VMware Advanced Security for Cloud Foundation

Security designed for the modern data center

Purpose-built security for VMware Cloud Foundation

- Improve data center security and simplify operations while achieving strong ROI.
- Protect workloads and networks from the moment they are deployed.
- Enable workload and network security purpose-built for VMware Cloud Foundation.

Legacy data center security approaches are not working

Data breaches are increasingly devastating, often wiping out billions in market capitalization and damaging brand reputation and trust with customers. This damage rarely results from a single compromised server; it results from attackers moving laterally (east-west) through the data center from a single point of compromise, often for months as they locate, harvest and exfiltrate sensitive data. Most security professionals know this but struggle to adequately protect their data centers.

In a 2021 VMware Threat Analysis Unit™ threat report, it was found that nearly 77 percent of attackers used Remote Desktop Protocol (RDP) with either valid accounts or brute-forced credentials to move laterally within networks.[1] If security teams can detect lateral movement before the attackers reach their intended targets, they can prevent the attacker from successfully completing the mission.

In addition, companies are bolting on dozens of security products in their data center to protect themselves. This is creating massive operational complexity, with most organizations struggling with integration challenges and misaligned controls.

Modern infrastructure requires modern security

The data center has outgrown legacy security products. It's time to replace multiple legacy bolt-on solutions with security designed for the modern data center. Modern security solutions need to help eliminate the trade-off between security and operational simplicity.

IT and security teams require increased visibility and the ability to harden workloads against attack across their environment. Modern security solutions must also scale across private and public cloud environments, virtual machines (VMs) and containers. Security teams require a unified system for identifying risk, prevention and detection/response, and infrastructure teams need better visibility for system hardening and easier collaboration with the security operations center (SOC).

[1] VMware. "2020 Threat Landscape." May 2021.

Solution benefits

- Mitigate risk – Eliminate blind spots and misaligned controls with disparate tools.
- Ensure compliance – Enable complete coverage across network, workloads and web applications.
- Simplify operations – Lower CapEx and OpEx with software-based distributed architecture and policy automation; no network re-architecture needed.

Introducing VMware Advanced Security for Cloud Foundation

VMware Advanced Security™ for Cloud Foundation™ uses a unique, intrinsic approach to deliver unified protection for workloads and network traffic that's easy to operationalize, while enabling customers to replace multiple legacy security solutions. Eliminating the trade-off between security and operational simplicity, this solution does not require deployment or management overhead, and scales across private cloud environments, VMs and containers.

VMware Cloud Foundation™ operates at the heart of an intrinsically secure, software-defined data center where organizations house their most sensitive data and business-critical applications. VMware Cloud Foundation comes with VM-level encryption to protect unauthorized data access both at rest and in motion, network micro-segmentation, and encryption for data at rest. Building on this foundation, Advanced Security provides advanced security at strategic points in the data center covering workloads, network and web applications. The solution enables security that's simply turned on from the start, not bolted on and deployed later.

Advanced Security:

- Delivers more accurate security with deep knowledge and visibility of the application workloads across the data center. Enforcement is contextual to the type of application, resulting in lower false positives.
- Ensures there are no blind spots. It secures every workload and every hop. There's no need to selectively filter traffic. It scales across private and public cloud environments, VMs and containers.
- Eliminates the trade-off between security and operational simplicity. Built into the infrastructure, there is no deployment or management overhead. The solution also includes automated policy formulation and management.

VMware specifically addresses the internal data center security challenge with Advanced Security. Each component is purpose-built for the data center and together deliver a unique and more comprehensive data center security solution. The solution tightly integrates into VMware vSphere®, the industry standard for data center workloads, enabling world-class security to follow workloads wherever they go through their entire life.

Secure workloads

World-class data center security starts with a strong foundation for properly protecting data center workloads. According to the Verizon 2021 Data Breach Investigations Report, the leading asset category involved in breaches is servers. With workloads running on these servers, protecting them is the foundation for strong data center security. VMware Carbon Black Workload™ protects workloads with real-time system audit and remote remediation, next-generation antivirus (NGAV), and endpoint detection and response (EDR).

Carbon Black Workload is tightly integrated with vSphere to yield a seamless lifecycle management experience, reducing the need to deploy antivirus or other agents within each VM. With Carbon Black Workload, you can secure workloads at every point in the security lifecycle:

- Harden/identify risk – Understand the current state of more than 2,500 artifacts on any workload, with the ability to run ongoing assessments to track IT hygiene and take immediate action with live, remote access.
- Prevent – Use adaptive prevention for known/unknown malware, fileless attacks, and more. Stop more malware by combining exploit prevention, machine learning, and file reputation. Shut down unknown attacks with behavioral analytics and ransomware decoys. Easily adapt prevention to detected behavior in your environment.
- Detect and respond – Leverage industry-leading detection and response capabilities, and enhance visibility with highlighted suspicious workload events. Detect anomalous activity with threat intelligence and frequency analysis, and feed response actions directly back into hardening and prevention.

