

CUSTOMER SUCCESS STORY

How a European-based financial services organization **automated its endpoint management process across 2,000 endpoints** with **ManageEngine Endpoint Central**

About the Organization

This European-based banking and financial services organization with more than 1,000 employees. The IT team manages close to 2,000 endpoints across Windows 11 laptops and virtual desktop infrastructure instances, covering a cloud and physical device environment that operates under the GDPR and other data protection regulations.

Windows 11 laptops

Virtual desktop infrastructure

Cloud

Physical devices

GDPR

INDUSTRY

Banking, financial services and insurance

LOCATION

Europe

ORGANIZATION SIZE

Mid-size organization

COMPETITORS EVALUATED

Microsoft Intune/SCCM

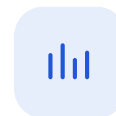
KEY BENEFITS



Licensing costs reduced through consolidation of multiple endpoint management tools into one platform



Routine administration automated across patching, reporting, software inventory, and endpoint management



Patch compliance visibility improved and vulnerability remediation accelerated on around 2,000 endpoints.



IT team able to support the full environment without increasing headcount



BitLocker management, device control, and asset inventory centralized from a single console



GDPR compliance supported through automated patch tracking, audit trails, and centralized compliance reporting



Before implementing ManageEngine Endpoint Central, the organization managed its endpoint estate through multiple endpoint management solutions to meet their endpoint management requirements. This fragmented approach created compounding problems in cost, administration, and security.

01

High operational costs from multiple tools

Running separate products to address different endpoint management tasks meant paying for multiple licensing arrangements and maintaining separate integrations. As the environment grew to include virtual desktop infrastructure alongside physical laptops, the overhead of managing disconnected tools became an increasingly visible expense.

02

Complex administration and fragmented management

With endpoint management split across tools, IT administrators had no single view of device status, patch compliance, vulnerabilities, or software inventory. Each task required working in different systems, and the lack of a unified console made administration more complex and time-consuming.

03

Limited automation and inefficient patching

Routine tasks including patching, reporting, and software inventory required significant manual effort. Patching processes were inefficient, with limited visibility into compliance status across the estate. For a financial services organization with GDPR obligations and internal audit requirements, these gaps in automation and visibility created both operational and compliance risk.

“

“High operational costs, complex administration, fragmented endpoint management, limited automation, and inefficient patching processes were the major challenges we faced before implementing ManageEngine Endpoint Central.”

Anonymous, Senior cloud endpoint management engineer



Evaluating the Market

Before selecting Endpoint Central, the team evaluated Microsoft Intune/SCCM. After comparing both options against the organization's requirements for consolidation, cost efficiency, and the breadth of endpoint management capabilities needed, Endpoint Central was chosen on seven grounds:

ALTERNATIVE EVALUATED

Microsoft Intune/SCCM

The team chose **ManageEngine Endpoint Central** on the following seven grounds:

- 1

Consolidation and simplicity
Replaced various products with one platform addressing all endpoint management functions.

2

Ease of use and deployment
The cloud endpoint management team is now empowered to manage around 2,000 endpoints without heavy overhead.

3

Cost and value
Reduced licensing costs by bringing multiple endpoint management functions under a single platform.

4

Patch management and security capabilities
Automated patching and vulnerability management across Windows 11 laptops and virtual desktop infrastructure.

5

Remote management and support
Remote desktop access to resolve endpoint issues from a central console without requiring physical presence.

6

Support and vendor trust
Confidence in ManageEngine's support and track record as a vendor.

7

Deployment flexibility
Configurable to fit the organization's environment, including virtual desktop infrastructure alongside physical laptops.

With Endpoint Central deployed across around its 2,000 endpoint estate, the organization replaced multiple tools with a single platform covering patch management, vulnerability management, BitLocker management, device control, asset inventory, compliance reporting, automation, and remote support.



