# Cisco IOS-XR with Live Protect

## Autonomous router defense at line rate: Reduce vulnerability exposure before the next patch window

### Autonomous defense for mission-critical routing networks

Modern service provider and enterprise networks have reached a critical inflection point. With autonomous AI tooling compressing the window between public vulnerability disclosure and weaponized zero-day attacks to under 38 hours, traditional mitigation models—relying on emergency maintenance windows, traffic rerouting, and multi-month operating system patching cycles—can no longer keep pace.

Cisco IOS-XR natively integrates Live Protect, embedding autonomous runtime exploit mitigation directly into the carrier-grade routing engine. By applying Cisco validated shields directly in memory, Live Protect acts as a high-assurance compensating control that neutralizes exploit attempts—such as memory corruption, buffer overflows, and control-flow hijacking—without waiting for full OS upgrades and without requiring disruptive reboots.

Live Protect operates seamlessly across Cisco® 8000 routers to drastically reduce exposure days. Rather than simply avoiding software patches, it enables SecOps and NetOps teams to complete permanent software fixes through orderly, scheduled release workflows.

© 2026 Cisco and/or its affiliates. All rights reserved.

### Key customer benefits

- **Instant runtime resilience:** Neutralizes zero-day exploits in seconds, closing the 38-hour vulnerability exposure window without waiting for OS upgrade cycles.
- **Zero-impact speed:** Natively embedded in the IOS-XR kernel—delivering multiterabit defense with zero added latency, zero jitter, and no external middleboxes.
- **100% in-service continuity:** Applies validated vulnerability shields with zero service disruption, zero route flapping, and no router reboots required.
- **Streamlined SecOps and lower TCO:** Eliminates emergency patching overtime, avoids SLA breach penalties, and provides telemetry into Splunk®, Cisco Crosswork®, and security operations center tools.

## Executive/Strategic vision quote

“Zero-day vulnerabilities now outpace traditional patching workflows. Live Protect on IOS-XR eliminates that exposure window by automatically shielding vulnerabilities directly inside the router’s operating system—delivering instantaneous resilience with zero network downtime.”

– Strategic Vision, Cisco Service Provider Security and Routing

## Operational lifecycle: From advisory to patch

- **Stage 1 – Advisory:** Cisco Talos® and PSIRT teams publish critical vulnerability guidance and the permanent fixed-software path.
- **Stage 2 – Validated policy:** Cisco delivers signed, release-specific shield policies ready for immediate runtime deployment.
- **Stage 3 – Monitor or enforce:** Teams safely evaluate operational telemetry in Monitor mode before activating active enforcement.
- **Stage 4 – Patch and retire:** Permanent software upgrades are deployed during scheduled maintenance windows, cleanly retiring the temporary shield.

## Supported platforms and Licensing model

- **Supported platforms:** Cisco 8000 Series (Silicon One®)
- **Licensing model:** Embedded natively under Cisco IOS-XR Software Innovation Access (SIA) Essentials subscription and Cisco Enterprise Agreement 3.0.
- **No standalone product IDs:** No separate hardware appliances, sidecar licenses, or add-on feature PIDs required.
- **Management integration:** Cisco Crosswork Network Automation and standard IOS-XR telemetry pipelines.

## Next steps

Transition your routing infrastructure from reactive emergency patching to autonomous defense. To schedule a live dCloud demonstration, contact your Cisco account representative or visit cisco.com/go/iosxr.

© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C45-6807406-00 11/26