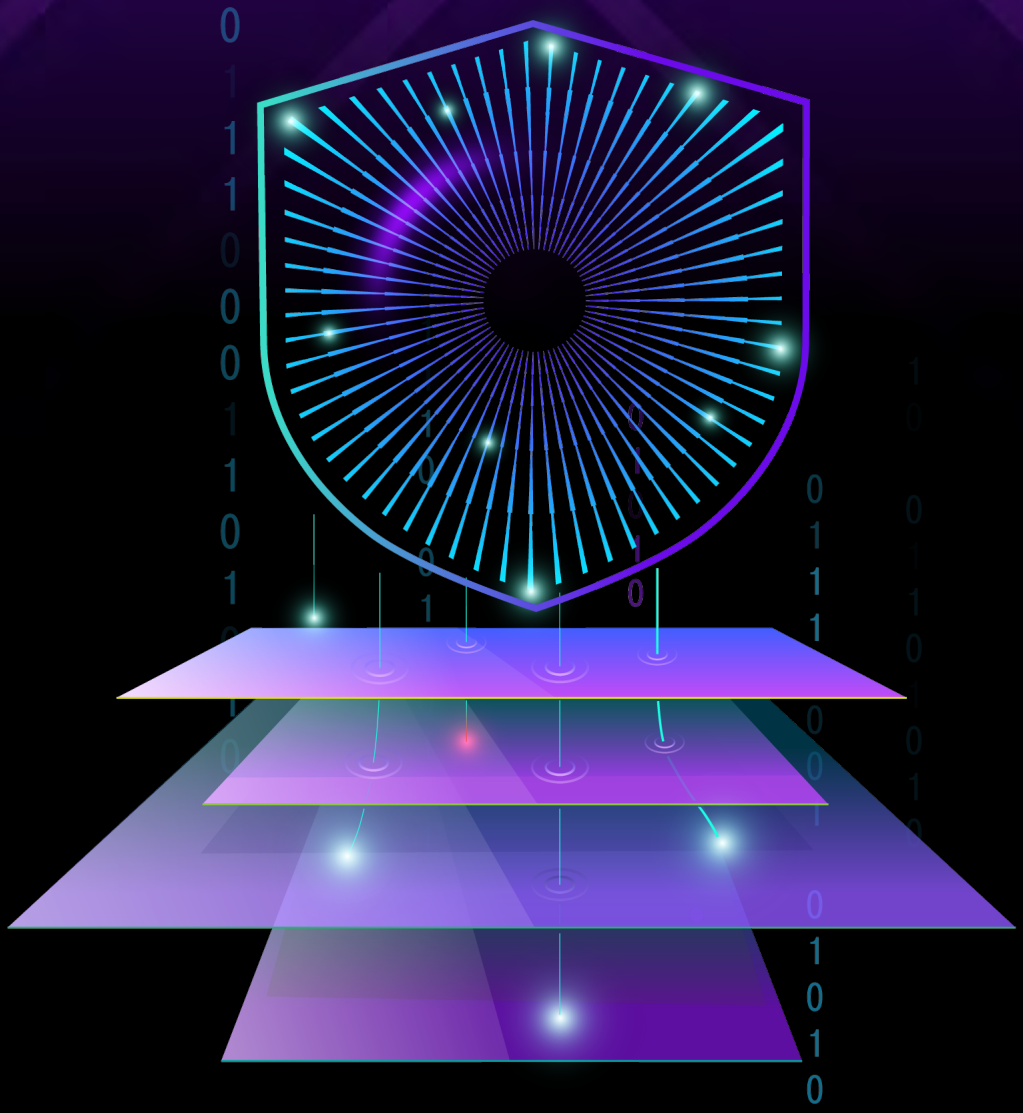
STATE OF THE

SOC

REPORT

SMARTER SIGNALS STRONGER LAYERS

AI-ENHANCES. DEFENSE-IN-DEPTH WINS.



N-ABLE Adlumin
Security Operations

SECOND EDITION
2026

Table of Contents

Executive Summary: State of the SOC 2026 3

Key takeaways 4

The 2025 threat landscape 6

The perimeter exploitation playbook 7

The single-layer fallacy: Why “good enough” isn’t enough 8

Security resilience redefined for 2026 11

What’s the minimum viable security resilience for SMBs? 14

How correlation stops compromise 17

The next layer: AI as a weaponized attack surface 18

Closing: Depth is the new defense 21

Executive Summary:

Welcome to the 2026 State of the SOC Report

Last year, N-able Technologies explored how AI and human analysts work together to deliver cyber resilience. This year, we're examining a fundamental shift in the threat landscape and what it reveals about the security strategies that succeed versus those that fail.

This report is grounded in telemetry and frontline response data from the Adlumin Managed Detection and Response (MDR) provided by the N-able SOC, spanning more than 900,000 alerts observed between March and December 2025.

After a steady increase of cloud-focused attacks, 2025 marked a dramatic return to network and perimeter exploitation: 18% of all alerts stemmed from network and perimeter (Unified Threat Management or UTM) exploits.

Organizations continue to invest in new security technologies, yet we observed how an overreliance on single layers of defense persists across the industry, creating a perception of safety that does not align with the operational realities of modern environments. This "magic bullet mindset" often conceals architectural blind spots and undermines a SOC's ability to detect, respond, and support recovery at scale.

