WHITE PAPER

Zecurit Endpoint Manager

A Modern Approach to Unified Endpoint Management

How modern IT teams can manage, secure, and support distributed endpoint environments through a unified, cloud-native platform spanning device management, security enforcement, automated patching, BitLocker encryption, and compliance reporting.

Published by	Category	Audience
ZECURIT	ENDPOINT MANAGEMENT	IT TEAMS, MSPS, SECURITY LEADERS

EXECUTIVE SUMMARY

The Endpoint Management Imperative

Modern organisations operate within increasingly diverse and distributed IT environments. Employees work across offices, homes, and remote locations using laptops, desktops, and mobile devices, and the footprint keeps expanding. Managing these endpoints securely while maintaining productivity has become one of the most critical challenges facing IT teams today.

Traditional endpoint management tools were built for a different era: centralised networks, uniform device types, and employees who worked from a single location. That world no longer exists.

> **Industry Research:** Endpoint devices represent one of the largest attack surfaces in modern organisations, with thousands of unmanaged or poorly configured devices often operating outside traditional network boundaries.

Zecurit Endpoint Manager is a cloud-native Unified Endpoint Management (UEM) platform that helps organisations standardise endpoint operations, improve visibility, and maintain control across distributed environments. It consolidates patch management, automated software deployment, BitLocker encryption, device control, power management, remote troubleshooting, and compliance reporting into a single unified interface.

This white paper examines the challenges driving the need for modern endpoint management, the full capability set required to address them, and how Zecurit Endpoint Manager is built to meet those demands.

THE PROBLEM

The Modern Endpoint Management Challenge

Over the past decade, the IT landscape has shifted dramatically. Distributed workforces, cloud-first application stacks, and an explosion of device types have fundamentally changed how organisations must approach endpoint management.

01

Device Proliferation

Organisations now manage hundreds or thousands of devices across Windows, macOS, and Linux, each with its own update cadence and configuration requirements.

02

The Remote Workforce

Remote and hybrid models have moved employees off corporate networks. Legacy tools lack the reach to maintain visibility over devices outside the traditional perimeter.

03

Expanding Security Risks

Unpatched systems, unauthorised peripherals, disabled encryption, and misconfigured devices expand the attack surface. Endpoint hygiene is a frontline security concern.

04

Software Management Complexity

Manually ensuring every device runs correct software versions and patches is unsustainable at scale. Without automation, inconsistencies accumulate quickly.

05

Limited Visibility

Many IT teams operate with incomplete or stale inventory data. Without real-time information on device health, hardware changes, and software installations, informed decision-making becomes guesswork.

06

Compliance Pressure

Frameworks including HIPAA, ISO 27001, PCI-DSS, and GDPR demand documented evidence of device posture and policy adherence. Manual tracking creates audit risk and compliance gaps.

These challenges don't exist in isolation; they compound one another. A gap in visibility creates a security risk; a security risk creates a compliance exposure. Addressing them requires a unified, automated approach.

BACKGROUND

What Is Unified Endpoint Management?

Unified Endpoint Management (UEM) is the modern standard for managing and securing all endpoint devices from a centralised platform, regardless of device type, operating system, or user location.

A fully capable UEM platform enables organisations to:

- **Discover and inventory** all endpoint devices automatically
- **Monitor device health** continuously and in real time
- **Deploy software and patches** consistently at scale
- **Enforce security policies** across device groups
- **Manage drive encryption** and recover keys centrally
- **Control peripheral access** and communication ports
- **Support remote troubleshooting** without physical access
- **Automate routine tasks** with cross-platform scripting
- **Optimise power consumption** across the device fleet
- **Generate compliance reports** for regulatory frameworks

By consolidating these functions into a single platform, UEM reduces operational complexity and enables IT teams to move from reactive to proactive device management.

THE SOLUTION

Introducing Zecurit Endpoint Manager

Zecurit Endpoint Manager is a cloud-native Unified Endpoint Management platform designed to simplify IT operations and strengthen endpoint security across the entire device lifecycle: from initial onboarding through ongoing maintenance and eventual retirement.

Built for modern IT environments, Zecurit requires no on-premise infrastructure. IT teams gain centralised control over all managed endpoints through a web-based management console, accessible from anywhere. A single lightweight agent handles patch management, software deployment, configuration enforcement, BitLocker management, device control, automation, and remote troubleshooting across Windows, macOS, and Linux endpoints.

Patch Management · Software Deployment · IT Asset Management · Configuration Management · BitLocker Management · Device Control · Remote Access & Tools · Remote Script Execution · Power Management · Monitoring & Alerts · Compliance Reporting

PLATFORM

Core Platform Capabilities

Patch & Update Management

Unpatched systems remain one of the most exploited attack vectors. Zecurit automates the full patch lifecycle, from detection through deployment to compliance verification, eliminating the manual effort and exposure windows created by reactive patching.

