



WHITEPAPER

Live Patching - Tenable Technology Alignment Strategy

Challenges

The risk of attacks and prioritization of vulnerabilities continue to be a challenge for many organizations. Even with advanced artificial intelligence and machine learning, SecOps, DevOps, and NetSecOps must adjust the security asset risk priority strategy daily. Each enterprise area, including cloud, on-premise, remote access, and application systems, all share a common problem with increased attack surfaces, application vulnerabilities, and security breaches. Even with containment strategies, zero-trust, and enterprise identity, organizations still suffer financial and image-damaging security events along with increased risk and compliance regulation exposure. The need for automated application security testing and integrated vulnerability management with effective responses, has never been greater.

On average, enterprises find 870 vulnerabilities per day across 960 IT assets. Cybersecurity teams don't have the time or resources to handle all vulnerabilities, so the need to prioritize is obvious.



**On average,
enterprises find**

870

vulnerabilities per day across

960

IT assets.



Do you know where the most vulnerable assets reside?

Global threats against the client system change every day. Some of these attack vectors will change several times a day. SecOps are fully aware they can not patch every system with vulnerabilities or even high-risk exploited hosts.

With Tenable's groundbreaking algorithm embedded in their [vulnerability priority rating](#) (VPR) platform, organizations can identify which of its assets are most at risk by a well-defined composite risk score.

Most of the largest enterprises to the smallest cities and counties will leverage several composite scoring methods to better gauge the priority for assets requiring urgent remediation capabilities, including patching the OS, the kernel, or maybe even spinning down a container orchestration to support CI/CD development.



VPR makes it a more suitable tool for prioritizing remediation efforts than the [Common Vulnerability Scoring System \(CVSS\)](#). CVSS uses a similar scoring based on the confidentiality, integrity, and availability model by VPR and provides a much more total score including

- Critical High, Medium, and Low
- Two-component levels – technical impact and threat.

VPR collects CVE information then begins to process the data, placing vulnerability into a risk scoring range. Organizations leveraging Tenable. IO will have the means to determine which asset needs to be remediated first to help reduce the risk. [Tenable's predictive prioritization algorithms](#) give clients the latest threat to their attack surfaces. Tenable's VPR strategy is compelling in helping organizations prioritize remediation while tracking continuous evaluation of issues against attack surfaces.



[97% reduction](#) in vulnerabilities that need to be fixed first



[With Tenable VPR](#), there is no need to use an add-on vulnerability prioritization product.

What is the role of live patching in reducing organizational risk?

[In a recent Ponemon report](#), 58% of respondents indicated that their Security Operations Center (SOC) was ineffective in managing the increase in security challenges. 49% report too many false positives, lack of incident response resources, and ineffective vulnerability management platforms impacting their daily workstream. In addition to false positives causing inefficiencies, 42% of respondents indicated that false positives interfered with threat-hunting teams.

How could TuxCare's live patching of the Linux kernel and associated libraries, including OpenSSL and glibc, contribute to reducing organizational risk?

By live patching Linux hosts, TuxCare helps reduce security vulnerabilities and risk inside several critical surfaces by removing kernel vulnerabilities before they become exploited. With the ability live patch without the need to reboot the host, clients can focus their SecOps resources on other higher priority assets reported into the Tenable VPR portal. TuxCare's live patching solution resides in memory on the host. TuxCare continuously updates the kernel as new vulnerabilities are discovered.

Reducing as many attack surfaces and vulnerabilities as possible is a charter for most SecOps and NetSecOps teams. TuxCare's KernelCare Enterprise family of solutions helps reduce more attack surfaces with live patching. In a recent study, only 29% of organizations reported sufficient visibility into attack surfaces. TuxCare's risk-based protection strategies patch and maintain complete business criticality of all Linux hosts regardless of their location in the environment.



Solution

Leveraging TuxCare Live Patching to Help Decrease the Attack Window

Clients leverage TuxCare’s live patching solution, KernelCare Enterprise, to help reduce their attack surface by eliminating open CVEs targeting specific kernel code and Linux OSs.



KernelCare Enterprise by TuxCare is a lightweight kernel module





KernelCare Enterprise performs live kernel security patches in memory during production operations without rebooting the individual host systems



KernelCare Enterprise provides live patching for ALL major Linux distributions on over 4,000 kernel versions and growing

Live patching additional hosts in development, staging, and QA is recommended.

