Mitigate Data Center Networking Security without Disruption in Real Time

The cost of vulnerabilities in critical data-center infrastructure

Data centers, powering AI backend and inference systems, are vital to modern business. However, their critical role also heightens risk. An unpatched CVE or 0-day attack can lead to financial loss, reputational damage, and service disruptions.

In today's threat landscape, this "patching gap" is a critical vulnerability. While attackers take just hours to exploit a CVE, defenders often require weeks or even months to test and deploy patches across production environments.

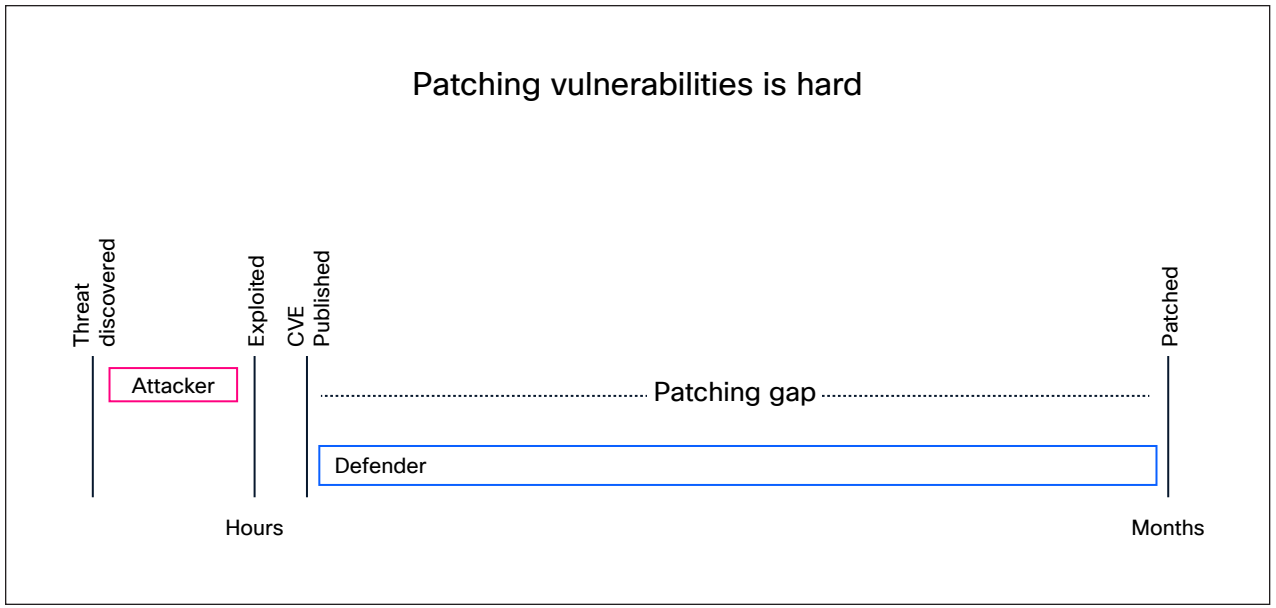

Figure 1. Patching vulnerabilities is challenging

Cisco® Live Protect changes the game by providing immediate vulnerability shielding for Cisco Nexus® switches, allowing you to stop attacks without stopping your network. Maintaining data center infrastructure requires consistent security and reliable uptime. Traditional CVE patching often causes disruptions and downtime. Cisco Live Protect for N9000 Series switches offers real-time shields to mitigate vulnerabilities instantly, ensuring continuous protection and stability—without emergency maintenance or urgent upgrades.

Why Cisco Live Protect?

Traditional patching requires maintenance windows, reboots, and potential downtime. Cisco Live Protect offers a revolutionary approach to security:

- **Zero downtime:** Apply security policies to live systems without a switch reboot.
- **Immediate protection:** Shield vulnerabilities as soon as a threat is discovered, long before a standard PSIRT upgrade is scheduled.
- **Continuous re-validation:** Maintain a secure posture with eBPF-powered security observability.
- **Operational efficiency:** Security SMUs (shields) are removed once a full PSIRT-bundle upgrade is applied.

