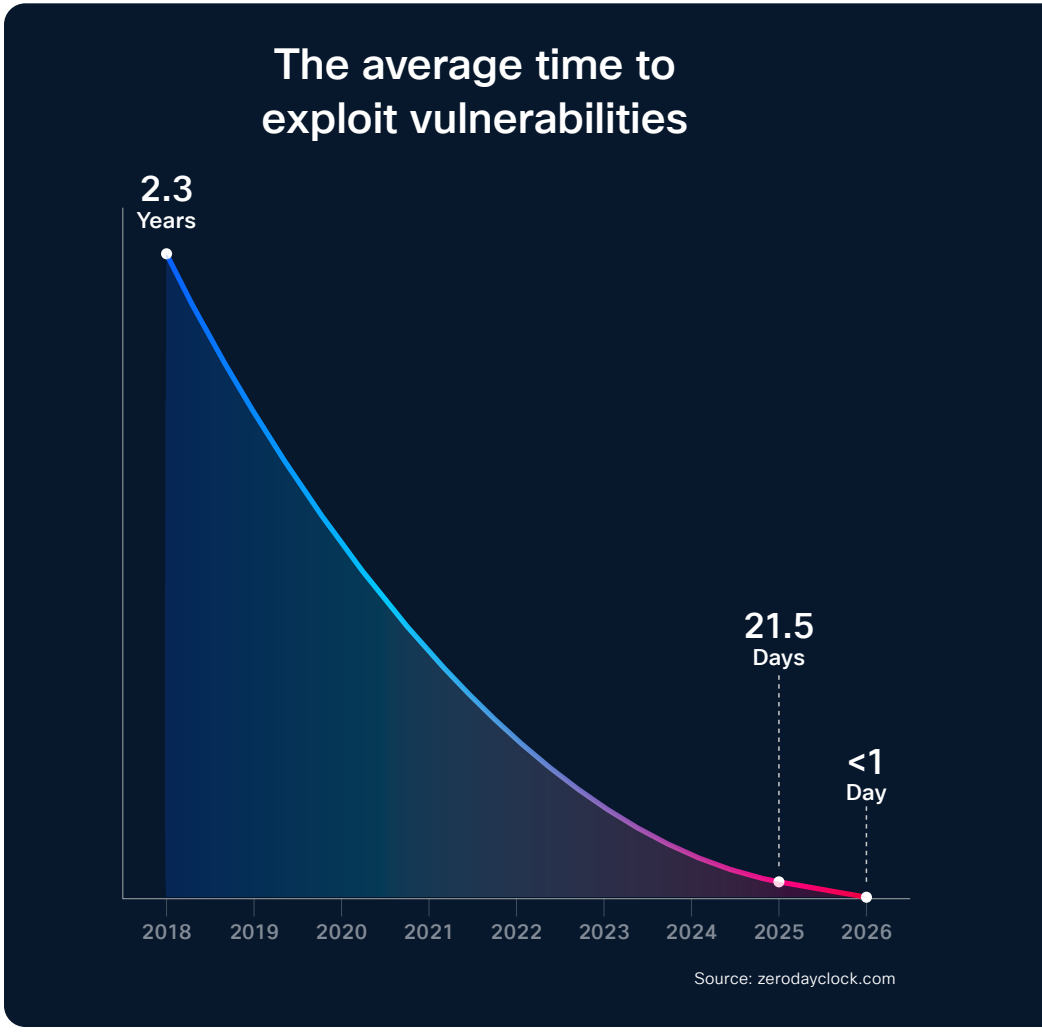

Live Protect
A new operating model for infrastructure

The Exploit Window Has Collapsed

For years, infrastructure teams could rely on a familiar rhythm. Critical network and security systems were tested carefully, rolled out deliberately, and changed sparingly. That model made sense when exploitation often lagged disclosure by weeks or months and when the greater operational risk seemed to be an urgent, unplanned change to the systems everyone depended on.

Two things have fundamentally altered the threat environment and changed the viability of the old paradigm. First, infrastructure—switches, routers, firewalls, wireless controllers, management systems, and the software that runs them—has become a primary attack surface.

