ManageEngine
Endpoint Central

Endpoint Central for Education

Improve student experience, teacher efficiency, IT productivity, and everyone’s safety.

The ultimate goal of a school IT admin is to make teaching and learning as easy and effective as possible - because technology was invented for this very reason. just as we in IT want automation toolsets, users want tools to help them do their jobs with as little effort as possible. When users come to a blocker, it’s up to IT to provide them with a means of doing what they need to do. If you don’t do this, they will find a way, and it will probably not be what we would choose.

Want to improve learning with classroom technology that’s easy to use with minimal training while increasing student engagement and ultimately their success.

Teachers

Are looking for simpler, low-cost operations that can meet regulatory needs and provide a safer environment for staff and students.

Administrators

Wants to enable education technology that is easy to administer, cost-effective, reliable and secure.

IT teams

Are looking for the technology differentiator that can enable educational excellence and promote true digital learning, while maximizing the budget.

Education leaders

IT goals	Challenge	Features
Keep an updated inventory of equipment, computers, software licenses, and others.	1. Inaccurate and outdated data 2. Scattered devices 3. Relies on manual processes 3. Relies on manual processes 5. Multi-OS types 6. Difficulty integrating inventory systems with other IT management tools.	1. Centralized control over chromeOS, Windows, macOS, Linux, Android, iPhone, iPad, tvOS 2. Consolidated data from devices, software, licenses, and certificates in a single view. 3. Real-time IT asset discovery, tracking, and reporting 4. Expiry dates, over-usage, and under-usage of software licenses 5. Soon-to-expire, expired, and unidentified warranty details of software and hardware 6. Certificate creation, distribution, and renewal Manages user accounts and device through student lifecycle management 7. Distribution server and summary server to handle a split, growing IT environment 8.Get granular, out-of-the-box reports on every activity performed
Provisioning learning devices	1. Rapid turnover, yearly student rotation 2. Unequal access to devices for students on and off campus	1. Easy device onboarding and offboarding 2. Automatic setup with zero-touch enrollment 3. Dynamic grouping based on grades/departments for policies 4. Security baseline enforcement for passwords, camera, configurations, etc. 5. Standardized OS images of both live and offline devices 6. Bulk OS deployment to remote machines using PXE, USB, and ISO 7. Vendor/hardware independent OS imaging 8. Customizable OS images for different roles/departments 9. Pre-configured device setup templates like email Wi-Fi for immediate use.

IT goals	Challenge	Features
Support remote learning	1. Personal devices accessing school network 2. Providing secure remote access to school network 3. Keeping faculty accessible to remote students	1. Separate and encrypt school data from personal data with logical containers 2. Push VPN and antivirus configurations 3. Remotely wipe or factory reset lost/stolen devices 4. Per-app VPN and HTTPS proxy for secure access to apps 5. Deliver study guides, presentations, and ebooks directly to devices with sandboxing. 6. Off-campus troubleshooting via remote access 7. Auto-install video conferencing tools 8. Broadcast announcements right on the student's screen
Providing necessary learning tools and applications	1. Manually deploying 2. Ensuring compatibility 3. Blocking unwanted application installation 4. Frequent visits to IT department for getting apps	1. Deploy software with 10,000+ predefined templates with inbuilt install/ uninstall switches 2. Store packages storage in network share repository or HTTP repository Automate, silent mobile app distribution, installation, and updates 3. Cutom software whitelisting and blacklisting policies based on roles/ curriculum. 4. Student/faculty self-service portal with admin-approved software, mobile apps, and patches 5. Temporary access to specific applications for guest lecturers, visiting parents, and external auditors
Maintain up-to-date hardware and software	1. Prioritizing patches 2. Patching without disrupting learning 3. Ensuring compatibility with legacy systems 4. Compatibility issues	1. Automate patch scanning, testing, and deployment with flexible scheduling options 2. Test patches for stability before deployment and have them auto-approved after meeting approval criteria

