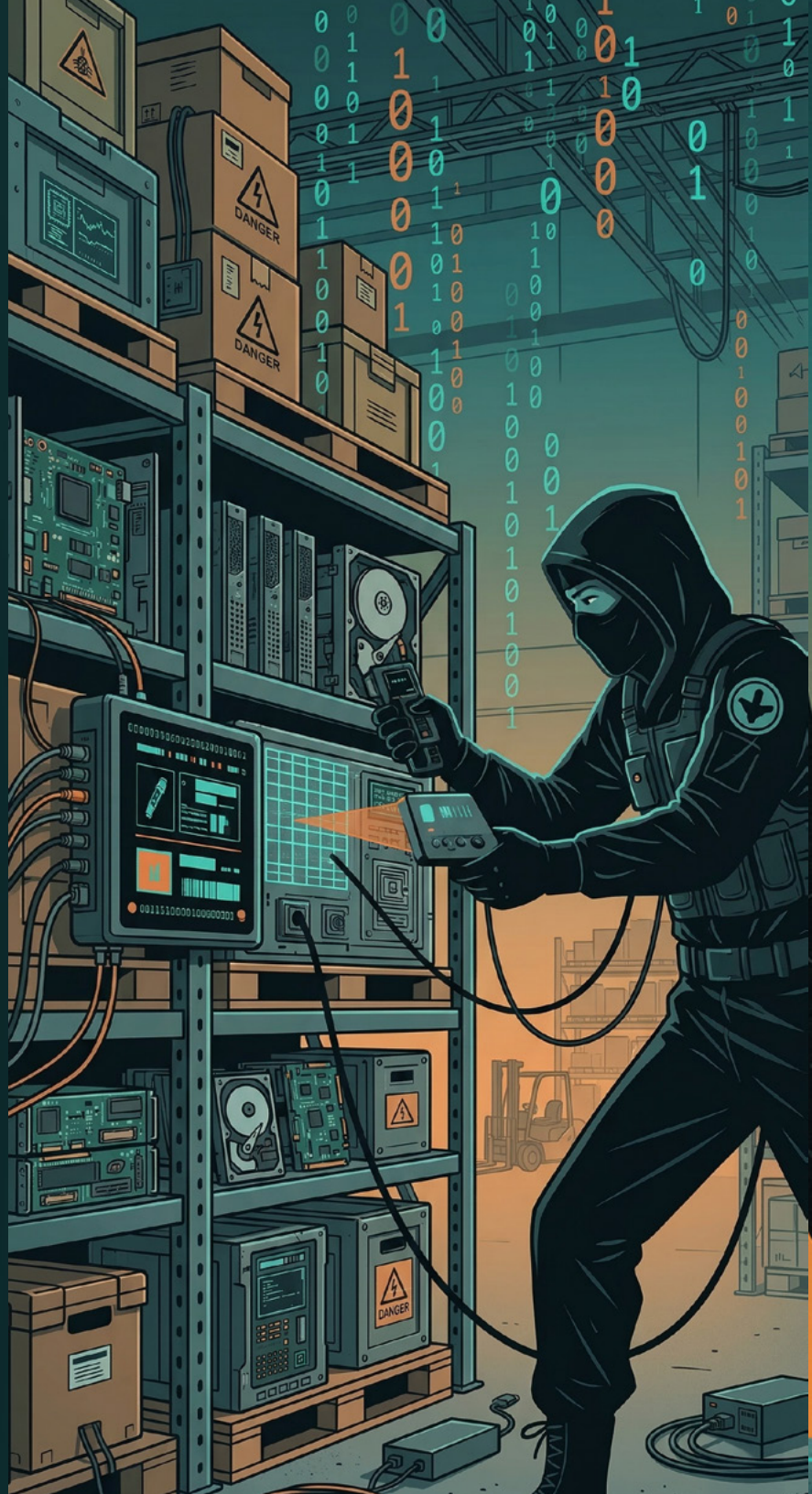
LUMEN®

BLACK LOTUS LABS® by Lumen

Manufacturing report

The 2026 Lumen Defender Threatscape Report

Why visibility at breach misses the plot



Think of modern cybercriminals and nation-state actors as their own version of an elite heist crew. Instead of cracking safes, they're assembling malicious proxy networks and accelerating operations with generative AI. For manufacturers—where uptime, safety, and supply chain continuity are paramount—it's now critical to gain visibility into these operations before they disrupt production environments, compromise operational technology (OT), or impact connected ecosystems.

