ZECURIT Endpoint Manager

PRODUCT DATASHEET

Manage, Secure, and Automate Every Endpoint from a Single Cloud Console.

Unified Endpoint Management, IT Asset Management, Patch Management, Remote Support, and Security Compliance in one cloud-native platform.

Cloud-Native SaaS Platform | **Single Lightweight Agent** | **100+ Built-In Reports** | **Windows, macOS & Linux** | **MSP Multi-Tenant Architecture** | **Enterprise Security Controls**

EXECUTIVE OVERVIEW

Today's Challenge

Modern IT teams manage an increasingly diverse fleet of devices across multiple locations, operating systems, and user types. Patch gaps expose critical vulnerabilities. Fragmented tools create dangerous operational blind spots. And the administrative cost of running separate standalone solutions for asset tracking, patching, remote support, and compliance keeps growing with every newly onboarded device. Without a unified platform, security incidents are discovered too late, audits are incredibly painful, and IT staff spend hours on mundane tasks that should take minutes.

The Zecurit Solution

Zecurit Endpoint Manager is a comprehensive cloud-based unified endpoint management and security platform that gives IT teams a single, centralized console to discover, manage, secure, and support every Windows, macOS, and Linux device across the enterprise. By seamlessly combining IT asset management, patch management, automated software deployment, device control, BitLocker encryption, configuration management, integrated remote support, and compliance reporting into one lightweight agent, Zecurit completely eliminates tool sprawl, minimizes manual effort, and ensures every endpoint remains highly secure and permanently audit-ready.

PLATFORM ARCHITECTURE OVERVIEW

ZECURIT CLOUD CONSOLE

IT Asset Mgmt	Patch & Vuln	Remote Support
Software Deploy	Device Control	BitLocker Mgmt
Config Mgmt	Automation	Compliance

Single Lightweight Agent (Windows, macOS, Linux)

STRATEGIC COMPARISON & PLATFORM METADATA

Why Replace Multiple Tools?	
Traditional Approach	ITAM + Patching + Remote Support
Zecurit Approach	Single Consolidated Platform
Agents	Single Unified Lightweight Agent instead of Multiple Agents
Consoles	Single Management Console instead of Fragmented Consoles
Security	Unified Security Controls replacing Fragmented Security Tools
Infrastructure	Cloud-Native SaaS minimizing on-prem architecture management

Platform Metadata Specs	
Deployment	Cloud-hosted SaaS Architecture
Supported OS	Windows, macOS, Linux Cross-Platform Support
Architecture	Multi-tenant, MSP-ready Engine
Agent Delivery	Single Lightweight Background Agent
Access Controls	Granular Role-Based Access Control (RBAC)

CORE PLATFORM CAPABILITIES

IT Asset Management (ITAM)

- **Asset Discovery:** Automatic agent-based discovery for domain and workgroup models with real-time asset onboarding and zero manual configuration steps.
- **Hardware Inventory:** Granular tracking of CPU, Memory, Storage, Motherboard, TPM, BIOS, Monitors, Battery, Network Adapters, and connected USB/peripheral devices with real-time asset change tracking alerts.
- **Software Inventory:** Full tracking of all installed applications across every endpoint with version-level detail, change history log, and installation timestamps.
- **Warranty & Lifecycle Management:** Centralized device warranty status and expiry tracking with vendor coverage visibility, refresh cycle planning based on age/usage, and audit-ready lifecycle history tracking from procurement to retirement.

Software Asset Management (SAM)

- **Software License Management:** Track license entitlement vs. actual active installations, detect over-licensed and under-licensed software, and generate scheduled compliance reports for audit teams.
- **Software Metering:** Monitor real application usage frequency tracking to identify unused licenses for cost reclamation, justifying renewals with empirical utilization data.
- **Prohibited Software Detection:** Gain instant detection of unauthorized or prohibited applications with automated alerts for immediate administrative review and remediation.
- **Normalization & Categorization:** Automate consolidation of duplicate or variant software records into a clean, consistent inventory for precise license reporting.