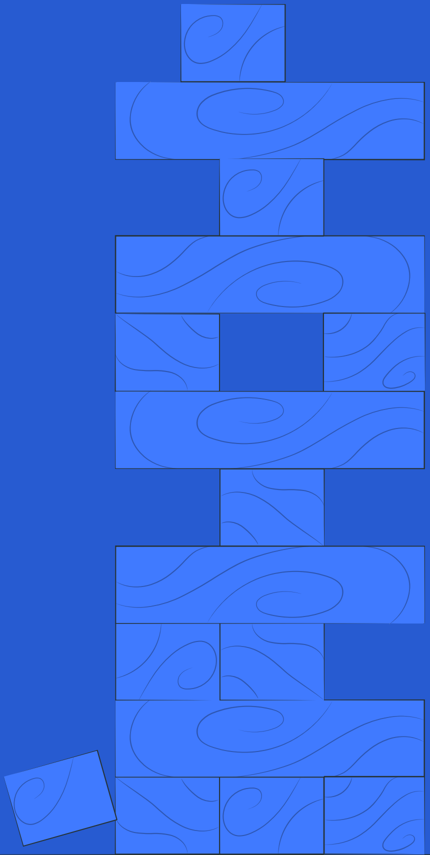
IT goals	Challenge	Features
		3. Create custom patch groups based on severity or application type 4. Get flexible deployment policies, like critical patches can be deployed during breaks, while regular updates can be scheduled for after school hours 5. Continuously checks devices against set configurations and policies, alerting for any deviations. 6. Customize deployment schedules with pre- and post-deployment checks, installation time checks 7. Perform selective patching by declining problematic or less critical patches temporarily or permanently 8. Automated patch management and app updates 9. Hardware health monitoring and alerts 10. Scheduled maintenance and update windows 11. Patch compatibility assessment, pre and post deployment checks 12. Driver management 13. Mobile apps auto-updates
Providing internet safety	1. Exposure to inappropriate content 2. Traditional restrictions are bypassed by tech-savvy students 3. Obsession with online games and illicit software 4. Cases of cyberbullying	1. Web filtering 2. Context-aware keyword filtering. 3. Websites allowlisting/blocklisting 4. Browser extension/plugins management 5. Browser isolation

IT goals	Challenge	Features
	5. Social engineering attempts 6. Inability to track student's online activity 7. Protecting students from the dark side of internet	6. Apply browser restriction and mandate the use of only trusted/approved browsers 7. Monitor usage of add-ons, extensions, and plugins in various browsers, malicious advertisements 8. Enforce a browser kiosk mode allowing only approved websites and web apps 9. Isolate unauthorized websites to create a secure sandbox to keep that activity secluded from your network
Active threat detection and remediation	1. Lack of threat intelligence 2. Lack of dedicated IT security personnel 3. Assuming you won't be attacked 4. Balancing threat detection with minimizing disruptions to learning 5. Traditional security	1. Automated threat intelligence and continuous vulnerability assessments 2. AI-assisted behavior-based malware detection 3. Deep-learning based online/offline reactive malware protection MITRE TTPs-based incident forensics 4. Quarantine malware-infected devices 5. Dedicated ransomware protection with a proven <1% false positive rate 6. Patented data backup protection 7. Single-click recovery and rollback 8. Audit and remove end-of-life software, peer-to-peer software, and insecure remote-sharing software
Protect data	1. Personal data about students, faculty, and staff 2. Sensitive information like test scores, research data and intellectual properties 3. Ensuring compliance with data protection regulations	1. Scan and locate sensitive data in your network. Text and images with PII, health charts, financial records can be detected and labeled as sensitive. 2. Categorize structured and unstructured sensitive data based on pre-defined or custom data rules 3. Dictate exactly which cloud applications can be used to upload data