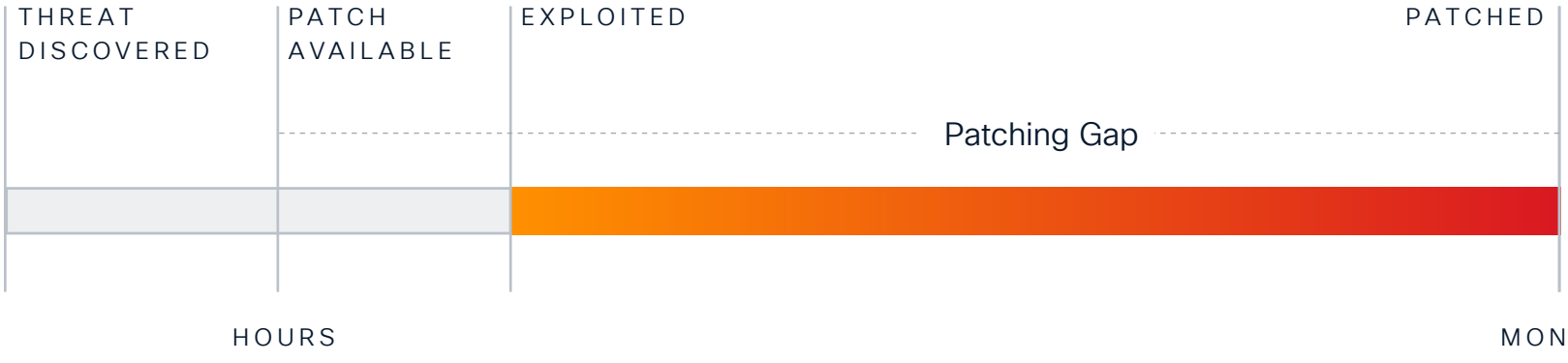
Second, a new generation of frontier AI models has taken a major step forward in their ability to find vulnerabilities in any software system. These models are getting better at understanding large, mature code bases, surfacing obscure interdependencies, and helping attackers move faster from vulnerability research to exploit attempts. And their capabilities are only accelerating.



The patching gap is where exposure becomes urgent: a known weakness, reachable systems, and remediation that still takes time.

The combination of these two factors has collapsed the exploit window. Frontier AI models are compressing the vulnerability timeline. Attackers no longer need weeks of manual analysis to understand how a flaw works or how to exploit it. With AI-assisted tooling, they can compare patched and unpatched code, identify the vulnerable path, and generate working exploit logic far faster after an advisory is released. The exploit window has shrunk from months or even days to just hours.

AI-speed attacks compress the patching window



The patching gap is where exposure becomes urgent: a known weakness, reachable systems, and remediation that still takes time.

48%
of network assets worldwide are now aging or obsolete

40%
of the top-targeted vulnerabilities directly impact EOL devices

32%
of the top-targeted vulnerabilities were at least 10 years old

Sources: Update Critical Cisco Report, Talos Year in Review 2025

A Paradigm Shift is Required

The industry—including vendors, their customers and partners—must adapt to this new world. The old approach was to sweat assets, defer change, and save major updates for annual or semiannual patch cycles.

As Volt Typhoon and Salt Typhoon showed, infrastructure is a prime target. Aging and end-of-life systems often remain exposed because patching them carries real operational and financial risk. In many environments, those systems technically can be patched, but teams delay because the business impact of downtime, regression, or failed upgrades is too high. In critical infrastructure, such as power grids, water plants, and manufacturing lines, the problem can become even harder—some systems cannot be patched safely without interrupting essential services.

When known weaknesses remain reachable, attackers do not need to find a new doorway. They only need the existing one to stay open long enough. Mix in AI-driven vulnerability discovery and automated exploitation, and we have reached a tipping point.

Organizations of every size need to adopt a new mindset. Modernizing infrastructure from the edge inward and implementing security best practices such as zero trust and segmentation are no longer optional. They are a requirement.

However, the bigger shift is operational. Infrastructure teams need to move away from large, infrequent upgrade events and toward a cloud-like model of smaller, safer, continuous changes. That is the new mindset: reduce the size of each change, increase the frequency of protection, and make adaptation part of normal operations rather than an emergency response.

