WHITE PAPER: **June 2024**

Secure your Private Cloud with VMware vDefend™

vmware®
by Broadcom

Securing the VMware Cloud Foundation™ Private Cloud

VMware Cloud Foundation™ makes it possible to transform your data center into a truly modern private cloud by providing self-service consumption and delivery capabilities. For all the benefits that modernizing a traditional virtualized environment into something that's more cloud-like can bring, though, it also requires modernizing your security strategy. Organizations that continue to rely on yesterday's approach to securing their private cloud will find themselves struggling to keep pace with today's increasingly sophisticated threats.

VMware vDefend™ was engineered to deliver granular policy enforcement at scale, detect anomalous behavior, and protect from advanced threats. It secures east-west traffic within the VMware Cloud Foundation™ private cloud. Built from the ground up to work together, VMware vDefend™ offers a plug-and-play experience with VCF.

In a world where breaches continue to become more costly and devastating, it's taking security teams far too long to detect threats that have breached their network's perimeter. Across industries, the average cost of a data breach climbed above $4.3 million in 2023.[1] That same year, the average amount of time elapsing before security teams realized that attackers had gained access to their environment grew to 203 days.[2]

It remains commonplace for security solutions and controls to be deployed at the private cloud's perimeter. For decades, this industry-wide norm was considered a best practice.

But today's threats are bypassing the perimeter at an alarming rate. Once attackers are able to achieve this, flat internal network designs make it easy for them to move laterally across computing environments. In fact, such lateral movement was observed in a full 44% of the breaches studied by VMware's global threat research team in 2022.[3] This is too many: once attackers have found an initial entry point into these environments, whether through compromised credentials, a drive-by download of malware, or by exploiting a zero-day vulnerability, they've essentially gotten the keys to the kingdom, with ample time to conduct reconnaissance, discover and exfiltrate sensitive data, deploy ransomware, or otherwise do harm.

Without security measures in place to effectively detect and block lateral movement, attackers will be able to use techniques that require less skill and effort to evade detection and achieve their objectives. They can focus most of their attention on bypassing the perimeter, knowing that once they've accomplished this, it will be relatively easy to find, access, and compromise high-value data, intellectual property, or other organizational crown jewels.

Common threats inside the private cloud

Unauthorized Access	Software Vulnerability Exploits	Lateral Movement
Today's cyber threat landscape may well be the most dangerous of all time. Sophisticated attackers armed with social engineering techniques and advanced malware are constantly probing the perimeter of the environment, in search of a way in. Once they've breached the perimeter of the private cloud, there may be few or no controls blocking unauthorized access to resources inside it.	Hundreds of thousands of known software vulnerabilities are catalogued in the Common Vulnerabilities and Exposures (CVE) database, with tens of thousands more being discovered each year. Even organizations with mature vulnerability management programs are challenged to keep up, and many still rely on at least a few legacy systems or network protocols that can no longer be updated.	Rarely is the initial entry point into a network an attacker's intended target. Once inside, the attacker will aim to maintain access undetected while they explore the environment, concealing their activities within east-west traffic and looking for valuable assets to ransom or exfiltrate. Perimeter-based controls cannot stop lateral movement.

1. IBM, Cost of a Data Breach Report, 2023.
2. Verizon, 2023 Data Breach Investigations Report.
3. VMware, 2022 VMware Global Threat Report.

The VMware vDefend™ Distributed Firewall, VMware vDefend™ Firewall, and Security Intelligence can be purchased as part of the VMware vDefend™ SKU. Advanced Threat Prevention capabilities are available within the VMware vDefend™ Advanced Threat Prevention SKU.

Most organizations follow one of the two most common approaches to protecting their network's interior (detecting and blocking threats in east-west traffic), but neither is optimal. The first approach is to deploy hardware, such as physical firewalls, in an effort to gain visibility and control over internal traffic. This approach is cost prohibitive, isn't scalable (since the appliances have fixed capacity limits) and can impede network performance due to traffic hairpinning. The other approach is to deploy software agents, which is operationally complex and can't be relied on for use cases beyond segmentation. The agent-based approach is also inherently vulnerable to workload compromise: if a threat actor gains control of the host operating system, they can simply disable the agent.

What's needed instead is an entirely new approach, a security solution that can enforce granular micro-segmentation at the virtualization layer, but can also go beyond this to provide deep visibility and advanced security controls to protect from sophisticated attacks such as ransomware. This requires coverage of all the adversarial tactics and techniques commonly employed today, from methods of defense evasion and privilege escalation to sending out command-and-control communications.

