Ensure Data Center Security Without Disruption—Mitigate Threats in Real Time

Contents

When managing your critical data center network infrastructure, security and uptime are non-negotiable. Traditional patching for CVEs can lead to operational disruptions and unacceptable downtime for critical systems. With Cisco Live Protect support for Cisco Nexus 9000 Series switches, you can address emerging vulnerabilities immediately by deploying real-time shields that mitigate CVE exploitation. This proactive solution allows you to maintain continuous protection and operational stability—without the need for emergency maintenance or urgent code upgrades in your data center.

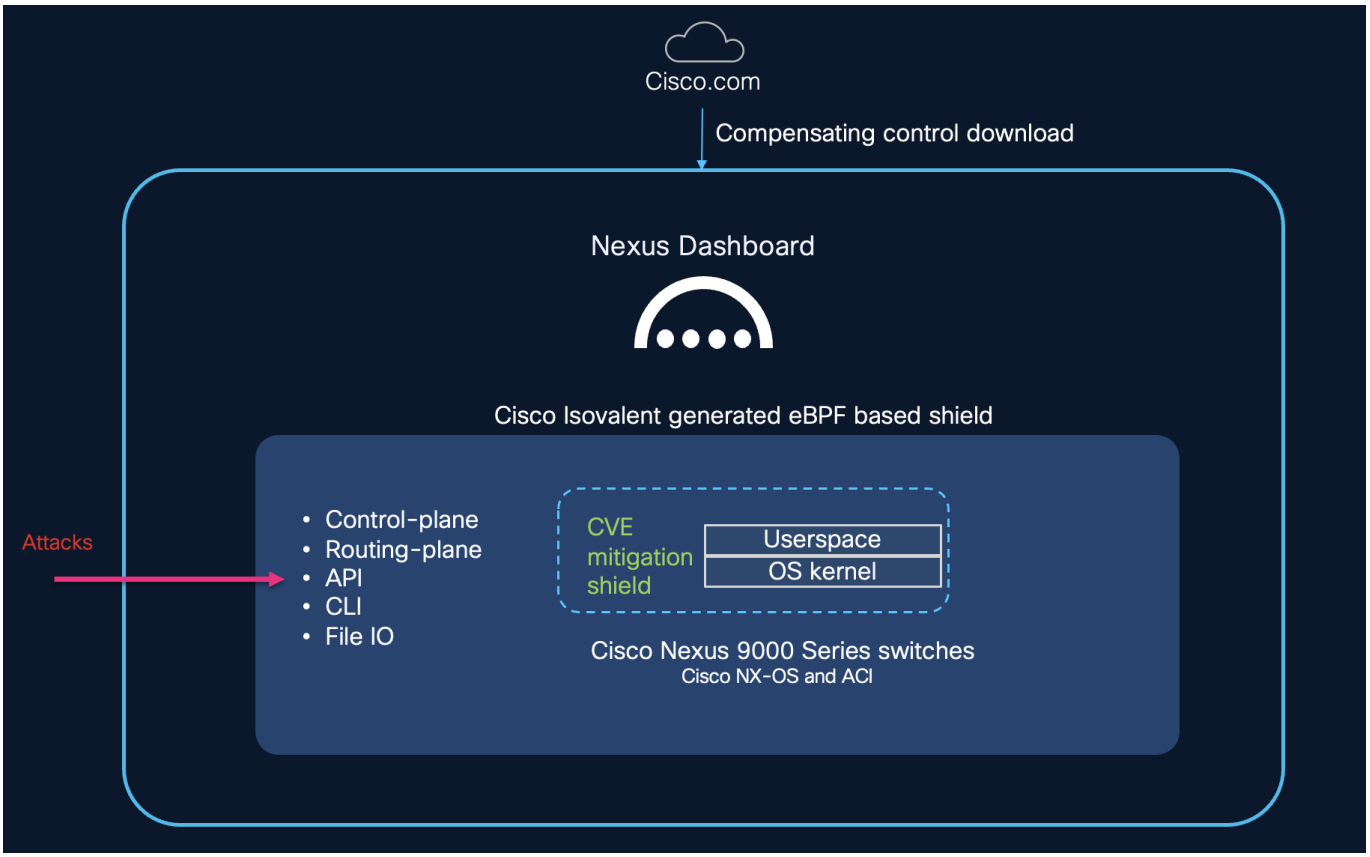

Figure 1.
Live Protect and CVE mitigation for Cisco Nexus 9000 Series Switches

Your Cisco Nexus data center network is the backbone of your business, powering applications, connectivity, communication, and growth. However, this critical infrastructure faces constant threats—from newly discovered privilege escalation vulnerabilities to DDoS attacks targeting network control traffic—that require swift response. Traditional approaches to addressing these vulnerabilities often rely on software upgrades, which can lead to operational downtime, higher mean time to repair (MTTR), and increased risk during transitional phases, especially in large-scale data center environments.