Modern cyber operations look less like isolated break-ins and more like carefully staged heists. Long before ransomware is deployed or a breach is disclosed, threat actors invest significant time assembling the infrastructure that will power their campaigns—using generative AI to continuously scan for exposed edge devices, validate stolen credentials, stand up proxy networks, and test command-and-control (C2) paths. Most manufacturers only detect these activities once they intersect with perimeter defenses or plant-level systems, by which point the operational groundwork has already been laid—putting production lines, supply chains, and worker safety at risk.

Lumen sees these campaigns much earlier.

Backed by our threat research and operations arm, Black Lotus Labs®, Lumen operates from its own vantage point—inside a global internet backbone. Rather than relying on post-infection signals from endpoints or perimeter devices, we analyze backbone-level telemetry to identify coordinated infrastructure behavior as it emerges.

This includes early-stage signals such as large-scale scanning, credential validation, botnet enrollment, proxy formation, and rapid C2 rotation—often days or weeks before those same Internet Protocol (IP) addresses or domains are observed targeting any single manufacturer or industrial ecosystem.

What are edge devices?

Edge devices—such as routers, switches, firewalls, and VPN gateways—refer to internet-facing infrastructure and services that sit at the boundary between an organization's internal environment and the public internet, providing access, routing, or control, but typically operating outside traditional endpoint security visibility.

Who Is Black Lotus Labs?

Black Lotus Labs is the threat research and operations arm of Lumen, combining unmatched network visibility with expert research, machine learning, and automation to conduct original threat discovery and uncover threat actor infrastructure.

LUMEN®

From this comprehensive viewpoint, Lumen has identified a major shift for 2026: **modern cyberattacks are increasingly driven by exposure, with threat actors optimizing their targeting for vulnerable edge devices and services.**

This shift has significant implications for the manufacturing sector. While endpoint detection and response (EDR) and traditional security controls remain essential, attackers are increasingly bypassing these defenses by exploiting exposed edge infrastructure and converged IT/OT environments. As manufacturing advances toward Industry 4.0, connected factories, industrial internet of things (IIoT) devices, and distributed operations expand the attack surface. Managing exposure at the edge is now as critical as protecting the plant floor and core systems.

Informed by insights from Black Lotus Labs, this manufacturing report breaks down the key trends we observed in 2025, outlines our top predictions for 2026, and provides actionable steps to help manufacturing security leaders disrupt adversarial activity earlier—before it impacts production uptime, supply chain integrity, or operational resilience.

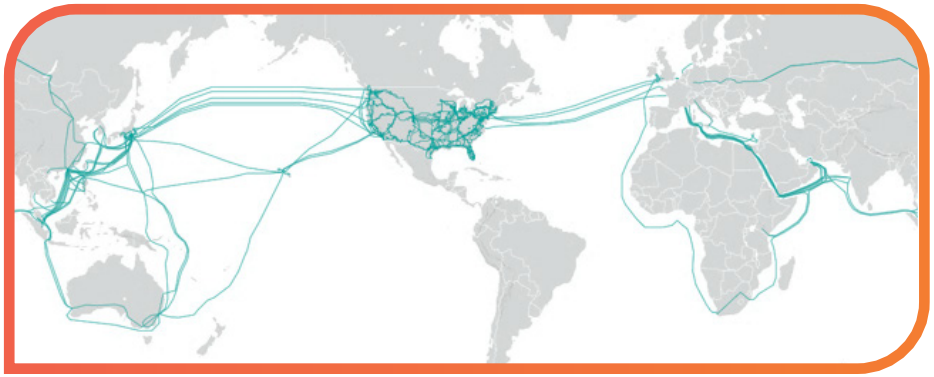
Download the complete 2026 Lumen Defender Threatscape Report for additional insight →

1. The Center for Applied Internet Data Analysis (CAIDA), AS Rank, January 2025.

Inside Lumen's internet backbone

Lumen manages and operates one of the largest, most connected, and most deeply peered networks in the world.[1] Black Lotus Labs provides:

- Visibility into 99% of public IPv4 addresses
- Daily monitoring of 200B+ NetFlow sessions and DNS queries and 46,000 C2s
- Daily tracking of 2.3M unique threats
- 5,000+ C2s disrupted in 2025



View live threat analytics →

LUMEN®

2025: Year in review

Cyber threats in 2025 were shaped less by individual malware families and more by the infrastructure attackers built, borrowed, and hid within. Obfuscation networks and botnets became foundational tools, with multi-layered chains of compromised routers, small office/home office (SOHO) devices, IoT/IIoT hardware, and virtual servers blending malicious activity into everyday traffic. For manufacturers, this constant churn complicated attribution and strained traditional detection models—particularly across converged IT/OT environments and globally distributed operations.

