VMware for Secure Government

Enforcing a Zero Trust Ransomware Defense

Nicholas Morpus

Get Started

vmware®

The Evolution of Malicious Actors

"Malicious cyber activity has evolved from nuisance defacement to espionage and intellectual property theft, to damaging attacks against critical infrastructure, to ransomware attacks and cyber-enabled influence campaigns designed to undermine public trust in the foundation of our democracy."

– National Cybersecurity Strategy 2023

As the National Cybersecurity Strategy indicates, cybersecurity is rapidly evolving from minor nuisances into a serious national security concern. Sensitive data, crucial national infrastructure, national defense resources, and major pillars of the U.S. economy are all targets of internal hacking groups as well as foreign actors.

Several alleged state-sponsored attacks have made headlines recently, highlighting the need to improve federal, state, and local cyber defenses. Two of these attacks, the SolarWinds hack and the Office of Personnel Management (OPM), stand out as examples of foreign states breaching highly sensitive government systems and resources.

The Significance of the SolarWinds Breach

The SolarWinds hack was a highly sophisticated cyber-attack that targeted SolarWinds, a leading provider of network management software. The attack was carried out by a state-sponsored group and it impacted numerous US government agencies and private companies.

By inserting malicious code into SolarWinds' Orion system, attackers were able to gain access by targeting this third party and building a backdoor that allowed them to access the systems of victim organizations. This method allowed attackers the ability to move throughout target systems undetected by impersonating user accounts, disguising their behaviors as legitimate traffic.

The implications of the SolarWinds hack are significant, as it demonstrated the ability of highly skilled cyber actors to infiltrate even the most secure networks. The old ways of protecting the perimeter and scrutinizing packets moving in and out of that perimeter are no longer enough. The SolarWinds hack exposes the need for smarter, context-aware security systems that evaluate user and device posture and behavior, as well as lateral protections that prevent movement even if attackers gain access.

The attack exposed significant vulnerabilities in the supply chain, highlighting the need for increased scrutiny of third-party vendors and their security practices. This raises concerns about cyber-attacks potential to disrupt critical infrastructure, including energy grids and financial systems.

The SolarWinds hack showed that no organization is immune to cyber-attacks and that even organizations with advanced security measures can be compromised.

The Significance of the OPM Breach

The Office of Personnel Management (OPM) hack was a significant data breach that occurred in 2015 and impacted over 20 million current and former US government employees. Setting the stage, the OPM hack remains one of the largest and most significant data breaches in US history. It is believed (but not confirmed) that the attack was carried out by state-sponsored hackers, who were able to steal sensitive personal information, including Social Security numbers, employment histories, and security clearance information.

These attackers were able to gain access to the OPM network by means of stolen credentials and once inside, they installed a backdoor that allowed them to come and go undetected. Like the SolarWinds hack, The OPM breach is a textbook example of the lack of security infrastructures for preventing lateral movement and evicting attackers abusing legitimate ports and protocols. Without contextually aware security solutions, detection capabilities, and expansive threat intelligence, the largest hurdle hackers face is the initial breach. But once inside, they are given a free stay and take whatever they want without consequence.

The OPM hack exposed sensitive information that could be used for identity theft, espionage, or other malicious purposes. The breach also highlighted the need for increased investment in cybersecurity and improved security practices across all government agencies.

This is the New Normal

Unfortunately, ransomware is the new normal and this threat is here to stay. As workloads are provisioned across heterogeneous environments and networks become more complex, the attack surface will continue to expand. This means threat actors are finding new ways to exploit vulnerabilities and inefficiencies in existing government defenses, either via machines or people.

Once threat actors breach your perimeter defenses, they move laterally through legitimate ports and protocols to not only exfiltrate or ransom resources but to stay within networks for extended periods of time.

Ransomware Facts

1. A ransomware attack occurs every 11 seconds[1]
2. 44% of intrusions perform lateral movement[2]

1. Cybersecurity Ventures. “Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) By 2021.” Steve Morgan, October 21, 2019
2. VMware Contexa

Federal Directives on Cybersecurity

The federal government has put forward multiple directives and guidance materials to strengthen the cyber defenses of the United States for both the private and public sectors. These include:

- National Cybersecurity Strategy 2023 – White House
- Executive Order on Improving the Nation's Cybersecurity - CISA
- NIST Special Publication 800-207 – Zero Trust Architecture

Out of these three guidance materials, we've distilled four distinct initiatives called out by the federal government:

1. Implement Zero Trust Architecture (NIST 800-207)
2. Improve Detection of Cyber Threats on Federal Government Networks
3. Improve Investigative and Remediation Capabilities
4. Implement Ransomware Defenses

These initiatives cover the bases for updating legacy cybersecurity practices in favor of modern, cloud-smart, and resilient defensive strategies needed to tackle the threats of today and tomorrow.