Cisco Live Protect redefines how enterprises address software vulnerabilities. With the Isovalent Tetragon agent integrated directly into NX-OS, Live Protect uses eBPF kernel-level controls to shield against privilege escalation vulnerabilities and network control-plane DDoS attacks. These real-time protections operate in either monitor or enforce mode, keeping your data center switches secure from CVEs—without the need for upgrades, reboots, patching, or downtime. By running Cisco Live Protect on your Nexus switches, you can stay ahead of cybersecurity threats and maintain uninterrupted business operations.

Cisco NX-OS features native integration of the Isovalent Tetragon agent, providing advanced kernel-level security that adapts to evolving CVE threats and scales with your network.

- **Advanced Threat Prevention:** NX-OS delivers kernel-level visibility and enforcement, providing strong protection against zero-day attacks, privilege escalation, and sophisticated DDoS threats.
- **Granular, Real-Time Security Controls:** Customize and deploy compensating controls in monitor, log, or enforce mode, enabling instant mitigation of CVEs with Cisco eBPF-based security shields.
- **Uninterrupted Security and Rapid Response:** Instantly deploy security shields and mitigations in real time—without reboots, disruptive updates, or maintenance windows—empowering network admins to quickly respond to vulnerabilities and maintain uninterrupted uptime.

The Cost of Vulnerabilities in Critical Data Center Infrastructure

Data centers, including AI backend and inference front-end systems, are now essential to every aspect of business operations. However, this critical role increases risk—just one unpatched CVE or zero-day attack can cause major financial loss, reputational harm, or service outages. Traditional patching methods require downtime, leaving organizations vulnerable during the process.

Network downtime is more than a technical setback; it's a business disruption. Cisco NX-OS Live Protect delivers real-time shielding against vulnerabilities, ensuring continuous security without interrupting daily operations.

How It Works

Cisco NX-OS Live Protect uses advanced eBPF technology to deliver real-time security for data center network devices. Configuration is flexible, allowing management on individual devices via NX-OS CLI or API, or 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.

Key Features

- **Real-Time Threat Protection:** Instantly access and apply the latest CVE compensating controls from Cisco for rapid response to new vulnerabilities.
- **Automated Shield Deployment:** Tetragon compiles CVE controls into eBPF policy shields, which are deployed in monitor or enforce mode for immediate mitigation.
- **Version Control & Rollback:** Every eBPF policy is versioned, allowing for safe rollbacks and flexible policy management.
- **Comprehensive Observability:** Monitor policy activity in real time and export logs to Nexus Dashboard, Splunk, or your preferred collector for integration with existing security tools.

Components

- **Cisco NX-OS 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.

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

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 & E-Commerce	• Secure payment and customer data • Minimize downtime during peak periods • Real-time CVE and zero-day protection • Compliance with PCI DSS
Government & Public Sector	• Centralized security orchestration • Zero-day threat response • Regulatory compliance • Protect sensitive information and ensure public service uptime
Telecommunications & Service Providers	• Defense against advanced threats (e.g., DDoS) • Maintain uninterrupted network performance • Automated security operations • Centralized policy management
Energy & Utilities	• Secure critical control systems • Real-time CVE and zero-day attack mitigation • Regulatory compliance • Maintain resilience and uptime
Education & Research	• Protect intellectual property and sensitive data • Continuous access to digital resources • Real-time threat response

Industry	Key Use Cases for Cisco Nexus and Live Protect
	• Automated security operations
Manufacturing	• Secure OT and IT environments • Real-time mitigation of vulnerabilities • Protect intellectual property • Ensure operational continuity

Cisco Nexus switches with Live Protect offer a unique advantage by delivering real-time, kernel-level security against vulnerabilities without requiring reboots or downtime. This solution enables instant, automated threat mitigation and centralized management across the network, reducing business disruption and manual effort. With seamless integration into existing NX-OS and ACI environments, comprehensive compliance support, and future-ready protection, Nexus switches help organizations maintain continuous security and operational resilience in today's dynamic threat landscape.

Protect your data center with NX-OS Live Protect for real-time, automated security and zero downtime. Learn more on our Live Protect blog or contact your Cisco representative today.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA Cxx-xxxxxx-xx 03/25