

Cisco **Security**

Closing the Exposure Window

An exposure response model for the AI-accelerated threat era

Watch

Watch Cisco's briefing on how AI is compressing the exposure window and what defenders can do next.

A new standard for exposure response to AI-speed risk

Frontier models can now help analyze code, test hypotheses, and iterate through complex steps that once required scarce security expertise. With these capabilities, AI is compressing the time between vulnerability discovery, disclosure, and exploitation.

This changes how organizations need to protect infrastructure and applications. Traditional detection, response, mitigation and remediation still matter, but they're no longer enough when attackers can move faster than many teams can inventory, prioritize, and remediate risk.

Infrastructure is a prime target because aging and end-of-life systems often cannot follow normal patch/upgrade cycles.

When known weaknesses remain reachable, attackers don't need a new doorway; they only need the existing one to stay open long enough.

Security now needs an exposure response model: validate what is exposed, shield priority risk when patches or upgrades can't move fast enough, contain potential blast radius before exposure spreads, and give operations teams the telemetry and governance to act at the speed this threat environment demands.

The exposure window is shrinking. Defenders have to control every hour inside it.



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

Measure how fast exposure becomes action

AI-assisted attackers are shrinking the time between disclosure and exploitation.

They can analyze vulnerable code paths, test exploitation hypotheses, and scale activity once weaknesses are known. That changes what security teams need from vulnerability management. A prioritized patch list alone isn't enough.

A key operational question:

Once exposure is confirmed, how quickly can you turn it into a controlled response?

Four metrics that make exposure governable

Time to visibility

How fast can we determine what is vulnerable, reachable, owned, and material?

Time to protection

How fast can we reduce reachability or apply a validated temporary control?

Time to containment

How fast can we pre-position controls that limit potential blast radius?

Time to remediation

How fast can we deliver the durable fix, with testing and validation in place?

The goal is not to replace remediation. It’s to make every hour of exposure more controlled.

Control every hour inside the exposure window

An exposure response model for the AI-accelerated threat era

01

Find exposure

Identify vulnerable systems, reachability, ownership, business context, and affected identities before risk becomes impact.

Time to visibility

02

Shield priority exposure

Reduce who and what can reach vulnerable systems and apply validated temporary protections while durable fixes proceed.

Time to protection

03

Contain blast radius

Limit the blast radius of exposed systems, identities, sessions, and workloads if exploitation succeeds.

Time to containment

04

Govern response and remediation

Coordinate evidence, testing & validation, response actions, and durable fixes so teams can act quickly without losing control.

Time to remediation

Cisco helps security teams use existing controls and new AI-era capabilities as one response motion.

Time to visibility

A vulnerability flags risk. Context decides action.

Find exposed paths, not just vulnerabilities

Not every vulnerability is a fire drill. Exposure validation helps you focus on the ones that demand your attention. Instead of a patch/upgrade list, the goal is a simple decision - patch/upgrade, mitigate, or accept the risk.

Critical questions and powerful tools

What is vulnerable, and where is it running? Is it reachable externally, internally, or both?	Who owns the affected system or workload? What identities, systems, or services can reach it?	What action should reduce risk now?
Discovery & context inputs The raw signal, plus everything around it • **Scanners and third-party tools** find the vulnerability • **Cisco telemetry confirms** it is live and reachable • **Cisco AI Defense** adds AI application context • **Cisco Identity Intelligence** adds identity and access context • **Cisco Secure Access** adds access-path context	**Exposure correlation** Turns raw signals into answers • **Splunk Exposure Analytics** puts findings in a single view • **Cisco IQ** adds cross-portfolio risk context	**Protection decision** Five moves without guesswork • **Patch/upgrade normally** • **Shield now** • **Reduce reachability** • **Monitor closely** • **Accept risk**

More >

AI-accelerated vulnerability discovery

Time to protection

Patches and upgrades are the fix. Shielding narrows the exposure window.

Reduce exposure without stopping the business

After disclosure, the exposure window opens for operators as well as attackers. Patching and upgrades remain the durable fix, but security teams need a way to reduce exploitability before every affected system can be updated.

Shielding narrows the exposure window in two ways.