The 2026 State of the SOC Report underscores a central theme: organizations that achieve true business resilience consistently adopt a genuine defense-in-depth strategy. The findings highlight how resilience emerges not from any single control or capability, but from the combined strength of layered visibility, coordinated detection, rapid response, and continuous improvement across the security stack.

Top Attack Vector Keeps Shifting

"When one door locks, attackers try the window."

- 2023 → Endpoints
- 2024 → Cloud
- 2025 → Network and Perimeter
- 2026 → Will AI be next?

Key takeaways:

TRADITIONAL SOC MODELS HIT BREAKING POINT

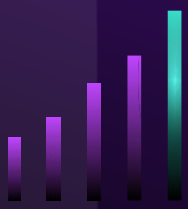
2 alerts per minute: average alert rate for the N-able SOC

Human-driven SOCs can't scale at this velocity. Organizations that haven't shifted to AI-centric operations are operating in constant triage mode, not true security posture.

NETWORK PERIMETER REEMERGES AS PRIMARY DEFENSE LAYER

18% of alerts now originate from network edge— a dramatic reversal from 2024

After years of "the perimeter is dead," attackers are exploiting the return-to-office and hybrid infrastructure seams. UTM and network-layer defenses are no longer optional.



SOAR IS REDEFINING THE RESPONSE LAYER

500% year-over-year surge in SOAR— orchestrated alert workflows

The volume crisis has made manual playbook execution obsolete. Organizations without orchestration are drowning, those with SOAR are staying ahead of the curve.

AI DOESN'T HELP THE SOC — IT DRIVES IT

90% of investigation is automated by AI

This isn't AI augmentation; it's AI operation with human oversight. The SOC analyst role has fundamentally shifted from investigator to decision-maker and threat hunter.

THE ENDPOINT CENTRIC STRATEGY LEAVES HALF THE RISK UNSEEN

50% of attacks bypass endpoint controls entirely

Cloud-native breaches, identity compromises, and lateral network movement render endpoint-only strategies fundamentally incomplete. Multi-layer visibility is the new baseline.

Key takeaways:

Key themes of 2025

TARGETING DISTRACTED DEFENDERS

While thousands of security professionals gathered at Black Hat USA 2025 to learn about threats, the N-able SOC noticed attacks appearing out of nowhere, fully formed, deep inside customer networks. SOC managers across the industry reported the same pattern.

The timing was deliberate. **Attackers timed campaigns to coincide with major security conferences—launching attacks while defenders were distracted.**

DEMOCRATIZING SOPHISTICATED FIREWALL EXPLOITS

The biggest vulnerability of 2025 was an exploit of one of the most well-known firewalls that became widely weaponized. State-level actors created sophisticated exploits that were packaged into tools accessible to lower-skilled attackers. What started as a complex attack became a mass-market weapon. **Script kiddies who couldn't write their own exploits could now compromise enterprise firewalls.**

2025 Adlumin SOC Snapshot

TOP ALERTS

ALERT	COUNT
Endpoints:	345,694
Cloud:	291,100
Network:	107,216
Perimeter:	29,971

TOP SOAR ACTIONS

ACTION	COUNT
Account Disables:	73,401
Passwords Resets:	47,656
Endpoint Remediation Actions:	22,857
Windows Defender Scan:	18,621
Remote Isolation:	2,977

The 2025 threat landscape:

When the perimeter came back

In last year's State of the SOC report, the N-able SOC statistics showed that virtually all detections came from the endpoint or the cloud. But in 2025, we saw a dramatic rise in network- and perimeter-focused detections **(107,216 network alerts and 29,971 UTM alerts)—representing 18% of all alerts.**

The data proves the point: Layered security is essential and automation is critical

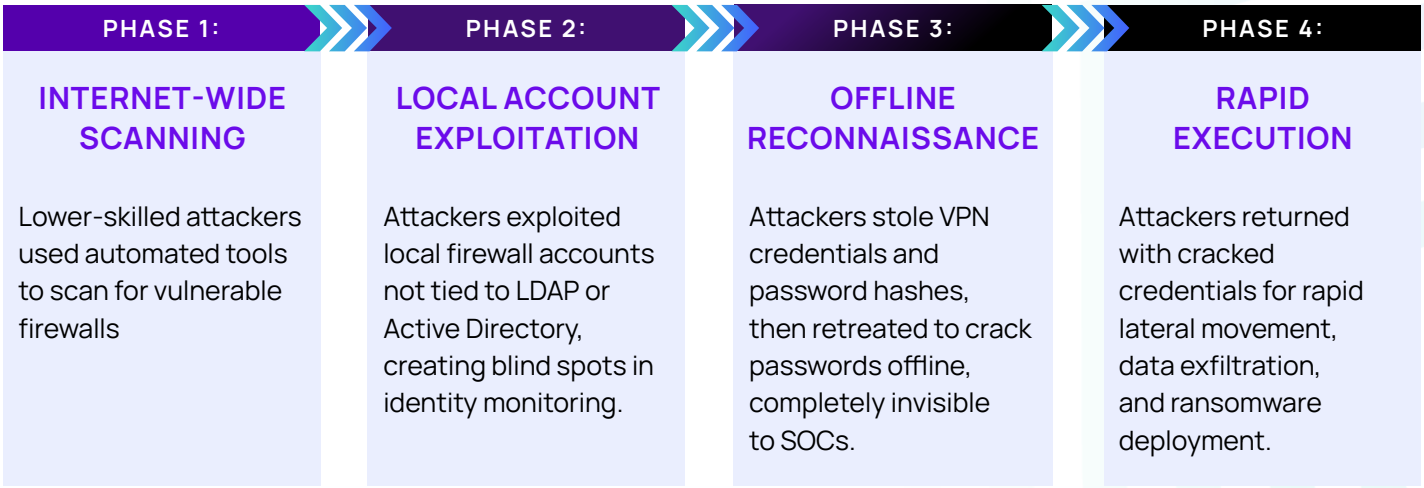
While endpoint and cloud still represent the majority of detections, network and perimeter layers caught 137,187 threats that fell outside the visibility of endpoint-only controls. These weren't minor threats, many were initial stages of attacks that would have become full breaches without multi-layer visibility.