From inside the global internet backbone, Black Lotus Labs observed a clear escalation in both scale and intent. Criminal and nation-state actors alike relied on millions of vulnerable, often end-of-life (EoL) devices to create moving targets. SOHO and IoT devices allowed attackers to "live off the land" while disguising operations behind residential IP space and trusted network pathways. Shared use of compromised infrastructure further blurred the lines between criminal and state activity, increasing the risk of missed detections and delayed response while exposing production systems, supply chains, and sensitive intellectual property to greater risk.

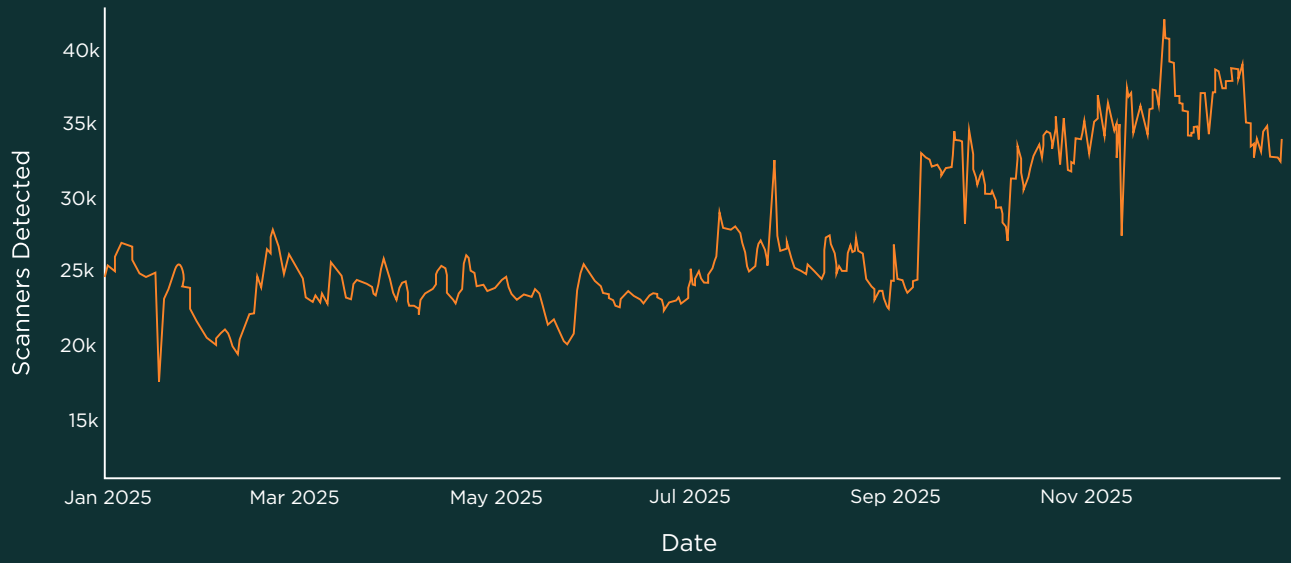
The following six insights capture how these operations took shape throughout 2025.

1 Generative AI changed the tempo, unleashing attacks at machine speed.

Threat actors embraced automated tasking, scanning, infrastructure rotation, and C2 management in 2025, in addition to adopting new generative AI-enabled attack vectors. This automation sustains malicious campaigns indefinitely with minimal oversight. Human operators step in only to update exploits, payloads, or targeting, while machines handle execution at scale.