A New Operating Model for Infrastructure

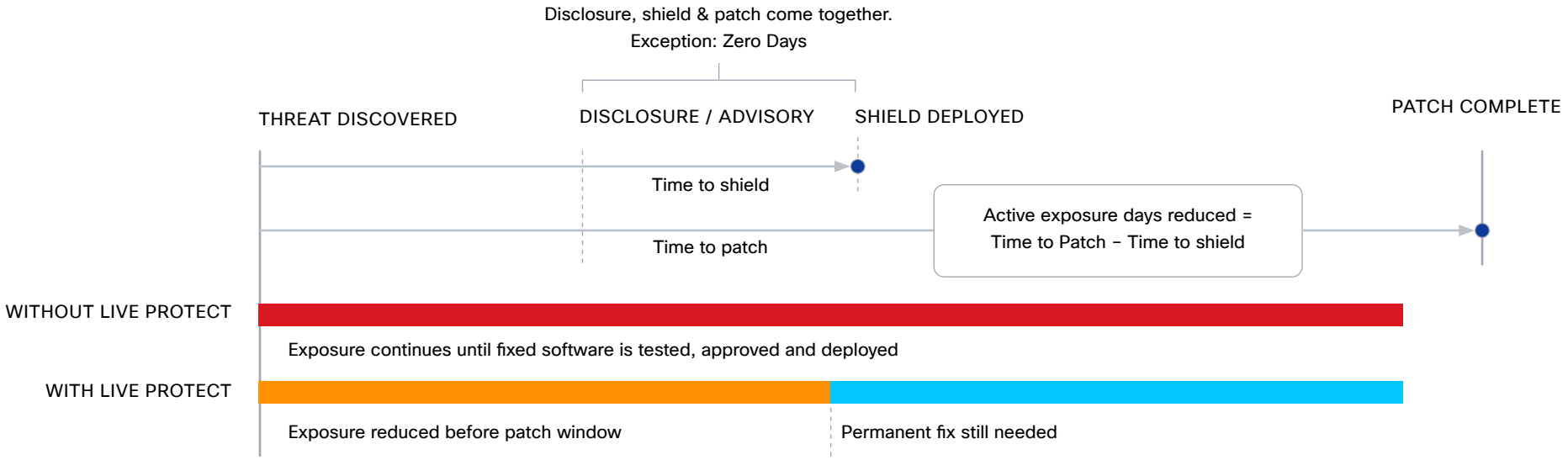
The objective is to keep systems running while making protection more continuous. This is the strategic intent behind Live Protect—a runtime protection capability embedded directly into supported Cisco devices.

Live Protect helps Cisco customers reduce the exposure gap between vulnerability disclosure and patch completion. It applies Cisco-validated runtime protection, called a Vulnerability Shield, to supported Cisco products and releases designed to help teams reduce exposure while they test and deploy the permanent software fix.

Reduce the exposure window with Live Protect

Live Protect is not a patch. It does not replace the need for core lifecycle discipline or permanent software updates. Instead, it serves as a temporary, targeted shield that mitigates the risk of a specific vulnerability with a few clicks. It is intended to be an emergency control that is applied to a running system without disrupting that system between more frequent maintenance windows.

For network, infrastructure, and security teams, the value is practical: reduce risk earlier, preserve uptime, and avoid turning critical advisories into an immediate reboot or emergency upgrade. For platform teams, it provides operational continuity while they plan the permanent fix and maintain patching discipline. And for security leaders, it creates a measurable protection motion—reduce exposure now and complete remediation on schedule.



A precise combination of technology, expertise, and process

Live Protect combines Cisco runtime technology, Talos threat intelligence expertise, and the Cisco Product Security Incident Response Team (PSIRT) workflows into one validated protection motion. Live Protect uses eBPF (Extended Berkeley Packet Filter) technology to run small, sandboxed programs inside the operating system kernel. This provides deep visibility and precise control to intercept exploit attempts at the source, without changing the kernel source code or requiring a system reboot.

The unique capabilities of eBPF allow us to create fine-grained, pinpoint controls that block a known vulnerability from being exploited. A Vulnerability Shield can be as specific as "do not allow this particular process to access this particular file." In simple terms, if that process should never access that file, we block it. The other advantage is that the shield has a negligible performance impact.

Live Protect is not a "Do It Yourself" runtime rule. When a vulnerability is disclosed, Cisco Talos analyzes the exploit path and creates a shield. Cisco then validates the shield through our internal engineering processes to help verify it is targeted, effective, and performant. Once deployed, the shield acts as a stopgap, designed to protect the system while the team prepares a permanent patch. Once the patch is applied, the shield is retired.

Cisco validates each shield before operators deploy it

01 → PSIRT advisory intake

02 → Talos exploit analysis & shield design

03 → Shield testing

04 → Disclosure, shield & patch release

05 → Operators stage & deploy

Together with the PSIRT workflow, Talos analysis, and Cisco engineering review, customers can have confidence that a shield will protect supported infrastructure until the permanent patch can be safely deployed.

Operationalizing Live Protect

Live Protect Shields are delivered as part of the Cisco advisory and patch workflow. When Cisco publishes a security advisory, customers can see affected products, supported releases, fixed software guidance, and any available shields. If a Vulnerability Shield is available, customers can deploy it, monitor activity, and move to enforcement. Shields can be managed through the supported product workflows in Cisco Cloud Control, as well as CLI and APIs.

