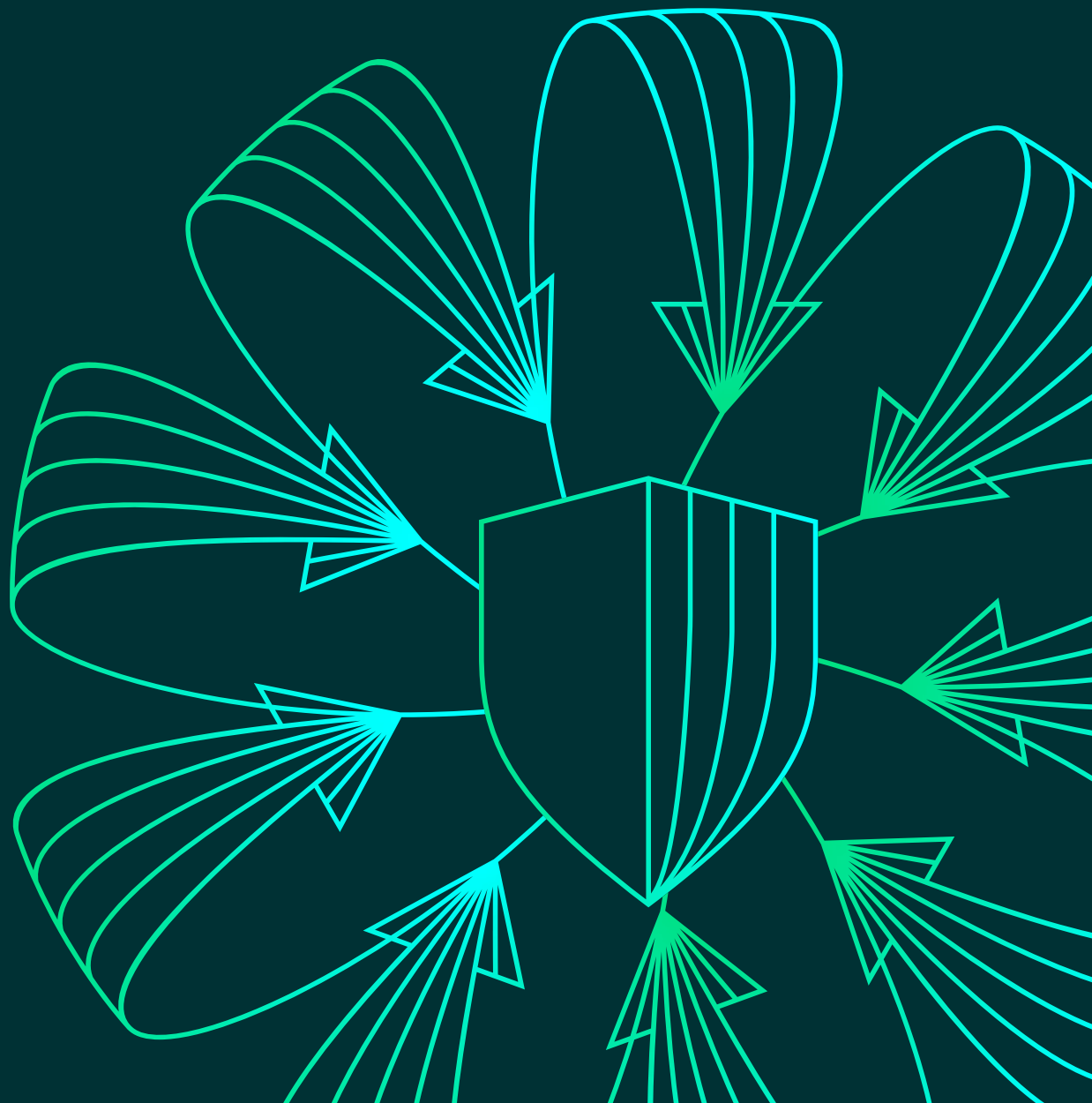


Unified endpoint management

The ultimate buyer's guide



Contents

- 3 Defragging endpoint management
- 3 A unified approach to UEM
- 4 Understanding UEM
- 5 Strategic benefits of implementing UEM
- 6 Key considerations when choosing a UEM partner
- 7 The Unisys advantage
- 8 The UEM implementation and migration process
- 8 Get started with Unisys

Defragging endpoint management

Most IT leaders want the same thing: a workforce that's productive and secure, no matter what device people reach for or where they're working from. Unified endpoint management (UEM) is how that ambition becomes achievable at scale, bringing every laptop, phone, virtual desktop, meeting room, and IoT sensor under one policy engine and one clear view.