- Automatic missing patch detection by severity
- CVSS-based vulnerability prioritisation
- Windows Update policy management
- Scheduled maintenance window control
- Real-time patch status monitoring
- Centralised patch approval and deferral
- Patch compliance reports for auditors

Comprehensive IT Asset Management

Accurate asset visibility is the foundation of effective endpoint management. Zecurit automatically collects and maintains detailed records across hardware, software, and licences, giving IT teams a single source of truth for the entire asset estate.

- Automatic device discovery and onboarding
- Software inventory with real-time version tracking
- Software metering for usage-based licence optimisation
- Geo location tracking for physical asset accountability
- Full hardware inventory (CPU, RAM, storage, peripherals)
- Software licence entitlement vs. installation monitoring
- Warranty management and expiry tracking
- Hardware and software change alerts

Automated Software Deployment

Manual software distribution at scale is operationally inefficient and prone to inconsistency. Zecurit's deployment engine ensures consistent, reliable software distribution with a fraction of the manual effort, including pre-install validation to prevent failures before they happen.

- Pre-install validation (disk space, registry, services)
- Flexible targeting by device, group, or individual endpoint
- Pre/post installation script execution
- Silent installation with no user interruption
- Off-hours scheduling and phased rollouts
- Real-time deployment status monitoring

Policy-Based Configuration Management

Consistency in device configuration is a security and operational imperative. Zecurit enables scalable governance through named configuration profiles that can be independently associated with specific device groups or individual endpoints, keeping policy creation and deployment as separate, flexible steps.

- Centralised profile management for device groups
- Windows Update policy enforcement
- Security hardening configurations
- Firewall rule creation and deployment
- Local user and group management
- Script-based configuration automation

BitLocker Management

Drive encryption is a foundational security control, but managing BitLocker at scale across a distributed fleet has historically required Microsoft BitLocker Administration and Monitoring (MBAM) infrastructure. With MBAM 2.5 SP1 end-of-support arriving in July 2026, Zecurit provides a cloud-native alternative that eliminates the infrastructure overhead while delivering superior management capabilities.

- Centralised drive encryption policy enforcement
- Automatic recovery key backup and rotation
- BitLocker compliance reporting
- TPM authentication management (TPM-only, TPM+PIN, passphrase)
- Multiple BitLocker profiles by department or security tier
- TPM availability and version reporting

Device Control

Removable storage, Bluetooth, wireless adapters, and unauthorised peripherals represent significant data exfiltration and malware introduction vectors. Zecurit's device control capability enables policy-based enforcement across every peripheral category, including offline enforcement when endpoints are disconnected from the network.

- Allow, block, or trusted-only rules by peripheral category
- Wireless adapter and Bluetooth restriction
- BadUSB keystroke injection prevention
- Audit-ready connection and block event logs
- Removable storage and CD-ROM drive management
- Keyboard and printer access enforcement
- Offline policy enforcement (agent-side)

Remote Access & Diagnostic Tools

When device issues arise, rapid resolution minimises downtime. Zecurit provides IT administrators with a comprehensive remote management and diagnostic toolkit, enabling issue resolution without physical device access and with full session auditing for compliance.

- Unattended remote desktop access
- Secure encrypted file transfer
- Wake on LAN for off-hours access
- Two-way chat during active sessions
- Advanced diagnostic tools (processes, services, network)
- Remote reboot, shutdown, and logoff
- Multi-monitor support
- Session confirmation and full audit logging

Remote Script Execution & Automation

Repetitive IT tasks, system remediation, configuration changes, and software management workflows can all be automated through Zecurit's scripting engine. Scripts can be executed across thousands of endpoints simultaneously, turning hours of manual work into single-click operations.

- PowerShell, Bash, Python, VBScript, and batch support
- Targeted deployment to groups or individual devices
- Runtime parameter control and custom exit codes
- 100+ pre-tested script templates
- Centralised script repository with tag-based organisation
- Scheduled execution and on-demand triggering
- Real-time execution monitoring and failure alerts

Power Management

Energy consumption across a large endpoint fleet represents a significant operational cost and environmental impact. Zecurit's power management capability automates device power cycles, enforces granular power policies, and provides visibility into usage patterns to eliminate wasted energy without compromising availability.

