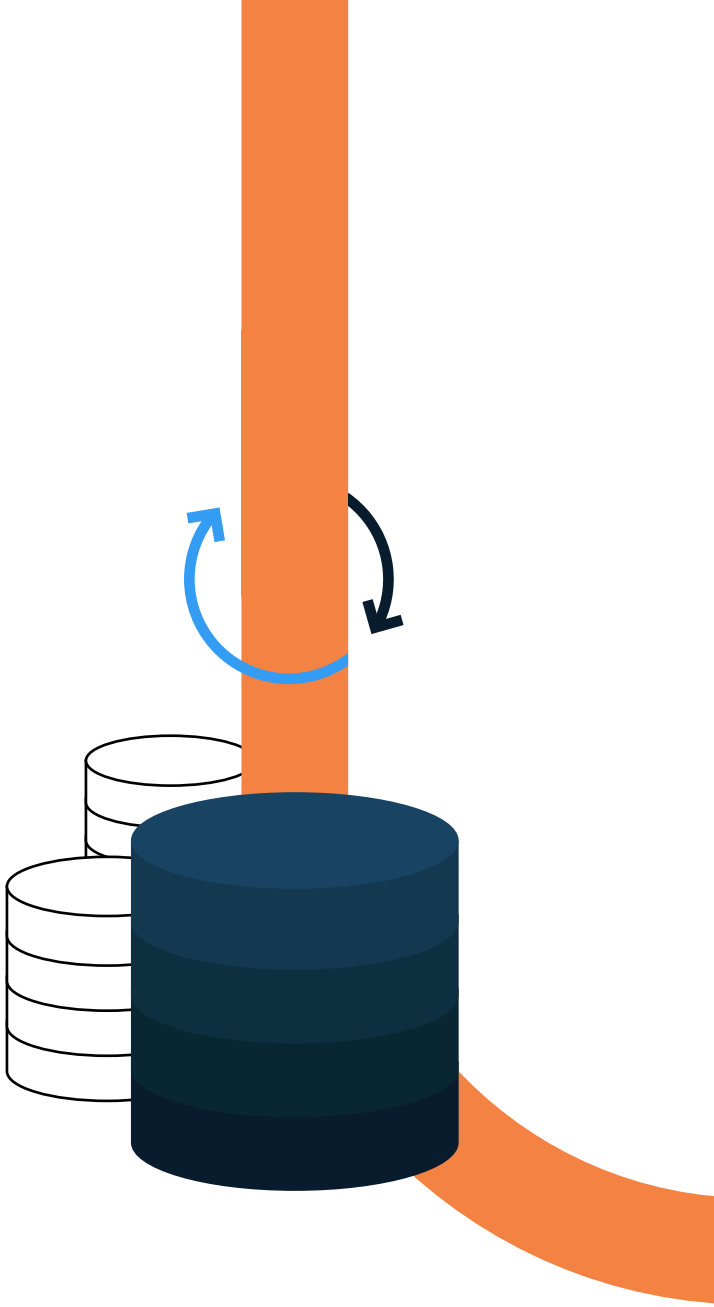
TuxCare
We Take Care of Linux

WHITEPAPER

KernelCare Live Patching with CrowdStrike Linux Host Protection

Challenges

Reducing exposure to production systems is a constant challenge for all SecOps and DevOps teams. As more vulnerabilities surface in Linux hosts, creating a change control event remains an operational challenge for organizations. Hackers continuously scan public-facing systems looking for a wide range of vulnerabilities. Once they discover an exploitable vulnerability, hackers will attempt to load rootkits and other tools to create a launch platform for their internal attacks.



Buying Time Until the Next Patching Cycle

CrowdStrike's Falcon light-weight agents help stop many exploits, including reducing the attack surfaces before, during, and after a zero-day attack against all hosts, including Linux systems. With this level of protection, organizations can strategically plan out their patching cycles to improve the mean-time to patching (MTTP) exposure window.

Managing Mean-Time-to-Patch Timelines

According to Infosec the mean time between patching (MTTP) for vulnerabilities is "between 60 and 150 days, and security and IT teams tend to take at least 38 days to push out a patch." Closing the exposure window is critical to reducing the risk of attacks and exploits. However, many organizations will schedule patches after they have tested and scheduled for a possible system reboot.

Security patching a system is critical to blocking a hacker's attempt to control a system. Many Linux systems and Microsoft solutions issue several patches weekly, monthly, and sometimes daily.

How will SecOps and DevSecOps keep up with all the kernel upgrades and maintenance updates?

