

CUSTOMER SUCCESS STORY

Centralized, automated, and compliant: How the Catholic Education Diocese of Bathurst manages 17,000 endpoints with ManageEngine Endpoint Central

About the Organization

The Catholic Education Diocese of Bathurst is a K-12 education organization based in Bathurst, New South Wales, Australia. In operation for over a decade, the organization now runs 36 campuses, and serves more than 12,000 students with a staff of around 2,000.

Its 27-person IT team manages approximately 17,000 endpoints across five operating systems, covering MacBooks, iMacs, Windows devices, Chromebooks, iPads, and interactive display devices for education.

- MacBooks
- iMacs
- Windows
- Chromebooks
- iPads
- Interactive displays

INDUSTRY

Education (K-12)

LOCATION

Bathurst, New South Wales, Australia

COMPETITORS EVALUATED

- Microsoft Intune / SCCM
- Ivanti Neurons

KEY BENEFITS



Automated patching across 17,000 endpoints, replacing manual, inconsistent update cycles



Self-service application portal reduces IT support tickets and routine software installation requests



Remote troubleshooting delivered across campuses and offsite locations with no physical access required



Centralized visibility for device inventory, software licenses, and compliance status



Faster device onboarding through OS imaging and automated provisioning



Single platform replaced multiple disconnected tools across a multi-OS environment



Business Challenges

02

Before implementing ManageEngine Endpoint Central, the organization faced several operational and management challenges across endpoint administration, remote support, device compliance, and software asset management. These issues were directly impacting IT efficiency, user productivity, and overall operational visibility.

01

Patching and update management

Managing operating system and third-party application patching across multiple devices and locations was a significant challenge. Devices were often not consistently updated due to users working remotely, devices being offline, or relying on manual intervention. As a result, security gaps began to emerge, and maintaining consistent compliance across the endpoint estate became increasingly difficult. Limited visibility into patch status also made it harder for the IT team to identify missing updates, generate reports, and remediate vulnerabilities on time.

02

Remote IT support

Providing remote support to staff and students across different campuses and offsite locations was difficult and often delayed issue resolution. Traditional troubleshooting methods required multiple calls, user interaction, or physical access to devices, which increased downtime and reduced productivity for both end users and the IT team. Supporting remote and hybrid users efficiently became increasingly complex without a centralized management platform.

03

BYOD and device management

Managing a mixed environment of organization-owned and BYOD devices created inconsistencies in policy enforcement, software deployment, and security controls. Ensuring devices met compliance requirements while still providing users with flexibility was difficult. Lack of centralized visibility into device inventory and configurations made troubleshooting and governance more challenging.

04

Software license tracking and asset visibility

Tracking software installations, license usage, and application compliance was largely manual and lacked accurate reporting. It was difficult to identify unused licenses, monitor unauthorized software installations, and maintain proper license compliance during audits. The absence of reliable asset visibility also impacted budgeting and software planning decisions.

These challenges collectively increased operational overhead for the IT team and reduced overall organizational productivity. More time was spent on repetitive administrative tasks, manual troubleshooting, and compliance checks instead of strategic initiatives. Delays in support, inconsistent patching, and limited visibility also increased security risks and impacted the end-user experience.

Evaluating the Market

Before selecting Endpoint Central, the IT team evaluated Microsoft Intune/SCCM and Ivanti Neurons. After comparing the options against their operational requirements, device complexity, and scale, the team chose Endpoint Central based on the following competitive advantages:

ASSESSED

Microsoft Intune / SCCM

ASSESSED

Ivanti Neurons

After comparing the alternatives, the team chose **ManageEngine Endpoint Central** based on the following decisive factors:

- 1

Ease of use and deployment
Straightforward enough for an IT team to deploy and operate across a 17,000-endpoint estate without specialist onboarding.
- 2

Cost and value
Enterprise-grade capabilities at a price point suited to an educational organization balancing its operational and IT investments.
- 3

Patch management and security capabilities
Automated patching and security coverage across five operating systems and a highly mixed device fleet.
- 4

Remote management and support
Reliable remote troubleshooting and support across multiple campuses and offsite locations.
- 5

Asset and software management
Centralized hardware and software inventory with license tracking and compliance reporting built in.
- 6

Automation and productivity
Policy-driven workflows and self-service tools to remove repetitive manual tasks from IT team workload.
- 7

Scalability and multi-site managemer
A platform capable of growing with the organization across 36 campuses and 17,000 endpoints.
- 8

Deployment flexibility
Options to deploy in a way that matched the Catholic Education Diocese of Bathurst's existing infrastructure and architecture.

The Endpoint Central Solution

After implementing Endpoint Central, the Catholic Education Diocese of Bathurst was able to centralize endpoint management, automate patching, streamline remote support, improve visibility across devices, and gain better control over software assets and compliance. The platform has become a core operational tool across seven key areas.



“Before implementing ManageEngine Endpoint Central, our organization faced several operational and management challenges across endpoint administration, remote support, device compliance, and software asset management. These issues were directly impacting IT efficiency, user productivity, and overall operational visibility.”

Aathioli Sivaprakasam, IT security manager, Catholic Education Diocese of Bathurst



1. Automated patch management

Automated deployment of operating system and third-party application patches has significantly improved its security posture and reduced manual efforts by the IT team. Scheduling, testing, and compliance reporting are now streamlined across all managed devices. Devices that were previously falling behind on updates due to remote working or manual processes are now consistently patched, closing the security gaps that had previously left the organization exposed.



