



Mastering IT Agility in a Seismic Shift

9 exceptional journeys from reactive
chaos to proactive confidence.

The stakes have never been higher.

IT Operations is transforming rapidly in an era of great change. The industry landscape shift is seismic.

1. Endpoint Chaos

Disparate operating systems and idle devices falling off the radar.

2. Vulnerability Panic

The relentless cadence of zero-days and manual CVE mapping.

3. The Resource Drain

Lean teams and tight budgets severely constrained by minimal scripting capabilities.



The Shift: Reactive Vulnerability to Proactive Agility

The Stale Era

Visibility

Blind spots, lost idle devices, and manual audits

Connectivity

Bound to local servers and clunky VPN dependencies

Remediation

Waiting for user reboots and scouring Reddit for CVEs

Scalability

Fragmented third-party tools and manual clicks

The Agile Era

Real-time, cloud-based telemetry across all assets

Cloud-native tethering needing only an internet connection

Automated mapping of CVEs to specific OS patches

Automated cross-platform scripts executed globally

9 Diverse Journeys. 1 Unified Outcome.

Damartex

Retail (3000+ Emp)



Hurdle: Fragmented manual patching tools.

Tractor and Equipment

Manufacturing (700 Endpoints)



Hurdle: Lost idle devices and remote connectivity.

Mueller Water

Manufacturing



Hurdle: Rapid zero-day response (Log4j).

AC Transit

Government & Transit



Hurdle: Legacy apps and interdivisional silos.

Mid-Sized Ed Co

Education Services



Hurdle: 50/50 Mac and Windows split.

Union School District

Education



Hurdle: Scouring the internet for CVE context.

Lyncourt School District

SLED (100 Endpoints)



Hurdle: Physical lock-out from server room.

City of Edinburg

Local Government (900 Endpoints)



Hurdle: Securing off-site police cars and tablets.