- Scheduled wake and shutdown with Wake-on-LAN retry logic
- Remote one-click shutdown, wake, restart, and logoff
- User activity and logon history reports
- Granular AC and battery power schemes
- Advanced battery management and threshold configuration
- Power usage and system uptime reports

Monitoring & Alerts

Proactive monitoring is more effective than reactive incident response. Zecurit's alerting engine provides real-time notifications across security, hardware, software, storage, licence, and certificate events, surfacing issues before they escalate into incidents or audit findings.

- Security alerts (firewall, BitLocker, antivirus status)
- Prohibited software installation alerts
- Licence expiry and compliance breach alerts
- Hardware change detection (USB, memory, disks, adapters)
- Disk space threshold notifications
- Certificate expiry and self-signed cert detection

OUTCOMES

Business Impact

Organisations that adopt a modern endpoint management platform can realise measurable operational benefits. These outcomes matter not only for IT operations teams but for business and security leaders evaluating the return on endpoint management investment.

01

Reduced IT Workload

Scripting, patch automation, and software deployment reduce manual effort across routine device management activities.

02

Faster Patch Response

CVSS-prioritised patching and automated deployment accelerate vulnerability remediation across the entire fleet.

03

Audit Readiness

Pre-built reports mapped to HIPAA, ISO 27001, PCI-DSS, GDPR, CIS, and NIST streamline audit preparation significantly.

04

Lower Downtime

Remote troubleshooting, diagnostic tools, and proactive monitoring reduce the operational impact of device incidents.

05

Stronger Encryption Coverage

Centralised BitLocker management ensures drive encryption is consistently enforced, with keys always recoverable.

06

Reduced Energy Costs

Automated power management policies reduce electricity consumption by eliminating idle-device waste across the fleet.

07

Licence Cost Optimisation

Software metering and licence entitlement monitoring surface unused seats and over-licensing, reducing unnecessary spend.

08

Data Loss Prevention

Device control policies block unauthorised removable storage and peripheral access, reducing exfiltration risk.

09

Scalable Operations

Cloud-based management scales with organisational growth without additional infrastructure investment.

BENEFITS

Organisational Benefits

- **Improved IT Efficiency**

  Automation across patch deployment, software distribution, configuration enforcement, and scripted remediation reduces the volume of manual, repetitive tasks, freeing IT staff to focus on higher-value initiatives.

- **Enhanced Security Posture**

  Centralised BitLocker enforcement, USB device control, CVSS-prioritised patching, and proactive alerting across security events collectively reduce the likelihood of a breach going undetected across the endpoint fleet.

- **Greater Operational Visibility**

  Real-time hardware and software inventory, geo location tracking, warranty monitoring, and certificate visibility give IT and leadership teams a comprehensive view of the endpoint environment, eliminating the blind spots that create risk.

- **Faster Issue Resolution**

  Remote desktop access, diagnostic tools, Wake on LAN, and file transfer capabilities reduce resolution times, minimise employee downtime, and eliminate the need for costly on-site support in most scenarios.

- **Regulatory Compliance Support**

  Over 100 built-in reports with pre-built templates mapped to HIPAA, ISO 27001, PCI-DSS, GDPR, CIS, and NIST controls, with scheduled delivery to stakeholders, reduce the burden of compliance evidence collection.

- **Scalable IT Operations**

  Cloud-based infrastructure means organisations can expand endpoint management coverage without provisioning additional hardware or deploying on-premise servers, supporting growth without proportional cost increases.

USE CASES

Who Uses Zecurit Endpoint Manager

ENTERPRISE IT

Centralise the management of thousands of endpoints spanning distributed offices and remote workers. Enforce consistent security policies, patch compliance, BitLocker encryption, and device control at scale from a single console.

MSPS

Deliver patch management, remote monitoring, endpoint security, and compliance reporting across multiple client environments from a single platform, without maintaining separate tooling or infrastructure for each client.

SECURITY TEAMS

Monitor device security posture continuously, enforce BitLocker and firewall policies, control peripheral access, detect unauthorised changes, and generate audit-ready compliance documentation for regulatory frameworks.

GROWING ORGANISATIONS

Establish structured, scalable endpoint management practices from the ground up, without the infrastructure complexity of traditional enterprise tooling. Scale the platform as the device fleet grows.

ARCHITECTURE

Why Cloud-Based Endpoint Management Matters

Cloud-native endpoint management platforms provide meaningful advantages over traditional on-premise approaches. Zecurit Endpoint Manager is built on cloud architecture to deliver these benefits while maintaining enterprise-grade security and data protection standards.