When threats were detected, we saw a 5x year-over-year increase in automated Security Orchestration, Automation, and Response (SOAR) actions: Last year, SOAR actions represented just 1 in 20 of all responses, while **this year the SOAR share jumped up to almost 1 in 4 responses**. This shows that containment increasingly happens at machine speed and supports the value of modern security platforms for rapid, large-scale incident response.

The TL;DR lesson: Without visibility across identity, perimeter, network, endpoint, cloud, and (soon) AI layers, organizations are blind to critical attack stages. Defense-in-depth has always been best practice. Now it's the difference between swiftly containing an incident and suffering organization-wide impact.

The perimeter exploitation playbook

Attacks followed a consistent four-phase pattern. These weren't zero-days, these were known vulnerabilities organizations hadn't patched, combined with better exploitation tools. This is also why attacks appeared sudden. The reconnaissance phase was completely dark. By the time attackers returned, all prep work was done.



Why it worked: What made perimeter attacks so effective in 2025

Perimeter accounts not integrated with centralized identity management:
Organizations monitoring Active Directory for suspicious logins never saw attacks using local firewall accounts.

No network traffic analysis to detect lateral movement:
Even when attackers were inside the network, organizations without network monitoring couldn't see them moving between systems.

Flat networks providing unrestricted post-VPN access:
Once attackers gained VPN access, many networks had no internal segmentation. VPN access meant access to everything.

Offline password cracking is invisible to security tools:
Traditional security monitoring can't detect attacks happening outside the network.

The single-layer fallacy: Why “good enough” isn’t enough

Let’s be honest: Small to medium-sized businesses (SMBs) aren’t neglecting security. They’re working hard to decide where limited budgets and resources will have the greatest impact. The real issue is the growing overconfidence in single-layer solutions.

1 ENDPOINT DETECTION AND RESPONSE (EDR)

While 86,580 EDR alerts caught significant threats, network alerts (107,216) and perimeter/UTM alerts (29,971) caught attacks that endpoint tools never saw. Across multiple MDR investigations, the N-able SOC observed these network- and perimeter-based indicators appear days before any malicious activity reached the endpoint, many of which were the initial stages of attacks that would have become full breaches.

WHAT EDR CATCHES:

- Malware execution on endpoints
- Suspicious process behavior and fileless attacks
- Credential theft attempts from memory
- Local privilege escalation
- Unauthorized software installation

WHAT EDR MISSES:

- Network reconnaissance (port scanning, service enumeration)
- Lateral movement using legitimate tools (RDP, PowerShell remoting)
- Perimeter exploitation (firewall compromises, VPN attacks)
- Cloud attacks (API abuse, identity attacks in cloud services)
- Identity-based attacks that don’t touch endpoints
- Offline password cracking and reconnaissance

2 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

A SIEM doesn't create visibility, it aggregates and correlates the visibility you already have. Of the 909,155 total alerts processed in 2025, nearly half never touched the endpoint. Without data from multiple layers, correlation is impossible.

WHAT SIEM CATCHES:

- Whatever logs you send it (aggregation and correlation)
- Patterns across multiple data sources (if properly configured)
- Historical analysis and trend identification
- Compliance reporting and audit trails

WHAT SIEM MISSES:

- Anything from sources you're not monitoring
- Real-time threats if correlation rules aren't tuned properly
- Context from layers you haven't integrated
- Attacks in blind spots where you have no visibility

3 MULTI-FACTOR AUTHENTICATION (MFA)

SOAR capabilities performed 73,401 account disables and 47,656 password resets in response to credential-based attacks in 2025. If MFA were a complete solution, these numbers would be far lower. MFA is a critical control, but it's not a catch all, and attackers can bypass it through push fatigue, token theft, and social engineering. Perimeter accounts not tied to centralized identity bypass MFA entirely.