Beaumont

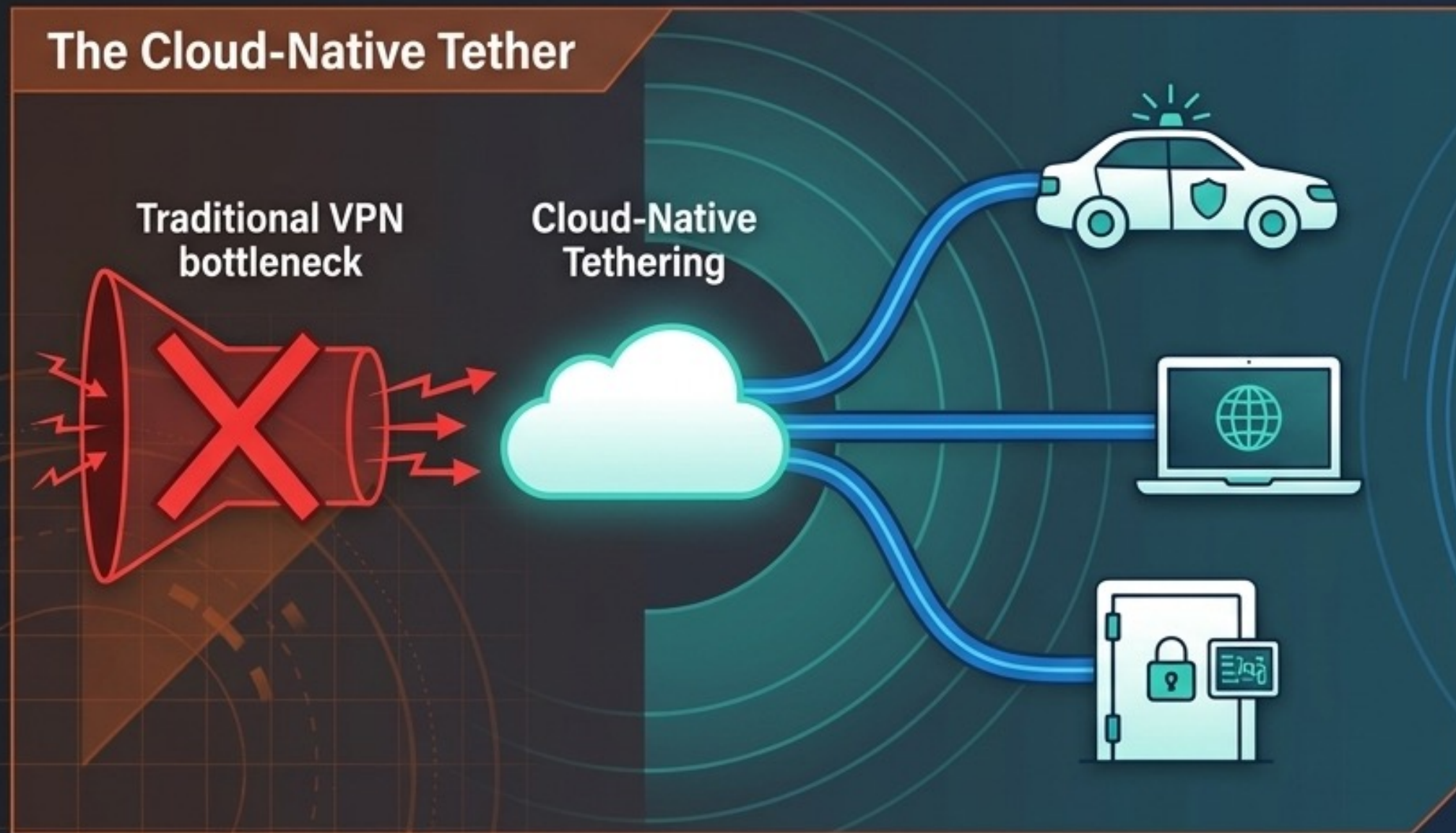
Enterprise



Hurdle: Lack of trust in patching effectiveness.

Pillar I: Breaking the Physical Perimeter

Manage devices without line-of-sight. When endpoints leave the building, security shouldn't drop off.



City of Edinburg



Managing 900 endpoints, including off-site police cars and Mobile Digital Communicators (MDCs). No VPN needed; no returning to City Hall.



Lyncourt School District

During a construction project, the IT team was physically locked out of their server room. A cloud-native solution allowed them to remotely run updates and maintain security without physical hardware access.

Pillar II: Unifying the Fragmented Stack

Insight: End the console-switching fatigue. Treat disparate operating systems with a single standard of compliance.

The Multi-OS Funnel



Mid-Sized Ed Co

Tasked with bridging a strict 50/50 split between Mac and Windows for a fully remote workforce.

Automox was the only product I found that worked for us – and it works perfectly.

— Michael King, IT Manager

AC Transit

Broke down geographical and interdivisional silos across departments to gain real-time visibility and maintain device compliance across a complex transit environment.

UNIFIED PANE OF GLASS DASHBOARD

Pillar III: The Speed of Security

Insight: When a zero-day drops, hours matter. Stop manually mapping CVEs to patches.

The Zero-Day Timeline



Crisis Averted (Mueller Water & Log4j)

In December 2021, Log4j zero-days dropped daily. Using Automox, Mueller scanned every endpoint, located affected devices, and ran patches to temporarily remediate the issue globally—saving the IT team’s holidays.

Process Upgraded (Union School District)

Previously relied on Reddit threads and colleagues to map vulnerabilities. Now utilizes a single platform that automatically maps CVEs to available patches by OS, drastically accelerating response times.

Pillar IV: Automating the Mundane

Insight: Win back hours. Empower lean teams to execute at enterprise scale.



Tractor and Equipment

Managing 700 endpoints across three states. Slashed time spent on patching by 50%, allowing the team to complete exponentially more tasks.

Beaumont

Overcame severe cybersecurity anxiety and deep mistrust of previous tools (which left machines years out of date).

What I've told colleagues... was that it just works. The fact that I have a system I can trust that 'just works' is amazing.

— Angela Wright, CTO

The Secret Weapon: Automox Worklets™

Canned scripts (PowerShell or BASH) deployed to automate complex operations at scale—whether moving files, patching custom software, or managing uninstalled applications.

The Worklet Engine



The Edinburg Philosophy

If you can script it, you can automate it.