2. Remote desktop and troubleshooting

The remote support functionality is crucial for assisting users across campuses and remote locations. IT staff can troubleshoot issues, transfer files, and resolve incidents quickly without requiring physical access to devices, greatly reducing downtime. Traditional troubleshooting that once required multiple calls or on-site visits now gets resolved from a central console, with far less disruption to staff and students.



3. Software deployment and application management

Centralized software deployment enables the team to push applications, updates, and configuration changes efficiently to devices. This has improved consistency across the environment and simplified application lifecycle management. It has also saved the IT team considerable time that was previously spent on manual, one-by-one software installations across a geographically spread estate.



4. Asset management and reporting

Hardware and software inventory tracking provides clear visibility into device status, installed applications, and license usage. This has improved compliance monitoring, auditing, and planning for renewals and upgrades. What was previously a largely manual and inaccurate process is now a live, centralized view of the full asset estate.



5. OS imaging and device provisioning

OS deployment and imaging capabilities help standardize device builds and accelerate onboarding of new devices. This has reduced setup time and improved consistency across staff and student endpoints. Rather than building each device from scratch, the team can apply a standard image and have a device ready for use far more quickly.



6. MDM for mobile devices

The MDM capabilities within Endpoint Central have significantly improved the way the Catholic Education Diocese of Bathurst manages, secures, and supports mobile devices across the organization. The team can now configure security settings, deploy Wi-Fi and email profiles, enforce passcode requirements, manage application access, and restrict unauthorized device features from a single platform. This has reduced manual configuration efforts and improved standardization across both organization-owned and BYOD devices.

From a security perspective, device encryption enforcement, remote lock and wipe capabilities, compliance monitoring, and application management capabilities empower the team to quickly take action when devices are lost, stolen, or non-compliant. Automated alerts and reporting make it easier to identify outdated or non-compliant devices and remediate issues before they become bigger problems.

“One of the biggest benefits has been the ability to enforce consistent device policies across both organization-owned and BYOD mobile devices. We are now able to configure security settings, deploy Wi-Fi and email profiles, enforce passcode requirements, manage application access, and restrict unauthorized device features from a single platform.”

Aathioli Sivaprakasam, IT security manager, Catholic Education Diocese of Bathurst

Results & Impact

Since deploying Endpoint Central, the Catholic Education Diocese of Bathurst's IT team has seen improvements across every area of endpoint management:

CHALLENGES BEFORE

- Devices often not consistently updated due to remote working, offline status, or reliance on manual intervention.
- Remote support delayed by the need for multiple calls, user interaction, or physical device access.
- BYOD and mixed-ownership devices creating inconsistent policy enforcement and security controls.
- Software license tracking largely manual with no reliable reporting for audits or planning.
- Manual software installation requests consuming IT team time and delaying user access.
- Device setup time and inconsistency across the estate due to no standardized imaging process.
- Multiple disconnected tools with no single compliance or audit view.

SOLUTIONS AFTER

- ✓ Automated patch management schedules, tests, and reports compliance across all managed devices, with no manual intervention required.
- ✓ Remote desktop and troubleshooting tools enable IT staff to resolve incidents, transfer files, and assist users across all campuses and offsite locations without physical access.
- ✓ MDM capabilities enforce consistent security settings, Wi-Fi and email profiles, passcode requirements, and application access across both organization-owned and BYOD devices from a single platform.
- ✓ Hardware and software inventory provides clear visibility into device status, installed applications, and license usage, improving compliance monitoring and renewal planning.
- ✓ Self-service application portal lets users install approved applications without IT assistance, reducing support tickets and routine service requests.
- ✓ OS imaging and automated provisioning standardize device builds and accelerate onboarding for staff and student endpoints.
- ✓ Single platform with centralized reporting covering patch status, device configurations, software compliance, and license usage.

Time savings and the ROI across every workflow

One of the most measurable ROI outcomes from implementing Endpoint Central has been the reduction in IT support workload through the self-service application portal. Routine software deployment tasks that previously required manual effort are now automated or user-driven. This has enabled the IT team to focus more on strategic projects, security improvements, and higher-value operational tasks instead of repetitive software installations.

Staff can access required applications immediately through the portal without waiting for IT scheduling or remote sessions. This has reduced downtime and improved overall user experience and productivity. At the same time, centralized management, automated patching, remote troubleshooting, and self-service capabilities have reduced the number of support escalations and manual administrative tasks across the environment.

By controlling which applications are available through the self-service catalogue, the Catholic Education Diocese of Bathurst has also improved software standardization while reducing unauthorized software installations and configuration inconsistencies. Because these capabilities scale across 17,000 endpoints without requiring additional IT headcount, the team is now able to support a much larger device and user base than would have been possible under the previous manual model.

“The automation and self-service capabilities have enabled the IT team to support a larger number of devices and users more efficiently without requiring additional staffing resources. ManageEngine Endpoint Central has improved operational efficiency, reduced repetitive support workload, and streamlined endpoint management processes.”

Aathioli Sivaprakasam, IT security manager, Catholic Education Diocese of Bathurst



Looking Ahead

07

The Catholic Education Diocese of Bathurst has built a strong, scalable foundation for endpoint management with Endpoint Central. With automated patching, centralized MDM, a self-service application portal, OS imaging, and real-time asset visibility all running from a single platform, the IT team has moved from reactive, manual operations to proactive, policy-driven management across 36 campuses.

As the organization continues to grow its student population, staff numbers, and device estate, Endpoint Central gives the IT team the capacity to scale without proportional increases in workload. New devices are provisioned faster, software is deployed consistently, and compliance status is visible at any point without manual data gathering.



See it on your fleet.

Bring every endpoint — across every OS and every campus — under one console.

[Request a demo →](#)