In other words, what's needed is comprehensive lateral security that was purpose-built for the modern private cloud. VMware has answered the call by making it possible to build a private cloud that's both scalable and secure—with VMware Cloud Foundation™ and VMware vDefend™.

Introducing VMware vDefend™

VMware vDefend™ includes distributed L7 stateful firewalling and advanced threat prevention capabilities that can help organizations achieve zero trust and protect themselves from ransomware and other sophisticated threats. Built into the hypervisor, the solution scales seamlessly to meet your evolving needs. Each component of the solution stack works with all others across L2-L7, providing the control and visibility you need to detect and block threats. This natively integrated security stack can be managed centrally from a single console, simplifying operations, smoothing your path to micro-segmentation, and making it easy to implement advanced threat prevention controls.

VMware vDefend™ makes it simple and easy to achieve granular network micro-segmentation by giving security teams access to powerful tools like AI-driven rule recommendations and intent-based policy enforcement.

But even though micro-segmentation can help prevent the lateral movement of threats, alone it's not enough to combat the most sophisticated attacks. Advanced Threat Prevention (ATP) features provide additional threat visibility, detection, prevention, and alerting capabilities to eliminate blind spots and identify intruders within your environment. Built into the hypervisor, intrusion detection/prevention (IDS/IPS) capabilities provide the deep packet inspection that's needed to keep attackers from exploiting vulnerabilities. ATP can also secure your private cloud by blocking malware and stopping threats that were engineered to evade standard security tools.

These capabilities combine to provide comprehensive lateral security defense, informed by broad and deep AI-powered threat analytics. VMware vDefend™ includes:

- **VMware vDefend™ Security Intelligence:** Granular application discovery, network traffic analytics, and policy recommendations give your team the necessary visibility to create and manage effective micro-segmentation policies. Secure critical workloads with software-defined virtual segments, and enforce smart, consistent policies everywhere.
- **VMware vDefend™ Distributed Firewall and VMware vDefend™ Gateway Firewall:** Secure traffic across virtual, container, and physical workloads with a software-defined L7 firewall solution that delivers policy automation linked to the workload lifecycle. Simplify your security architecture by making it easy to create virtual zones and achieve micro-segmentation.
- **VMware vDefend™ Advanced Threat Prevention:** ATP includes signature and behavior-based intrusion detection/prevention capabilities, network traffic analytics, network detection and response, and network sandboxing. These capabilities let you see whether traffic and communication patterns are normal, so that you can prevent and block threats early in the attack lifecycle.

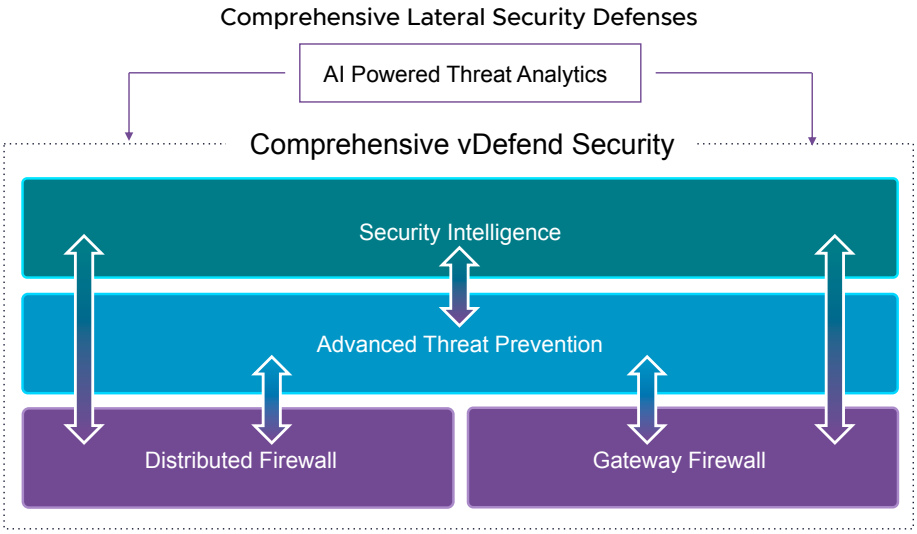

Figure 1: Fully Integrated Security Stack – Plug and Play Experience with VCF

You Cannot Protect What You Cannot See

VMware vDefend™ delivers both network and threat visibility to give security professionals a panoramic view of all workloads and traffic across the entire private cloud.