Monitoring and Real-Time Alerts

- **Security Alerts:** Instant notifications for disabled Windows Firewalls, FileVault/BitLocker decryption events, or stopped Antivirus/Antimalware core services.
- **Hardware & Software Alerts:** Component addition or removal detection (CPU, RAM, Storage, TPM, USB, Networks) and instant alerts for prohibited software installation or commercial software changes.
- **Disk Space & Infrastructure Alerts:** Percentage-based thresholds on overall and individual drive utilization acting as early-warning notifications to prevent system downtime.
- **License, Compliance & Certificate Alerts:** Tracking of expired licenses, compliance violations, and SSL/TLS certificate expiry windows, along with untrusted root CA or self-signed certificate detection.

Patch Management Automation

OS & Third-Party Patching: Streamlined management of Windows OS, drivers, and popular third-party applications (browsers, productivity tools, developer utilities) side-by-side.

- **Approval Workflows & Scheduling:** Enforce structured pilot group testing and manual/automated patch reviews prior to fleet rollout. Define exact maintenance windows to avoid disruption, featuring automated retries for failed deployments.
- **Compliance Reporting:** Real-time installation tracking with instant alerts for unpatched critical devices and customizable, scheduled report delivery directly to auditors and management.

Software Deployment & Configuration Management

- **Silent Installation:** Zero-touch background deployment with elevated privilege support and fully configurable post-install restart behaviors.
- **Pre-Install Validation & Scripting:** Check available disk space, registry keys, running services, and duplicate configurations dynamically. Execute custom PowerShell, VBScript, or batch scripts before or after installation to handle complex setups.
- **Centralized Profile Management:** Group multiple security policies into named baseline configuration profiles (Firewall, Windows Update policy deferrals, password enforcement, local user/group manipulation) and apply them uniformly.
- **Power Management & Automation:** Schedule wake/shutdown cycles with Wake-on-LAN support, control granular AC/battery power schemes, and generate comprehensive uptime logs.

Enterprise Device Control & BitLocker Management

- **Policy-Based Device Blocking:** Allow, block, or trust peripheral categories (removable storage, legacy ports, wireless/Bluetooth adapters, smart card readers) with active BadUSB keystroke injection blocking and print output prevention.
- **Offline Policy Enforcement:** Device control configuration rules stay fully active on locally disconnected endpoints without network connectivity.
- **BitLocker Encryption Enforcement:** Drive encryption configuration with granular TPM policy control (TPM+PIN, passphrase) and automated key backup to Active Directory or secure central cloud storage with rotation rules.

Remote Access, Support & Scripting Automation

- **Unattended & Ad-Hoc Access:** Full background control for after-hours updates, alongside instant on-demand sessions generated via simple email or join links with no prior end-user software installation.
- **Advanced Diagnostic Tooling:** In-session tools including Remote Task Manager, direct command prompts, event log viewer, registry access, service manager, and encrypted two-way file transfer.
- **Scripting Repository:** Multi-platform execution support for PowerShell, Bash, Python, VBScript, and batch files backed by a library of 100+ pre-built script templates for instant fleet deployment.

DESIGNED FOR HIGH-PERFORMANCE TEAMS

- **IT Operations Teams:** Consolidating fragmented management tools and drastically reducing operational overhead.
- **Managed Service Providers (MSPs):** Managing multiple isolated customer environments fluidly from a single multi-tenant console.
- **Security & Compliance Teams:** Enforcing strict patch timelines, monitoring system baseline metrics, and preparing audit trails for HIPAA, ISO 27001, PCI-DSS, or SOC 2.

Get Started with Zecurit Endpoint Manager

Eliminate endpoint tool sprawl, secure your fleet, and streamline your IT workflow today.

Start Free Trial: 14 days, no credit card required. Sign up at: zecurit.com/signup

Schedule a Live Demo: See custom use cases built for your fleet: zecurit.com/demo

Explore Platform Features: Read documentation: zecurit.com/endpoint-management/features