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

	CROWDSTRIKE	TuxCare
Protecting Linux Hosts against attacks	CrowdStrike Falcon Pro, Enterprise, Elite, and CWP support various Linux operations, including Amazon Linux, AWS Graviton processors, Red Hat, CentOS, Oracle, SUSE, Debian, and Ubuntu.	TuxCare KernelCare Enterprise provides live patching of the Linux kernel on all major Linux distributions.
Reducing the MTTP window exposure	CrowdStrike lightweight agents protect with advanced AI & ML security engines protect hosts between patch cycles.	TuxCare KernelCare Enterprise lightweight agents reside as kernel modules. The agent executes live patching in memory at configurable intervals without rebooting.
Reporting into Falcon Spotlight	CrowdStrike agents report to a Falcon Spotlight that shows valuable endpoint data including successful patches.	TuxCare reports updated successful live patching status in Tuxcare ePortal and in popular management tools via integrations.

A Technical Solution from TuxCare

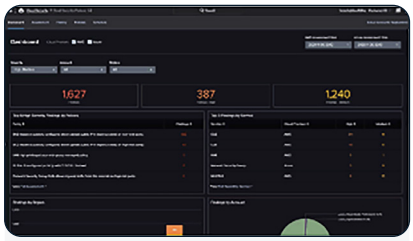
Server reboots and service restarts make you vulnerable and non-compliant. KernelCare Enterprise takes on most of the patching lifecycle tasks and completes them in four steps without a system reboot, reducing typical patch cycle tasks by 60%. Once this process is finished, your Linux kernels are protected against all known kernel vulnerabilities.

- Rebootless Linux Kernel Patching & Custom Patching
- Works On-prem & in the cloud
- Private patch server for gated infrastructures - ePortal
- Out-of-the-box integration with patch management & vulnerability assessment tools

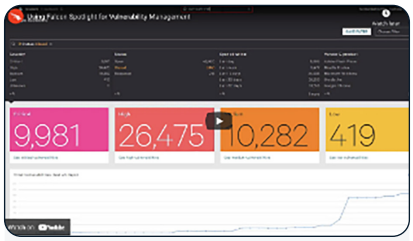
Interconnecting with CrowdStrike's Solution Stack.

Here is an example of an ideal workflow between TuxCare and CrowdStrike aligning to reduce attack surfaces:

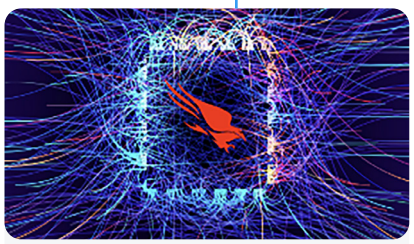
CROWDSTRIKE



CrowdStrike's Falcon Sportlike is uniquely positioned to address that need by providing real-time information through a cloud-delivered while overcoming many of the challenges with legacy network-based vulnerability solutions.



Cloud security posture management that detects and prevents misconfigurations and controls, plane threats, eliminates blind spots, and ensures compliance, across AWS, Azure, and Google Cloud.



The Falcon Fusion SOAR framework integrates with the industry-leading CrowdStrike Falcon® platform.

TuxCare

- Rebootless Linux Kernel Patching & Custom Patching
- Works On-prem & in the cloud
- Private patch server for gated infrastructures - ePortal
- Out-of-the-box integration with patch management & vulnerability assesment tools

Enabling TuxCare live patching for critical systems helps organizations reduce attacks while not impacting the hosts or existing connections. Clients leverage endpoint security from CrowdStrike to gain incredible protection value between essential patching cycles.

Patching complex systems continues to be a challenge for every organization.

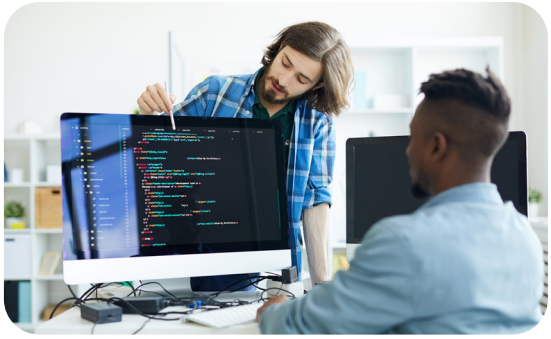
For example, production systems, critical databases, and Internet of Things (IoT) devices must stay up 100% with minimal downtime. Often, these devices and systems have regulated service level agreements requiring uptime with minimal system downtime.

The ultimate goal is to reduce the attack surface through live patching without the need to wait to reboot critical hosts.

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 called KernelCare Enterprise.

- Live patching reduces the window because patches can be applied since there is no need to wait for reboots or service restarts.
- The automation portal provides the window because IT teams can reduce the time it takes them to take new patches through staging and testing, then apply them.
- TuxCare patch management services have delivered patches and bug fixes for various Linux distros for over ten years.
- TuxCare is approaching 1 million in 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 CrowdStrike

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI). It offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 5 trillion endpoint-related events per week in real-time from across the globe, fueling one of the world's most advanced data platforms for security.

To know more,
visit tuxcare.com