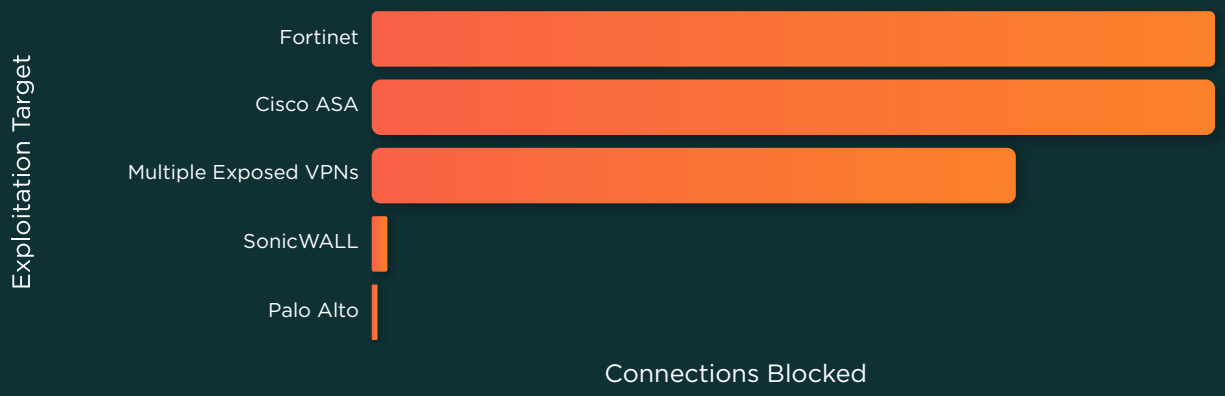
For manufacturers, this acceleration is especially consequential. As Industry 4.0 initiatives expand IIoT adoption and connected factory environments, attackers can rapidly identify exposed devices, validate credentials, and probe plant networks faster than traditional defenses can respond. This scalability is forcing security leaders to rethink detection—shifting toward earlier signals that can disrupt attacks before they impact production uptime, safety systems, or supply chain operations.

Total malicious scanners detected per day (2025)



The massive volume of malicious scanning indicates attackers' commitment to taking a systematic, continuous inventory of internet-facing devices and services. Botnet operators, initial access brokers, and advanced actors use this scanning to assess the opportunity space for their exploits on edge devices before they ever launch an attack.

Top enterprise edge devices brute forcing events tracked by Black Lotus Labs (October–December 2025)



Using Black Lotus Labs' brute force detections, we blocked significant traffic from attack attempts in Lumen Defender Essentials and Plus against enterprise edge devices. This chart represents the five most-targeted devices based on connections blocked by Lumen Defender Essentials and Plus between October–December 2025.

LUMEN®

2 Attackers moved deeper into the network itself—hiding in the infrastructure.

In 2025, we saw sophisticated adversaries shift more of their attention away from endpoints to vulnerable, less-secured devices at the edge, like routers; VPN gateways; firewalls; and remote access infrastructure that connect plants, suppliers, and enterprise systems. Here, they can "live in the middle," stealing credentials to access the protected information beyond while hiding their activity inside the connective tissue of the internet.

Sophisticated attackers know that completing the heist in a single sitting may alert defenses. By lurking in devices outside the reach of standard security controls and reaching back out days, weeks, or even months after the initial access, attackers can delay action. In manufacturing environments, this prolonged dwell time increases the risk of undetected lateral movement between IT and OT systems—creating potential pathways to disrupt production lines or compromise operational processes.

3 Criminal ecosystems professionalized, adopting the polish of legitimate SaaS.

Gone are the days of crude panels and chaotic infrastructure. In 2025, cybercriminal operations became indistinguishable from professional software businesses. We saw adversaries assemble polished platforms—complete with customer support and subscription tiers—as a way to scale access, automate abuse, and lower the barrier to entry for cybercrime.

For manufacturers, this industrialization of cybercrime translates into more frequent and scalable threats—from ransomware campaigns targeting production continuity to credential harvesting aimed at supplier portals and operational systems. Disrupting these ecosystems requires identifying infrastructure growth patterns early, before they are leveraged to impact manufacturing operations or partner networks.

4 Malware-backed proxy networks became full-fledged economies of disguise.

Adversaries can spend months, sometimes even years, laying the groundwork for their next operation. That's why we saw threat actors industrialize their entry and escape routes in 2025.

Compromised home routers, IoT/IIoT devices, and high-volume virtual private server (VPS) hosts became rentable identities—on-demand personas that can be purchased for a few dollars' worth of cryptocurrency. This tactic allowed attackers to disguise themselves as trusted remote employees, bypassing geofencing, ASN-based blocking, IP reputation checks, and many Zero Trust location signals.

In manufacturing, where remote access to plants, third-party vendor connectivity, and distributed workforce models are increasingly common, this tactic directly undermines identity and access controls—raising the risk of unauthorized access to production systems, engineering environments, and supply chain platforms.

