The Three Pillars of Business Resilience

Pillar 1: Endpoint Resilience (N-central)

The Problem: Endpoints are where attacks begin. Drift, unpatched systems, and blind spots create vulnerabilities.

The Solution:

- Continuous network discovery prevents blind spots
- Built-in vulnerability and patch management eliminates weaknesses
- Automation enforces security standards at scale. Agentic AI coworker built in
- Turns every device from a liability into a line of defense

AI Inside N-central — What to Say:

N-zo, your Agentic AI Coworker built right into N-central. N-zo gives technicians a natural language interface to query device health, surface anomalies, and get guided recommendations—without ever leaving the platform. And for teams building custom workflows or integrations, N-central now includes an **MCP server**, enabling AI-powered tooling to connect directly with N-central data and actions programmatically.

AI-assisted scripting and automation cut hours of manual work to minutes by translating natural-language requests into ready-to-run scripts — accelerating autonomous endpoint management and enabling technicians at every skill level to make an impact.

This means a junior tech can describe a task in plain English — "restart the print spooler service on any device where it's stopped" — and get a working, deployable script in seconds. No PowerShell expertise required. No senior engineer pulled off other work.

An AI-powered developer portal also accelerates tech stack integration to customers' systems and third-party tools that enable their end-to-end business processes.

Additional AI-driven enhancements within N-central are coming soon, designed to deliver faster insights, clearer risk awareness, and greater operational efficiency — helping IT teams stay ahead with more intelligent support as these capabilities roll out.

The AI punchline: *"Your techs aren't constrained by skill. They're constrained by the tools they're running on. N-central's AI removes that ceiling — automating the repeatable work so every tech operates like your best tech."*

Pillar 2: Security Resilience (Adlumin)

The Problem: You can't stop every attack. The question is: how much damage will it cause?

The Solution:

- Unified visibility across users, endpoints, identities, and cloud
- AI-powered detection and automated response reduces dwell time

- Fast containment limits blast radius
- Continuous learning adapts to ever evolving threats

AI Inside Adlumin — What to Say:

> Advanced AI threat detection models continuously analyze access patterns, identify unauthorized activity, and map lateral movement across environments to enable rapid containment. This isn't rule-based detection that attackers know how to evade — it's behavioral AI that learns what normal looks like in each specific environment and flags deviations the moment they appear.
>
> Automated threat triage uses AI to identify, enrich, and assign 90% of alerts to the appropriate response workflow, reducing analyst workload and accelerating response times. That means your security team — or your clients' security team — is no longer drowning in noise. They're working the 10% that actually requires human judgment, with full context already attached.

The AI punchline: *"Attackers are using AI to move faster. Your detection and response has to move at the same speed. Adlumin's AI SOC doesn't just flag threats — it triages them, enriches them, and routes them to the right response automatically. Ninety percent of the noise handled before a human ever sees it."*

Pillar 3: Data Resilience (Cove)

The Problem: Most businesses fail not because they were breached, but because they couldn't recover.

The Solution:

- Cloud-native, immutable backups isolated from production network.
- Launching DRaaS capabilities for near-instant back to business after a disaster
- Built-in anomaly detection identifies threat actor attacks on backups
- TrueDelta technology enables frequent backups with up to 60X less data movement
- Set-it-and-forget-it reliability—it just works

AI Inside Cove — What to Say:

> Automated recovery testing uses AI to validate recoverability without full test restores, saving time while increasing confidence. This is a fundamental shift in how backup health is verified. Instead of scheduling manual restore tests — which most teams do quarterly at best, and many skip entirely — Cove's AI continuously validates that backups are actually recoverable. You know your recovery will work before you need it, not after.
>
> Combined with TrueDelta technology and immutable, cloud-isolated storage, Cove doesn't just protect your backups — it continuously proves they work.

The AI punchline: *"Most teams find out their backup didn't work when they need it most. Cove's AI validates recoverability continuously — so when the worst happens, the answer to 'can we recover?' is already yes."*

What about AI? How are you using AI? What is N-able Resilience AI?"

AI is fundamentally changing the threat landscape, and the way organizations must think about resilience. In an environment where attacks unfold in minutes, resilience has to operate continuously. Our focus is on embedding AI directly into the systems our customers use every day, introducing agentic AI capabilities that customers can choose to use. This will help automate tasks, boost efficiency, and keep humans firmly in control, so resilience becomes a built-in operating discipline rather than a reactive response.

AI Capabilities Embedded Across the N-able Platform

The AI-driven approach from N-able unifies visibility, response, and recovery, helping businesses achieve enterprise-grade outcomes without enterprise-level complexity or cost.

Unified Endpoint Management: AI-Powered Automation

Meet **N-zo**, your Agentic AI Coworker built right into Ncentral. N-zo gives technicians a natural language interface to query device health, surface anomalies, and get guided recommendations—without ever leaving the platform. And for teams building custom workflows or integrations, Ncentral now includes an **MCP server**, enabling AI-powered tooling to connect directly with Ncentral data and actions programmatically.

AI-assisted scripting and automation cut hours of manual work to minutes by translating natural-language requests into ready-to-run scripts. This accelerates autonomous endpoint management and operational improvement of workloads by enabling technicians at every skill level to make an impact.

AI-powered developer portal accelerates tech stack integration to customers' systems and third-party tools that enable their end-to-end business processes.

Additional AI-driven enhancements within our UEM products will be available soon, designed to deliver faster insights, clearer risk awareness, and greater operational efficiency, helping IT teams stay ahead with more intelligent support as these capabilities roll out.

Security Operations: AI-Driven Threat Detection and Response

Advanced AI threat detection models continuously analyze access patterns, identify unauthorized activity, and map lateral movement across environments to enable rapid containment.

Automated threat triage uses AI to identify, enrich, and assign 90% of alerts to the appropriate response workflow, reducing analyst workload and accelerating response times.

Data Protection: Intelligent, AI-Enhanced Recovery

Automated recovery testing uses AI to validate recoverability without full test restores, saving time while increasing confidence.

As AI continues to reshape both offense and defense, N-able is investing to expand its AI capabilities, helping customers deliver measurable outcomes and enabling organizations to operate securely in an increasingly complex digital world.