WHAT MFA CATCHES:

- Unauthorized login attempts with stolen passwords
- Credential stuffing attacks
- Brute force password attacks
- Login attempts from unauthorized locations (when paired with conditional access)

WHAT MFA MISSES:

- MFA bypass techniques (push notification fatigue, social engineering)
- Session token theft and replay attacks
- SIM swapping attacks
- Attacks on local firewall/perimeter accounts not tied to centralized identity systems
- Attacks that don't require authentication (perimeter exploits, network reconnaissance)
- Credential theft itself (MFA only prevents credential use, not theft)

4 UNIFIED THREAT MANAGEMENT (FIREWALL WITH UTM)

Firewalls with UTM are a critical first line of defense. The N-able SOC observed an increase in activity with attackers exploiting firewall vulnerabilities, misconfigurations, and VPN access to gain entry. Many of these exploits never triggered endpoint or identity alerts. Without additional layers of visibility, firewall compromises can quickly become full breaches.

WHAT FIREWALL WITH UTM CATCHES:

- Inbound attacks and malicious traffic
- Known exploits and malware signatures
- Unauthorized access attempts at the perimeter
- Network-based threats and intrusion attempts
- Web filtering and application control

WHAT FIREWALL WITH UTM MISSES:

- Attacks that exploit vulnerabilities in the firewall itself
- Attacks originating inside the perimeter (phishing, insider threats)
- Compromised credentials used for legitimate VPN access
- Lateral movement once attackers are inside the network
- Endpoint-based attacks (malware execution, local privilege escalation)
- Cloud-based attacks (API abuse, identity attacks)
- Encrypted traffic that passes through without deep inspection

Without visibility across identity, perimeter, network, endpoint, cloud, and AI layers, organizations are blind to critical attack stages.

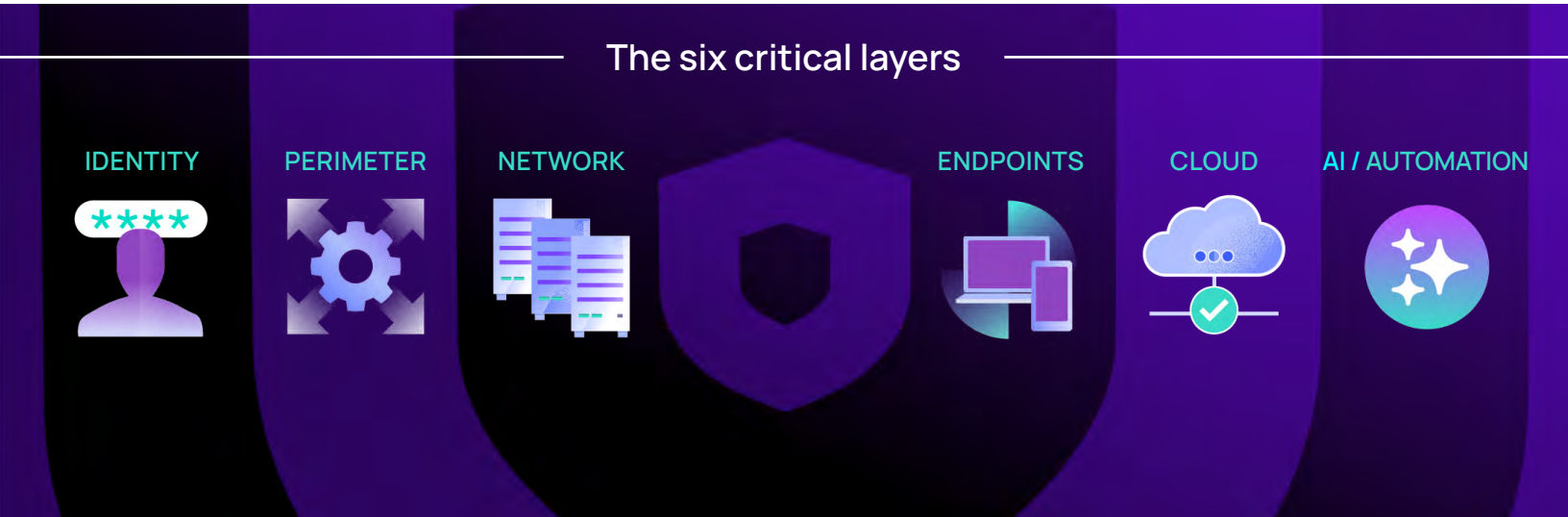
N-able State of the SOC Report

Security resilience redefined for 2026

Modern cyberthreats don't just aim to break through your defenses; they aim to disrupt your business. **What organizations need now is true security resilience**, the ability to withstand attacks, maintain operations during disruption, and recover quickly without lasting damage.

To build this kind of resilience, organizations can strengthen and coordinate six essential layers of defense. Each layer provides critical visibility and response capability, but together they form a unified approach that allows teams to detect threats earlier, contain them faster, and recover with confidence.