5 Nation-state & criminal crews blurred together on shared infrastructure.

In classic heist films, every crew has its signature—the safe expert, the hacker, the criminal mastermind. But in 2025, those signatures overlapped. Nation-states piggybacked on criminal infrastructure; cybercriminals reused tooling forged by intelligence services. Attribution became less about ownership and more about intent.

For manufacturers—particularly those in critical infrastructure, advanced manufacturing, or globally integrated supply chains—this convergence raises the stakes. The same infrastructure used for financially motivated attacks today may support intellectual property theft, industrial espionage, or disruptive operations tomorrow. This overlap complicates attribution and elevates both cybersecurity and geopolitical risk considerations.

6 The global backbone transformed from a conduit into an early-warning system.

2025 underscored how threat actors are constantly exploring new attack vectors and using AI to accelerate the speed and sophistication of their operations. This transforms the global internet backbone from an invisible highway for threat actor transport into a critical detection and disruption layer.

As adversaries weaponize routers, appliances, and management planes, the infrastructure layer itself becomes the first theater of operation. Backbone telemetry exposes patterns that endpoint logs alone can't catch, from the quiet appearance of a new proxy node to botnet recruitment, automated scanning, or the sudden regeneration of C2 servers as operators prune and replace infrastructure at machine speed.

For manufacturers, this upstream visibility is essential to identifying and mitigating threats before they reach factory floors, disrupt operations, or cascade across supply chains.

Together, these insights surface a critical shift for defenders in 2026: the decisive battleground is no longer just the endpoint—it's the infrastructure beneath, which is now powered by generative AI.

LUMEN®

Campaign spotlight: J-Magic

First spotted in September 2023, J-Magic is the silent stakeout of the cybercrime world. Rather than scanning aggressively or beaconing outward, the operators behind J-magic planted a passive listener directly onto enterprise-grade Juniper routers that only activated under precise conditions. Observed J-Magic targets spanned semiconductor manufacturing, energy and solar technology, industrial manufacturing, and IT and network services.

J-magic was built to live where defenders least expect malware to reside. The implant is a custom variant of cd00r, executed entirely in memory, with no firmware modification and no persistent disk artifacts. Upon execution, it renamed itself to mimic a legitimate Junos OS process and overwrote its command-line arguments to erase forensic clues.

Its architecture was designed to exploit the lack of host-based monitoring on enterprise routers, which are rarely power-cycled. Malware tailored for routers is designed to takeadvantage of long uptime and live exclusively in-memory, allowing for low-detection and long-term access compared to malware that burrows into the firmware. Roughly 50% of J-Magic's targeted devices appeared to function as VPN gateways, placing them directly in the authentication and access path for remote users.

Disruption & Defense

Black Lotus Labs detected J-magic by translating malware logic into network-level analytics, identifying the unique packet conditions and correlating them with Juniper device banners to reduce false positives. This detection required upstream visibility into TCP behavior, highlighting why backbone-level observation is essential for uncovering passive, infrastructure-resident threats.

Black Lotus Labs shared IoCs, detection guidance, and hunting recommendations to help organizations identify similar activity in their environments.

Key takeaway

J-magic reinforces a critical shift in modern threat operations in which perimeter devices are becoming the payload. By targeting enterprise routers with passive, memory-only malware, attackers gained visibility and access that endpoint defenses never saw. There were no alerts, no suspicious processes on user machines, and no obvious indicators until the operator decided to activate the backdoor.

J-Magic also shows that modern attackers don't always rush the vault. Sometimes they hide nearby—watching traffic, waiting for the signal, and keeping their tools invisible until the right opportunity strikes.

2026 threat predictions

In 2026, the most dangerous cyber operations won't look radically different at the moment of impact. Breaches will still begin with stolen credentials, exploited edge devices, or trusted infrastructure abused at scale. However, what will change is how fast those operations are assembled through the proliferation of generative AI tooling, how little forensic evidence they leave behind, and how effectively attackers blend into the background noise of the internet itself.

From Black Lotus Labs's vantage point inside the global internet backbone, we believe four shifts are already coming into focus.

Prediction 1: Setup gets faster as adoption of generative AI and agents goes mainstream

Speed is a crucial element of every good heist. In 2026, we expect to see a sharp acceleration in AI-enabled chained exploit paths targeting edge devices and internet-exposed management interfaces, including the routers, VPN gateways, firewalls, and remote access systems that connect plants, suppliers, and enterprise environments. We believe attackers will increasingly rely on AI-driven agents that evaluate privilege levels, identify adjacent trust relationships, select the next best exploit path, and adapt tactics mid-operation based on network response.