Dimension	Traditional On-Premise	Cloud-Native UEM
Deployment Speed	Weeks to months	Hours to days
Infrastructure Overhead	High (servers, MBAM, databases)	Minimal
Remote Device Coverage	Limited	Comprehensive
Scalability	Constrained by hardware	Elastic
Updates and Maintenance	Manual	Automatic
BitLocker Key Management	Requires MBAM (EOL July 2026)	Native, cloud-hosted
Accessibility	Network-dependent	Global

FRAMEWORK

The Endpoint Management Lifecycle

Effective endpoint management is not a single action but an ongoing operational cycle. Organisations that mature their endpoint practices typically work across seven interconnected stages. Zecurit Endpoint Manager is designed to support all seven stages from a unified platform, reducing the need for separate point tools at each step.

1

Discover

Identify all devices connecting to the environment

2

Inventory

Maintain accurate hardware, software, and licence records

3

Configure

Apply policies, encryption, and security settings at scale

4

Deploy

Distribute software and patches consistently

5

Monitor

Track health, compliance, security posture, and power usage

6

Support

Diagnose and resolve issues remotely

7

Report

Generate operational and compliance reporting

GOVERNANCE

Compliance & Reporting

Demonstrating compliance with regulatory frameworks requires consistent, accurate, and timely reporting across endpoint posture, security controls, software licencing, and user access. Zecurit provides over 100 built-in reports designed to support IT operations and prepare organisations for security audits without manual evidence gathering.

FRAMEWORK

Pre-Built Compliance Templates

Report templates mapped to HIPAA, ISO 27001, PCI-DSS, GDPR, CIS Controls, and NIST, ready for use without custom configuration.

SECURITY

Security Posture Reports

Surface BitLocker gaps, TPM availability, Windows Firewall status, and antivirus health across all endpoints before auditors do.

LICENCES

Software & Licence Reports

Detect prohibited applications, track recently installed software, and analyse licence compliance and vendor entitlements across the fleet.

CERTIFICATES

Certificate Reports

Track SSL/TLS certificate expiry, detect self-signed or weak-algorithm certificates, and prevent service outages with configurable advance warnings.

HARDWARE

Hardware Inventory Reports

Categorise devices by manufacturer, OS version, type, age, disk usage, and memory to plan refresh cycles and procurement decisions.

DELIVERY

Scheduled Report Delivery

Automatically email reports to stakeholders on a daily, weekly, or monthly schedule in PDF, CSV, or XLS format without manual effort.

LOOKING AHEAD

The Future of Endpoint Management

The endpoint landscape continues to evolve rapidly. Hybrid work models, cloud-first strategies, and heightened cybersecurity standards are reshaping what organisations need from their endpoint management platforms. Key capabilities that will define the next generation include:

Zero Trust — Zero Trust security integration: managing endpoints as an explicit trust boundary rather than assuming implicit security within the corporate network, with continuous verification of device health and user identity before granting access.

Compliance — Expanded compliance framework coverage: continuous, policy-driven validation against emerging regulatory standards, with real-time compliance dashboards rather than periodic point-in-time audits.

AI Analytics — AI-driven device analytics: predictive identification of device failures, security risks, and anomalous behaviour before they become incidents, drawing on fleet-wide telemetry.

SecOps **Integrated security operations:** tighter alignment between endpoint management and broader security tooling including EDR, SIEM, and SOAR platforms for coordinated incident response.

Sustainability **Fleet-wide sustainability reporting:** as organisations face increasing pressure to demonstrate environmental responsibility, endpoint power management data will feed into carbon footprint tracking and sustainability commitments.

Zecurit is designed to support the evolving needs of modern endpoint management as organisations continue to adapt to new operational, security, and regulatory requirements.

CONCLUSION

Modern Endpoints Require a Modern Approach

Effective endpoint management is no longer optional; it is a prerequisite for operational resilience and security in modern organisations. As device diversity grows and workforces become increasingly distributed, IT teams need tools that provide real-time visibility, intelligent automation, robust security enforcement, and audit-ready compliance reporting from a single platform.

Zecurit Endpoint Manager delivers on that requirement: a unified, cloud-native platform that centralises device management, automates patch deployment, enforces BitLocker encryption, controls peripheral access, optimises power consumption, and enables remote troubleshooting at scale, without the infrastructure complexity of legacy tooling.

By replacing fragmented point tools, eliminating manual processes, and providing the compliance evidence frameworks that regulators require, Zecurit Endpoint Manager helps IT teams operate more efficiently while maintaining strong security posture. As organisations continue to adapt to distributed work environments and evolving cyber threats, a platform of this breadth plays a critical role in maintaining operational resilience.

About Zecurit

Zecurit develops cloud-based IT management solutions designed for modern IT teams. The Zecurit platform helps organisations manage endpoints, track assets, enforce security policies, and securely support distributed workforces through centralised, easy-to-use tools.

To learn more about Zecurit Endpoint Manager, start a free 14-day trial or contact the Zecurit team.