The six critical layers



IDENTITY

2025 data:

identity alerts

detected threats at this layer

WHAT IT INCLUDES:

Multi-factor authentication (MFA), conditional access policies, geofencing, privilege management, identity behavior analytics, password policies, single sign-on (SSO) with proper controls

WHAT IT PROTECTS AGAINST:

Credential theft, account takeover, privilege escalation, insider threats, unauthorized access

PERIMETER

2025 data:

UTM alerts

caught perimeter-level threats

WHAT IT INCLUDES:

Next-generation firewalls, VPN security and monitoring, network segmentation and DMZ architecture, intrusion prevention systems (IPS), web application firewalls (WAF), DDoS protection

WHAT IT PROTECTS AGAINST:

Inbound attacks, malicious traffic, unauthorized access attempts, known exploits, network-based threats

NETWORK

2025 data:

network alerts

detected threats invisible to other layers

WHAT IT INCLUDES:

Network traffic analysis (NTA), lateral movement detection, network segmentation enforcement, DNS security, internal firewall rules, micro-segmentation in virtual environments

WHAT IT PROTECTS AGAINST:

Lateral movement between systems, reconnaissance activity, east-west traffic attacks, command-and-control (C2) communications, data exfiltration attempts

ENDPOINTS

2025 data:

endpoint-layer detections

(345,694 endpoint + 86,580 EDR)

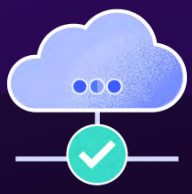
WHAT IT INCLUDES:

Endpoint detection and response (EDR), behavioral analysis, application control/whitelisting, patch management, anti-malware (behavioral, not just signature-based), device encryption

WHAT IT PROTECTS AGAINST:

Malware execution, suspicious process behavior, local attacks, credential theft from memory, unauthorized software installation

CLOUD



2025 data:

cloud alerts

showed continued cloud targeting

WHAT IT INCLUDES:

Cloud Security Posture Management (CSPM), Cloud Access Security Broker (CASB), cloud Identity and Access Management (IAM), API monitoring and security, container security, serverless security

WHAT IT PROTECTS AGAINST:

Cloud misconfigurations, API abuse, identity attacks in cloud environments, data exposure, unauthorized access to cloud resources

AI / AUTOMATION

2025 data:

This layer is still emerging—

most organizations aren't monitoring AI as an attack surface yet

WHAT IT INCLUDES:

AI agent monitoring, orchestrator security, agent-to-agent (A2A) protocol oversight, behavioral analysis of AI actions, audit logging of AI decisions

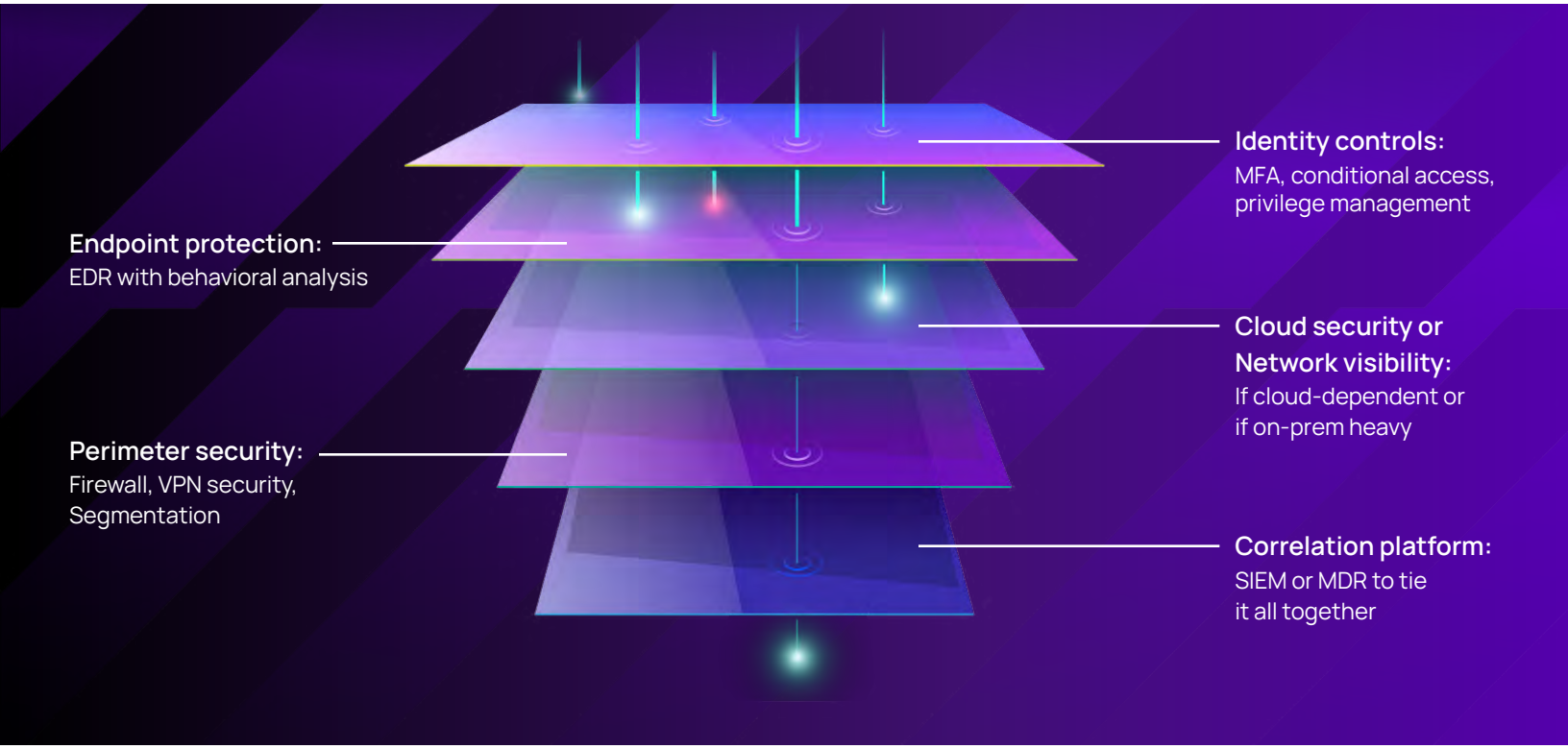
WHAT IT PROTECTS AGAINST:

AI agent hijacking, orchestrator compromise, AI poisoning, automated attack chains, malicious AI-to-AI communications

What's the minimum viable security resilience for SMBs?

