# VMware® vDefend™ Firewall

## Achieve Zero Trust in the private cloud with comprehensive lateral security

### Key benefits

**No blind spots:** Get complete coverage across all flows from L4 to L7 with software-defined firewalling deployed into the hypervisor and across workloads running on physical servers. Gain visibility into everything from user behaviors to processes as well as workload context to identify and block threats. Isolate critical services and applications from the attack surface.

**No network changes:** Radically simplify firewall deployment and operations by eliminating changes to the network and avoiding traffic hair-pinning. Replace multiple appliance-based solutions with a software-defined, per-workload stateful L7 firewall to reduce CapEx by up to 50 percent.

**Security as code:** Deliver "security as code" with an API-driven, object-based model that provides policy recommendations, automates deployment, configuration, and operationalization, and ensures new workloads receive appropriate security policies.

**Dynamic policy orchestration:** Achieve agile security with smart policy management. Pre-create policies before workloads are deployed, and ensure workloads maintain policies throughout their lifecycle—regardless of where they live or move. Write policy once and enforce it everywhere.

### Complete firewall protection to secure east-west traffic inside the modern private cloud

Today's threat actors, more sophisticated than ever, are turning to Gen AI, zero-day exploits, and advanced ransomware—alongside known vulnerabilities—to bypass traditional security and infiltrate your private cloud. Once they've breached the perimeter, they'll strive to move throughout the infrastructure, making east-west a key battleground. With a software-defined Layer 7 solution combining distributed and gateway firewalling capabilities, you can enforce granular, context-aware policies for every workload and easily segment the network to stop threats from spreading laterally. VMware vDefend Firewall provides visibility into and control over a much greater percentage of east-west traffic, securing 11 times more of your network flows. Accelerate your Zero Trust journey with a modern, distributed solution purpose-built to secure traffic in the VMware Cloud Foundation (VCF) private cloud.

### Operationalizing lateral security at scale

VMware vDefend Firewall is a software-defined L7 firewall designed to secure traffic across physical and virtual workloads. A single solution comprises VMware vDefend Distributed Firewall and VMware vDefend Gateway Firewall capabilities to deliver consistent protection into the hypervisor and across workloads running on physical servers. Stateful firewalling and complete visibility into all applications and flows give you superior security with policy automation linked to the workload lifecycle. Unlike traditional firewalls requiring network redesign and traffic hair-pinning, VMware vDefend distributes firewalling capabilities to each host, radically simplifying the security architecture. This is a much more straightforward operational model, making it easier for security teams to secure the infrastructure, create virtual zones, and protect critical applications. VMware vDefend customers see an average of 59% fewer breaches, while accelerating security deployment by 45%.[1]

1. Data derived from VMware customer interviews by a third party.

## Use cases

### Implement zero trust

Gain visibility into traffic and easily create network segments or virtual zones by defining them entirely in software. This makes it possible to segment an application in minutes with no changes to the network and no need to deploy discrete appliances or re-route traffic.

### Automate micro-segmentation

Automatically generate policy recommendations based on an intrinsic understanding of application topology. Easily create, enforce, and manage granular micro-segmentation policies while leveraging an object-based policy model for automation.

### Enforce consistent policies everywhere

Extend consistent L7 security controls across all applications and workloads, regardless of whether they're running on physical or virtual servers, in containers, or anywhere else. A single management console makes it simple to maintain visibility and control across complex architectures.

### Extend unified protection across branches

Deliver the same security policies to all your workloads in your main data center and branches, with no need to purchase or manage separate appliances.

### Block advanced threats

Leverage additional capabilities available in the Advanced Threat Protection (ATP) add-on to monitor traffic flows at every host, identify malicious traffic on a per-hop basis, and apply sandboxing to thwart initial access.

