Analyst Brief, sponsored by:
Cisco

Find It Before They Do: Why Device Inventory Is Your First Line of AI-Era Defense

Why device-level inventory and exposure identification, coupled with sound security best practices, is the foundation AI-enabled services must deliver first

Written by:
Rob Brothers
Program Vice President

Leslie Rosenberg
Program Vice President

Published:
July 2026

Frontier models have compressed the vulnerability discovery-to-exploit window from months to roughly 38 hours. This brief will help companies understand how to minimize these threats.

I. Introduction

Frontier AI models can now discover vulnerabilities, generate working exploits, and chain weaknesses into complete attack paths at machine speed. Running multiple frontier models in parallel, researchers analyzed roughly 1.8 billion lines of code across 25-plus languages in eight weeks — work that historically took years. Bad actors have now created their own models, and the result is a discovery-to-exploit window that has collapsed from roughly 90 days to about 38 hours. IDC research also finds that by 2029, 50% of Global 2000 enterprises will suffer combined annual losses exceeding $100 billion from infrastructure tech debt and failure to modernize against AI-powered attacks.

Against that timeline, the limiting factor is no longer finding problems — it's more than knowing what you have; it's the ability to assess the impact and pinpoint where to focus and take action (insights that help prioritize in a timely way). This brief sharpens IDC's frontier-threat point of view around that reality: organizations and the services partners that support them must prioritize identifying vulnerabilities holistically across the environment, encompassing end-of-life (EOL), end-of-support (EOS), and last-day-of-support (LDOS) equipment, as well as all reachable devices as part of a sound security practice. An accurate inventory and exposure map is the precondition for every other control. The following are best practices companies should undertake continuously to help thwart attacks.

At a glance

Key stats

$100 B+

Projected combined G2000 losses by 2029 from AI-era infrastructure tech debt.

50%

Of G2000 enterprises exposed to compounding losses without modernization.

0

Dominant incumbents established in agentic AI security services.

Source: *Securing the Agentic Enterprise: Part 1 — Updating IDC's Cybersecurity Capabilities Assessment Framework for the AI Age* (IDC #EUR154585226, June 2026)

Priority 1: Identify exposures and prioritize vulnerabilities before attackers do

An accelerated threat timeline changes the sequence of a sound response. Generic IT asset hardening and governance frameworks matter, but they sit downstream of a larger problem: building and maintaining a precise, holistic picture of what is running, what is unsupported, and what is truly reachable and vulnerable to an attacker. The most vulnerable systems are devices that have not been tracked or monitored and have reached LDOS or end of vulnerability and security support (EoVSS); recent IDC studies found that approximately 20% of network devices are seven years or older, meaning a broad spectrum of assets are at risk.

- Prioritization must weigh both sides of the risk equation. True vulnerability prioritization isn't just about how severe a flaw is; it's about how severe a flaw is on a device that matters. Customers need visibility that combines vulnerability severity with device criticality

and network context, so effort focused on what actually threatens the business, not just what scores highest in isolation.

- Risk doesn't wait for end-of-life. Vulnerability exposure isn't confined to devices past their last day of support. Fully supported devices can be just as vulnerable to missed patches, delayed upgrades, or configuration and hardening gaps. An effective program must continuously assess all devices, not just those approaching or past LDOS.
- Assessment must be continuous, automated, and broader than common vulnerabilities and exposures (CVEs). Point-in-time scans and CVE-only checks leave blind spots. Customers need an always-on vulnerability assessment capability that automates the path from disclosure to impact analysis — and that impact analysis must account for more than known CVEs alone, incorporating configuration weaknesses, exposure, and device context to reflect real-world risk.

Priority 2: Long- and short-term guidance on device management and evaluation

Short term

- Address technical debt directly. Old assets cost more to support and pose undue risks within organizations, and unsupported assets often have limited or no remediation path when new vulnerabilities surface. Modernization is a security and operational-risk conversation, not a routine refresh cycle.
- Follow a clear sequence. Inventory and prioritize what is unsupported or nearing LDOS/EoVSS; reduce exposure through isolation and close monitoring, then build a phased modernization plan tied to budget cycles and change windows.