Prioritization is unavoidable—no organization (and certainly not SMBs) has endless security budget and resources. But, limited resources don't have to mean trade-offs or weakened defenses. By focusing on what delivers the most value now, teams can build momentum, maturity, and meaningful resilience.

The N-able SOC consistently identified threats earlier in the attack lifecycle—often before lateral movement or credential abuse escalated, in environments where these controls were in place.



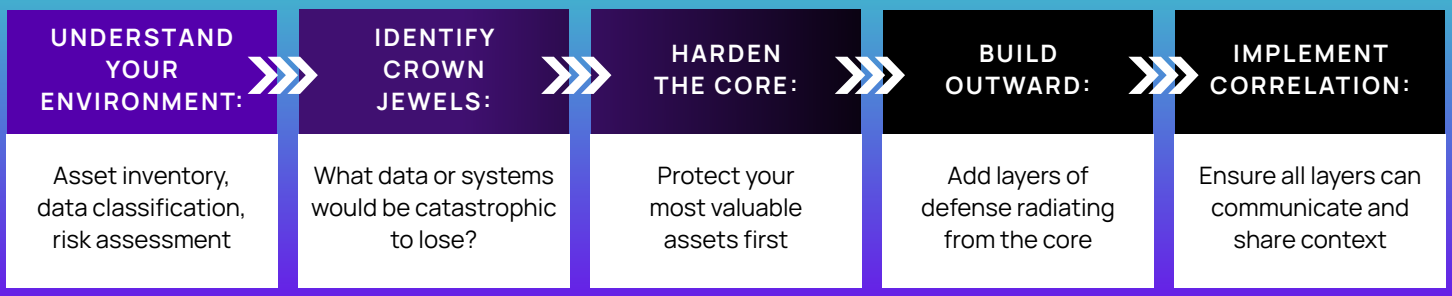
MULTI-LAYER VISIBILITY SPOTS ATTACK EARLY

The N-able SOC observed an incident where attackers leveraged weak VPN credentials to compromise an administrative account, then shifted to offline credential cracking and scheduled-task persistence—remaining invisible until rapid execution. **Without visibility beyond the perimeter, this attack would have appeared "sudden," despite hours of preparation occurring in the dark.**

The flip: Securing from the inside out

Legacy thinking will say start at the perimeter and work inward, build your defenses from outside to inside, following the attack path from left to right in the kill chain. But today's threat landscape and the sheer speed of attacks demand a different approach.

The Zero-Trust Prioritization Framework



How to prioritize without compromise

Build capability as you invest

Organizations are wisely investing in AI-powered technologies. By pairing those investments with targeted skill-building, teams can unlock the full value of these tools and accelerate operational readiness.

Turn a broad toolset into integrated intelligence

Most organizations already have powerful tools in place. The next step is connecting them. Integrating alerts and correlating data reduces noise, sharpens clarity, and enables faster, more confident decision-making.

Use automation where it excels: speed and scale

Automation is ideal for high-volume, repeatable tasks. But the most complex decisions still benefit from human insight. By balancing fast automation with expert oversight, organizations ensure both efficiency and accuracy.

AUTOMATED RESPONSE HALTS HOLIDAY ATTACK IN MINUTES

The N-able SOC observed multiple holiday-period incidents where attackers deliberately launched campaigns during early-morning hours when internal teams were unavailable. **Fortunately, correlation across multiple signals combined with automated response enabled containment within minutes preventing escalation.**

The advantages of multi-layer correlation

Even with the right foundational layers in place, the real power only emerges when they operate as a unified system. Multi-layer correlation connects the signals coming from identity, endpoint, cloud, network, and perimeter controls, transforming isolated alerts into a clear, actionable picture of an unfolding attack.

Instead of treating each alert as a standalone event, correlation reveals the relationships between them, surfacing patterns, reducing noise, and enabling teams to detect threats earlier and respond with far greater confidence and speed.

AI is automating up to

90%

of investigations with human-led oversight

SPEED	CONFIDENCE	SCOPE
Automated correlation eliminates the time spent manually investigating whether separate alerts are related. Instead of an analyst spending time determining that three alerts are part of the same attack, correlation provides that context instantly.	Single alerts always carry uncertainty: Is this a false positive or a real threat? Correlated alerts reduces that uncertainty. When multiple layers confirm the same attack pattern, confidence is high enough to take immediate action without fear of disrupting legitimate business operations.	The full attack timeline becomes visible right away. You can see where the attack started, what the attacker has accessed, and where they're trying to go next. This complete picture enables targeted containment instead of broad, disruptive responses.

