Akamai Solution Brief

Rapidly Remediating Vulnerability Risks with Tenable and Akamai

Vulnerability scans mean nothing without a corresponding action. By unifying Tenable's vulnerability intelligence with Akamai's software-defined microsegmentation, organizations can prioritize exposures, automate enforcement, and isolate high-risk assets until remediation is complete. This integration turns static CVE data into actionable security policy, protecting your environment before threats can take root.

The challenge: From insight ... to inaction

Most organizations are overwhelmed by vulnerability data. According to research, over **60% of breaches** stem from known but unpatched vulnerabilities, many of which had been exposed for months before exploitation.[1]

The problem isn't about visibility; it's about how to respond. Scanning tools can generate long lists of relevant Common Vulnerabilities and Exposures (CVEs), but without an effective way to translate that insight into real-time network protections, the window for vulnerability abuse and escalation remains wide open.

Security teams need a better way to prioritize risk and enforce isolation, especially in hybrid cloud and container environments where the attack surface is constantly evolving.

The solution: Vulnerability management with Tenable and Akamai

Together, Tenable and Akamai Guardicore Segmentation offer a closed-loop, risk-based approach to vulnerability management.

This integration enables organizations to:

- **Automatically label Reval map assets** with relevant CVE and risk score metadata from Tenable.io or Tenable.sc
- **Continuously sync asset tags** and statuses between solutions, ensuring real-time alignment between discovery and enforcement
- **Enforce segmentation policy** that proactively isolates high-risk or unpatched systems
- **Identify unmanaged assets** discovered by Akamai Guardicore Segmentation and make them available for scanning in Tenable
- **Trigger remediation workflows** based on asset risk profiles and environment-specific policy

With a bidirectional API integration, the solution supports dynamic tagging; assets that are patched in Tenable can have their labels and segmentation policy automatically updated in Akamai Guardicore Segmentation, reducing security team overhead and response time.

Benefits for your business

Accelerate remediation
Apply real-time segmentation based on live CVE and risk data from Tenable

Contain threats instantly
Isolate vulnerable or exploited assets before attackers can move laterally

Automate enforcement
Create policy triggers tied to vulnerability status so protection starts before patching

Reduce security debt
Prevent long-tail vulnerabilities from lingering in the environment

Strengthen compliance
Use CVE-based labels and segmentation to support mandates like HIPAA, PCI, and ISO 27001

[1] Costs and Consequences of Gaps in Vulnerability Response, ServiceNow and Ponemon Institute Survey

Akamai

Use case: Isolating high-risk CVEs before they're exploited

Imagine that you discover a high-severity CVE affecting your Linux workloads. Tenable flags the exposure immediately. With this integration:

- That CVE is automatically imported as a label in Akamai Guardicore Segmentation, allowing you to tag the relevant assets.
- Assets and workloads tagged with that CVE are quickly isolated from critical systems via dynamic segmentation policy.
- With assets secured, security teams are alerted and begin vulnerability remediation.
- Once the patch is applied, the isolation policy is lifted automatically.

This scenario reflects the kind of proactive, policy-driven response that modern security frameworks like Zero Trust and Continuous Threat Exposure Management (CTEM) demand.

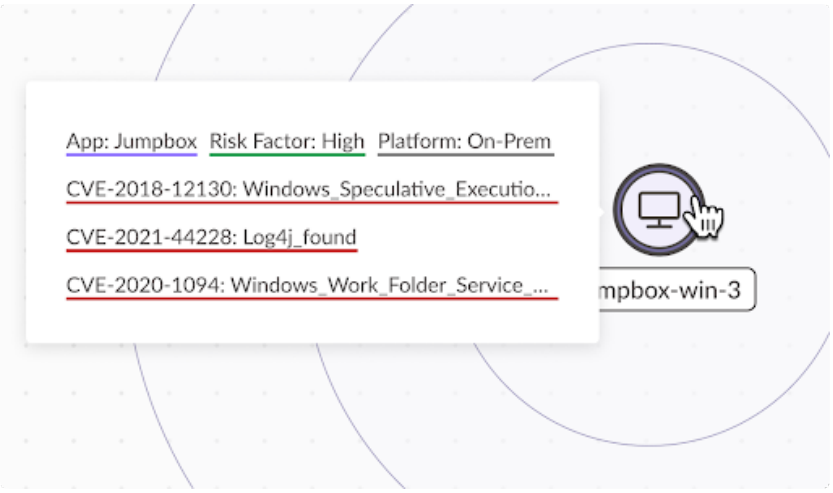

Fig.1 CVE-based labels are applied to the jump box

See how Tenable and Akamai Guardicore Segmentation work together to turn risk insight into enforcement. Talk to our team today.

| Published 10/25