TuxCare
We Take Care of Linux

WHITEPAPER

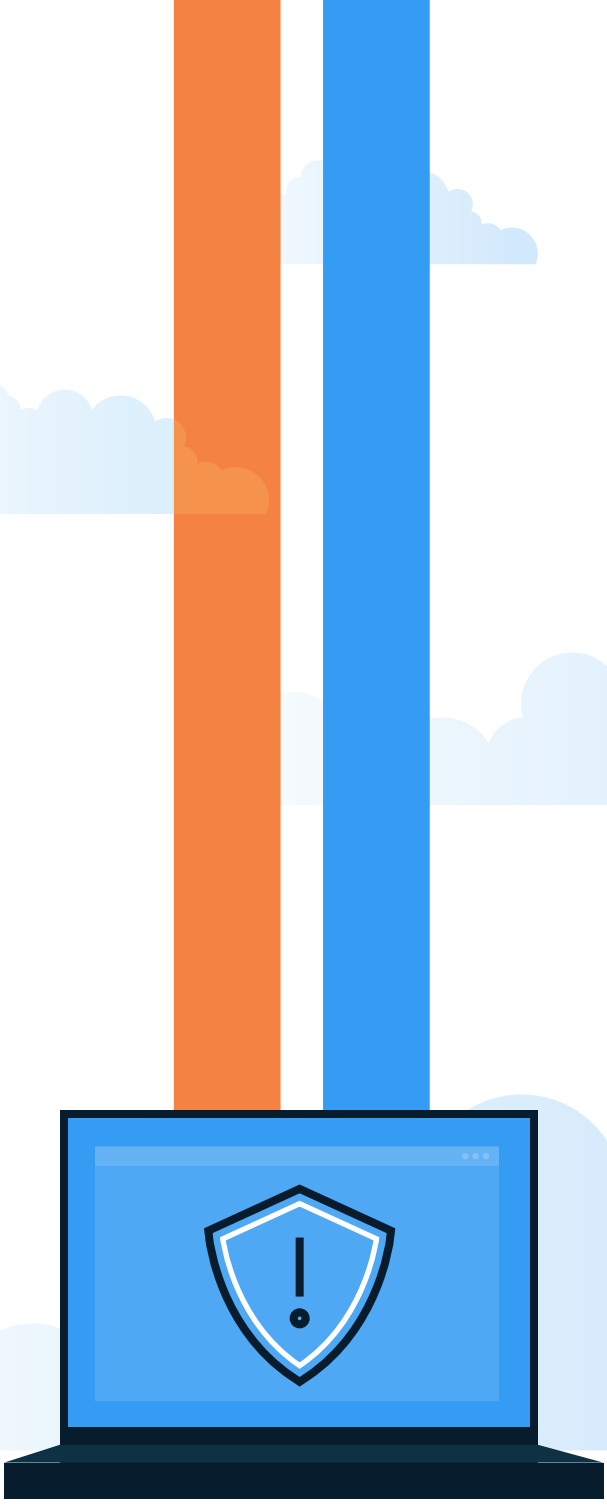
Tuxcare Live Patching - Qualys Technology Alignment Strategy

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 will 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 demonstrating the deep experience and capability of any SecOps team.



Qualys vulnerability 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

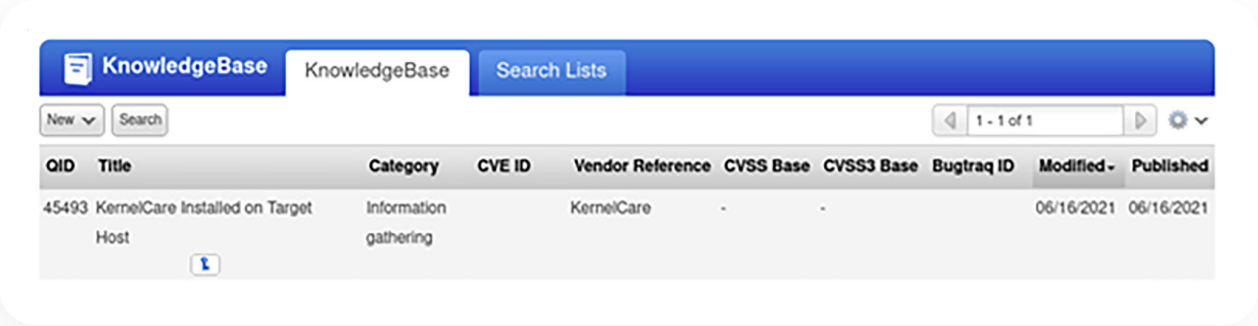
Live patching of additional hosts in development, staging, and QA is recommended.