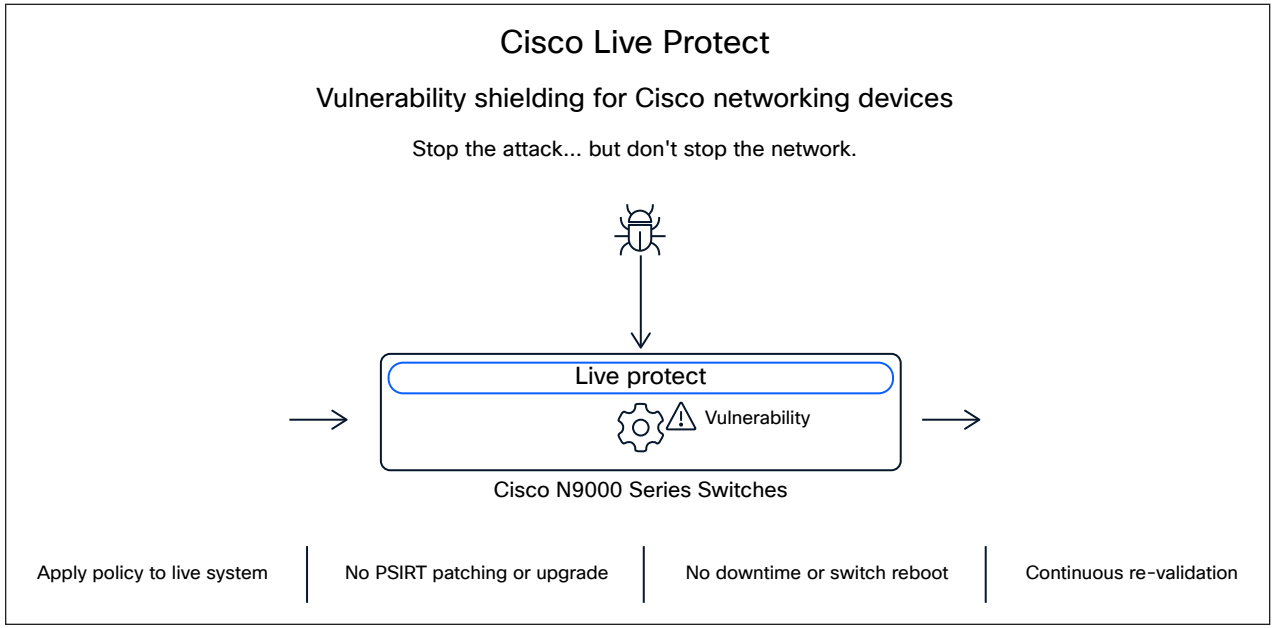

Figure 2. Live Protect

Innovation powered by eBPF

Cisco is the first to market with an enterprise-grade Tetragon agent built directly into Cisco NX-OS starting with the 10.6(1)F release. By leveraging eBPF (extended Berkeley Packet Filter), Live Protect provides deep kernel-level visibility and enforcement for:

- Privilege escalation prevention
- Control-plane protection
- API and CLI security
- File I/O monitoring

Supported platforms

Live Protect is available for Nexus customers with an **Essentials license or higher**.

Platform support (Cisco NX-OS 10.6(2)F):

- Cisco N9300 and N9200 fixed platforms (≥24GB RAM)
- Cisco N9300 Smart Switches
- Cisco N9400 Series Switches

How it works

Cisco Live Protect uses advanced eBPF technology to deliver real-time security for data center network devices. Configuration is flexible, allowing management on individual devices through Cisco NX-OS CLI or API, for full automation across your data center fabric through CI/CD pipelines. Nexus Dashboard provides centralized orchestration, offering instant visibility into CVE-affected devices, automating the deployment of security shields, and continuously monitoring their effectiveness.

Components

- **Cisco Live Protect:** delivers kernel-level protection on network devices using eBPF technology.
- **Tetragon Agent:** compiles CVE compensating controls into deployable eBPF policies
- **Nexus Dashboard:** centralized console for orchestration, visibility, and monitoring across all Cisco Nexus switches
- **Integration tools:** APIs, CLI, and CI/CD pipeline support for seamless automation and management

