Cisco Live Protect

(Isovalent's Cilium Tetragon)

Cisco Partner
https://cs.co/1page

Cisco **Live Protect** is a real-time vulnerability shielding feature designed to reduce exposure to critical vulnerabilities on supported bellsCisco products during the period between vulnerability disclosure and the deployment of permanent patches or software fixes without requiring upgrades, reboots, or downtime.

Benefits:

- Reduces vulnerability exposure before patching.
- Maintains continuous operations without requiring reboots.
- Provides lifecycle governance through integrated workflows: monitor, enforce, disable, and retire protections.
- Several CVEs can be totally blocked live without a reboot or a software upgrade with Enforcement Mode.
- Live Protect is available at no additional cost on select Cisco platforms and is integrated into the product lifecycle.

Modes of Operation:

- **Monitor:** logs and reports matching policy events without enforcement, allowing teams to assess impact before applying protection.
- **Enforce:** actively blocks or mitigates detected threats in real time.
- **Disable:** temporarily disables a deployed policy without uninstalling it.

Features:

Tetragon: a flexible observability and runtime enforcement tool that applies policy and filtering directly with eBPF. allowing for reduced observation overhead, tracking of any process, and real-time enforcement of policies.

eBPF: A software development technology that allows custom, event-driven code to run directly within the kernel of the OS without needing to change the kernel itself.

Live Protect Policy: The deployable policy that may implement a Vulnerability Shield, subject to product, release, delivery path, mode, management, and lifecycle support.

Vulnerability Shield: A specific type of Live Protect policy provided and validated by Cisco. It targets a selected, validated vulnerability condition on supported Cisco products to provide runtime protection.

Live Detect: A threat identification system that works alongside Live Protect, allowing administrators to apply pinpoint compensating controls to a running switch or router.

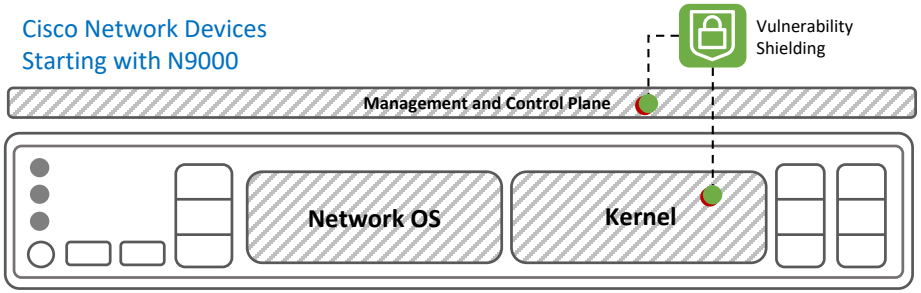
FAQs:

Q: Does Live Protect replace patching?
A: No. Live Protect is a compensating control designed to mitigate risk during the interim period between vulnerability disclosure and remediation. Customers should continue to prioritize regular software maintenance and deploy permanent patches or fixed software releases.

Q: Is every vulnerability eligible for Live Protect?
A: No. Shield availability is determined by a range of factors, including the nature of the vulnerability, exploit characteristics, supported platform, software release, policy, mode, and Cisco validation status.

Q: Can customers monitor before enforcing?
A: Where supported, yes. Monitor mode records matching events without active enforcement, enabling an assessment of potential operational impact before transitioning to a full enforcement policy.

Q: What products support Live Protect?
A: Availability is specific to the supported Cisco product, software release, policy, mode, delivery path, management surface, and lifecycle support. We recommend that customers consult Cisco security advisories and product documentation to identify the specific protections available for their infrastructure. Read below for the latest information on supported products.



Resources:

Live Protect (Blog)	Cloud Control (Blog)	Tetragon.io	LP for Nexus
Live Protect FAQ's	Cisco Security Advisories	Supported Products	Public Page

Example SKU: ***n/a***