Business Value

	Qualys.	TuxCare
Protecting Linux Hosts against attacks	Qualys Cloud Agents also protect virtual environments – like cloud workloads, VDI, public/private clouds, Kubernetes, and Docker. Flexible installation options make it easy to include COE, primary server, Docker/Kubernetes, and VDI images.	Tuxcare KernelCare Enterprise provides live patching of the Linux kernel on all major Linux distributions.
Kernel Aware protection	Qualys is KernelCare-aware and provides the correct output for "information gathered."	Tuxcare KernelCare enterprise lightweight agents reside as kernel modules. The agent executes live patching in memory at configurable intervals without rebooting.
Reporting into Tenable VPR Platform	Qualys' report reflects accurate vulnerabilities when systems are protected with TuxCare's KernelCare Enterprise.	Tuxcare communicates updated successful live patching status in Tuxcare ePortal and popular management tools via integrations.

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.

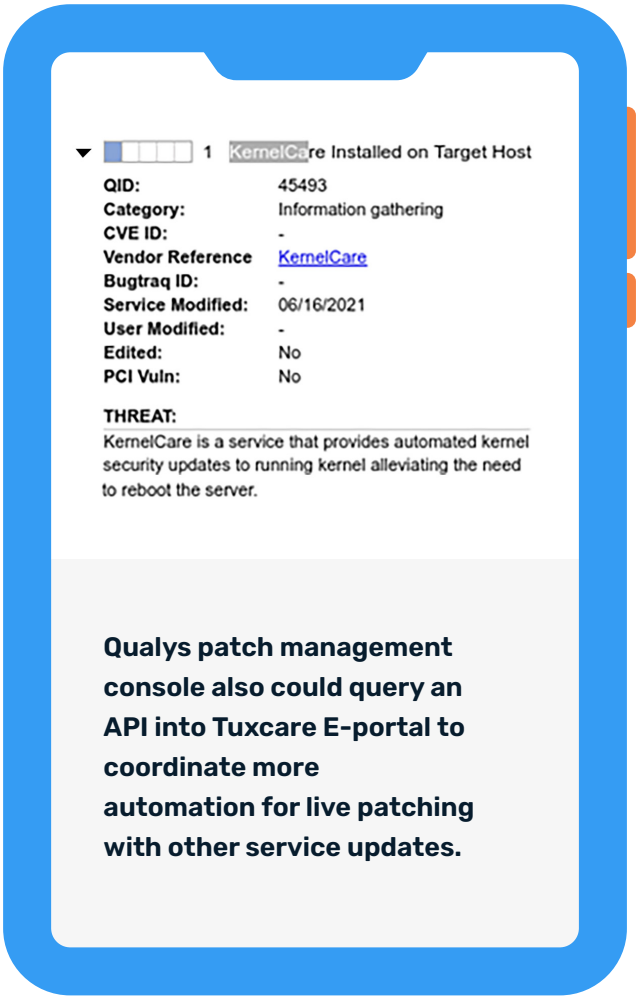


Tuxcare KernelCare provided Qualys with a kcarectl –Uname command-line utility that shows the kernel's patched version, representing the kernel's security level up to the reported patched version. KernelCare provides a report by running careful–patch–info (and through API) that presents the CVEs patched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

Tuxcare's KernelCare Enterprise e-portal 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 also could query an API into Tuxcare E-portal to coordinate more automation for live patching with other service updates.



Qualys patch management console also could query an API into Tuxcare E-portal to coordinate more automation for live patching with other service updates.

About TuxCare

TuxCare team came a long way from the first release of our first service – KernelCare – six years ago. Based on customer demand, we kept adding integrations to vulnerability scanners, reporting and automation tools, and an improved ePortal; all of which now comprise KernelCare Enterprise.

- TuxCare patch management services have delivered patches and bug fixes for various Linux distros for over ten years.
- TuxCare supports over 1 million production workloads secured and supported by our services.
- We have over 1500 customers from multiple industries around the world.
- TuxCare has patched more than 2,000 vulnerabilities without reboots over the years.
- We have supported more than 40 Linux distributions.
- We assist clients in maintaining their compliance requirements and regulatory mandates.

Learn more at: https://tuxcare.com/live-patching-services/kernelcare-enterprise/

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.

To know more, visit tuxcare.com