Network Visibility

Understanding communication patterns in a virtualized private cloud requires deep visibility into virtual machine (VM) to VM traffic. Traditional network visibility solutions leave security teams blind to traffic flowing between VMs, because they use network taps that can only see traffic traveling between physical hosts or network switches.

VMware vDefend™ Gives You the Answers You Need to Secure Your Private Cloud

- How many applications are communicating with one another?
- What micro-segmentation policies need to be created and enforced?
- Are these communications normal or abnormal?
- Which of the thousands of alerts your team is getting are caused by real attacks?

VMware vDefend™ is instrumented directly within the virtualization layer. This turns the virtualization layer—once a blind spot—into the security professional's best tool for visibility and control. VMware vDefend™ Intelligence provides visibility into application communications and automates security deployment at scale, making it easy to create zones and segments. AI-powered analytics can recommend rules, policies, and groups to mitigate your organization's greatest risks.

Threat Visibility

Today's threat actors are often able to conceal their presence within an environment for extended periods of time—sometimes hundreds of days if not longer. To be able to detect and stop these malicious activities, defenders need comprehensive visibility, showing the steps being taken, the hosts involved, and the attack stages these activities represent. Visibility should span the full set of adversarial tactics and techniques outlined in the MITRE ATT&CK framework, a global knowledge base detailing the attack behaviors threat researchers have observed in the real world.[4]

In the VMware vDefend™ Network Detection and Response dashboard, alerts are accompanied by rich context, so that security professionals can see at a glance which anomalous behaviors have been observed, which resources are impacted, which steps in an attack sequence have been taken, and what evidence is present.

Accelerate Your Zero Trust Journey

Zero Trust Security replaces the outdated assumption that everything within the enterprise network perimeter is secure and can be trusted. In a zero trust architecture, policies and controls need to be enforced to secure both users' access to resources and workloads' communications with one another. The first of these objectives can be achieved by implementing Zero Trust Network Access (ZTNA); the second requires secure workload access, which can be enforced with VMware vDefend™.

Robust network micro-segmentation is the foundation of zero trust. VMware vDefend™ provides all the capabilities you need to achieve micro-segmentation, giving you tools to secure your infrastructure, create virtual zones, and secure applications. With VMware vDefend™ Intelligence, you'll get comprehensive visibility and receive detailed policy recommendations. With the VMware vDefend™ Distributed Firewall and VMware vDefend™ Firewall, you can enforce those policies to establish virtual zones for consistent micro-segmentation across your private cloud.

4. MITRE Corporation, MITRE ATT&CK Knowledge Base.

Micro-Segmentation Use Cases: Setting the Foundation for Zero Trust

Secure Infrastructure	Secure Virtual Environments	Secure Applications
Applications need access to common services like Active Directory, DNS, software update delivery, logging, and others. These critical services are prime targets for bad actors to exploit because they can be used to enable access to additional workloads in the data center. The **VMware vDefend™** Distributed Firewall can help secure access to these services to prevent lateral movement. This gives security teams a quick win, making it a great starting point from which to advance on your zero trust journey.	Many applications run in multiple environments such as production, user acceptance testing, quality assurance, and development. Code updates, policy changes, and service expansions are usually created in development environments and moved up the stack to production. There are many reasons that access to the different environments may need to be restricted. The **VMware vDefend™** Distributed Firewall makes it possible to achieve this in a few clicks or a handful of API calls.	Realizing zero trust security requires understanding the workloads that are critical for the organization's day-to-day operations in great detail. Securing east-west communications between these workloads is essential for preventing malicious lateral movement. This means ensuring that only verified traffic is allowed. **VMware vDefend™** Intelligence can help you gain all-important visibility and win the battle against real world threats.

Is Segmentation Enough?

No matter how careful and thorough your micro-segmentation strategy, today's advanced threats may still be able to find their way in. With attack surfaces constantly expanding and new vulnerabilities being discovered faster than organizations can patch them, even the most robust security barriers can fail. Attackers are stealthy and continue to evolve their ability to exploit trusted processes, protocols, and software to conceal their activities as they explore and traverse the network.

Each of the following risks and vulnerabilities can be leveraged to move between virtual zones or network segments:

Application vulnerabilities

Attackers can exploit unknown or newly-discovered but still-unpatched vulnerabilities in commonly-used software applications to move within already-compromised environments. Think of the Log4j vulnerability, for instance, which remains unpatched in thousands of organizations' software supply chains.

