



WHITEPAPER

# Tuxcare Live Patching - Qualys Technology Alignment Strategy

# Challenges

Organizations continue to migrate their digital assets across hybrid multi-cloud environments for better computing, storage, and expansion of business offerings. Many of these new workloads may reside inside a virtual private cloud, a Docker container, or on a hyper-converged platform like Nutanix and VMware. With such a dispersed landscape of hosts, how can an organization maintain a high state of operational and security readiness?

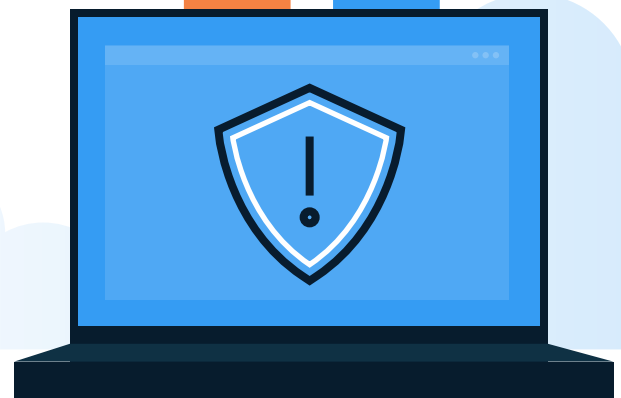
## How do you reduce false positives in your environment?

Identifying the highest security risk assets is critical to the organization's SecOps and risk management teams. By leveraging market-leading solutions, including [Qualys](#) vulnerability scanning and patch management systems, organizations can stay ahead of zero-day attacks by first protecting their most exposed systems. [Qualys' world-class solution](#) portfolio includes visibility into containers, supporting the deep experience and capability of any SecOps team.

[Qualys](#) scans the systems looking for known vulnerabilities. Yet, sometimes scanning systems will report a false positive. Many SecOps teams will spend hours researching and verifying false positives and negatives.

[In a recent Ponemon report](#), 58% of respondents indicated that their Security Operations Center (SOC) was ineffective, and 49% said that the reason behind inefficiencies is too many false positives. In addition to false positives causing inefficiencies, 42% of respondents indicated that false positives interfered with threat-hunting teams.

How can these teams reduce their false positives while maintaining the highest state of readiness?



# Solution

## Leveraging KernelCare 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 OS systems.



KernelCare Enterprise by TuxCare agent 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 of additional hosts in development, staging, and QA is recommended.

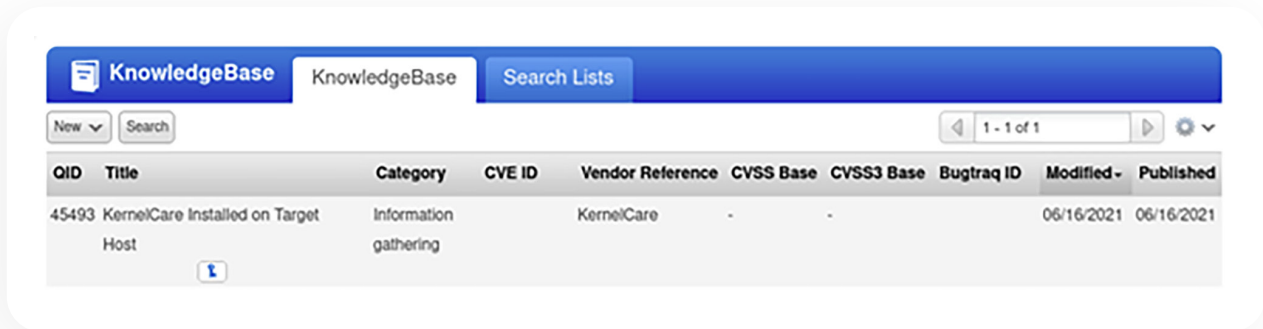
## Business Value

<p><b>Protecting Linux hosts against attacks</b></p>	 <b>Qualys.</b> <p>Qualys Cloud Agents also protect virtual environments – like cloud workloads, VDI, public/private clouds, Kubernetes, and Docker containers. Flexible installation options make it easy to include COE, primary server, Docker/Kubernetes, and VDI images.</p>	 <b>TuxCare</b> <p>TuxCare KernelCare Enterprise provides live patching of the Linux kernel on all major Linux distributions.</p>
<p><b>Kernel Aware protection</b></p>	<p>Qualys is KernelCare aware and provides the correct output for "information gathered."</p>	<p>KernelCare Enterprise operates as a recurring task residing as kernel modules. It executes live patching in memory at configurable intervals without rebooting.</p>
<p><b>Reporting into Qualys</b></p>	<p>Qualys’ report reflects accurate vulnerabilities when systems are protected with TuxCare’s KernelCare Enterprise.</p>	<p>TuxCare communicates updated successful live patching status in TuxCare ePortal and popular management tools via integrations.</p>



## Interconnecting with Qualys Solution Stack

TuxCare, a global leader in live patching Linux hosts, integrates into Qualys to help reduce false positive reporting. Qualys aware, TuxCare loads into memory and provides live patching for kernel vulnerabilities without rebooting any services. Many hosts worldwide protected by TuxCare need live patching because their services can not be taken down.