Initiative 1

Implementing Zero Trust Architecture

The day-in and day-out activities of the Federal government deal with unimaginable amounts of sensitive information, tools, resources, and systems. Everything from social security and critical infrastructure to governance and national defense relies on the security of those systems, tools, and data.

The protection of the federal cyber infrastructure is paramount to the safety, security, and continuing prosperity of the United States, and with the evolution of cyber threats, the legacy security methods we've come to know simply aren't enough anymore.

Zero Trust: A New Security Mindset

Government security is thoroughly wrapped up in identity: who is accessing what, when, where, why, and how. Government buildings rely on clearances, badges, guards, and verifications. Nothing is left to chance, and no one is given the benefit of the doubt. Our federal cyber strategy must be built on this foundation as the bedrock principle of "Zero Trust ."

Put simply, Zero Trust means no user, device, or application is trusted to access sensitive resources. Any and everything that wishes to access a specific resource must:

1. Provide validation of identity and access level
2. Continuously provide that validation while resources are accessed

Just as the name suggests, there is no implied trust of any user, device, or application seeking access to resources.

Let's dive deeper and clearly understand what Zero Trust means. NIST SP 800-207 lists seven specific tenets that must be followed to adhere to a true Zero Trust model:

1. **All data sources and computing services are considered resources:** In this case, anything owned and operated by a government agency must fall under the Zero Trust paradigm in order to maintain a secure environment. This includes all kinds of devices (computers, smartphones, routers, switches, servers, smart devices, etc.), software as a service (SaaS) applications, VOIP networks, security grids, and any other technology that functions within the agency. This even includes personal devices that can access government resources.
2. **All communication is secured regardless of network location:** Traffic must be subject to the Zero Trust framework, no matter where network communication occurs whether it is remote or on-premises. Continuous authentication is necessary from any location.
3. **Access to individual enterprise resources is granted on a per-session basis:** This tenet is based on the principle of least privileged access. Each granted session is given to a user only with the least privileges necessary to complete the task at hand.

4. **Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes:** Access to resources must be given only under certain contexts that take into account factors such as the device used to access them, the time and date of the request, previously observed behavior, credentials, network location, device analytics, and many others. These contexts are measured up against a set of allowable access rules set by the government agency.
5. **The enterprise monitors and measures the integrity and security posture of all owned and associated assets:** As the name implies, in a Zero Trust framework, no user, device, or other asset is inherently trusted. The security posture of every asset must be evaluated and measured up against the policy rules before access is granted.
6. **All resource authentication and authorization are dynamic and strictly enforced before access is allowed:** Zero Trust is a continuously verifying process that requires a constant cycle of identity verification, anomalous activity monitoring, and policy enforcement.
7. **The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture:** The continuous collection of information regarding assets and resources allows for baselining and security policy improvement.

Zero Trust isn't any one tool, policy, device, or solution. Zero Trust is a mindset and security philosophy that is all about continuous verification. Zero Trust will help government agencies protect their resources from insider threats as well as outside attackers. The need for continuous verification coupled with contextual access policies guards resources from outside threat actors as well as insiders looking to access and exfiltrate sensitive materials.

Initiative 2

Improving Detection of Cyber Threats on Federal Government Networks

When dealing with cyber threats, it's far more beneficial to detect and prevent threats, rather than react to an attack after it is already in progress. Old defensive strategies include basic firewalls, packet inspection, access control lists, and other legacy perimeter security strategies. While these strategies still have their place and must be maintained, there are newer attack vectors that must be addressed using modern protections.

Attacks are increasingly relying on legitimate ports and protocols to circumvent these legacy defenses. Not only are attackers getting through defenses through legitimate means, but they're also setting up shop within networks for extended periods of time, moving laterally throughout the infrastructure.