Network protocol vulnerabilities

Many network protocols in widespread use remain insecure, and thus vulnerable by default. Examples include Telnet and Remote Desktop Protocol (RDP), which is included with Windows operating systems and relied on for access to office desktop computers by many remote employees.

Operating system vulnerabilities

Older operating systems such as Windows 7/8 have passed their end-of-life and are no longer receiving vendor support, including security updates. These operating systems typically have significant vulnerabilities that cannot be remediated. Still, many organizations continue to rely on software than can only run on these legacy systems.

Human error

No matter how well-trained or well-intentioned, people will always present a major security risk to your environment. They may inadvertently download malware while browsing the web, click on a malicious link in a phishing message, or surrender account credentials in a social engineering attack.

To protect your enterprise's information assets from attacks taking advantage of these sorts of vulnerabilities, you'll need to go beyond segmentation.

Defending against today's known and unknown threats requires advanced capabilities spanning the entirety of the attack sequence. These include threat prevention (to keep bad actors from gaining initial access to your systems and networks), threat detection (to immediately alert on anomalous and potentially malicious behavior), and protections against data encryption and exfiltration.

Safeguard Against Known and Unknown Threats and Protect Against Ransomware

Threat actors are always innovating, testing out novel exploits and new techniques for concealing their presence in an environment. But they're also looking for low-hanging fruit, seeking to leverage known exploits and familiar patterns of attack. Because some traffic patterns must always be permitted to allow applications to work normally, access control—and careful segmentation—isn't enough to detect all intrusions. That's why threat detection must be grounded in deep, granular visibility.

VMware vDefend™ Advanced Threat Protection leverages three complementary technologies to detect threats within the network. Our network sandbox looks deep inside every artifact and uses advanced AI and machine learning (ML) to identify potentially malicious files and prevent them from executing. Distributed IDS/IPS inspects traffic at every workload, analyzing all packets using industry-leading signature sets and protocol decoders to find and block known threats. Finally, with Network Traffic Analytics and Network Detection and Response (NTA/NDR) capabilities, we examine network traffic and flow records to detect suspicious behavior.

Together, the advanced threat prevention capabilities offered by VMware vDefend™ protect your private cloud from both known and unknown threats such as vulnerability exploits and zero day attacks.

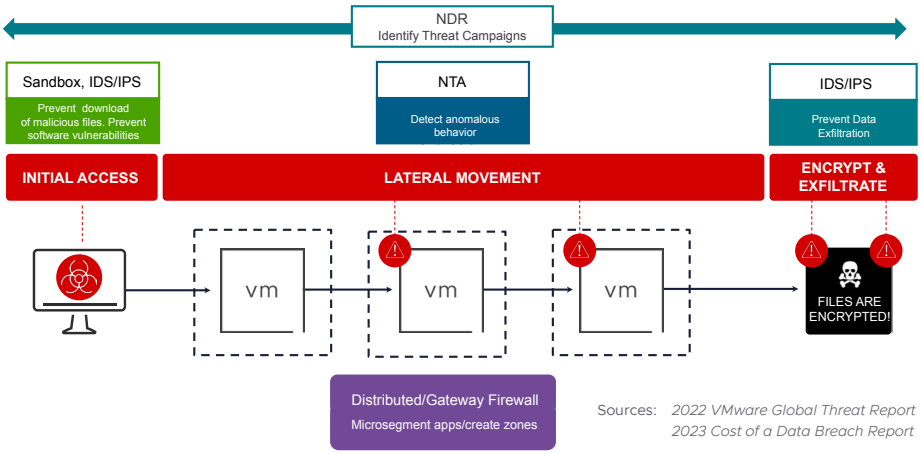

Figure 2: VMware vDefend: Multi-Layer Protection Against Malware and Ransomware

	Sandbox	Network traffic analytics (NTA)/ Network detection and response (NDR)	Intrusion detection system (IDS)/Intrusion prevention system (IPS)
What it does	Block the download of malicious files, including zero day attacks	Alert on anomalous traffic and suspicious behaviors	Protect from known software vulnerabilities. Alert on command-and-control attacks
What it prevents	Initial access to your network	Lateral movement	Known vulnerability exploits and data exfiltration during ransomware attacks
What sets VMware apart	Ability to analyze the binaries in the memory, detect reuse of know malicious code and ability to analyze behavior.	Advanced correlation engine that draws on multiple threat sources. AI-based detection of malicious on-network behavior	Inspection of every flow on every host. Ability to virtually patch CVEs' before the next scheduled server maintenance window

VMware vDefend™ Advanced Threat Protection capabilities can help security professionals protect their organizations from advanced threats like ransomware. Implementing ATP helps in all of the following use cases.

