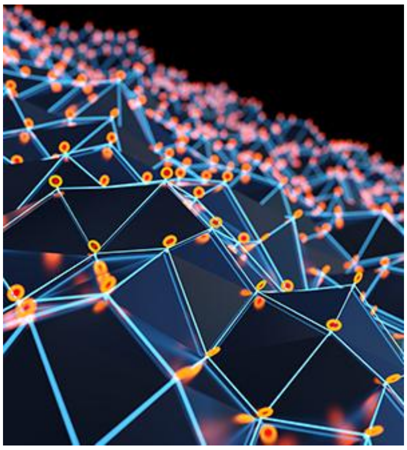
PL
DELIVERING SEAMLESS CONNECTIVITY WITH CableLabs
THE AI FACTORY BACKBONE WITH NOKIA
NAVIGATING NIS2 SUPPLY CHAINS
INTEGRATING INTENT-BASED NETWORKS
TRANSPARENT ENTERPRISE SERVICES
THE FIBER RESURGENCE
UNIFIED NETWORK SECURITY
AI & HYBRID NETWORKS
LIQUID COOLING & STRANDED POWER
DESIGNING SELF-HEALING NETWORKS
NETWORK TRANSFORMATION

www.pipelinepub.com
Volume 22, Issue 3

# Reinventing Endpoint Management: The 10-in-1 Architecture for the Modern Enterprise and MSP

By: Koroush Saraf - VP Product Management, ZPE Systems



In today's hyper-connected world, cybersecurity demands a holistic approach that encompasses network security, endpoint security, and cloud security. Companies like Palo Alto Networks and Fortinet have excelled at fortifying the network perimeter, while endpoint protection platforms such as CrowdStrike and Microsoft Defender have focused on detecting and responding to threats at the device level. Yet, a critical gap persists: the lack of comprehensive endpoint lifecycle management. This oversight leaves organizations exposed, creating fertile ground for successful cyberattacks. And threat actors increasingly exploit endpoint-level vulnerabilities in addition to attacking the network perimeter.

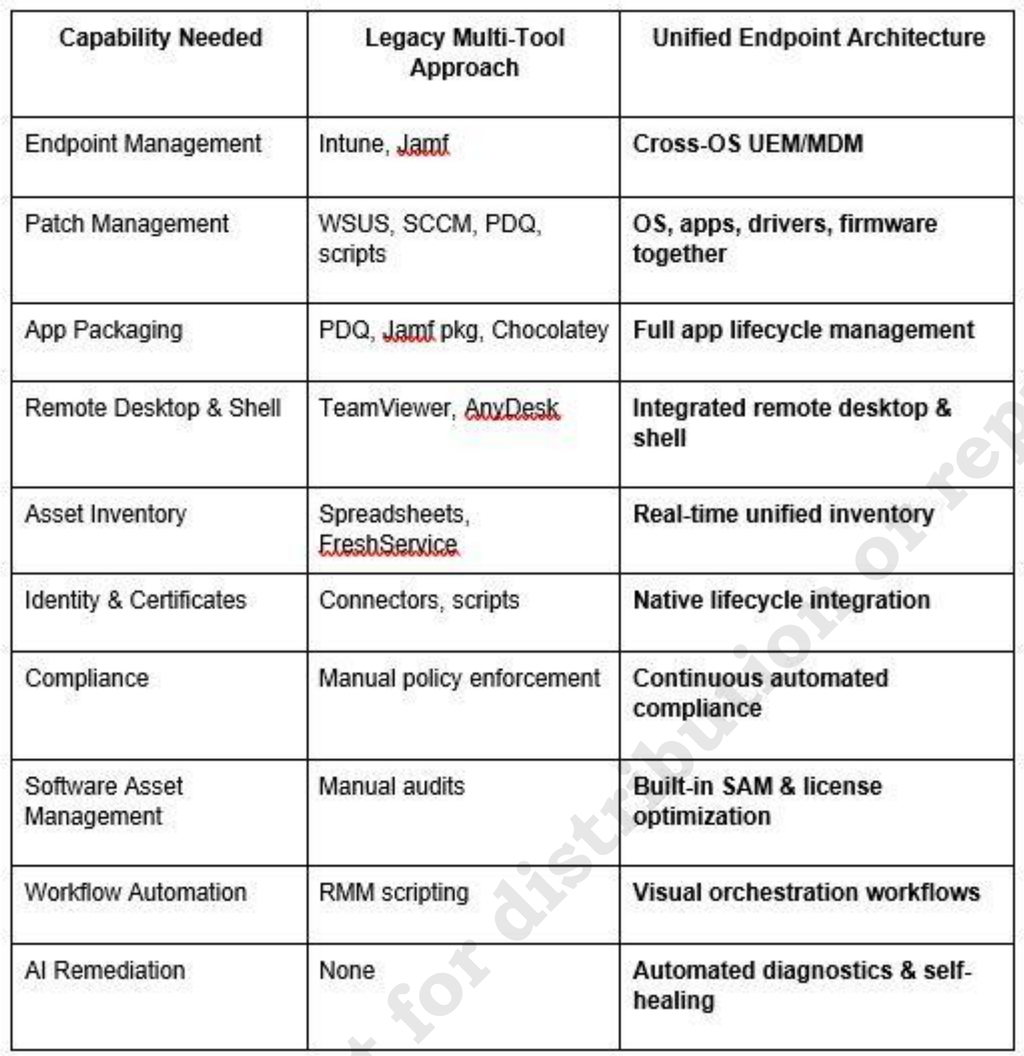
The problem is systemic. Without proactive management throughout an endpoint's lifecycle—from provisioning and patching to decommissioning—vulnerabilities accumulate. Unpatched software, outdated drivers, and unmanaged applications become entry points for malware, ransomware, and advanced persistent threats. Traditional endpoint security tools are reactive, kicking in only after a threat is detected. But prevention requires more: ongoing maintenance that ensures devices are hardened from the start and remain secure over time.