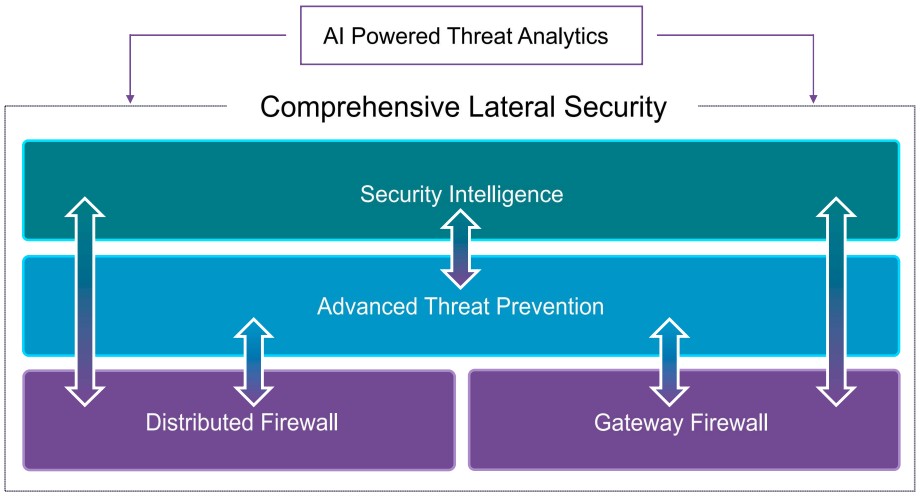


**Figure 1:** VMware vDefend – A fully Integrated security stack

## A firewall purpose-built to secure today's private cloud

### Key capabilities

- **Distributed architecture:** Instances built into the hypervisor and those running on physical servers can be managed as a single firewall, eliminating blind spots, and simplifying deployment.
- **Consistent policy enforcement:** Deliver uniform protection by extending the same threat prevention capabilities across all applications and workloads, no matter where they're running, with combined distributed and gateway firewalling managed within a single console. Infrastructure-independent policy management allows for portability across environments and supports robust disaster recovery planning.
- **Elastic throughput:** VMware vDefend scales with workloads automatically, offering massive scale and eliminating the throughput constraints typical of appliance-based firewalls.
- **Scalable traffic flow analysis:** VMware vDefend Security Intelligence provides visualization, analysis, and monitoring of traffic flows for complex modern applications, no matter whether they're running on VMs or in containers, and enables micro-segmentation at scale, no matter how large the network.
- **Access control:** VMware vDefend supports consistent enforcement of Layer 2-7 access policies, including application- and user identity-based controls and URL filtering.
- **Secure connectivity services:** Securely connect branch offices to your main data center and simply consistent deployment and management at scale.

| | VMware vDefend Distributed Firewall | VMware vDefend Gateway Firewall | VMware vDefend Firewall with Advanced Threat Prevention |
|---|---|---|---|
| L2-L7 firewalling | X | X | X |
| User identity-based access control | X | X | X |
| Application identity-based access control | X | X | X |
| L2 and L3 VPNs | | X | X |
| Intelligent flow visualization and policy recommendations | X | | X |
| URL filtering | X | X | X |
| TLS decryption | | X | X |
| IDS/IPS | | | X |
| Network traffic analysis | | | X |
| Network sandbox | | | X |
| Network detection and response (NDR) | | | X |

## Lateral Security in the Private Cloud

Traditional firewall solutions weren't designed to deliver the scalability, agility, and cost-effectiveness that security and networking teams need. VMware vDefend Firewall with Advanced Threat Prevention is distributed, software-defined, and operationally simple, making it easy to achieve robust east-west security at the scale needed to secure today's business-critical applications and computing ecosystems. With this comprehensive solution suite, security stakeholders can rest easy, knowing that they can mitigate risk, enable compliance, and move at the speed of development—all without increasing costs.

For more information on VMware vDefend Security solutions for private cloud, please visit https://www.vmware.com/solutions/nsx-firewall.html

vmware® by Broadcom


Item No: VMware vDefend Firewall_JR2 4/24