Advanced Threat Protection Use Cases

Virtual Patching	Malware Prevention	Threat Investigation
The majority of breaches involve the exploitation of known but unpatched vulnerabilities. VMware vDefend™ offers a unique architecture that makes it possible to put distributed IDS/IPS in front of every workload for signature-based threat detection, as well as to block exploits, command-and-control communications, lateral movement, and data exfiltration.	Modern-day malware tends to be highly evasive and polymorphic, so advanced sandboxing technologies are needed to detect it. VMware Malware Detection & Prevention leverages the Guest Introspection framework to intercept files before they are written to disk, passing them though a three-stage analysis process. This includes local static analysis as well as dynamic analysis in our advanced sandbox environment, which provides deep insights into malware behavior.	Too many alerts and false positives are among the key obstacles holding organizations back from achieving their security goals. VMware vDefend™ Advanced Threat Prevention has a unique distributed architecture that does not require network redesign, port mirroring, taps, or sensors to deliver complete east-west visibility. Together with an AI/ML-based anomaly detection engine, this comprehensive visibility gives security analysts correlated, actionable insights, so they can focus on true threats.

Extending Lateral Security Across Your Private Cloud

VMware vDefend™ Advanced Threat Prevention offers a full suite of capabilities that complement each other and combine into a cohesive layer of defense. ATP enhances detection fidelity, reduces false positives, and accelerates remediation, while decreasing manual effort in security operations.

Along with the use cases described above, VMware vDefend™ gives you additional capabilities for protecting your ecosystem.

1. **Protect VCF Infrastructure.** VCF architecture is primarily composed of two types of domains: the management domain and virtual infrastructure (VI) workload domains. The management domain is a special-purpose workload domain dedicated to infrastructure management tasks and including specialized management components such as NSX Manager, vSphere and the vCenter Server and Platform Services Controllers. VMware vDefend™ was designed to be able to secure the management domain. It also allows users to define global policies that limit how workload domains communicate with one another. VMware vDefend™ can secure all traffic as it enters and leaves the workload domains. All of the zero trust and ransomware protections discussed above can be implemented in all workload domains.
2. **Secure Ransomware Recovery.** Should a ransomware attack ever take place, VMware vDefend™ can work together with VMware Live Recovery to help you safely recover your data from the last known-clean backup. VMware Live Recovery is an easy-to-use, on-demand disaster recovery solution that was purpose-built to work with VMware vDefend™. The VMware vDefend™ Distributed Firewall can aid you in isolating the environment while last known-clean recovery point is being identified. ATP capabilities such as IDS/IPS can also block anomalous file movements to help protect you against data exfiltration.

3. **Compliance.** VMware vDefend™ provides the broad network coverage and granular control needed to meet requirements for multiple regulatory regimes. Individual regulations may have more specific requirements. PCI-DSS and HIPAA, for instance, mandate that IDS/IPS be in place because organizations need to be able to analyze east-west traffic to detect lateral threat movements. This is available with VMware vDefend™ Advanced Threat Prevention. VMware vDefend™ can also simplify compliance. Because all security policies can be managed and visualized from a single console providing an overview of all traffic flows within the network, it's easy for auditors to verify which policies are deployed.

Conclusion

In recent years, the threat landscape has changed dramatically, but many organizations haven't yet implemented essential capabilities for robust protection against these evolving threats. Plus, application architectures have transformed, leaving many security professionals without much-needed visibility and control. This gives threat actors an advantage: once they're gained access to an environment, they can remain there, undetected, while working to expand the scope of the attack.

Today, lateral security is critical element in every effective and efficient security architecture. It's necessary for establishing zero trust, and gives security professionals greater situational awareness. With VMware vDefend™ for VMware Cloud Foundation, enterprise security teams can confidently mitigate real-world risks inside their private cloud. VMware vDefend™ capabilities can accelerate your zero trust journey and help you defend against the most prevalent and destructive threats, including ransomware. All of this is delivered simply and efficiently, at cloud scale, with zero appliances.

To learn more about VMware vDefend Security solutions for private cloud, please visit:

https://www.vmware.com/products/vdefend-distributed-firewall.html

https://www.vmware.com/products/vdefend-advanced-threat-prevention.html

vmware® by Broadcom

Item No: Secure your Private Cloud with VMware vDefend_JR3 6/24