The obstacle is how endpoint management works in most organizations today. It once meant keeping laptops patched. Now it spans an entire estate, and most of it comes with its own console, agent, and team.

That fragmentation can show up in:

The IT productivity tax. Engineers log in to multiple portals, reconcile inventory that disagrees, and push the same policy change three times.

Unseen vulnerabilities. Manual split patching stretches patch latency into weeks, leaving known exploits on the devices nobody watches: signage, kiosks, and meeting room kits.

Slow operating system (OS) migrations. Without unified migration, Windows 11 and major macOS or Android transitions stretch into multi-quarter projects.

A frustrating employee experience. When a laptop, phone, and meeting room answer to three different tools, people hit broken sign-ons and dropped connections that no single console can trace.

A growing attack surface. Set-and-forget endpoints sit outside the patch cycle, the asset registry, and threat detection — exactly the profile attackers look for.

The good news? Every one of these is fixable once you bring endpoints together.



A unified approach to UEM

UEM works as an operating model. It's a commitment to consistent governance and security for every endpoint an organization depends on: a knowledge worker's Windows laptop, an IoT sensor on a restaurant kitchen fryer, or a digital signage display in a retail store. A rugged handheld and a laptop remain distinct devices.

UEM ties everything together with accountability: one contract, one service-level agreement, one operational team, and one vendor responsible for the outcome.

Understanding UEM

At its core, UEM manages every endpoint your organization owns, from laptops to meeting rooms to IoT sensors. It's the successor to a decade of point tools, such as mobile device management (MDM), enterprise mobility management (EMM), client management, and patch managers. Policy, security, and analytics travel with the device, not the console.

Five pillars set it apart from traditional device management.

Centralized visibility and control

A unified view of Windows, macOS, iOS, Android, Linux, virtual, and IoT endpoints, with a single rule that propagates everywhere.

1

Automated patching and OS transitions

Cloud-orchestrated patches, app updates, and full OS migrations on a continuous wave-based cadence, with real-time tracking and pre-defined rollback.

2

AI-powered security and compliance

Behavioral threat analysis, data loss prevention, hard disk drive encryption, and conditional access enforced at the device.

3

Application life cycle management

Centralized provisioning, updates, security, and retirement for apps across any network, with a self-service catalog for users and license control for IT.

4

Advanced analytics and proactive telemetry

Continuous device monitoring that surfaces fading batteries, spotty Wi-Fi, and configuration drift.

5

Strategic benefits of implementing UEM

Adopting UEM delivers advantages that can improve your security posture, cost base, employee experience, and scalability ceiling at the same time.

Stronger security and Zero Trust enablement



UEM makes the endpoint a first-class Zero Trust enforcement point. Conditional access weighs device compliance, encryption state, patch level, and identity before granting access to corporate resources. A non-compliant device, whether a contractor's laptop or a meeting room PC, is held out of sensitive applications until it is remediated. Security teams move from chasing alerts to running a continuously verified estate.

Reduced total cost of ownership



A holistic UEM solution consolidates capabilities that once needed 5 to 10 separate tools: MDM, EMM, client management, patch management, software distribution, mobile threat defense, configuration management, and asset tracking. Organizations typically retire three to six tools in the first year, recovering license spend and the overhead of maintaining each console and agent.

Elevated employee experience



Consistent sign-on, self-service app access, and automated fixes pushed before people notice add up to real productivity gains. Ticket volume drops as routine issues self-heal, and the tickets that remain resolve faster because the diagnostic data is already in the console.

Room to scale



Wave-based deployment lets the same team manage 1,000 endpoints or 100,000-plus without growing headcount in lockstep. Policy changes propagate in minutes. Acquisitions and major workforce shifts become configuration events rather than multi-quarter integration projects.

Sustainability and resource optimization



Continuous health monitoring (battery condition, thermal behavior, storage wear, performance trend) replaces reactive refresh cycles with data-driven retention. Devices stay productive longer, hardware spend flattens, and the carbon footprint of unnecessary replacement shrinks, contributing to corporate sustainability targets rather than just an IT metric.

Key considerations when choosing a UEM partner

Selecting the right partner is crucial to realizing the expected benefits. Use the criteria below to find a provider that meets your current needs and supports your organization's future growth.