Secure web applications

The web server is the front door of the data center, and VMware NSX® Advanced Load Balancer™ and its web application firewall (WAF) safeguard this frequent point of attack. Customers using hardware-based solutions with fixed capacity have turned off WAF security filtering under heavy loads due to performance concerns, leaving critical servers vulnerable. The unique, scale-out software architecture of the NSX Advanced Load Balancer WAF scales capacity elastically to help deliver maximum security filtering, even under peak loads. The NSX Advanced Load Balancer WAF uses a rich understanding of applications, automated learning, and app-specific rules to provide strong security with lower false positives. The solution includes full-featured load balancing, a WAF with advanced rate limiting, URL filtering, advanced SSL/TLS decryption and re-encryption, distributed denial-of-service (DDoS) protection, L4 and L7 access control lists, and powerful security analytics.

Secure east-west data center traffic

Behind the web tier, network and micro-segmentation with stateful Layer 7 inspection of network traffic help prevent lateral movement of attackers. However, with multi-cloud environments on the rise, the attack surface will continue to expand. This will invite greater proliferation of common ports and protocols that will be used by the attacker to move laterally and exfiltrate data once inside an organization's network. The attacker focuses their efforts on living and hiding within the common noise of an organization's networks. Having visibility into this noise to identify the attacker will become more essential than ever before when defending today's multi-cloud environments.

VMware has taken an automated, distributed and enterprise-wide approach to securing multi-cloud environments and preventing advanced threats from entering and operating within multi-cloud environments. VMware NSX Advanced Threat Prevention is an add-on to the VMware NSX Distributed Firewall™. NSX Advanced Threat Prevention provides protection against advanced threats. It increases fidelity, reduces false positives, and accelerates remediation while simultaneously reducing the amount of manual work that analysts must do.

NSX Advanced Threat Prevention incorporates multiple detection technologies and includes logic that combines information from all of the following:

- VMware NSX Distributed IDS/IPS™ is a distributed and application-aware intrusion detection and prevention system for east-west network traffic.
- VMware NSX Sandbox™ powers complete malware analysis for NSX security with full-system emulation to enable accurate detection and prevention of unknown and advanced threats.
- Network traffic analysis detects anomalous activity and malicious behavior as it moves laterally across multi-cloud environments, providing security teams with real-time intelligence.
- VMware NSX Network Detection and Response™ combines aggregation, correlation and context engines that provide powerful east-west security capabilities within the data center and in multi-cloud environments. The aggregation engine collects signals from individual detection technologies and combines them to reach a verdict (malicious or benign) on network activities. The correlation engines combine multiple related alerts into a single campaign. The context engines collect data from multiple sources (including sources outside NSX) to add useful context to the information provided to analysts.

Each technology has its individual role to play, yet they all work together to provide a cohesive defensive layer against advanced threats. Workloads on a VMware multi-cloud platform are the only ones protected from advanced threats by NSX Network Detection and Response, which is AAA certified by SE Labs.

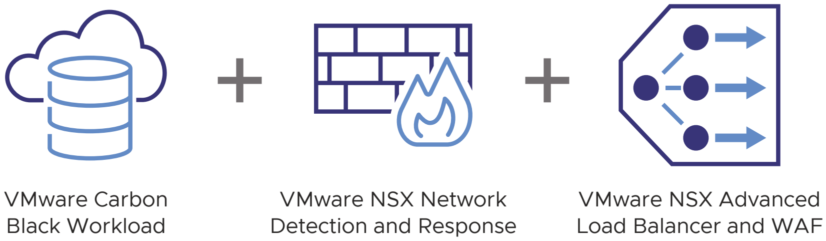
+
+
VMware Carbon Black Workload
VMware NSX Network Detection and Response
VMware NSX Advanced Load Balancer and WAF

Figure 1: VMware Advanced Security for Cloud Foundation is purpose-built to protect the modern data center and applications.

Learn more

For more information or to purchase VMware products, call 877-4-VMWARE (outside North America, +1-650-427-5000).

Read our customer stories to learn how others are using VMware Cloud Foundation.

Visit the following VMware Cloud Foundation resources:

- VMware Cloud Foundation product page
- VMware Cloud Foundation Blog
- Twitter: @VMwareVCF
- LinkedIn
- YouTube
- VMware Cloud Foundation Community
- VMware Cloud Foundation Resource Center

No more trade-off between security and simplicity

VMware Advanced Security for Cloud Foundation brings together world-class workload protection, intrusion detection and prevention, and a web application firewall for public and private clouds based on VMware Cloud Foundation. The data center has outgrown legacy security products. It's time to modernize by adopting distributed, scale-out software solutions that reduce costs and complexity, and enable the agility that businesses need.

Workloads are more secure on VMware Cloud environments

At VMware, we take an intrinsic approach to delivering security, building it into the infrastructure everywhere workloads are deployed, with deep inspection of the workloads and the associated network traffic. When you design security upfront as part of the infrastructure, you can build it differently, and it simply works better.

Take the example of firewalling, traditional appliance-centric firewalls require significant network redesign and hairpinning of data center traffic. With the NSX Distributed Firewall, we have distributed the firewall to every workload, reducing blind spots while radically simplifying the operational model. This is simply not practical with appliance-centric firewalls, whether based on hardware or a VM.