Edge devices are already prized because they sit at the crossroads of authentication, encryption, and routing and often lack deep forensic visibility. Agentic AI simply accelerates how quickly attackers can move through those devices.

For manufacturing security leaders, this compresses the window between initial exposure and operational impact—whether that's disruption to production lines, unauthorized access to OT systems, or compromise of critical engineering data. As attacker speed increases, proactive visibility becomes essential to maintaining uptime and operational resilience.

Prediction 2: Targeting will focus on opportunity at the edge

Malicious scanning for edge devices and exposed services is continuous and indiscriminate, with continuous malicious scanning representing 33% of all malicious traffic blocked by Lumen Defender Essentials & Plus. Firewalls, VPN gateways, remote management interfaces, identity services, and load balancers are probed relentlessly across all sectors. When a reachable device is found—especially one with weak authentication, missing patches, or limited logging—attackers move quickly, using whatever technique is most effective at the moment.

For manufacturers, this means risk will increasingly be defined by exposure. The rapid expansion of IIoT devices, connected factories, and distributed operations has significantly increased the attack surface. Organizations that prioritize asset visibility across IT and OT environments, enforce strong patching and access controls, and retire unsupported systems will be better positioned to reduce risk.

This trend also reinforces the urgency of modernizing legacy OT and industrial control systems that were not designed with today's threat landscape in mind.

Prediction 3: The real signals lie in the network

By the time defenders investigate a compromised firewall or router, the most important evidence will already be gone. That's why we believe detecting adversary networks in addition to individual tools will be essential in 2026.

From our perspective, the earliest signals won't come from device telemetry. They'll emerge from how infrastructure behaves collectively, such as rapid C2 rotation, sudden proxy layer emergence, orchestration traffic patterns, and coordination across geographies.

For manufacturers, augmenting endpoint and plant-level security with network-level intelligence will be key. This enables earlier detection of campaigns before they impact production environments, disrupt supply chains, or propagate across interconnected facilities and partners.

Prediction 4: The best disguises will be legitimate infrastructure

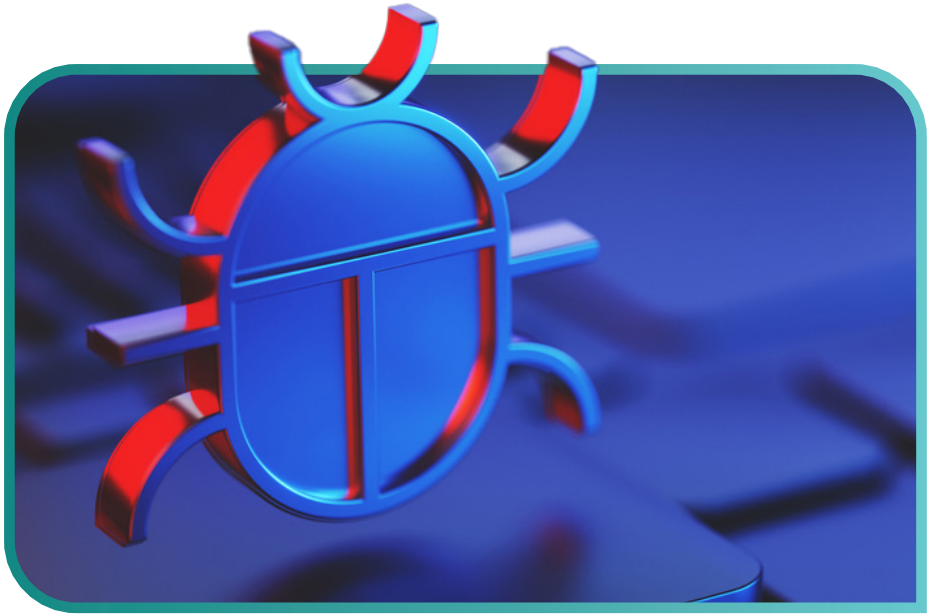
In 2026, we predict that adversaries will rely even more heavily on malware-backed proxy networks, SOHO-based botnets, hijacked VPS infrastructure, and "clean-looking" residential IP spaces to hide their operations in plain sight. These tactics obscure attribution; blur the boundaries between criminal and nation-state activity; enable shared infrastructure across multiple campaigns; and allow attackers to rent, trade, or reuse capabilities at scale.