Key consideration	What to look for	Unisys offering
Comprehensive multi-OS capabilities	Can the provider manage Windows, macOS, iOS, Android, Linux, and ChromeOS equally well?	Full support across all major OS families plus meeting rooms, signage, kiosks, and IoT managed in a single console using the same policy model
Migration expertise at scale	Can the provider run massive, complex OS and software migrations without breaking enterprise productivity?	Proven wave-deployment methodology backed by RemoteOS, with high reported success rates on remote device recovery
Advanced AI and behavioral threat protection	Does the solution stop threats reactively or get ahead of them with machine learning?	Behavioral analysis layered with crowdsourced threat intelligence to detect, contain, and remediate risk at the endpoint
Infrastructure and IT service management (ITSM) integration	How smoothly does the solution connect with your existing ticketing systems and asset registries?	Automated, bi-directional data flows with leading ITSM platforms and custom dashboards that surface UEM telemetry inside the tools your teams already use
Visibility and granular analytics	Does the solution give real-time diagnostic reporting on the health of every device?	Role-based views for operations, security, and executive audiences
Global footprint with local nuance	Can the provider support distributed software as a service tenants and workforces across regions and time zones?	A global engineering and operations team with regional data residency options and multilingual support

The Unisys advantage

While many providers offer automated tooling, Unisys combines deep endpoint engineering, a global migration record measured in millions of devices, and full integration with our broader Digital Workplace Solutions portfolio. Here's how the Unisys Unified Endpoint Management solution stands out.

End-to-end device management:

Unisys manages the full life cycle, from procurement and provisioning to security response, refresh, and secure retirement with verified data sanitization. One accountable partner, start to finish.

Automated OS transition playbooks:

Unisys codifies decades of migration experience into reusable playbooks that handle compatibility scanning, wave scheduling, rollback, and validation.

Agentic service desks:

AI-driven agents handle routine incidents end to end, freeing service desk teams to focus on what actually needs a human.

Alignment with digital employee experience platform:

UEM telemetry feeds an outcomes model measured in employee productivity and time-to-resolution, with commercial terms that can flex around experience metrics.

Engineering depth and global scale:

A dedicated UEM engineering practice and global delivery centers provide follow-the-sun operations across every major OS family and emerging endpoint class.

RemoteOS:

RemoteOS is an in-house recovery capability, with a patent filing in progress, that rebuilds no-boot and hardware-failure devices remotely with no technician visit and lands each one on the latest compliant operating system, drivers, and Basic Input/Output System every time.



Streamline your Windows migration

Every migration is a chance to fix more than the OS, and every laptop in your fleet is doing a different job. Upgrading them all the same way leaves savings on the table. Unisys pairs Windows migrations with a persona-based assessment. Browser-only teams move to lightweight setups, power users get full upgrades, and hardware spend drops without adding management overhead.

The UEM implementation and migration process

Transitioning to Unisys UEM is a well-structured process designed to minimize disruption and maximize value. We move in five clear phases, and you start seeing benefits well before the final wave lands. Throughout every phase, you have visibility of progress, and your users keep working.

Get started with Unisys

Endpoint fleets grow more diverse, more distributed, and more security-critical every day. Unisys helps you treat UEM as a strategic solution rather than a tactical tool swap, with the engineering depth and global delivery to back it up.

Start with a clear picture of where you stand. Check out the **UEM readiness scorecard** to assess your environment in minutes and pinpoint where unification will deliver the fastest gains. Then visit **unisys.com** to learn more, or **connect with our team** to convert your readiness into a plan built around your estate.

WEEKS 1–5

Planning and discovery

- Audit the current device landscape
- Surface legacy point tools
- Define compliance baselines

WEEKS 3–6

Architecture and design

- Build UEM tenant policies
- Stand up custom admin dashboards
- Create wave-migration schedules

WEEKS 6–9

Integration and testing

- Connect UEM to your ITSM platforms
- Test end-user agents on pilot groups

WEEKS 10–30

Wave deployment and migration

- Execute scaled rollouts with real-time tracking

ONGOING

Steady-state management

- Shift to proactive maintenance, continuous patching, and automated behavioral threat response

Please note these are tentative time frames that may vary based on the scope and complexity of the work.



unisys.com

© 2026 Unisys Corporation. All rights reserved.

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.

09/26 7196-12781