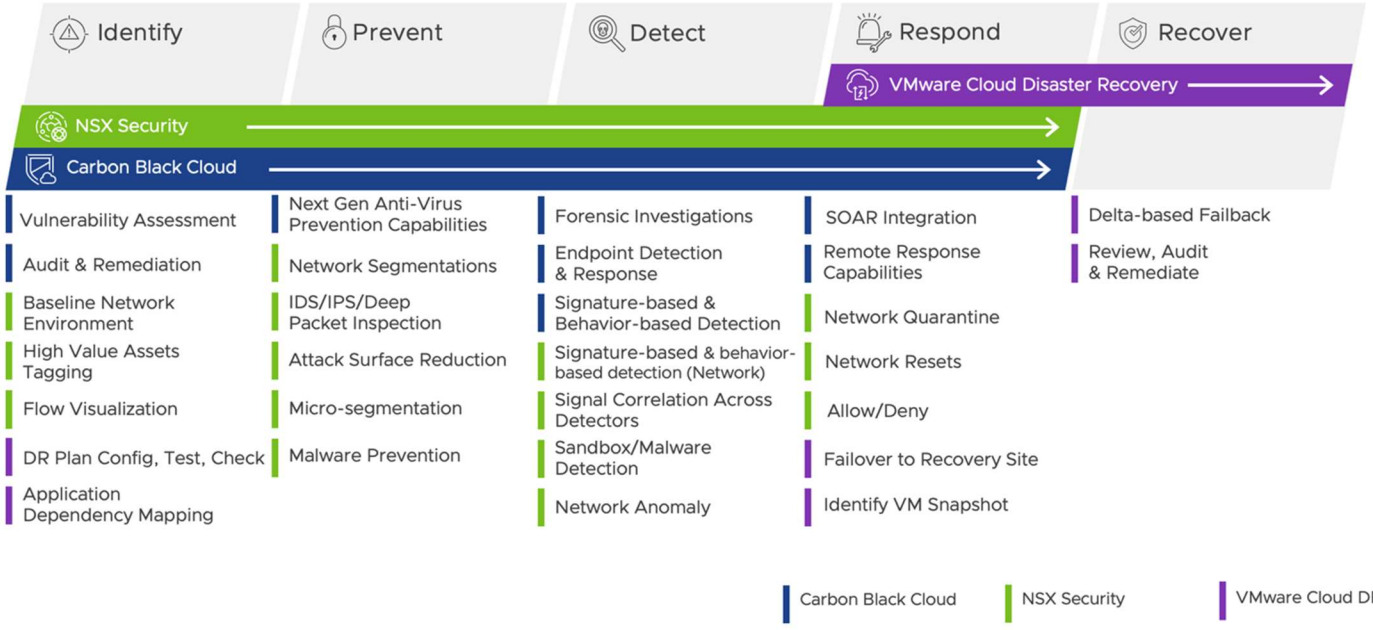
Detection & Response

Detection, response, and recovery capabilities for workloads inside a VMware environment are robust, ranging from simple reversion of snapshots to elaborate orchestrated failover to alternate sites. There are a variety of tools available to VMware customers to help handle 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 help organizations detect ransomware early, minimize the damage caused by an attack, and recover from the attack as quickly as possible. The key components of a ransomware detection and recovery strategy include:

- **Prevention:** The first line of defense against ransomware is prevention. This includes measures such as keeping systems and software up to date, implementing security best practices, and training employees on how to recognize and avoid phishing attacks.
- **Detection:** Ransomware detection and recovery rely on advanced detection tools to identify ransomware attacks. This includes endpoint protection solutions that use behavioral analysis and machine learning algorithms to detect anomalous behavior and prevent the spread of ransomware, like VMware Carbon Black and Workspace ONE.
- **Response:** Once ransomware has been detected, a quick and effective response is critical to minimizing the damage. This includes isolating infected systems, quarantining affected files, and taking steps to prevent the spread of the ransomware to other systems.

VMware has a comprehensive software stack for ransomware detection and recovery, from virtualization, backup and recovery, monitoring, detection, network isolation protection, to 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 uses a single lightweight sensor and an easy-to-use console

in order to understand attackers' behavior patterns, enabling real-time detection and prevention of never-before-seen attacks, and alerting IT staff quickly to anomalous behavior.

Behavioral analysis lies at the foundation of VMware Carbon Black Cloud, ensuring the best possible security by understanding how attackers operate. Most endpoint security solutions only record data when they deem an activity as suspicious, often missing earlier activities that are essential for determining the root cause. In contrast, VMware Carbon Black Cloud continuously monitors and analyzes endpoint activity, regardless of whether it appears benign or malicious.