1. Patch management and vulnerability management

Before Endpoint Central, patching close to 2,000 Windows 11 laptops and virtual desktop infrastructure instances involved limited automation and compliance visibility. Updates were manual, inconsistent, and left the team without a reliable picture of what was patched and what was not.

With Endpoint Central, automated patch deployment runs across the full estate on schedule, vulnerability remediation is accomplished faster, and the team monitors compliance status across every endpoint at any point. The security posture the organization needs to maintain as a financial services entity is now actively monitored rather than manually assembled.



2. BitLocker management and device control

For an organization in the banking and financial services sector operating under the GDPR, consistent encryption and access control across all endpoints are compliance requirements with zero tolerance for gaps. Earlier, enforcing BitLocker and device control policies across the network required manual configurations that were slow, prone to drift, and difficult to audit.

With Endpoint Central, the team gained a centralized console to deploy and enforce these policies uniformly across their entire managed estate. The result? No per-device manual steps. No configuration gaps. Any device that falls out of policy is flagged instantly, giving the team visibility and control to act before it becomes a compliance risk, ultimately leading to a demonstrably consistent security posture and audit-ready compliance.





3. Asset inventory and automation

One of the more immediate gains from automation for the Endpoint Central has been the time returned to the IT team. Tasks that previously required manual effort, including reporting, software inventory tracking, and routine endpoint administration, now run automatically. The team has a centralized, accurate view of all software and hardware across 2,000 endpoints at any time, without chasing data from disconnected tools. The existing team can support the full environment without additional headcount, and the time freed from repetitive administration goes toward work that requires their attention.



4. Compliance reporting and GDPR audit readiness

Preparing evidence for GDPR compliance reviews and internal audits used to mean pulling data manually from multiple tools. With Endpoint Central, patch compliance tracking is automated, audit trails are maintained continuously, and configuration visibility is available on demand from a single console. When internal compliance teams or external auditors need evidence that endpoints are patched, configured to policy, and compliant, the team can produce it in minutes rather than hours.



