VMware HyperArmor

Solution Brief

"In 2025, up to 32% of exploited Common Vulnerabilities and Exposures (CVEs) were actively weaponized on or before their public disclosure date (zero-day/negative day exploitation)."

Cloud Security Alliance AI Safety Initiative - April 2026

Frontier AI has fundamentally altered the cybersecurity landscape, enabling highly sophisticated campaigns at a low cost. This advancement has drastically reduced the median time to exploit disclosed vulnerabilities.

Consequently, threat actors have shifted their focus from compromising individual virtual machines to attacking the hypervisor itself, where a single compromised ESX host grants control over hundreds of virtual machines simultaneously.

VMware HyperArmor delivers essential, active defense for VMware Cloud Foundation (VCF) and VMware vSphere Foundation (VVF), engineered to safeguard the ESX hypervisor against sophisticated, AI-accelerated cyber threats. By embedding security directly into the infrastructure layer, this solution provides proactive protection that ensures business continuity without the need for disruptive emergency maintenance cycles.

The challenge: AI-accelerated vulnerabilities

The modern threat landscape has shifted, significantly increasing risk for virtualized environments:

- **Rapid exploit timelines**: The time from vulnerability disclosure to active exploitation has drastically compressed—from 32 days in 2022 to just 5 days in 2023. (CSA, The collapsing exploit window: AI-Speed vulnerability weaponization, 2026-04-25) The average time to exploit in 2026 is 1.6 days. (Paramify)
- **Hypervisor-centric attacks**: Adversaries are increasingly targeting the ESX hypervisor directly. A single compromised host can provide unauthorized control over entire virtual machine fleets.

Defense in Depth Across VMware Cloud Foundation

VMware HyperArmor is designed to work seamlessly alongside the broader security capabilities in VMware Cloud Foundation by hardening the underlying ESX host against process execution exploits, unauthorized configuration changes, and credential theft.

- **Infrastructure Hardening (VCF)**: VCF is hardened out of the box with key capabilities that include centralized identity management, data-at-rest and data-in-transit encryption, live patching, and built-in infrastructure resiliency.
- **Proactive Hypervisor-Layer Protection (HyperArmor*)**: Adds a proactive layer of protection for the underlying ESX host against process execution exploits, unauthorized configuration changes, and credential theft.
- **Network-Layer Protection (vDefend*)**: Delivers strong lateral security with micro-segmentation and advanced threat detection and prevention, which uses deep traffic inspection to block emerging exploits and to deliver network-level virtual patching.
- **Cyber Recovery (VMware Live Recovery*)**: Provides secure, confident recovery from cyber-attacks to a prescriptive VCF-based isolated clean room, with built-in AI/ML-based recovery point validation and end-to-end workflow automation.

Together, this integrated and multi-layered approach secures the full infrastructure stack.

- **The patching paradox**: Traditional security methods rely on reactive patching, which is operationally disruptive and often requires maintenance windows that leave organizations exposed during critical vulnerability periods.

Key Benefits

- **Mitigate vulnerabilities earlier**: Closes the vulnerability exposure window by providing active virtual patching, buying critical time for security teams to test and deploy official vendor updates.
- **Continuously monitor and block**: Monitors management areas in real-time to block unauthorized execution and file writes without installing VM agents or adding performance overhead
- **Reject attackers at the door**: Delivers multi-factor authentication (MFA) for SSH directly in the login path, requiring a secondary TOTP challenge so attackers cannot reach the command line even with stolen admin credentials.

Key Capabilities

- **Virtual patching**: Mitigate vulnerabilities immediately without waiting for physical patch deployment.
- **Active defense and behavioral blocking**: Continuously monitor and fortify the ESX hypervisor with minimal overhead by blocking unauthorized executions and scripts.
- **MFA for SSH**: Neutralize stolen admin credentials by enforcing a secondary authentication challenge at the SSH layer.

VMware HyperArmor offers distinct advantages:

- **VCF fortification**: Security is built to secure the VCF stack, ensuring seamless alignment and stability.
- **Infrastructure-first design**: Engineered specifically for IT Operations and Infrastructure teams, prioritizing system integrity and uptime.
- **Developed and integrated by Broadcom team**: Leverage single source of support.
- **Full ESX visibility**: Provides centralized visibility and management across your VMware ESX host environments.

*May require additional licensing.

How to get started

Contact your VMware sales representative or visit the product page to schedule a demo and explore deployment options for your enterprise environment.

- Evaluate your current hypervisor security posture and identify critical ESX hosts.
- Deploy VMware HyperArmor across VCF and VVF stacks for instant active defense.

Copyright © 2026 Broadcom. All rights reserved.

The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Item No: vmw-bc-sol-brief-uslet-word-2026; Oct-26