CORRELATION STOPS THANKSGIVING ATTACK

In a Thanksgiving-morning incident, the N-able SOC detected domain trust discovery and lateral movement tied to a privileged account just minutes after initial access. **Although each signal alone appeared ambiguous, correlated activity across identity, endpoint, and network layers revealed an active compromise.** The SOC isolated affected hosts, disabled the account, and reset credentials before sunrise—stopping the attack before data theft or ransomware deployment.

How correlation stops compromise

Here's an example of how multi-layer correlation would stop a VPN compromise from blooming into a successful ransomware attack:

PERIMETER LAYER
VPN login from an unusual geographic location

Analyst assessment:
Low confidence alert—could be legitimate travel

+

NETWORK LAYER
Lateral movement attempts, SMB scanning across multiple systems

Analyst assessment:
Medium confidence—could be legitimate IT activity

+

ENDPOINT LAYER
Suspicious PowerShell execution, credential dumping attempt

Analyst assessment:
High confidence—likely malicious, but context unclear

Without correlation: The perimeter alert might be dismissed as travel. The network alert might be attributed to IT activity. By the time the endpoint alert triggered, the attacker would have already stolen credentials.

What correlation revealed: VPN compromise (unusual location) → immediate reconnaissance (SMB scanning) → credential theft preparation (PowerShell execution) = high-confidence incident requiring immediate containment

Why automation is critical: Of the 909,155 total alerts processed in 2025, 658,532 were automated alerts that required correlation across layers. Human analysts couldn't possibly review all of these manually in sufficient time—correlation had to happen automatically.

CORRELATION STOPS RANSOMWARE ATTACK

During a ransomware attempt detected at 5:00 AM on December 25, N-able's SOC identified a perimeter-initiated attack that began with VPN brute force and escalated through credential dumping and malicious scheduled tasks. **Because activity was correlated across identity, endpoint, and network layers, the SOC contained the incident in under 10 minutes—preventing data exfiltration, encryption, and downtime**

The next layer:

AI as a weaponized attack surface

Organizations are deploying AI agents and automation at an unprecedented pace, and that AI automation is increasingly taking over traditionally manual security and defense functions. Case in point: In our 2025 report, we estimated that 70% of all investigation and remediation could be automated through AI. Now, we've seen that jump up to **90% of all investigations** that could be AI-driven.

But while AI indeed holds great promise to be used for good in cybersecurity, it's critical to recognize and account for the risk that the AI at the core of these tools could be compromised and misused by malicious actors.

AI in Cybersecurity: A double-edged sword

THE GOOD (DEFENDERS)

2024

70% of investigation and remediation can be automated by AI

2025

9/10 AI can automate as much as nine out of ten investigative tasks

2026

99% of investigation and remediation can be automated by AI (estimated)

THE BAD (THREAT ACTORS)

2024-25

Experimental phase—attackers testing and tinkering

2026

Attack tactics begin to reach operational maturity

2027

Adverserial AI attacks accelerate

AI is amplifying both defense and risk in cybersecurity. For defenders, it offers meaningful gains in speed, consistency, and coverage, elevating detection and response and freeing teams to focus on higher value decisions. At the same time, adversaries are exploring AI to scale and refine their tactics.

What is adversarial use of AI?

Imagine a cloud orchestrator (AI) managing multiple customer environments through relay orchestrators communicating via agent-to-agent (A2A) protocols like those Microsoft and Google released in 2025.

How it gets used

If a malicious actor gains control of an orchestrator, they can wreak havoc. If the primary orchestrator is compromised, the malicious actor effectively has full control.

Attack scenarios

- **Orchestrator hijacking:**
  Attacker issues malicious commands to AI agents thinking they're legitimate
- **AI poisoning:**
  Malicious training data makes AI treat attacks as normal
- **A2A protocol exploitation:**
  Man-in-the-middle attacks between AI agents
- **Behavioral camouflage:**
  AI-generated attacks that look like legitimate AI behavior

The Future: How do we secure this new AI layer

Securing the expanding layer of AI-powered defenses requires visibility, control, and governance that matches the speed and scale at which these systems operate. That means being able to observe and audit AI behavior in real time, tightly controlling who and what can issue commands to AI systems, and monitoring how AI agents interact with each other across environments. Just as importantly, organizations must establish behavioral baselines, preserve decision trails for investigation and accountability, limit AI access to critical infrastructure, and keep humans in the loop for high-impact actions. Without these safeguards, AI systems risk becoming increasingly attractive targets for attackers.

What to do now: Preparing for the AI security challenge

Preparing for AI-driven threats starts with understanding where AI is being used today—and how those systems could be targeted tomorrow.