The result is a threat landscape where the attacker infrastructure itself becomes the capability. When cybercriminals blend into legitimate traffic flows, traditional indicators fail, reputation-based blocking lags behind reality, and ASN and geolocation filters lose relevance. This shift reinforces manufacturers' need to identify the emergence of malicious infrastructure early, before it is used to target production systems, disrupt operations, or compromise supply chain integrity.

Defense guidance: Stopping the heist before it happens

Modern threat operations aren't defined by a single exploit, piece of malware, or intrusion event. They are built as systems that are assembled over long periods of time, tested in pieces, and activated only when conditions are favorable.

The guidance below reflects patterns observed across Black Lotus Labs's telemetry and highlights where defenders can most effectively shift the balance.



1 **Defend the edge like it's the vault door**

Firewalls, VPN gateways, routers, and management interfaces offer privileged access, long uptime, and limited forensic visibility. Defenders should treat these gateway edge devices as high-value assets and assume that attackers will chain multiple edge weaknesses together—initial access, lateral movement, and persistence—before any endpoint alert fires.

- ☐ Thoroughly inventory internet-exposed services and management interfaces, including shadow IT and legacy devices.
- ☐ Monitor for anomalous authentication attempts and configuration changes on edge devices, even when traffic originates from residential or "benign" IP space.
- ☐ Plan for detection techniques that do not rely on host-based agents, especially for appliances and network gear.

LUMEN®

2 Shift from indicators to infrastructure awareness

While IoCs are still important, they often arrive late in the attack lifecycle after threat actors have already reached the perimeter. Infrastructure behavior like C2 relationships, proxy usage, traffic patterns, and routing dependencies reveal malicious activity far earlier than malware signatures. For defenders, this means that detection should focus on relationships rather than just IPs or hashes.

Priority actions:

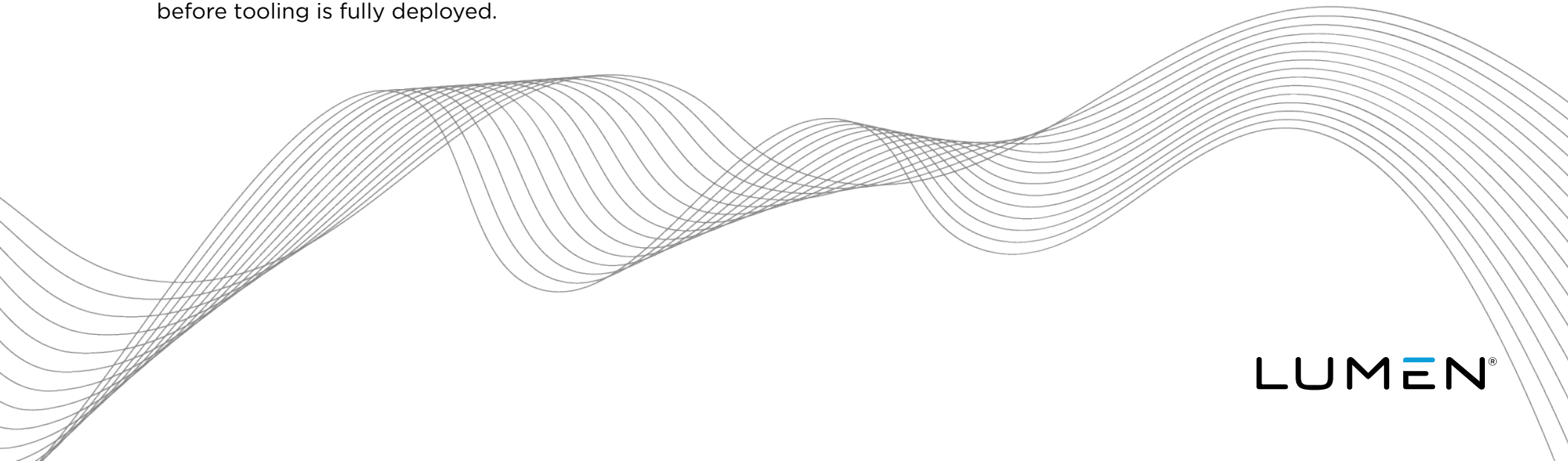
- ☐ Look for unusual data flows, including large outbound transfers to nearby geographic regions or unexpected cloud providers.
- ☐ Track how traffic enters and exits the environment, not just whether it is “known bad.”
- ☐ Correlate authentication activity, proxy usage, and outbound connections to identify emerging campaigns before tooling is fully deployed.