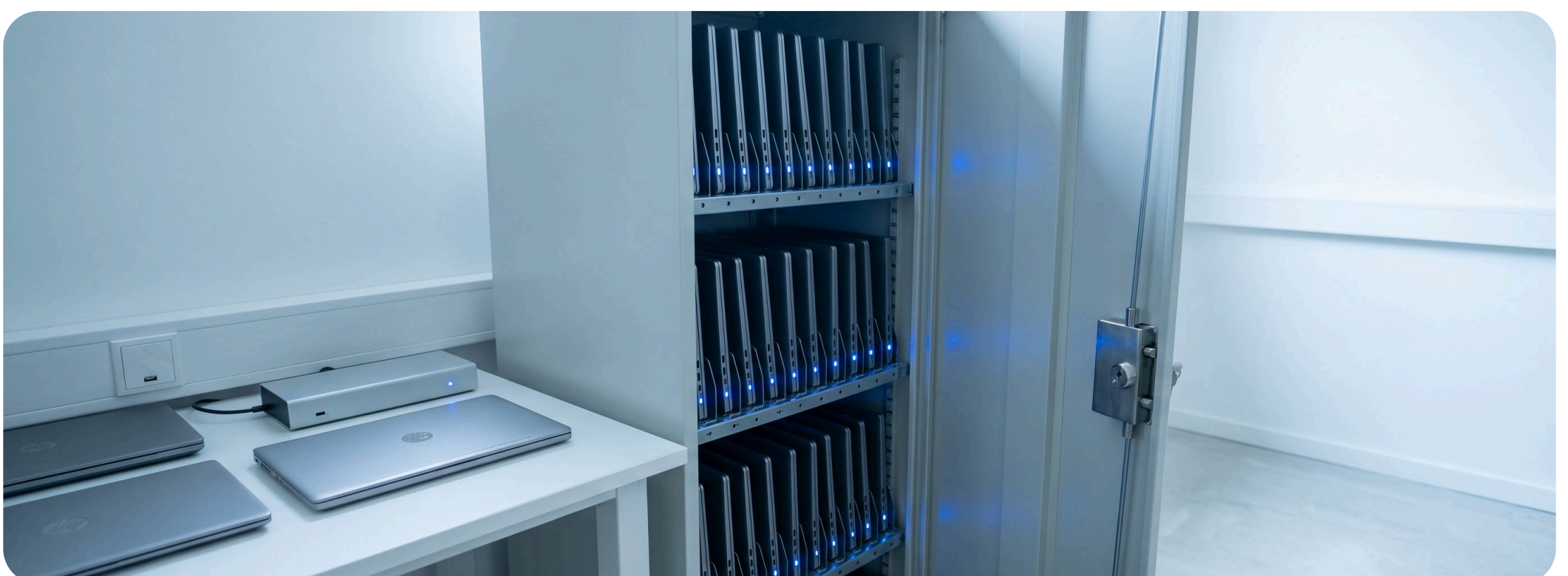
5. Remote management and support

The environment includes both physical Windows 11 laptops and virtual desktop infrastructure instances, and the IT team manages both from the same Endpoint Central console. For over 1,000-person organization, the ability to troubleshoot and remediate remotely from one platform has reduced resolution times and the effort that used to go into coordinating physical access.



“Endpoint Central automates patch compliance tracking, provides audit-ready reports, configuration visibility, and centralized reporting. This simplifies evidence collection, improves audit readiness, and supports internal compliance reviews.”

Anonymous, Senior cloud endpoint management engineer



Since deploying Endpoint Central, the organization has moved from a fragmented, multi-tool environment to a single platform covering the full scope of endpoint management:



CHALLENGES

- High operational costs from multiple separate endpoint management tools.
- Complex, fragmented administration across disconnected tools.
- Limited automation requiring significant manual effort for routine tasks.
- Inefficient patching processes with limited visibility into compliance status.
- IT team stretched by routine operational tasks, limiting capacity for strategic work.
- Compliance reporting requiring manual evidence collection for GDPR and audit requirements.

SOLUTIONS

- ✓ Licensing costs reduced through consolidation of multiple tools into a single platform.
- ✓ All endpoint management functions handled from a single, centralized console covering patching, inventory, compliance, and remote support.
- ✓ Patching, reporting, software inventory, and endpoint management tasks automated, freeing the IT team from repetitive administration.
- ✓ Patch compliance visibility improved and vulnerability remediation accelerated across all 1,800 endpoints.
- ✓ Existing team can now support the full environment without headcount increases, with more capacity available for strategic initiatives.
- ✓ Automated patch tracking, audit-ready reports, configuration visibility, and centralized reporting simplify evidence collection and support GDPR compliance.

Time savings and the ROI across every workflow

06

“

“ManageEngine Endpoint Central delivered measurable ROI by reducing licensing costs through the consolidation of multiple endpoint management functions into a single platform. The solution significantly decreased the time spent on routine administration through automation of patching, reporting, software inventory, and endpoint management tasks. The team was able to dedicate more time to strategic initiatives and service improvements rather than routine operational tasks.”