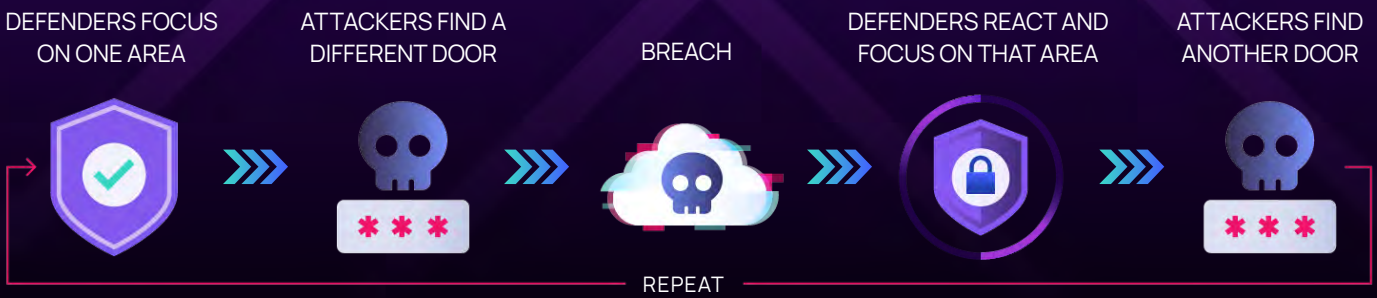
INVENTORY AI USAGE	ASSESS IMPACT IF COMPROMISED	PLAN FOR AI VISIBILITY	DON'T RELY ON AI TO SECURE AI	DESIGN FOR SCALE
Identify where AI tools are deployed and what systems, data, or networks they can access.	Determine what an attacker could do if they gained control of AI agents or orchestrators.	Ensure your security roadmap includes monitoring, baselining, and detection for AI activity.	Automation is essential, but human oversight remains critical for high-impact decisions.	AI will dramatically increase alert volume—making correlation, automation, and MDR capabilities essential for sustainable response.

50% of attacks bypass endpoint controls. Organizations that haven't shifted to AI-centric operations are in constant triage mode, not true security posture.

Depth is the new defense

2025's story is simple: Attackers shifted from cloud to perimeter because that's where the vulnerabilities were. Next year, they'll shift again. They always do.

It's a predictable cat-and-mouse pattern:



The only way to break the cycle:
Stop playing whack-a-mole. Secure all doors simultaneously.

Essential mindset shifts

- **From "protected" to "resilient":** The goal isn't perfection—it's resilience. Detect early, contain quickly, recover completely.
- **From "set it and forget it" to "continuous visibility":** Security is ongoing—continuous monitoring, regular tuning, periodic testing.
- **From "magic bullet" to "layered defense":** Security is the sum of multiple layers working together, with correlation between them.

THE EXTINCTION EVENT TEST

Ask yourself:

- If attackers breach your primary defense, what happens next?
- Can you detect them at the next layer?
- Can you contain them before they reach your crown jewels?
- Can you recover if they succeed?

If any answer is "no," you're missing defense in depth.

True business resilience

Defense in depth is simple math. Every layer you add multiplies the attacker's work while dividing their success rate. The 2025 data proves it: With visibility across endpoint, cloud, network, UTM, identity, and other layers, Adlumin Security Operations detected threats single-layer approaches would have completely missed.

Put another way: Organizations relying solely on endpoint monitoring would have missed 137,187 network and perimeter threats. With 145,074 automated SOAR actions executing containment at machine speed, layered security didn't just detect more, it responded faster.

In 2026, layered defense is critical to survival.

How integrated ecosystems reduce complexity

One challenge with defense in depth is that complexity buying and integrating 6+ separate security vendors creates its own problems. But with integrated ecosystems, these components are designed to work together. Correlation happens automatically. A single partner relationship delivers outcomes across all layers. Complexity is reduced while effectiveness increases.

THE N-ABLE ECOSYSTEM

N-ABLE N-central Endpoint Management	Strengthens endpoint resilience with real-time management, automated security hardening, and scalable operations.
N-ABLE EDR Endpoint Security	AI-driven endpoint detection and response strengthens device security and reduces your attack surface.
N-ABLE Adlumin Security Operations	AI-driven, human-led security operations delivering early detection, automated response, and resilience.
N-ABLE DNS Filtering DNS Security	Blocks malicious domains at the DNS layer to prevent phishing, malware, and ransomware threats
N-ABLE Mail Assure Email Security	Cloud-based email security with phishing and malware protection, continuity, and long-term archiving
N-ABLE Cove Data Protection™	Cloud-native data protection delivering resilient backup, flexible recovery, and business continuity.

Are you ready for the future?

Explore how Adlumin's advanced analytics, AI-driven solutions, and human expertise can help you stay ahead of evolving threats.

Take the tour

N-ABLE™

About N-able

N-able protects businesses from evolving cyberthreats. Our AI-powered cybersecurity platform delivers business resilience to more than 500,000 organizations worldwide, leveraging advanced end-to-end capabilities, simplified workflows, market-leading integrations, and flexible deployment options to improve efficiency and drive critical security outcomes. Our partner-first approach pairs our technology with experts, training, and peer-led events that empower customers to be secure, resilient, and successful. n-able.com

This content may contain forward-looking statements regarding future product plans and development efforts. N-able considers various features and functionality prior to any final generally available release. Information regarding future features and functionality is not and should not be interpreted as a commitment from N-able that it will deliver any specific feature or functionality in the future or, if it delivers such feature or functionality, any time frame when that feature or functionality will be delivered. All information is based upon current product interests, and product plans and priorities can change at any time. N-able undertakes no obligation to update any forward-looking statements regarding future product plans and development efforts if product plans or priorities change.