Long term

- Make modernization continuous. Life-cycle monitoring should surface aging assets and approaching end-of-support dates early rather than rediscovering them during the next incident.
- Bear in mind that peak LDOS exposure is arriving now, as COVID-era investments in switches, routers, wireless access points, and campus gear reach end of support simultaneously, exacerbated by new security mandates and rising technical debt.

Harden proactively while remediation is in progress

- **Hardening takes a few forms**. Reactive control occurs when a fix cannot be applied within the advised window (especially for high-exposure assets), and proactive control (support) reduces exposure regardless of which vulnerabilities emerge next. This includes issue-detection automation (i.e., proactive AI-driven prevention of potential threats and problems through AI) to identify issues before they disrupt operations, thereby avoiding risk, performance degradation, and downtime by delivering personalized visibility, actionable insights, and intelligent automation.
- **Mission-critical support**. When it comes to AI — including agentic AI — all managed support should be designed to maximize uptime and provide best-in-class user experiences, resiliency, and performance across mission-critical operations.

- **Human + AI expertise.** Advanced AI works in concert with the vendor's human experts to ensure operational simplicity and agility in the face of rapid change, providing ongoing support tailored to the enterprise's infrastructure, with contextualized recommendations and guidance that evolve with it. These should be provided regularly through QBRs, in-person engagements, or an on-demand digital channel. AI can gather data and correlate services and their associated ports to determine whether a vulnerability exists and whether action must be taken, such as disabling a service or port. Every service disabled and every path closed shrinks the attack surface and limits the blast radius of the next advisory, even before it is published, but a best practice is to use human oversight to ensure there is no disruption to a critical business service that AI may have overlooked.

Priority 3: Beyond inventory: Durable controls and agentic security operations

Device mapping is essential, but it is only one part of a durable defense. Organizations must extend this visibility to identify at-risk workloads and emerging AI agents. Closing identity gaps with strong authentication and continuous verification is critical. A comprehensive patching discipline of applications and workloads, supported by a software bill of materials and vendor attestation, is required to maintain a secure environment. Furthermore, implementing segmentation, advanced firewall protections, and an intrusion prevention system (IPS) is critical in preventing lateral movement during an intrusion. This layered approach ensures security operations evolve effectively alongside the sophisticated threats posed by frontier models.

At this stage, corporate IT and security must resolve these structural vulnerabilities by implementing architectural changes, such as segmentation and an agentic security operations center (SOC). The steady state is an agentic SOC in which AI agents handle detection, prioritization, investigation, and enrichment at machine speed, while analysts focus on high-consequence decisions within a framework of governance and auditability.

Considerations

Why AI-enabled advisory, professional, and support services improve the security posture

Building and maintaining device-level exposure intelligence at machine speed outpaces what most internal teams can sustain on their own. In a recent study on support services, IDC asked: "How important are the following technical features in deciding what type of support services agreement to purchase for your enterprise?" The number 1 answer was "Provides a portal for system health (security, patching and performance) and proactive suggestions to improve system health for vendors' equipment." This shows customers understand they have gaps in security and patching. Vendors are assisting by providing AI-enabled advisory, professional, and support services to close that gap by:

1. Creating network operational changes

According to recent IDC studies, most corporate IT staff are having difficulties staying trained on the latest technologies and operational processes. The problem is that AI changes the risks and the speed of those risks. Network design and management have become more critical; for example, a flat network means a larger blast radius when something is compromised; therefore, companies must change how they think. Slow, methodical change can't keep pace with exploit development that now moves in hours or minutes. Moreover, unpatched hardware, even when it's behind firewalls, becomes a far greater source of liability. Therefore, continuous vulnerability evaluation becomes table stakes.

2. Delivering a real-time inventory and reachability map, not just a patch list

AI-augmented services providers bring prebuilt installed-base intelligence and automated configuration analysis that identify devices that are LDOS, are genuinely exposed, and run affected code in days (rather than months, which an internal build typically requires).

3. Turning buying criteria into outcomes, not feature claims

Practitioners should look past relabeled automation by asking vendors hard questions:

- Does it help understand exposure faster than attackers can weaponize fixes?
- Does it help decide what to patch first?
- Does it reduce uncertainty rather than simply grow the backlog?
- Does it provide a road map for long-term resilience?