Baselining Government Networks

Network baselining is a critical process in network security that involves establishing a baseline of normal network activity. Organizations can identify patterns and establish a baseline of normal activity by monitoring network traffic and collecting data on network behavior. This baseline can then be used as a reference point for detecting anomalous behavior that may indicate a potential security threat.

The importance of network baselining lies in its ability to provide visibility into the network and enable the identification of deviations from normal behavior. This can help organizations detect potential threats in real-time and respond quickly to mitigate any potential damage.

Additionally, network baselining will help government agencies optimize their network performance by identifying areas where improvements can be made. By understanding the normal patterns of network traffic, organizations can identify areas of congestion or bottlenecks and adjust to improve network performance.

Better Visibility and Protection with IDS/IPS Packet Inspection

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are crucial security tools that can help protect against ransomware attacks. IDS/IPS systems work by monitoring network traffic for signs of suspicious activity and alerting security teams to a potential attack and actively blocking the traffic to prevent the attack from occurring.

By providing real-time threat detection and prevention capabilities, IDS/IPS systems play a critical role in protecting organizations from ransomware attacks and minimizing the impact of any successful attacks that do occur.

Chances are that most (if not all) government networks utilize some form of IDS/IPS solution at the perimeter. While this prevents intrusions at that point, what is to stop attackers from moving about the network if they make it past the outer perimeter?

Government agencies need to rethink the way IDS/IPS is structured in favor of a virtually distributed system. A software-defined distributed IDS/IPS eliminates the tradeoff between security and operational complexity by moving traffic inspection to every individual workload, rather than relying on hair pinning the traffic flow to a traditional firewall with IDS/IPS.

Not only does this reduce the complexity of the security infrastructure by eliminating the need for additional hardware-based firewalls, but also creates operational efficiency through centralized management of inspection policies.

The Need for AI and Machine Learning in Threat Detection

The legacy methods for threat detection relied on signature-based detection, packet capture and evaluation, manual policy setting, and other inefficient security practices. These methods simply aren't enough to prevent the sophisticated and modern attacks facing federal agencies today. Foreign states and other threat actors are employing complex attack strategies that include botnets, evolving malware codes, and other methods that evade known signature-based detection and remediation.

Artificial Intelligence (AI) and machine learning have become increasingly important tools in cybersecurity threat detection. AI and machine learning algorithms can analyze large amounts of data and identify patterns that may indicate the presence of a cyber threat. These algorithms can learn from threat intelligence data and adapt to new threats, making them highly effective at detecting and preventing attacks. For example, AI-based threat detection systems can analyze network traffic and detect anomalous behavior that falls outside of known threat signatures to enact preventative measures that stop an attack in its tracks.

Additionally, AI and machine learning algorithms can be used to identify and prioritize vulnerabilities in a system, allowing organizations to proactively address these issues before they can be exploited by cybercriminals. By leveraging AI and machine learning in cybersecurity threat detection, organizations can improve their overall security posture and reduce the risk of successful cyber-attacks.

Initiative 3

Improve Investigative and Remediation Capabilities

While it is always best to prevent attacks before they happen, there are times when defenses fail and cyber teams are faced with the challenge of stopping an attack in progress or picking up the pieces after a breach. Investigative and remediation capabilities provide agencies with the tools they need to stop cyber threats as they happen and plan out more robust defenses after the fact. After all, the more knowledge and preparation, the easier it is to stop future attacks before they begin.

Decrease Time-to-Resolution with Network Detection and Response (NDR) , Network Traffic Analysis (NTA), and Sandboxing

Network Detection and Response (NDR) is essential to modern cybersecurity strategies. NDR solutions provide real-time visibility into network activity, allowing organizations to quickly detect and respond to potential security threats. By monitoring network traffic, NDR solutions can identify anomalous behavior that may indicate a potential threat, such as malware infections, unauthorized access attempts, or data exfiltration. This information is then analyzed to determine the severity of the threat and initiate a response.

The importance of NDR lies in its ability to detect threats that may have gone unnoticed by traditional security measures, such as firewalls or antivirus software. NDR solutions provide a comprehensive view of network activity, allowing organizations to quickly detect and respond to potential threats before they can cause significant damage. Additionally, NDR solutions can provide valuable insights into network performance, identifying areas where improvements can be made to optimize network performance.

While legacy NDR employs signature-based detection to identify threats, modern NDR also utilizes network traffic analysis (NTA) to detect anomalous activity and malicious behavior that would otherwise go undetected. Lateral movement is such an anomalous behavior since it utilizes legitimate ports and protocols. NTA allows NDR to contextually read into protocol anomalies, traffic anomalies, and host anomalies to detect this lateral movement and begin the remediation process.