Live Protect changes the operating model from an all-or-nothing response to a staged, controlled workflow, providing three distinct modes of operation:

- **Monitor Mode**: Logs exploit attempts and policy hits without enforcement, allowing teams to verify the threat before taking action.
- **Enforce Mode**: Actively blocks or mitigates threat activity.
- **Disable Mode**: Temporarily disables a policy without uninstalling it.

This phased approach is designed to provide infrastructure teams the ability to shrink the exposure window significantly, reducing the pressure to rush through emergency patches that haven't been fully vetted while allowing for a more orderly, predictable maintenance schedule.

Customers manage protection from monitor to retirement

1 **Available**
Cisco-validated protection published

2 **Monitor**
Review hits and side-effects, pre-enforcement

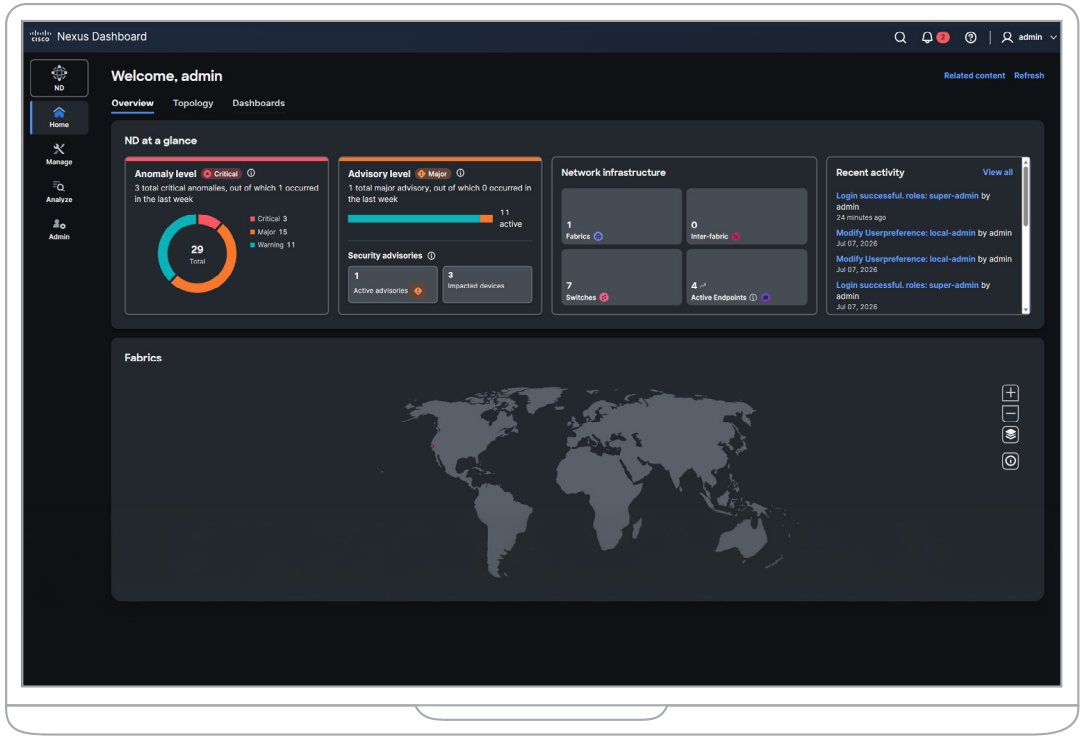
3 **Enforce**
Block or override targeted condition

4 **Patch**
Deploy fixed software

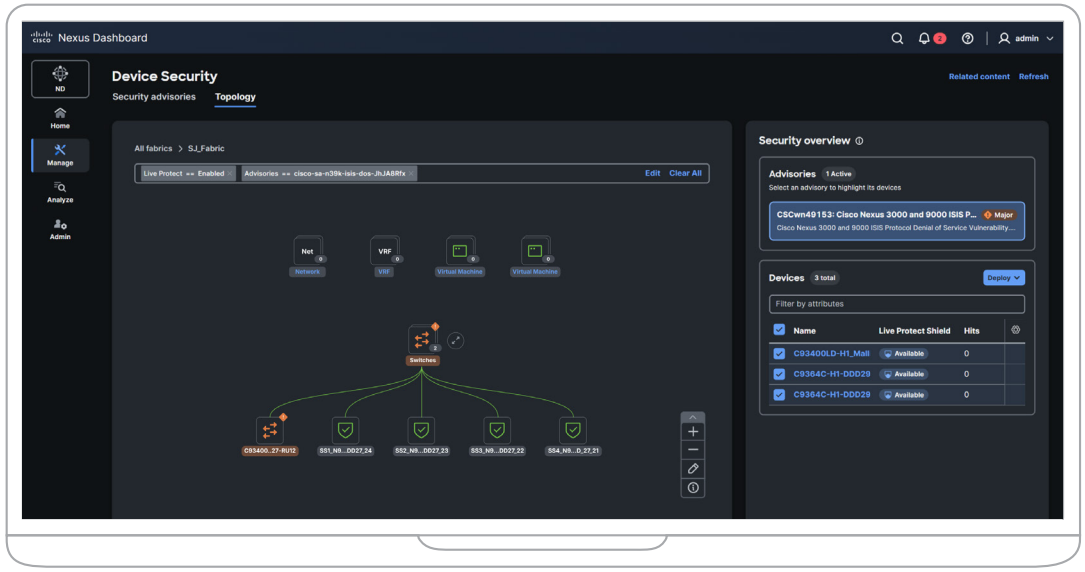
5 **Auto-retire**
When fixed software lands