While the current surge in disclosures will put most teams in firefighting mode, neither teams nor management wants to stay there. Does it collapse the discover-assess-act loop to match the shrinking time to exploit? AI-enabled services providers that can answer these will be able to anchor engagements to time-to-remediate and data-driven prioritization rather than billed hours.

4. Converting one-time assessments into continuous life-cycle coverage

LDOS refresh, exposure mapping, and agentic security are not one-time projects — they require continuous monitoring as disclosures arrive on a recurring, industrywide cadence. AI-enabled advisory and support services turn an initial device assessment into a sustained life-cycle relationship, keeping infrastructure aligned with a threat landscape and regulatory bar (NIS2, DORA, the EU AI Act) that are constantly evolving.

Conclusion: Essential guidance

- **Inventory before you invest**. Build a device-level, continuously refreshed inventory and reachability map before adding new controls — the assessment itself is the highest-value, lowest-friction services engagement.
- **Elevate LDOS and EoVSS above generic hardening**. Prioritize identifying unsupported and nearing-end-of-support devices; isolate and monitor them while a phased modernization plan is built, rather than defaulting to wholesale replacement.

- **Separate vulnerable-version alerts from true exposure**. Ask services partners how they confirm reachability, not just software version, before a device lands on a remediation list.
- **Choose partners building for machine speed**. Evaluate AI-enabled advisory and support providers on whether their own delivery models — telemetry, automation, knowledge graphs — can keep pace with patch windows that have collapsed to near zero.
- **Treat modernization and identification as continuous**. Infrastructure refresh cycles (LDOS, Wi-Fi 7, AI-ready fabric) should feed a standing inventory and monitoring practice, not a one-time project that goes stale before the next disclosure cycle.
- **Shift budget from access-time to execution-time controls**. Traditional perimeter and access governance no longer covers where agentic risk now lives; prioritize services and tooling built for continuous, in-session governance.

About the IDC analysts

Rob Brothers
Program Vice President, IDC

Rob Brothers is a Program Vice President within IDC's enterprise infrastructure global research domain and part of the cloud and infrastructure services subdomain. He leads IDC's Financing and Lifecycle Services programs. He focuses on worldwide support and deployment services for hardware and software and provides expert insight and intelligence on how enterprises should be addressing key areas for infrastructure hardware, end-user hardware, software, and services. He also has expertise in the latest asset financing options, which include as-a-service models such as device as a service. He draws on decades of industry experience to provide insights and actionable advice to assist vendors in developing, marketing, and delivering IT services. Rob's areas of expertise include, but are not limited to, enterprise storage, server, networking, client device and high-availability and mission-critical support services, virtualization and transformational services, and channel and partnering strategies.

More about Rob Brothers

Leslie Rosenberg
Research Vice President, IDC

Leslie Rosenberg is Research Vice President within IDC's Enterprise Infrastructure Global Research domain. She focuses on network life-cycle and infrastructure services as part of the Network Infrastructure and Services subdomain. Her research spans consulting and integration services surrounding network, compute, and storage technology deployments. She examines project-based services for established and emerging infrastructure technologies, with a focus on how life-cycle services offerings will evolve, impacting people, processes, tools/platforms, and methodologies around the globe. Her research evaluates services delivered by technology manufacturers, global systems integrators, cloud service providers, and telcos as they look to compete in the enterprise market.

More about Leslie Rosenberg

Message from the sponsor

Outpace the threat: resilience at machine speed

As frontier AI models compress the discovery-to-exploit window to hours, organizations need continuous visibility into what they run, what is unsupported, and what is genuinely exposed. Cisco Resilient Infrastructure Services is a flexible suite of support and professional services designed to help customers defend against and outpace advanced frontier model threats. Rooted in Cisco IQ's AI-powered insights, it gives IT and security teams always-on exposure visibility and personalized playbooks that collapse the discover-assess-act loop. Building on that clarity, it delivers a strategic roadmap to address structural weaknesses and the expertise to engineer infrastructure and agentic operations for proactive resilience. Delivery scales with flexible options that meet organizations where they are.

Learn more about Cisco Resilient Infrastructure Services.

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

IDC Research, Inc.
One Beacon Street, Suite 33100, Boston, MA 02108, USA
T +1 508 872 8200

blogs.idc.com | LinkedIn @IDC | www.idc.com

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community make fact-based technology decisions and achieve their key business objectives.