Broadcom Simplifies and Accelerates Private Cloud Lateral Security with VMware vDefend Innovations

March 26, 2025

New vDefend Capabilities Streamline and Enhance Private Cloud Lateral Security Implementation Against Advanced Threats and Ransomware

PALO ALTO, Calif., March 26, 2025 (GLOBE NEWSWIRE) -- Broadcom Inc. (NASDAQ: AVGO) today introduced new updates to VMware vDefend that enable organizations to up-level security planning and assessment, simplify lifecycle management and operations, and seamlessly scale security across application environments. As organizations develop security plans for VMware Cloud Foundation(R) (VCF), these new technologies and guidance tools enable improved time-to-implementation and help efficiently maintain security operations for all critical and non-critical applications.

“Organizations often navigate thousands of applications to power their business. This complexity makes it difficult to maintain visibility and lateral security across all applications,” said Umesh Mahajan, vice president and general manager, Application Networking and Security Division, Broadcom. “VMware vDefend simplifies how organizations achieve zero trust and private cloud security goals by cutting through complexity and providing a comprehensive lateral security implementation. The latest vDefend innovations further this efficiency by offering real-time security assessments, a next-generation security services platform to simplify operations, and micro-segmentation as code to further improve security operations.”

VMware vDefend is available as an Advanced Service for VMware Cloud Foundation.

Robust Private Cloud Security Planning and Assessment with Security Intelligence
It is essential for security teams to quickly detect and investigate potential breaches in their environment. This requires a proactive approach to security planning and rapid time-to-implementation across all application workloads. To support this, VMware vDefend introduces a Security Segmentation Assessment and Report in its Security Intelligence tool for lateral security visibility and threat analytics. It provides a real-time assessment of an organization’s security segmentation posture for implementing a zero trust private cloud initiative. The assessment analyzes application traffic to deliver timely, data-driven insights related to application interactions, pinpointing potential security gaps due to insecure network protocols and inappropriate application communication, measuring progress with a security segmentation score, and offering actionable and easy-to-implement policy recommendations. This assessment, along with rule recommendations, help organizations rapidly roll out lateral security protection on VMware vDefend Distributed Firewall across all their applications and stay ahead of potential breaches. The Security Segmentation Assessment Report is available today.

Simplified Security Operations
To establish a sophisticated security plan, organizations need a consistent, reliable platform and an optimized approach to micro-segmentation that allows customers to apply security as part of the application deployment process. vDefend addresses these needs by introducing new updates, including:

- **Updates to Security Services Platform (SSP):** SSP is a self-contained and scale-out platform that simplifies deployment of Security Intelligence as well as advanced threat prevention tools such as Network Detection and Response and Malware Prevention. The new SSP architecture greatly streamlines the user experience with a simplified network design, streamlined life cycle management, tailored user profile for security administrators, and easier workflows for configuration and deployment. The enhanced scale-out capability ensures that visibility and threat prevention automatically extend to large-scale VCF deployments.
- **Micro-segmentation as Code:** vDefend Distributed Firewall offers an optimized and streamlined approach to micro-segmentation. It is built into the hypervisor and applies security to every workload with an API-driven model that plugs into automation frameworks. This allows customers to apply lateral security as part of the application deployment process and seamlessly scale micro-segmentation across application environments. It features a declarative context-based model to deploy the full intent of customers’ vDefend security policy in a single, simplified manner and includes built-in automation that eliminates the need for external scripting. This rich policy model applies to both virtual machines and container workloads to ensure consistent lateral security protection.
- **Network Detection and Response Enhancement for Air-Gapped Environments:** The Network Detection and Response (NDR) capability of VMware vDefend now supports mechanisms for organizations to securely update threat intelligence in on-premises operations without external network access. This ensures that all detection, correlation, and response activities are executed with higher fidelity within the closed network leveraging both internally and externally sourced threat intelligence. NDR provides an additional layer of protection against targeted attack campaigns in sensitive, high-security or classified environments and supports industries with strict regulatory compliance.
- **VMware Validated Solutions design for secure VCF:** This best practice design guide[1] with prescriptive use case guidance enables security teams to rapidly roll-out zero trust lateral security for VCF’s management components and application workloads.

These capabilities are available today.

Third-Party Validation
Third-party research reports outline the impact and value of vDefend. vDefend recently received an AAA rating for Advanced Threat Prevention in the

SE Labs Advanced Security Test Report. The SE Labs methodology tests full chains of attack, including complex, multi-staged ransomware threats, and uses a variety of tools and techniques commonly employed by threat actors to analyze the performance of vDefend Advanced Threat Prevention. An AAA rating is the highest rating vendors can receive and indicates the use of best-of-breed threat detection algorithms.

Additionally, a recently commissioned Total Economic Impact™ (TEI) study conducted by Forrester Consulting on behalf of Broadcom, revealed that a composite organization representative of interviewed customers with experience using VMware vDefend:

- Reduced their cyber breach risk by 40%
- Cut security operations expenses by 25%
- Avoided a 12% increase in cyber insurance premiums

The study also showed that the composite organization realized a 116% return on investment using VMware vDefend. The full study can be accessed here.[2]

Supporting Quotes

“Deep application-level visibility and micro-segmentation for a zero trust private cloud is critical for us,” said Sarita Akula , senior manager, Infrastructure Platforms at University of Arts, London. “In a very short time, we enabled Security Intelligence's application analytics with SSP, successfully segmented certain critical applications, and laid the groundwork for enabling advanced threat detection and prevention capabilities of vDefend.”

“vDefend has been a critical technology in our journey to Zero Trust security for health care applications,” says Tyler Wertenbruch, IT technical manager at St. John’s Health. “With vDefend’s micro-segmentation-as-code capabilities, we were able to apply lateral security during the application on-boarding process, enabling us to ensure that security remains up to date and maintain a strong Zero Trust posture. We are looking forward to leveraging Security Intelligence's enhancements for deeper visibility and assessment of our application environment.”

"VMware vDefend's Security Intelligence hosted on the enhanced Security Services Platform has become a critical tool for quickly securing our customers' business applications", said Michael Law, managing consultant engineer at CDW, "These vDefend enhancements for lateral security are unmatched in the industry."

Additional Resources

- For more details on these updates, read the VMware vDefend blog or join our webinar
- Follow VMware vDefend social channels on LinkedIn and X

About Broadcom
Broadcom Inc. (NASDAQ: AVGO) is a global technology leader that designs, develops, and supplies a broad range of semiconductor, enterprise software and security solutions. Broadcom's category-leading product portfolio serves critical markets including cloud, data center, networking, broadband, wireless, storage, industrial, and enterprise software. Our solutions include service provider and enterprise networking and storage, mobile device and broadband connectivity, mainframe, cybersecurity, and private and hybrid cloud infrastructure. Broadcom is a Delaware corporation headquartered in Palo Alto, CA. For more information, go to www.broadcom.com.

(1) [1]VMware Validated Solutions: Lateral Security for VMware Cloud Foundation with VMware vDefend, March, 2025
(2) [2]Forrester Consulting, The Total Economic Impact™ Of Broadcom VMware vDefend, March, 2025

Media Contact:

Heather Haley
Broadcom Global Communications
heather.haley@broadcom.com
925-856-8042

Source: Broadcom Inc.