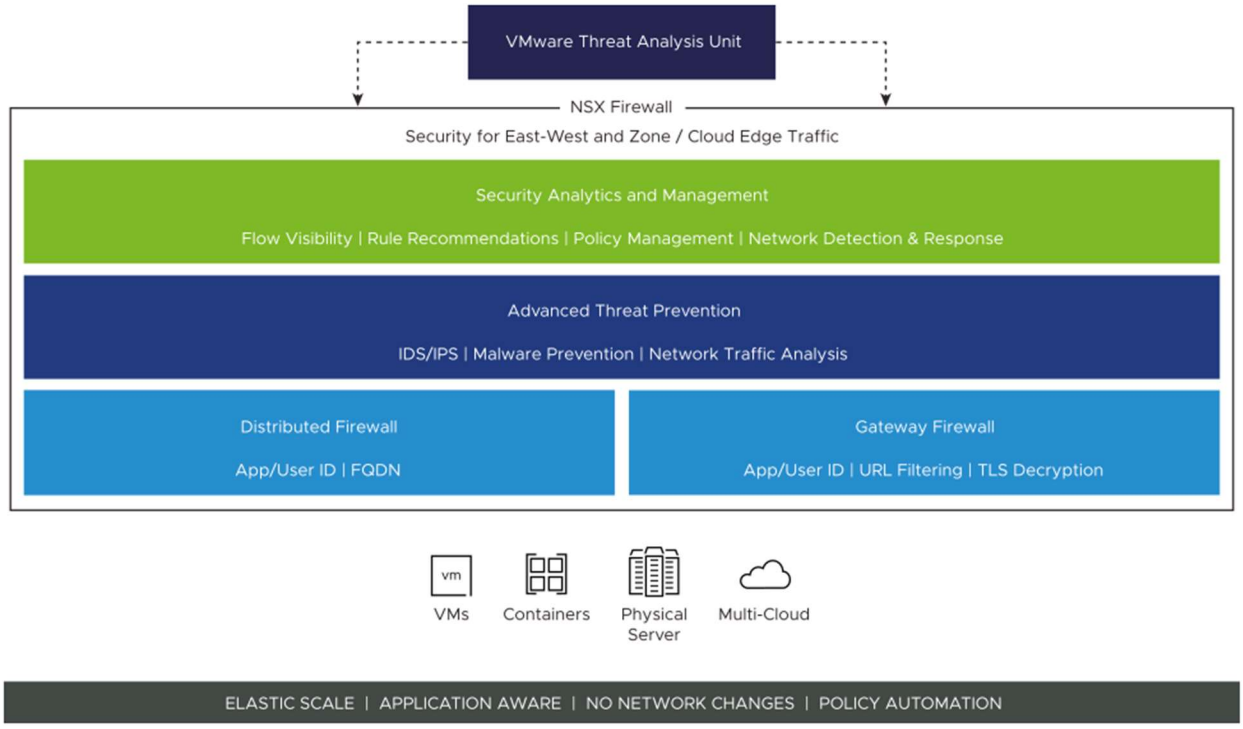
In addition to its advanced detection and prevention capabilities, VMware Carbon Black Cloud features built-in response capabilities within the console, significantly reducing the time to resolution. The platform allows administrators to search and filter events across the environment for the past 30 days, providing the necessary data for thorough investigation. Furthermore, the alert visualization feature presents an easy-to-understand view of events occurring during an attack, enabling security teams to quickly assess the situation and take appropriate action.

VMware Carbon Black Cloud caters to various needs, offering out-of-the-box protection for those who prefer a "set it and forget it" approach, as well as highly customizable policies. Supporting a wide range of endpoint and workload operating systems across diverse environments, VMware Carbon Black Cloud stands as a comprehensive and proactive defense mechanism, safeguarding organizations' critical data and systems from ever-changing cyber threats.

Intrusion Detection & Protection

Intrusion detection and prevention systems (IDPS) play a critical role in detecting attacks in progress. These systems continuously monitor network traffic and activities for malicious patterns, anomalous behavior, or known attack signatures, enabling the early detection of potential threats. By identifying and containing breaches in their initial stages, IDPS can significantly reduce the potential impact of an attack, limiting the spread of malware across the network.

During the recovery process from a ransomware attack, an effective intrusion detection and prevention system (IDPS) serves as a valuable tool in mitigating further damage and facilitating swift remediation. By providing real-time threat intelligence and



comprehensive visibility into the attack, an IDPS assists security teams in tracing the source of the infection, identifying vulnerabilities, and implementing appropriate countermeasures. Furthermore, intrusion prevention capabilities can block ongoing attempts to exploit the same vulnerabilities, ensuring that the organization can recover from the attack with minimal disruption and reduce the likelihood of future ransomware incidents. An IDPS offers 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 vRealize Log Insight is a powerful log management and analysis solution that enables organizations to gain real-time visibility into their infrastructure, applications, and security events. By collecting, centralizing, and analyzing log data from various sources across the IT environment, vRealize Log Insight helps security teams proactively detect potential attacks and breaches in workloads. Its advanced analytics and machine learning capabilities can identify patterns and anomalies that may indicate malicious activities, enabling security staff to quickly respond to emerging threats.

In addition to its detection capabilities, vRealize Log Insight also features customizable alerting, which ensures 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 likelihood of overlooking critical security events. Furthermore, vRealize Log Insight's integration with other VMware solutions, such as NSX and vRealize Suite, streamlines the monitoring and management process, allowing organizations to maintain a comprehensive security posture for their workloads.