## The Fragmentation of Legacy Tools

Enterprises and managed service providers (MSPs) often rely on a patchwork of legacy tools to handle endpoint management. A typical stack might include Intune for Windows and mobile devices, Jamf for Apple ecosystems, remote access solutions like TeamViewer or AnyDesk, deployment tools such as PDQ Deploy or Chocolatey, update systems like WSUS or SCCM, various RMM platforms, and a slew of custom scripts to fill the gaps.

This fragmentation breeds inefficiency. Tool sprawl leads to siloed data, where insights from one system don't inform another. IT teams face operational fatigue, juggling multiple interfaces and logins. Security gaps emerge as policies inconsistently apply across operating systems—Windows, macOS, iOS, Android, and ChromeOS. Costs balloon from overlapping subscriptions, while complexity slows down responses to incidents.

The outcomes are inconsistent at best. Onboarding drags on, patches miss deadlines, and compliance audits reveal blind spots. If your endpoint strategy is still a patchwork of RMM, MDM, and scripts, you’re already behind.



| Capability Needed | Legacy Multi-Tool Approach | Unified Endpoint Architecture |
|---|---|---|
| Endpoint Management | Intune, Jamf | **Cross-OS UEM/MDM** |
| Patch Management | WSUS, SCCM, PDQ, scripts | **OS, apps, drivers, firmware together** |
| App Packaging | PDQ, Jamf pkg, Chocolatey | **Full app lifecycle management** |
| Remote Desktop & Shell | TeamViewer, AnyDesk | **Integrated remote desktop & shell** |
| Asset Inventory | Spreadsheets, FreshService | **Real-time unified inventory** |
| Identity & Certificates | Connectors, scripts | **Native lifecycle integration** |
| Compliance | Manual policy enforcement | **Continuous automated compliance** |
| Software Asset Management | Manual audits | **Built-in SAM & license optimization** |
| Workflow Automation | RMM scripting | **Visual orchestration workflows** |
| AI Remediation | None | **Automated diagnostics & self-healing** |

## The Amplified Challenges for MSPs

For MSPs, these issues are magnified by the nature of their business. Managing multi-tenant environments means dealing with diverse client needs, often requiring different tools per customer. This leads to high per-device costs, as licenses and agents multiply across stacks.

Scaling becomes a nightmare. Adding clients demands more staff to handle the tool complexity, eroding margins. Service level agreements (SLAs) suffer when remediation takes hours instead of minutes, and customer satisfaction dips amid frequent disruptions. MSPs need consolidation to streamline operations, reduce overhead, and deliver consistent value—without sacrificing security or control.