Network sandboxing additional analysis of threats by deconstructing and inspecting files and URLs in a safe environment isolated from your network. This allows security teams the ability to analyze suspicious traffic and allow potential threats to unfold in a safe environment, identify dormant code, and document all of the CPU instructions executed by that code.

Overall, NDR, NTA, and sandboxing are critical components of any agency's cybersecurity strategy, providing real-time threat detection and response capabilities that are essential for maintaining network security in today's rapidly evolving threat landscape. However, part of the power behind these solutions is derived from the threat intelligence that is gathered to detect signature and anomalous-based behavior.

Understand More with Modern Threat Intelligence

Virtualized threat intelligence solutions provide organizations with real-time information on potential security threats, including new and emerging threats, as well as known threats that may have previously gone undetected. This information can be used to enhance security controls and improve incident response capabilities within workloads on a multi-cloud environment.

Threat intelligence solutions provide organizations with real-time analytics of vulnerabilities and threats to networks, endpoints, containers, and virtual machines, enabling them to respond before significant damage is done.

Threat intelligence software can also provide valuable insights into threat actors, tactics, techniques, procedures, and motivations, helping organizations better understand the threat landscape and identify potential vulnerabilities in their systems. This contextual analysis is crucial when developing network baselines and establishing Zero Trust policies that make sense for agency networks.

The Need for Efficient Ransomware Recovery

Recovering from a ransomware attack can be an incredibly difficult and complex process. Even if the ransom is paid, there is no guarantee that the decryption key will work or that the attackers will provide it at all.

In many cases, government agencies may need to rely on backups to restore their data, but these backups may also be compromised if they were connected to the network at the time of the attack. Additionally, restoring data from backups can be time-consuming, and it may be challenging to determine which files were affected and which backups are still viable.

Moreover, if the attackers exfiltrated data before encrypting it, organizations may face the additional challenge of ensuring that sensitive data is not leaked or used for further attacks. Overall, ransomware recovery can be a long and difficult process that requires significant resources and expertise, highlighting the importance of implementing effective security measures to prevent these types of attacks in the first place.

Initiative 4

Implement Ransomware Defenses

Ransomware is the threat du jour of most cybercriminals. The highest-profile attacks that have made national headlines typically involve large companies, but these threats are just as devastating for the public sector, if not more. In their ransomware fact sheet, CISA laid out examples of how ransomware has impacted the public sector, such as one county spending $1 million just to overhaul their equipment and acquire technical assistance, rather than pay the $1.2 million ransom caused by a malicious link.

Lucky for that county, their costs fell on the relatively small side. As of 2022, IBM estimates that the cost of a data breach in the United States costs $9.44 million, which is over twice the global average of $4.35 million.

While money is seemingly no object to the federal government, these numbers mean so much more when impacting state and local governments. Unlike the federal government, which is ostensibly allowed to run a yearly budget deficit, most state and local governments are not. Most state governments are required by law or their own constitutions to balance their yearly budgets. This means that a data breach via ransomware would devastate state governments, especially those already cash-strapped in the aftermath of the COVID-19 pandemic.

The stakes and costs are simply too high for government agencies to go on without an effective ransomware prevention and recovery plan at the network level.

The Power of Microsegmentation

Perimeter defenses are a crucial component of a ransomware defense, but as we all know, they are not impenetrable. It's important that government agencies set up distributed defenses that thwart threat actors that make it past the perimeter and attempt to move about a network laterally.

Microsegmentation is a network security concept that involves dividing a network into small, isolated segments to enhance security, such as at the workload level. With microsegmentation, each segment is sectioned off and all traffic entering and leaving the individual workload is subject to policy enforcement, filtering, and firewalling. This technique provides more granular control over network traffic and reduces the attack surface for potential attackers, reducing the risk of a breach.

Additionally, microsegmentation enables organizations to apply different security policies to each segment, depending on its risk level. For instance, a segment containing sensitive data can have

more stringent security policies than a less critical segment. This improves security posture to better protect against advanced threats like lateral movement, where attackers rely on one-size-fits-all policies to move about the network unimpeded.

