



INSIGHTS | **TECH BRIEF**

From Reactive Tools to Hypervisor Security: Broadcom's New Model

In chess, White has a subtle but important advantage because it gets to move first. While the first move doesn't guarantee victory, it offers a proactive opportunity to shape the contest rather than reacting to an opponent's strategy.

Cybersecurity has traditionally involved a constant struggle for that same advantage. While security practices such as vulnerability scanning, penetration testing, and code reviews are proactive in nature, defenders often operate at a disadvantage. Like chess, cyber defense teams must prepare for every possible move, while attackers only need to identify one exploit to make a formidable move.

The Inherent Advantage of Attackers

A primary attack method is to target exploitable vulnerabilities within systems and software. Traditionally, such vulnerabilities aren't discovered until researchers identify them in deployed products or attackers exploit them in the wild. Once a vulnerability becomes known, the race begins to develop, test, and deploy a patch before attackers capitalize on it. In these situations, defenders are forced into a reactive position, responding to their adversary's moves rather than taking the initiative.

The Vulnerability Window is Shrinking

This inherent disadvantage that defenders face is the compression of time. The critical window between the public disclosure of vulnerability and its first confirmed exploitation is shrinking, as attackers increasingly use advanced AI systems to accelerate vulnerability research and exploit development. According to a 2026 J.P. Morgan analysis based on Zero Day Clock data, the median time to exploitation fell from approximately one year in 2021 to about one day in 2026. The analysis projects that this window could shrink to as little as one minute by 2027.¹

PODCAST:
*Optimizing
VCF 9*



WEI VCDX Experts:
Mark Gabryjelski & Jason Shiplett



How Broadcom Is Reclaiming the Security Initiative

Technology leaders such as Broadcom believe that attackers shouldn't have the same default advantage that exists in chess. That's why they are integrating frontier AI models directly into their security engineering workflows to discover vulnerabilities, test exploitability, and accelerate patch development. Working at machine speed, integrated frontier AI can review large volumes of code, identify potentially insecure patterns, and test whether a flaw can be exploited in a controlled environment. Artificial Intelligence can even propose a patch for engineers to review and validate. In effect, Broadcom is working to give its security engineers the first move.

What is Frontier AI?

Space is no longer the final frontier. On Earth, AI has emerged as a new frontier that continues to advance, expanding the boundaries of what technology can analyze, create, and accomplish. Frontier AI refers to the most capable, general-purpose AI systems available at any given moment. It is the leading edge of what AI can do. As new models surpass older ones, that edge moves forward, and so do the opportunities and risks that come with it.

Attackers have already learned the value of harnessing the power of frontier AI. For example, they find vulnerabilities and design exploits for them at machine speed. In response, some security-focused organizations are now fighting fire with fire, deploying frontier AI to:

- Review source code at scale
- Prioritize patching based on real risk
- Identify architectural weaknesses
- Strengthen vulnerability programs
- Accelerate security testing across the environment

Frontier AI Deliver More than Speed

The power that frontier AI brings is more than just a first move advantage. A suspicious code pattern doesn't necessarily mean that an exploitable vulnerability exists. AI is helping companies like Broadcom also determine the conditions necessary for exploitation, allowing developers to distinguish between theoretical vulnerability weaknesses and ones that present meaning security risks.

Once a security risk is identified, AI can assist engineers in identifying the underlying cause, evaluating possible code changes, and performing regression testing to ensure that created security patches eliminate vulnerability. Notably, this assistance and testing must be executed without disrupting existing functionality or introducing additional weaknesses.

AI Enabled VMware vDefend

When Broadcom set out to raise the security bar for VMware Cloud Foundation, it moved away from reactive, agent heavy tools and took a different approach. VCF 9.1 introduces VMware vDefend, which embeds multi layered zero trust defenses directly into the hypervisor.

This AI driven platform brings together micro segmentation, hypervisor level intrusion detection and prevention (IDPS), and AI powered network detection and response that works in concert to deliver more value on constrained IT budgets. VMware vDefend extends this protection through virtual patching, which uses network-based controls to shield vulnerable workloads running on VCF while permanent fixes are developed, tested, approved, and deployed.

A Native Defense in Depth Strategy

Traditional security agents in hypervisor environments operate from within the guest operating system, which creates a fundamental vulnerability. If an attacker compromises the OS, the very agents designed to protect it can then be disabled. The foundation of the defense becomes part of the attack surface.

VMware vDefend takes a fundamentally different approach. Because Broadcom owns the ESXi hypervisor, VMware vDefend can enforce security policies at the hypervisor level. Imagine that level of security directly on every virtual NIC of your VMware environment. When enforcement happens below the virtual machine, attackers have significantly less ability to detect, circumvent, or disable it.

All this architecture is the foundation of Broadcom's broader defense-in-depth strategy for VCF private clouds. It creates a hardened private-cloud fabric designed to detect lateral movement, contain ransomware and other advanced threats, and apply compensating controls such as virtual patching for known exploits.

By integrating natively with VCF automation, self-service capabilities, and operational tooling, these controls help organizations respond to attacks more quickly and consistently than approaches that rely solely on endpoint agents.

Talk to WEI Today

WEI is proud to partner with Broadcom because we are dedicated to helping customers improve vulnerability and exposure management. Together, we achieve this by identifying the risks that matter most to customers and evaluating how effectively existing security tools address them. WEI guides customers toward practical risk-reduction priorities, beginning with secure software development so vulnerabilities are addressed before applications are released.

If you want to learn more about the proactive security strategy of VCF, our WEI virtualization engineers can help educate you and create an implementation strategy.

Sources:

1. Cembalest, M. (2026, July 22). Patchmageddon: The race to patch software vulnerabilities before zero-day cyber-exploitations proliferate. J.P. Morgan Asset & Wealth Management. <https://www.jpmorgan.com/content/dam/jpmorgan/documents/private-bank/eye-on-the-market-patchmageddon.pdf>

About WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. WEI works with clients to understand goals, integrate strategy with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.