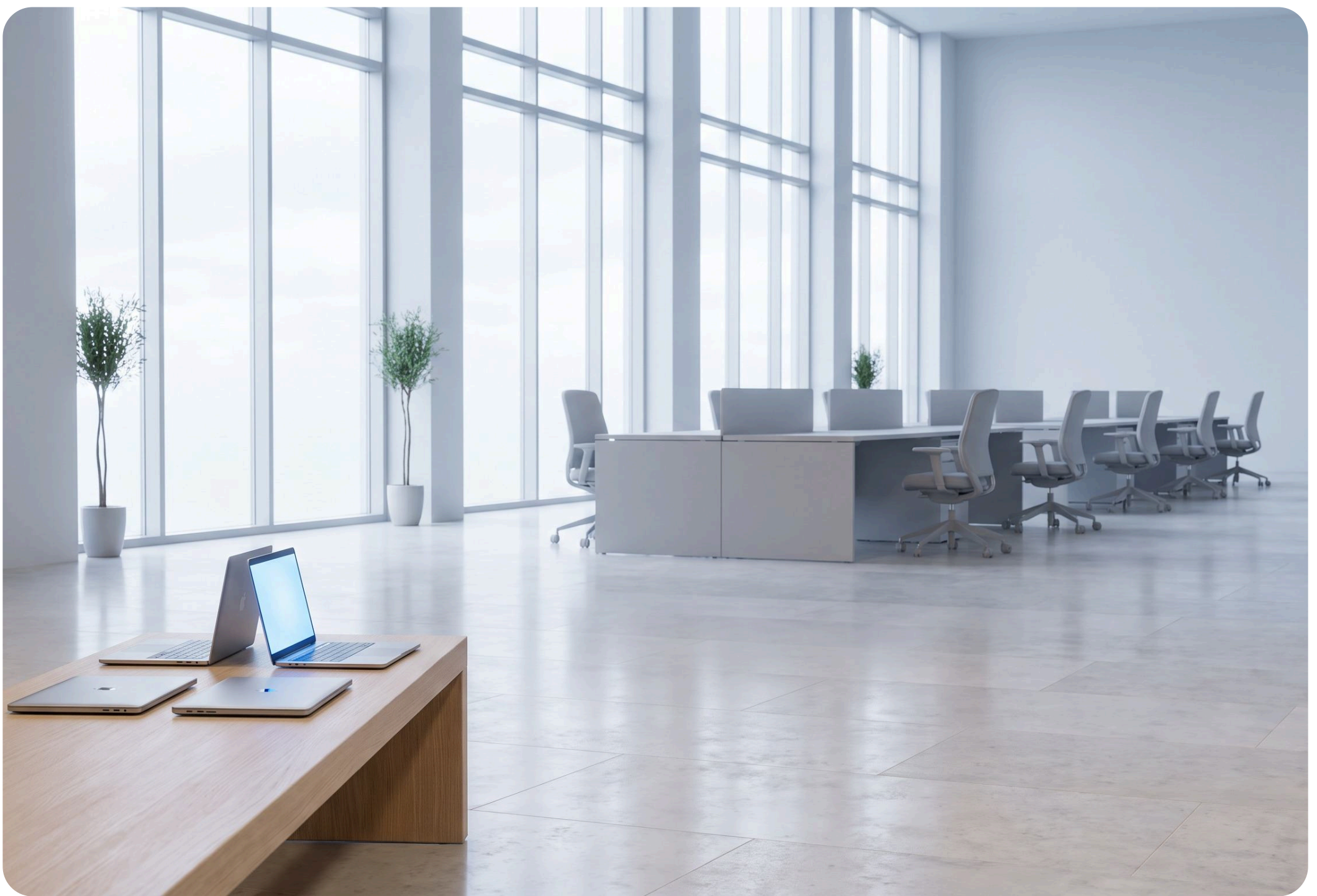
Anonymous, Senior cloud endpoint management engineer



Looking ahead

This European-based financial services organization has a solid, scalable endpoint management foundation with Endpoint Central. Patch management, vulnerability management, BitLocker management, device control, asset inventory, compliance reporting, and remote support all run from a single console across close to 2,000 Windows 11 laptops and virtual desktops.

As the organization grows and its endpoint estate evolves, Endpoint Central empowers the cloud endpoint management team to accomplish its governance and compliance standards without its previous fragmented tools and manual overhead. New endpoints are brought under management consistently, compliance evidence is available on demand, and the team retains full visibility and control from the same console.



See it on your estate.

Bring patching, encryption, device control, inventory, compliance, and remote support under one console.

[Request a demo →](#)