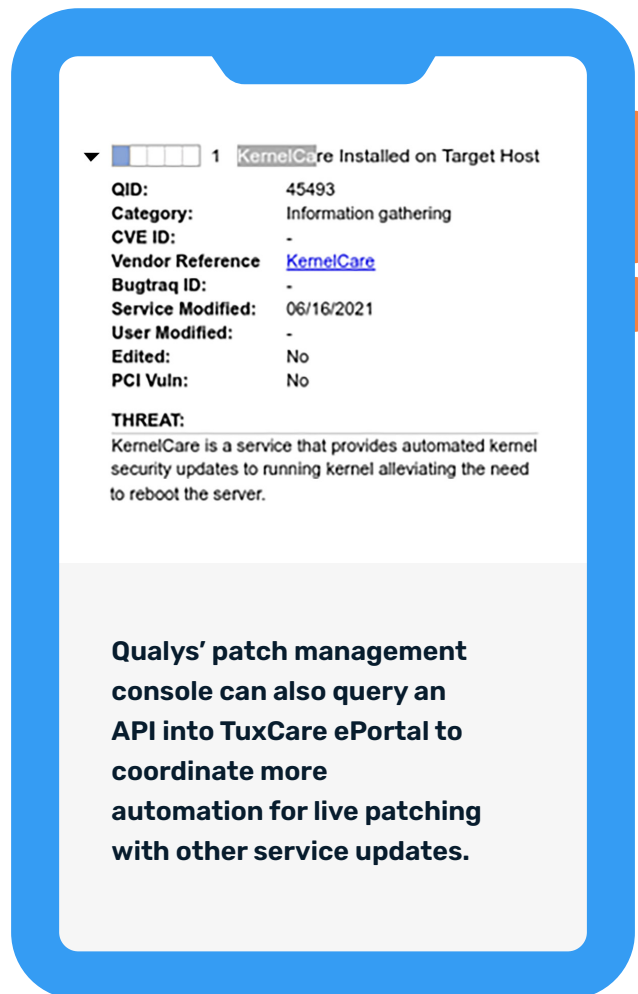
QID	Title	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3 Base	Bugtraq ID	Modified-	Published
45493	KernelCare Installed on Target Host	Information gathering		KernelCare	-	-		06/16/2021	06/16/2021

TuxCare KernelCare provides Qualys with a `kcarectl -Uname` command-line utility that shows the kernel's patched version, representing the kernel's security level up to the reported patched version. KernelCare provides a report by running `careful-patch-info` (and through API) that presents the CVEs patched by KernelCare in the currently running kernel.

Tuxcare's KernelCare Enterprise ePortal supports several versions of Linux and important shared libraries like OpenSSL and glibc.

KernelCare Enterprise integrates with Qualys automation tools to facilitate faster and more efficient patching, provides better control of your patching server, and gives you better round-the-clock support.

Qualys' patch management console can also query an API into TuxCare ePortal to coordinate more automation for live patching with other service updates.



▼ 1 KernelCare Installed on Target Host

**QID:** 45493  
**Category:** Information gathering  
**CVE ID:** -  
**Vendor Reference:** [KernelCare](#)  
**Bugtraq ID:** -  
**Service Modified:** 06/16/2021  
**User Modified:** -  
**Edited:** No  
**PCI Vuln:** No

**THREAT:**  
KernelCare is a service that provides automated kernel security updates to running kernel alleviating the need to reboot the server.

**Qualys' patch management console can also query an API into TuxCare ePortal to coordinate more automation for live patching with other service updates.**

# 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.



# About Qualys

---

Founded in 1999 as one of the first SaaS security companies, Qualys has established strategic partnerships with leading cloud providers like Amazon Web Services, Microsoft Azure, and the Google Cloud Platform, and managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, DXC Technology, Fujitsu, HCL Technologies, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding Cloud Security Alliance (CSA) member.