Additionally, utilizing microsegmentation in tandem with network detection and response provides SOC analysts with better visibility into network traffic, making it easier to detect and respond to potential threats. Implementing an effective micro-segmentation solution prevents the spread of threats within a network and maximizes the security of government infrastructures.

The Need for Application/API Security in the Era of the Cloud

The widespread adoption of the cloud and web-based applications is a double-edged sword that both boosts efficiency and productivity and opens the door for new security threats. Many web applications and APIs don't offer the necessary protections needed to guard sensitive data.

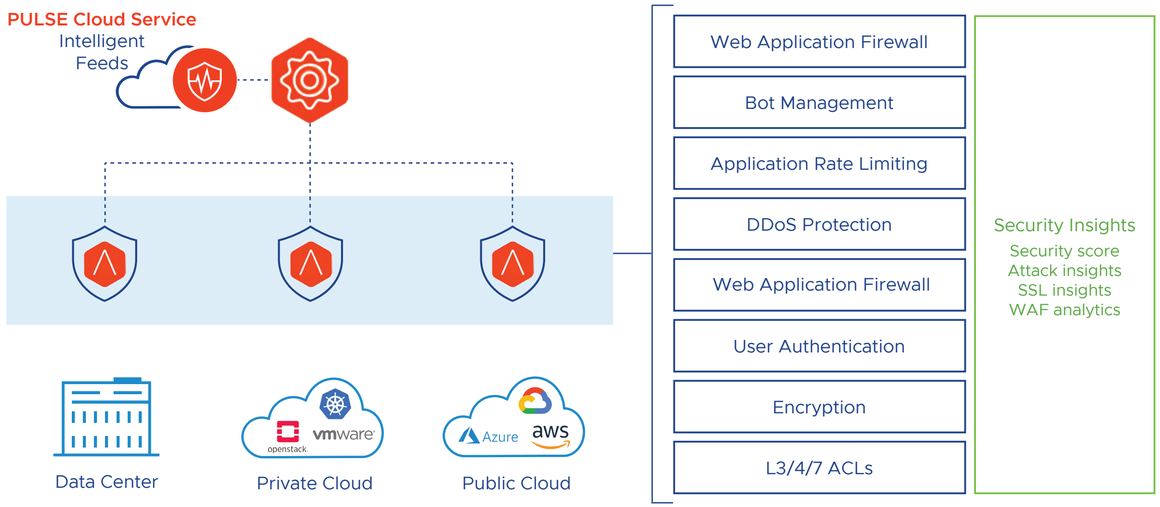

FIGURE 1: Application security solution high level architecture.

Government agencies, just like enterprises, are vulnerable to malware attacks from various sources. The most common ones include email attachments and file-sharing mechanisms. In response, companies have invested considerable resources, amounting to billions of dollars, in email security solutions to identify and isolate suspicious attachments. However, file uploads through web applications represent an additional attack vector that has not been given adequate attention.

A case in point is when corporate recruiters receive resumes with malware as a response to a job posting, which can then be inadvertently shared with hiring managers. To mitigate such risks, enterprises require robust, multi-layered defenses against web application vulnerabilities and cybersecurity threats to safeguard against malicious file uploads, viruses, malware, or other inappropriate content.

Web application firewalls (WAFs) are intended to protect businesses from web app attacks and proactively prevent threats. Yet, despite the potential security benefits, 90% of organizations find it complex to implement WAF solutions for three key reasons:

- **Complicated rule configuration:** Many modern WAFs are complex, requiring administrators to navigate a labyrinth of settings to configure security policies. Fine-tuning rules and customization for each application adds another layer of complexity.
- **Limited visibility and intelligence:** Most WAFs provide little visibility and lack attack behavior modeling and application learning. Once rule sets are established, it is difficult to keep them updated and monitor them in real-time to respond to changes or new security threats.
- **Slow scaling:** Traditional WAFs are inflexible and unable to provide the necessary scalability for growing volumes of encrypted traffic and variable loads. Hardware-based WAFs require significant overprovisioning.

However, there are more advanced web application protections and load balancers that utilize machine learning and other advanced features to provide malware protection, bot detection, signature-based threat detection, and elastic autoscaling to handle attacks. These web application firewall solutions help prevent attacks related to application corruption, denial of service, malware payload delivery used in ransomware attacks, and many others.