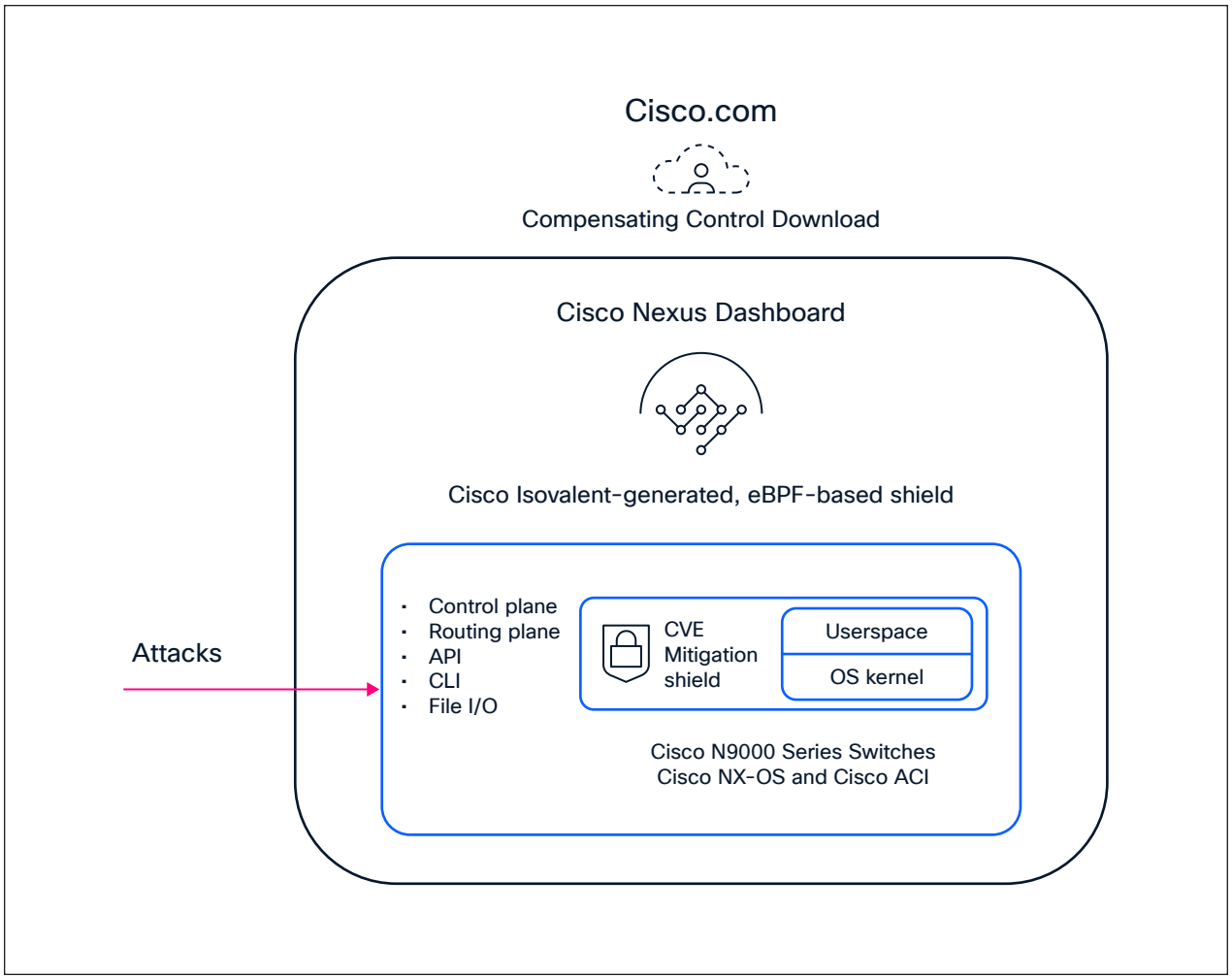

Figure 3. Live Protect and CVE mitigation for Cisco N9000 Series Switches

Live Protect ensures streamlined upgrades and continuous vulnerability mitigation in Cisco NX-OS and Cisco ACI® environments, maintaining uninterrupted security and performance from the infrastructure core across your entire system.

Learn more

Protect your data center with Cisco Live Protect for real-time, automated security and zero downtime.

Learn more on our Cisco Live Protect blog or contact your Cisco representative today.

Resources

Cisco Live Protect webpage

See Cisco Live Protect in action with video

Cisco NX-OS release notes.

Use cases

Industry	Key Use Cases for Cisco Nexus and Live Protect
Financial Services	• Real-time CVE mitigation • Zero-day attack protection • Minimize downtime for critical applications • Enhanced compliance and audit readiness
Healthcare	• Protect sensitive patient data • Real-time CVE mitigation • Continuous availability of healthcare systems • Compliance (e.g., HIPAA)
Retail and E-Commerce	• Secure payment and customer data • Minimize downtime during peak periods • Real-time CVE and zero-day protection • Compliance with PCI DSS
Government and Public Sector	• Centralized security orchestration • Zero-day threat response • Regulatory compliance • Protect sensitive information and ensure public service uptime
Telecommunications and Service Providers	• Defense against advanced threats (e.g., DDoS) • Maintain uninterrupted network performance • Automated security operations • Centralized policy management
Energy and Utilities	• Secure critical control systems • Real-time CVE and zero-day attack mitigation • Regulatory compliance • Maintain resilience and uptime
Education and Research	• Protect intellectual property and sensitive data • Continuous access to digital resources • Real-time threat response • Automated security operations
Manufacturing	• Secure OT and IT environments • Real-time mitigation of vulnerabilities • Protect intellectual property • Ensure operational continuity

C22-5771857-00 02/26