## Before vs. After: Legacy vs. Unified

The shift to a unified endpoint architecture transforms these pain points. Considering the prior figure. The "after" state, operations are streamlined, costs drop, and security strengthens.

## Transitioning to the End-State Architecture

Organizations don't need to rip and replace overnight. They can keep Intune during the transition, layering a unified 10-in-1 platform on top initially. This hybrid approach eases migration, allowing gradual consolidation. The long-term end state is an all-in-one architecture. It reduces vendors, agents, costs, and complexity—delivering up to 10× savings. Real-time operations replace polling, and automation handles routine tasks, freeing IT for strategic work.

## Strengthening Cybersecurity Posture

Next-generation firewalls (NGFW) and endpoint protection platforms are essential but inherently reactive. They detect and block threats after they've breached the perimeter or landed on a device. True prevention lies in proactive measures: patching endpoints and servers, ensuring correct drivers, updating applications, and optimizing software spend by removing underused or unwanted apps to reclaim licenses. Unified endpoint management (UEM) fills this preventive vulnerability gap. It extends to servers, including cloud VMs, enforcing consistent security across hybrid environments. This isn't just best practice—it's increasingly required for cyber insurance, as insurers demand evidence of robust lifecycle management to mitigate risks.

## Why Legacy Architectures Fail

Legacy systems falter in a modern threat landscape. Polling intervals mean delayed visibility—hours or days between status checks. Scripts are fragile, breaking with OS updates or environmental changes. Patch management is fragmented, covering OS but ignoring third-party apps where most vulnerabilities lurk. Vendor sprawl compounds the issue, with overlapping features and poor integrations. MSPs lack native multi-tenancy, forcing workarounds that compromise isolation. Remediation is slow, relying on manual intervention rather than automation.

## The 10-in-1 Architecture: Core Components

A modern 10-in-1 architecture integrates these essential functions into a single platform:

1. **Unified UEM/MDM**: Manages all endpoints—desktops, mobiles, servers—across OS ecosystems with real-time configuration and compliance.
2. **Patch Management**: Automates updates for OS, applications, firmware, and drivers, ensuring comprehensive coverage without manual effort.
3. **App Lifecycle and Packaging**: Handles packaging, deployment, and removal of apps, supporting silent installs and policy-based rollouts.
4. **Built-in Remote Desktop/Shell**: Provides secure, high-performance access, including unattended sessions, eliminating separate tools.
5. **Asset Lifecycle**: Tracks hardware and software from acquisition to retirement, optimizing inventory and reducing shadow IT.
6. **Identity & Certificate Integration**: Aligns with Zero Trust by managing identities, enforcing least privilege, and automating certificate issuance.
7. **Compliance Automation**: Continuous checks and enforcement, with real-time reporting to meet regulatory demands.
8. **Software Asset Management (SAM)**: Delivers usage insights, license reclamation, and spend optimization across the portfolio.
9. **Workflow Automation**: Drag-and-drop builders for provisioning sequences, including auto-detected drivers and updates.
10. **AI-Driven Remediation**: Proactively identifies and fixes issues, reducing tickets through self-healing algorithms.

This architecture isn't additive—it's integrative, creating synergies that legacy stacks can't match.

## Delivering Business Impact

For enterprises, the benefits are tangible. Tool and operational costs drop by up to 10× through consolidation. Support tickets halve as AI handles routine fixes. Onboarding accelerates from hours to minutes, boosting productivity. Compliance and security posture strengthen, minimizing downtime and breach risks. Operations unify under one dashboard, enabling data-driven decisions. MSPs gain even more leverage. Per-device costs plummet, inflating margins. They can serve more clients with existing staff, thanks to automation. SLAs improve with faster remediation, enhancing customer satisfaction. Onboarding new clients simplifies, reducing setup time and errors.

## The Imperative for Change

IT and security leaders must act now: modernize your endpoint strategy, consolidate fragmented tools, automate workflows, and fortify your cyber posture. Reduce complexity by adopting real-time UEM architectures that deliver prevention alongside detection. The shift is already underway. Forward-thinking organizations are reaping the rewards—lower costs, stronger security, and scalable operations. Don't get left behind in a world where endpoints are the new battleground.