Endpoint management is a core component of IT operations, but growing numbers of devices and remote and hybrid work models are straining traditional processes. IT teams lack visibility into endpoints and are struggling to manage them remotely and ensure strong security. These challenges are driving rapid adoption of modern endpoint management solutions.

30% of organizations say remote work and hybrid worker experiences are critical to meeting business objectives. 3

48% of devices are no longer detected by the organization’s IT department or their operating systems are outdated, putting them at risk. 4

35% of IT and security practitioners say too little visibility of endpoint devices is a major security concern. 5

62% of devices are new managed by the average enterprise. 6

30% of organizations say remote work and virtual workspaces are critical to meeting business objectives. 3

35% compound annual growth of the unified endpoint management market is expected through 2026. 7

48% of devices are no longer detected by the organization’s IT department or their operating systems are outdated, putting them at risk. 4

41% of organizations report no significant increases in help desk tickets in the past 2 years. 8

46% of endpoint security tools are failing to detect and block escalating threats. 9

66% of IT and security practitioners say that lack of visibility into endpoint devices is the greatest barrier to a strong security posture. 10

LEGACY ENDPOINT MANAGEMENT CHALLENGES

CHANGING WORKPLACE DEMANDS
Organizations must adapt to new models in which users work anywhere, utilize multiple devices, and require access to data that resides on-premises and in the cloud.

OVERBURDENED HELP DESK
Remote work and the growing diversity of endpoint devices have increased the number of help desk tickets and the time required to resolve problems.

OVERLAPPING & REDUNDANT TOOLS
Many organizations have implemented tools to address specific endpoint management requirements, leading to unnecessary costs and complexity.

SECURITY & COMPLIANCE
Endpoint threats are escalating, creating significant risk of a successful cyberattack that could compromise sensitive business assets and data.

FACTORS DRIVING ENDPOINT MODERNIZATION

STREAMLINED IT OPERATIONS
Unified endpoint management tools facilitate remote management and enable the automation of many routine tasks.

REDUCED SUPPORT COSTS
Patches and updates are pushed out automatically whenever devices idle, and organizations can utilize modern identity services to move toward a zero trust security strategy.

ENHANCED SECURITY
Mandatory logins and biometric authentication safeguard the security of the device and the organization.

MAXIMIZATION OF EXISTING INVESTMENTS
Organizations can consolidate endpoint management tools and capture more of the value of existing enterprise software licenses.

PROSYSIS
www.prosysis.com

1. TEKsystems
2. Infiniti Research Limited
3. 135K devices are now managed by the average enterprise.
4. Ponemon Institute
5. 66%
6. 46% of endpoint security tools are failing to detect and block escalating threats.
7. 30%
8. 35%
9. 48%
10. 62%

Want to learn more?
Please contact your ProSys team to discuss how we may better support your workplace environment.

www.prosysis.com