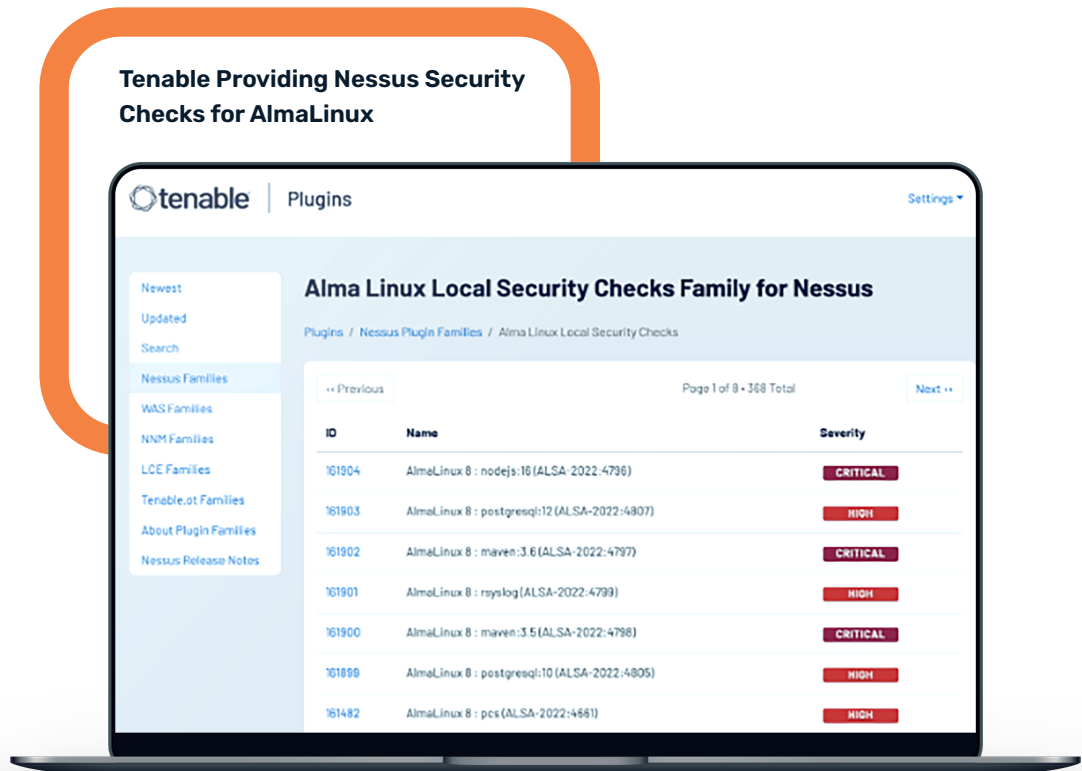
	 tenable	 TuxCare
Protecting Linux hosts against attacks	Tenable's VPR scoring helps clients prioritize their remediation of critical systems.	TuxCare KernelCare Enterprise provides live patching of the Linux kernel on all major Linux distributions.
Kernel aware protection	Tenable is kernel aware of a TuxCare recurring task residing in memory. Tenable is visible to TuxCare live patching activities.	KernelCare Enterprise operates as a recurring task residing as a kernel module. It executes live patching in memory at configurable intervals without rebooting.
Reporting into Tenable VPR platform	Tenable consolidates all vulnerability remediation and current risk scores into the VPR portal.	TuxCare reports updated successful live patching status in TuxCare ePortal and popular management tools via integrations.



Interconnecting with Tenable's Solution Stack

TuxCare KernelCare Enterprise security patching solutions are designed for large enterprises with thousands of servers. Without automated tools, security teams would incur high manual patching and scanning costs. Patching servers manually would require a lot of time and effort from multiple teams.

Example: AlmaLinux

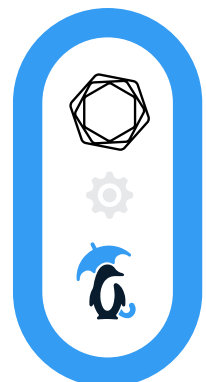


TuxCare's KernelCare Enterprise automatically provides Tenable scanners with all the information on what we have patched for all popular enterprise Linux distributions.

Tenable Visibility into TuxCare's KernelCare

TuxCare's KernelCare Enterprise will begin to feed data to Tenable scanners with the command `kcarectl -unamethen`, which shows the kernel's patched version, representing the kernel's security level up to the reported patched version. KernelCare provides a report by running `kcarectl-patch-info`, which presents the CVEs patched by KernelCare in the currently running kernel.

With 40+ Linux distributions supported by TuxCare, IT teams can be sure all enterprise systems stay compliant without service interruptions.



About TuxCare

TuxCare is a global leader in open-source security, providing unmatched expertise in patching for your entire Linux estate. We deliver security patches to popular Linux distributions, end-of-life systems, programming languages, and more – offering a comprehensive security solution for all your infrastructure needs.

With over 80,000 patches – and counting – delivered to our users, TuxCare's solutions reduce vulnerability exposure, minimize downtime, eliminate patching-related disruptions, secure your open-source supply chain, and maintain system stability and compliance.

TuxCare protects the world's largest enterprises, government agencies, service providers, universities, and research institutions, safeguarding over a million workloads (and growing). Our mission is to drive continuous innovation through open-source technologies while minimizing the risk of cyber threats and serving as a trusted technology partner for innovative organizations across the globe.



LEARN MORE AT
www.tuxcare.com

About Tenable

Empower all organizations to understand and reduce their cybersecurity risk

Cybersecurity is one of the existential threats of our time. New types of connected devices and compute platforms, from Cloud to IoT, have exploded the cyber attack surface. And more tools collecting more data doesn't equate to actionable insight for the CISO, C-suite, and Board of Directors. The old way of scanning on-premises IT devices for vulnerabilities is no longer enough. It's time for a new approach.

Approximately 40,000 organizations worldwide rely on Tenable to help them understand and reduce cybersecurity risks. Tenable's goal is to arm every organization, no matter how large or small, with the visibility and insight to answer four critical questions at all times: Where are we exposed? Where should we prioritize based on risk? Are we reducing our exposure over time? How do we compare to our peers?

Tenable is a Cyber Exposure Management company.