The Role of the Cloud Operating Model in the Fight Against Ransomware

The modern network infrastructure employs what is known as a hybrid/multi-cloud structure that utilizes a combination of on-premises private clouds and cloud-native resources. These infrastructures allow government agencies the ability to dip their toes into the capabilities of the cloud but open the door to disjointed security policies, no uniformity in policy enforcement, and a lack of visibility in traffic between these environments. This allows threat actors to slip between the cracks of existing cyber defenses and move laterally about different infrastructures undetected.

The cloud offers uniformity, visibility, and centralized control over your environment, which is an appealing notion when dealing with ransomware. The truth is agencies and enterprises alike are chasing the allure of the cloud operating model while clinging onto legacy hardware that they are reluctant to leave behind.

With that in mind, it's tempting to simply suggest that government agencies relinquish their existing on-premises network hardware in favor of a 100% public cloud-based approach. The problem is that this is an extremely time and resource-intensive process. So what if government agencies could realize the benefits of the cloud without discarding their old hardware and shifting their entire infrastructure to the public cloud?

This is the benefit of the cloud operating model. Introducing a cloud operating model via virtualization allows government agencies to tie together their existing infrastructures under a single unifying system that provides visibility in and between clouds, centralized policy controls, and efficient detection and remediation of threats. Implementation of a cloud operating model allows government agencies the ability to detect, respond to, and even recover from ransomware attacks in record time, all without fundamentally altering the existing network structure.

The power of the cloud operating model makes for the perfect segue into our final section.

How VMware Detects Threats, Prevents Attacks, and Enforces a Zero Trust Ransomware Defense

We've discussed numerous challenges facing government agencies now and, in the future, as well as the solutions needed to address them. The good news is that VMware is uniquely positioned to provide the Zero Trust ransomware defense needed to guard government networks against modern-day threat actors.

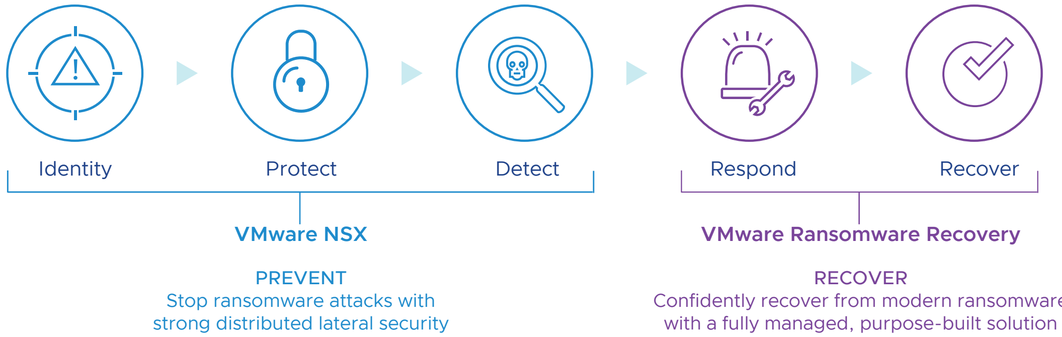

FIGURE 2: VMware delivers a strong defense which addresses the full ransomware protection cycle.

VMware in Government: Tackling Threats and Challenges to the State

VMware NSX consists of security capabilities and controls that prevent intrusion and lateral movement, detect anomalous behavior, and contain and evict threats before any damage is done. We embrace the cloud operating model and enable agencies to see more and stop more with no new network appliances.

Protecting Networks and Applications

NSX provides a baseline understanding of the inner workings of your applications, through deep visibility into traffic flows, connections, related services, and data patterns. Our microsegmentation capabilities allow us to stop the most obvious malicious traffic, but our protection abilities run so much deeper than that.

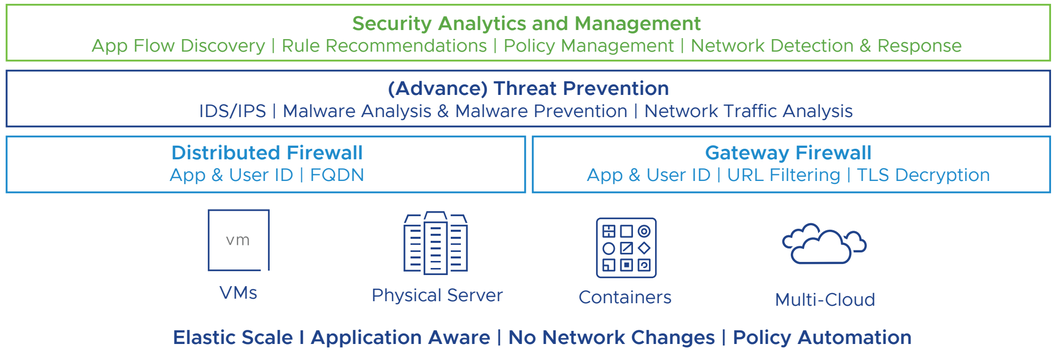

FIGURE 3: VMware Threat Analysis Unit — NSX Security for east-west and zone / cloud traffic.