Apply validated, temporary protections where available

Protect infrastructure using: Live Protect and Snort IPS

Reduce reachability everywhere else

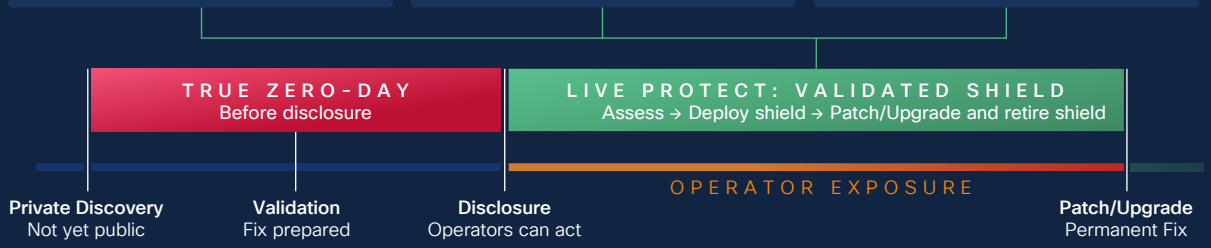
Reduce who and what can reach vulnerable systems using: Firewalls, Hybrid Mesh Firewall, Secure Access, Duo, and Identity Intelligence

Priorities for shielding priority exposure

1: For higher-priority vulnerabilities, reduce exposure before the durable fix is deployed

2: Preserve normal change control where risk can be safely reduced

3: Apply Cisco-validated, temporary protections to supported infrastructure as availability expands



The goal is to lower risk while remediation proceeds.

More >

Real-time vulnerability mitigation

Time to protection

Identity determines reach. Reach drives risk.

Reduce who and what can reach exposed systems

Exposure is not only about the vulnerable system. It is also about who and what can reach it, act on it, automate against it, or escalate from it.

In the agentic era, human users, service accounts, applications, APIs, and agents can all become paths that turn a known weakness into a wider security event.

Cisco helps teams use identity, access, and context to reduce risky reachability while durable remediation continues.

Decision path:

1: Who or what can reach it?

Identify users, devices, service accounts, applications, APIs and agents with access to exposed systems.

2: What can they do?

Assess privilege, automation rights, session context and escalation paths.

3: Where should access be reduced?

Restrict risky reach through identity controls, secure access, policy enforcement, and monitored approvals.

OUTCOME

Fewer risky identities, reduced privilege paths, tighter access control, and less chance that exposure becomes exploitation.

More >

Zero Trust in the agentic era

Time to containment

A compromise should not become a breakout.

Limit blast radius before a compromise spreads

Shielding reduces reachability to exposed systems. Containment assumes exploitation may still happen and limits what exposed systems, identities, sessions, and workloads could reach next. Cisco control points help teams pre-position segmentation and policy close to risk, so a successful exploit is less likely to become lateral movement.

Decision path:

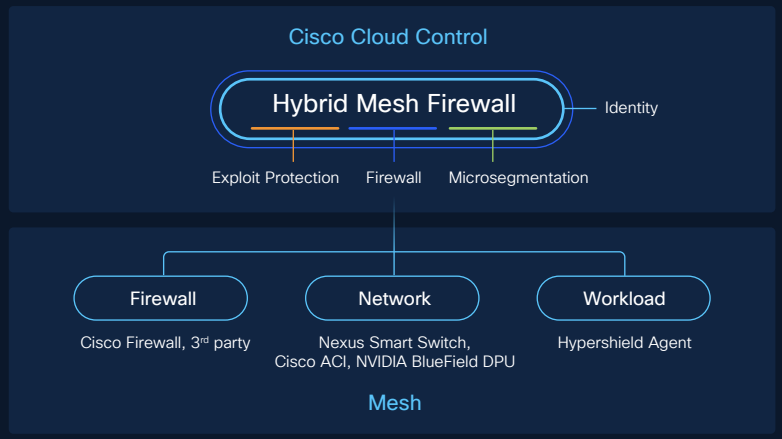
1: Where could compromise start? ▸ 2: What could it reach next? ▸ 3: Where should blast radius be limited?

Firewall inspection
Enforce policy across trust boundaries and inspect traffic with protocol context.

Smart Switch fabric enforcement
Limit movement closer to the server port in top-of-rack deployments.

Application and workload-aware policy
Constrain east-west movement across application environments and reduce paths between systems, services, and users.

One policy model, multiple enforcement points
Cisco Hybrid Mesh Firewall helps teams apply consistent policy across the firewall, fabric, access, and workload control points.



OUTCOME
If exploitation occurs, movement is contained and blast radius is limited while remediation proceeds.