Live Protect in Action

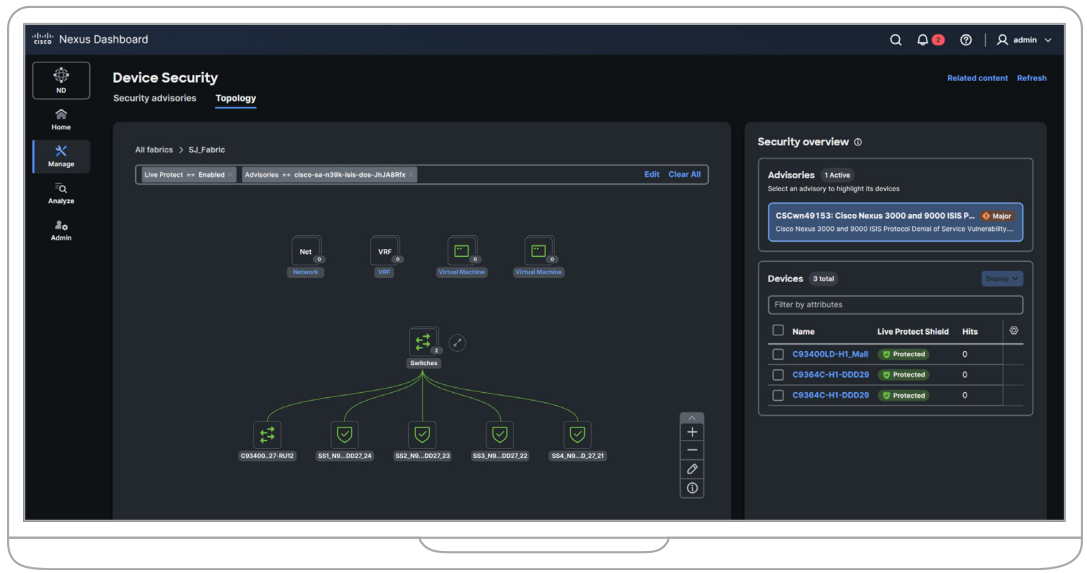
Cisco is currently shipping Live Protect on Cisco data center N9000 switches with plans to expand this across campus and branch switching as well as the Cisco Security portfolio. Live Protect is available in the Essential tier at zero additional cost on supported Cisco platforms and releases.



The Nexus Dashboard overview shows active advisories and impacted devices. Opening the Security advisories tab, administrators can see more detailed information about the advisory and Live Protect Shield availability.



The topology view of the Security advisories tab shows the impacted devices in orange. Details of the advisory and available shields, as well as the option to deploy the shields are shown in the list view on the right.



Once Live Protect Shields are deployed, the topology view changes to green and the list view shows the shield enforced and the device is protected. The vulnerability is now blocked without requiring a reboot to the system.

The Path Forward

Live Protect is an important step in Cisco's goal to embed resilience directly into the infrastructure fabric. As AI-powered tooling continues to evolve, the ability to apply Cisco-validated protections will become part of the baseline for enterprise infrastructure.

We will continue to take steps to harden infrastructure to prevent exploits, but vulnerability disclosures will still happen. What changes is how quickly and confidently we can respond. By moving toward a more dynamic, programmable operating model, we can maintain the uptime businesses require while ensuring our infrastructure remains secure.

The call to action is simple: start measuring the exposure gap. Know which infrastructure is supported, reachable, and owned. Build the operating muscle to review Cisco guidance, deploy validated protections where available, and complete patching on schedule.

Learn more at
Live Protect