VMware NSX Security is implemented at the virtualization layer, which allows us to look at the connections being made throughout your network and understand what is happening on those connections. This goes all the way down to the processes used to initiate the traffic. This allows us to capture high-fidelity data and enables our distributed IDS/IPS to analyze these connections for signature-based threats. Combined with our network detection and response, network traffic analysis, and network sandbox in a comprehensive threat Advanced Threat Prevention stack, we provide the detection and remediation capabilities needed to prevent attacks, such as ransomware.

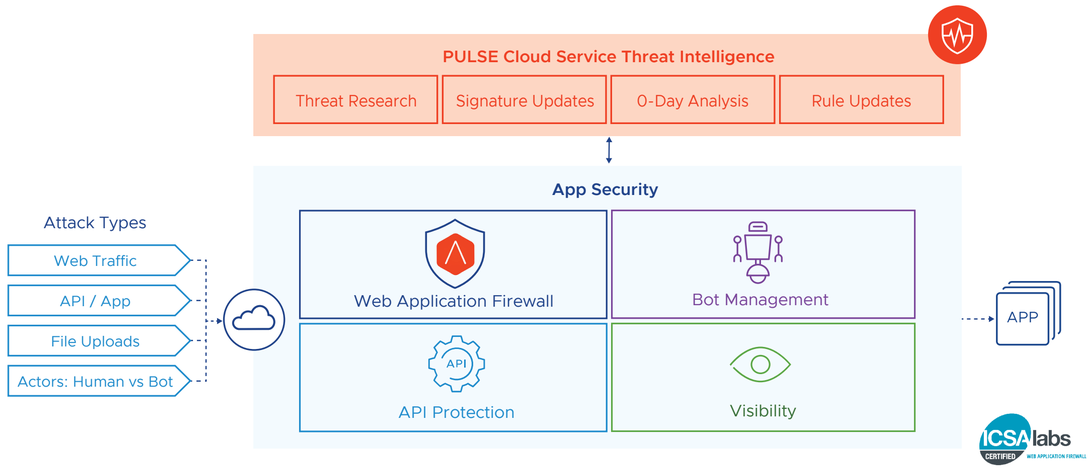

FIGURE 4: Application security solution — protect your application attack surface.

The same goes for web applications and workloads. VMware NSX Advanced Load Balancer provides content-aware web application security to protect against detrimental threats such as log4j and the rest of the OWASP Top 10 attacks. NSX Advanced Load Balancer integrates WAF, L7 DDoS mitigation, bot management, and more with threat intelligence services in a single, scalable platform. Combined with simplified administration through centralized policy management, you can organize operational consistency across all clouds and containers.

The truth is, workloads are more secure on VMware clouds, enabling government agencies the security functions they need to control their multi-cloud environments and prevent lateral movement.

The implementation of VMware NSX allows you to implement a true Zero Trust ransomware defense throughout your network infrastructure that is deployed and managed within a cloud operating model. Embrace full automation and consistent policy enforcement that'll bring your multi-cloud into the modern threat defense landscape.

Confident Recovery from Ransomware Attacks

VMware Ransomware Recovery is a fully managed Ransomware Recovery-as-a-Service solution that enables safe recovery from modern ransomware through behavioral analysis of powered-on workloads in an Isolated Recovery Environment (IRE) in the cloud.

Our guided workflow automation allows customers to quickly identify recovery point candidates, validate restore points using live behavioral analysis, and prevent reinfection with networking isolation capabilities. By boosting the collaboration between security and infrastructure teams, VMware fosters a simplified and frictionless strategy through the adoption of a singular solution that addresses the entire recovery operation.

Call to Action

For more information or a demonstration, contact a VMware representative today.

CONTACT

Get Started Today

Reach out to our sales team for additional info

CONTACT