To ensure that workloads have log forwarding agents installed and operating, and that they have access to log collectors in both their primary and failover locations, organizations should implement a robust log management strategy. Additionally, the log management systems should be hardened, 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 you can recover your data in case of an attack. However, not all backup copies can be trusted in the case of ransomware.

Typically, ransomware will target your most recent backups first, so it's crucial to have multiple backup copies, including older copies that were taken before the ransomware attack. It's also important to ensure that your backup copies are stored in a separate location, away from your production environment, so that they cannot be encrypted by the ransomware attack.

You should have a consistent process in place to test your backup and restore processes regularly to ensure that your backup copies are reliable and can be used to recover your data successfully. It is important to implement a backup strategy that provides immutable backups, meaning that backup data cannot be modified or deleted, providing an additional layer of protection against ransomware attacks.

When restoring data and services from a ransomware attack, it is recommended to use an isolated environment first to test the recovery process and to scan for ransomware before moving data, applications, and services back into production.

Failover vs. Restore

Failover and restore 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 restore recovers data or systems from a backup after an unexpected event. Failover aims to minimize downtime, while restore is a reactive approach to return affected systems to their previous state. Both are essential in minimizing the impact of unexpected events on operations, such as a ransomware attack. During an incident, your organization may need to decide which path to take.

vSphere Replication

VMware vSphere includes VMware vSphere Replication, which enables organizations to replicate workloads to an alternate site or cluster, managed directly from the VMware vSphere Client. These capabilities are managed manually and do not include the more advanced orchestration capabilities built into 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 helps 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 provide 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 quickly and easily 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 take 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 use 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 and will likely not protect from a ransomware attacks, as the replication can help spread the 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 used to have different version of the recovery state to get to a clean running version. The environment will likely be out of date though so another backup and recovery method will also need to 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 brought up to date and used for recovery. This approach provides a balance between cost and recovery time but may result in data loss. This can be effective ransomware recovery 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 rebuilt. This approach is the most cost-effective but has the longest recovery time and can result in significant data loss. This can be a very effective for ransomware recovery as the cold environment can be tested and kept in a known clean good 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 take place.

- **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 be aware of an attack before it happens.

Organizations should choose the proper 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 played out separately to make sure there is a fully comprehensive strategy for each situation.

VMware Cloud Disaster Recovery

VMware Cloud Disaster Recovery is a disaster recovery solution offered by VMware that provides 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 remain available in the event of a disaster.

The solution offers continuous replication and snapshots of the replicated backups, allowing customers to choose from many recovery points in the event of a ransomware attack. Customers can also create and test recovery plans and failover to the cloud with just a few clicks, providing a quick and reliable way to recover in the event of a disaster.

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

VMware Cloud Disaster Recovery is offered as a subscription-based service and requires a VMware Cloud on AWS subscription. The solution is designed to be easy to set up and manage and can be integrated with other VMware products and services.

VMware Cloud Disaster Recovery Pilot Light

VMware Cloud Disaster Recovery (VCDR) Pilot Light is a disaster recovery strategy that leverages cloud-based infrastructure to ensure rapid recovery of critical IT services in the event of a disaster. The Pilot Light approach involves keeping a minimal set of infrastructure and resources running in the cloud, ready to be activated in the event of a disaster.

In the context of VCDR, the Pilot Light approach involves 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, using minimal resources and incurring minimal costs. However, in the event of a disaster, the Pilot Light VMs can be quickly activated, 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 allow 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 provisioned 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 robust defense against ransomware threats. Additionally, it is crucial to maintain up-to-date backups, implement micro-segmentation, and use advanced threat prevention techniques to secure the virtual environment. By investing in 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.

Additional Resources

More resources covering ransomware preparedness, for both workloads and infrastructure, can be found at:

https://core.vmware.com/ransomware

In addition, VMware produces security hardening baselines and other security materials, how-tos, discussions, and guidance for vSphere and other cloud infrastructure products. You can find these materials at:

https://core.vmware.com/security

Thank you for prioritizing security in your environments.

Feedback

We appreciate feedback from our readers. If you have any thoughts, suggestions, or insights to share after reading this whitepaper, we encourage you to reach out to us. Your input plays a crucial role in helping us continually enhance the quality and relevance of our guidance and documentation.

Most VMware resources have a feedback mechanism on the web page where the content is found. This is true for this document, too:

https://core.vmware.com/ransomware-defense-and-recovery-strategies

Using this method helps ensure that both the authors and the relevant content team receive your comments. Thank you!

About the Authors

Jerry Haskins is a Solutions Architect responsible for collaborating on products within the VMware Partner Solutions Engineering Team in VMware's Office of the CTO. With over 20 years of experience in the IT industry, he has spent his career in innovative roles managing enterprise networks and data centers, working with virtualization technologies, microservices, CI/CD workflows, and HPC solutions.

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

Dale McKay is a Staff Technical Marketing Architect in the Network and Advanced Security group at VMware, specializing in security, virtualization, and networking. He has extensive experience implementing cybersecurity policies and procedures to meet client needs and building strong relationships with customers. As a technology evangelist and strategist, Dale's expertise is invaluable in delivering effective solutions to his clients.