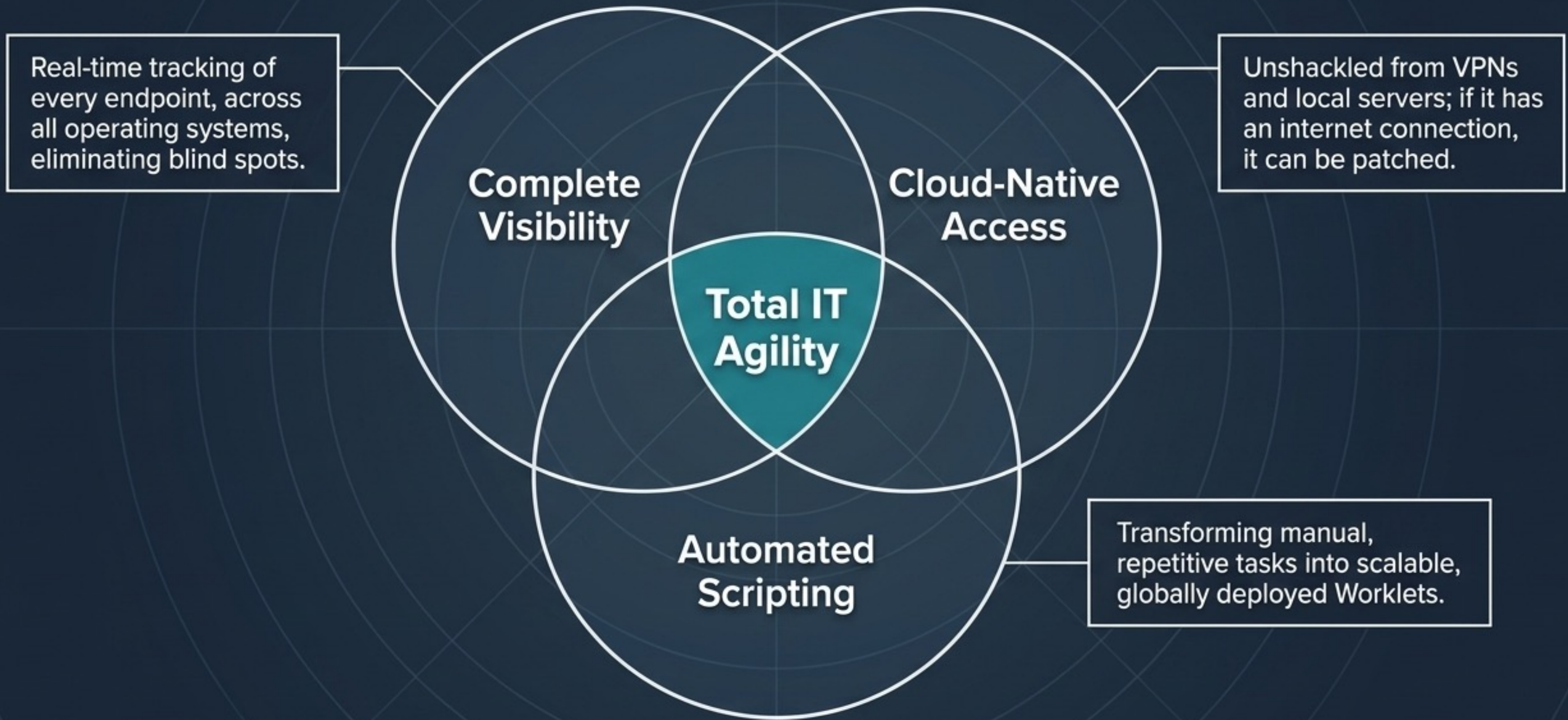
The Damartex Impact

Creating custom scripts for recurring problems enhanced the team's PowerShell skills and simplified software management.

"It was like adding a new specialist to the team."

— Tommy Devoye, Damartex

The Anatomy of Modern IT Agility



Lean teams moving faster, with greater confidence, at lower costs.

9 Distinct Journeys. 1 Shared Reality.

Slashed Complexity

Replaced fragmented third-party software and clunky VPN dependencies with a single source of truth.

Accelerated Security

Achieved fast vulnerability remediation, meeting strict cyber hygiene goals and securing Cybersecurity Insurance approval.

Maximum ROI

Reduced operating costs and massive time savings, allowing small teams to operate at enterprise capacity.

Restored Confidence

Automox gives us peace of mind.
— Lisa DeLapo, Union School District



Thoughtfully automated. Always updated. Quietly confident.

Step out of the reactive era. Save time, reduce risk, and slash complexity by automating OS, third-party, and configuration updates on all your Windows, macOS, and Linux endpoints.

Automate IT everywhere. Start a free 15-day trial to experience the unified grid.

WWW.AUTOMOX.COM