More >

Cisco Hybrid Mesh Firewall in action

Time to remediation

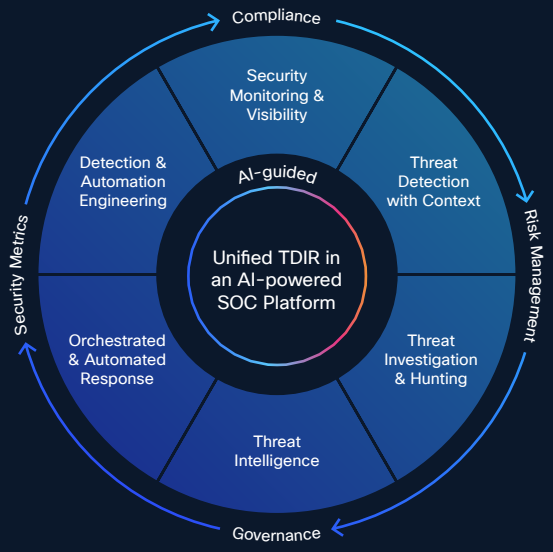
Signals don't close risk. Verified remediation does.

Turn signals into verified remediation

Cisco brings detection, investigation, and response workflows together with threat intelligence and approved action paths, helping teams move from signal to fix without losing governance.

Splunk Enterprise Security
Anchors threat detection, investigation, and response workflows.

Talos Intelligence
Adds current threat intelligence context.



The SOC Re-imagined

High-impact response actions still need clear authority before an incident starts. AI assistance is useful only when it operates inside that governed model.

Telemetry → Evidence.

Evidence → Decisions.

Decisions → Approved actions.

Approved actions → Verified remediation.

More >

Cisco Agentic SOC

Set priorities across the response cycle

Cisco helps teams validate exposure, shield what cannot wait, contain potential blast radius, and govern response through durable remediation.

Find exposure. Shield what can't wait. Contain blast radius. Govern remediation.

OPERATING PRIORITY	01 Find exposure	02 Shield priority exposure	03 Contain blast radius	04 Govern response and remediation
CISCO CAPABILITIES	Inputs: Scanners, Cisco telemetry Analytics: Splunk Exposure Analytics, Cisco IQ, Cisco AI Defense	Validated protections: Live Protect, Snort IPS Reachability controls: Firewalls, HMF, Secure Access, Duo, Identity Intelligence	Isolation controls: Firewalls, HMF, Smart Switch fabric enforcement, Secure Access, Duo, Identity Intelligence	Governed response: Splunk Enterprise Security, Talos, Cisco Agentic SOC
OUTCOME	Teams know what is exposed, reachable, owned and prioritized.	Reachability is reduced while durable fixes proceed.	If exploitation occurs, movement is contained and blast radius is limited.	Actions are evidence-based, authorized, and verifiable.

Close your exposure window and strengthen your security approach

An Action Plan for the AI Era: From exposure response to security resilience

Frontier models keep making the defender's clock tick faster. Reducing the exposure window is critical, but it is only one part of a broader security approach: strengthen the operating model, modernize infrastructure, and elevate security posture.

	Advance your security operating model	Modernize your infrastructure	Elevate your security posture
ASSESS EXPOSURE	Build a current inventory of assets, versions, exposure, owners, and business criticality. Map advisories to affected products and prioritize by reachability, business impact, and control options.	Identify unsupported, nearing end-of-support or hard-to-modernize infrastructure. Prioritize by exposure, business impact and whether there is a durable remediation path.	Discover human, non-human, service, application, API, and agent identities. Map exposure, lateral movement paths, privilege and access gaps.
ACT ON RISK	Evolve vulnerability, patch and upgrade operations. Define decision owners, change paths, compensating controls and closure accountability.	Harden infrastructure, reduce unnecessary services and management-plane exposure. Build a modernization plan for assets that cannot be patched, upgraded or protected fast enough.	Close identity, authentication and authorization gaps. Reduce reachability to exposed systems and pre-position segmentation to limit potential blast radius. Strengthen application patches/upgrades and agent protections where exposure could create broader risk.
OPTIMIZE RESILIENCE	Develop a predictable patching and upgrade rhythm. Track time to visibility, protection, containment, and remediation.	Plan for continuous lifecycle monitoring so unsupported risk does not rebuild.	Operate with evidence, intelligence, automation, and approved action paths. Strengthen monitoring, governed response and agent-assisted SOC readiness over time.



Go

See how ready your network is to defend against threats in the AI era with Cisco's diagnostic.

Read

Find out how Cisco's partnership with leading AI labs can help you navigate machine-speed risk.