3 Treat proxy networks as active threat infrastructure

Malware-backed proxy networks built from SOHO devices, IoT systems, and compromised VPS infrastructure allow attackers to blend into normal traffic and bypass traditional geofencing or reputation-based controls. Today’s defenders must not treat the residential IP space as a trust signal.

Priority actions:

- ☐ Monitor for suspicious activity originating from residential and VPS IP ranges, especially against authentication services.
- ☐ Actively identify and block open proxies and known malicious proxy services where possible.
- ☐ Recognize that attackers may deliberately accept higher detection rates during reconnaissance phases, then switch to cleaner proxy infrastructure for exploitation.



LUMEN®

4 Assume blurred lines between crime and espionage

2025 showed us that the same infrastructure can support both cybercrime and nation-state espionage. Threat actors are increasingly co-opting each other's access, tools, and data—making attribution less important than impact. Defenders must treat all unauthorized access incidents as potentially strategic.

Priority actions:

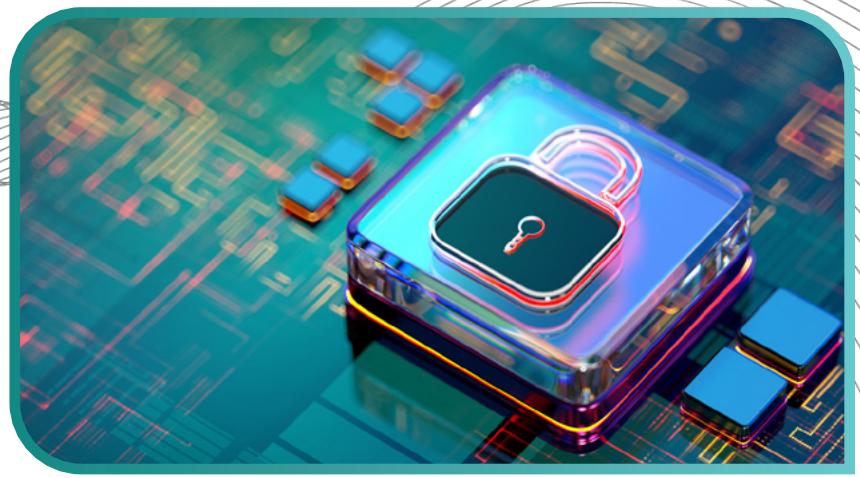
- ☐ Investigate compromises with the assumption that access may be resold, reused, or repurposed.
- ☐ Monitor for secondary activity after initial containment, especially lateral movement and data staging.
- ☐ Prioritize visibility into east-west traffic and unusual operator-driven behavior inside the network.

5 Use scale against the attacker

Attackers succeed by operating at scale. Security teams can regain the advantage by doing the same. For defenders, this means that they need to expand the scope of their visibility beyond individual assets to the network paths connecting them.

Priority actions:

- ☐ Leverage upstream telemetry, intelligence sharing, and automated response where possible.
- ☐ Integrate network-level detections with identity, endpoint, and cloud signals.
- ☐ Reduce attacker dwell time by blocking malicious infrastructure early, even when confidence is still emerging.



LUMEN®

The central lesson of 2025—and the defining risk for manufacturers in 2026—is this: modern cyber threats are built long before they are launched. Adversaries are rapidly assembling infrastructure ecosystems powered by generative AI, resilient proxy networks, compromised edge and IIoT devices, and shared criminal-state platforms. Organizations that combine strong cybersecurity fundamentals across IT and OT environments with upstream visibility and infrastructure intelligence will be best positioned to shrink attacker dwell time, disrupt malicious activity early, and prevent attacks before they disrupt production, compromise supply chains, or impact worker safety.

Lumen combines global internet traffic visibility with original research through Black Lotus Labs to spot malicious infrastructure as it forms—unlocking earlier detection of botnets, C2 systems, and nation-state activity. This same intelligence feeds operational defenses across the Lumen network, so as soon as Black Lotus Labs can detect, our customers can get protection.

Our approach does not replace endpoint, identity, or cloud security. It complements them by delivering additional intelligence so manufacturing organizations can better detect and disrupt threats earlier in the attack lifecycle. The result is a more proactive security posture that reduces operational risk, protects intellectual property, and strengthens resilience across increasingly connected and complex industrial environments.

LUMEN®