IT goals	Challenge	Features
		4. Inhibit screenshots or third-party utilities such as clipboard tools to copy data 5. Allow data transfer only through company domains and Outlook clients 6. Permit only trusted USB to copy data 7. Monitor sensitive file transfers and create mirror copies when necessary Leverage BitLocker and FileVault to encrypt data 8. Store data generated from work applications in data containers on personal devices
Monitor progress and provide support	1. Providing timely support or troubleshooting 2. Enhancing endpoint experience for learning 3. Balancing support requests with other IT responsibilities	1. Real-time remote support with multiple technician collaboration 2. Resolve issues via text, calls, and video 3. Record remote sessions for supervision or audit purposes 4. Improve device speed through disk cleanup and de-fragmentation 5. Monitor spikes in hardware performance indicators, application crashes with indicators 6. Endpoint experience and student’s overall experience with scores 7. Helpdesk integration for streamlined support
Conduct examinations efficiently	1. Distraction-free assessments 2. Keeping only necessary applications and websites running based on subjects and grade levels 3. Catching cheating attempts 4. Handing technical issues during exams	1. Kiosk mode to allow only exam-related applications and device functions to run 2. Lockdown browsers to allow only necessary websites 3. Capture student screen activity during exams. 4. Remote proctoring and monitoring 5. Block access to social media and entertainment

IT goals	Challenge	Features
	5. Effectively protecting examination results	6. Real-time technical support to students during exams 7. Distribute exam materials efficiently 8. Restrict access to exam results
Optimize costs	1. Identifying cost-saving opportunities without compromising functionality 2. Maximizing the use of existing devices 3. Implementing energy-saving measures 4. Optimizing software licenses 5. Balancing between cost and features of IT solutions	1. Track software usage frequency to reduce unnecessary renewals 2. Implement power-saving measures to lower energy consumption 3. Monitor license expiration and usage to save on unwanted spending and penalties 4. Track hardware assets, age, and condition to optimize replacement cycles 5. Forecast hardware failures and schedule maintenance proactively
Ensure compliance	1. Conducting regular audits 2. Identifying and mitigating compliance risks	1. Reports 2. Compliance monitoring and reporting 3. Policy enforcement and auditing tools 4. Automated compliance assessments 5. Security audits, and incident response 6. Meet HIPAA, CIS, ISO, GDPR, PCI, and other compliance standards with Endpoint Central's dedicated features 7. Create a virtual fence based on geo-location and mark devices leaving them as non-compliant and trigger a set of actions

Purpose-built for your institution



Student

1. Protects sensitive information with encryption.

2. Web filtering for age-appropriate online exploration.

3. Enables learning on a familiar, personal device anytime, anywhere, with BYOD policies.

4. Delivers study guides, training materials and notes directly to devices.

Faculty

1. Provides readily available tools for lesson planning, assignments, grading, and communication.

2. Provides pre-configured devices for non-teaching activity like student affairs, counselling and coaching.

3. Shares bulk or targeted announcements, results, events or reminders to students.

4. Grants temporary Wi-Fi and app access for guest lecturers, visiting parents, or external auditors.

Benefits of adopting Endpoint Central

Scalability

Endpoint Central grows alongside your institution, with no need to rip and replace your system. As you add more devices and users, the system can handle the increased workload without needing extra technical resources/upgrades. You won't be stuck with a solution that becomes obsolete as your network expands.

Flexibility

We support a wide range of endpoints types and operating systems. All with one single agent, a lightweight osftware that runs in the background with barely any resouce consumption. Yet with all this automation, Endpoint Central does not lose the human factor; it allows customizing the product based on your needs.

Ease of use

Endpoint Central is widely known to be easy to deploy, configure, and use. This includes features such as intuitive user interfaces, automation, and self-service capabilities.

Cost-effective

By automating tasks and specialized cost-saving features, Endpoint Central frees up funds in the long run for your team to focus on other strategic initiatives.

Integration

You can integrate it with other solutions that you have been comfortable with REST APIs and a streamlined process.

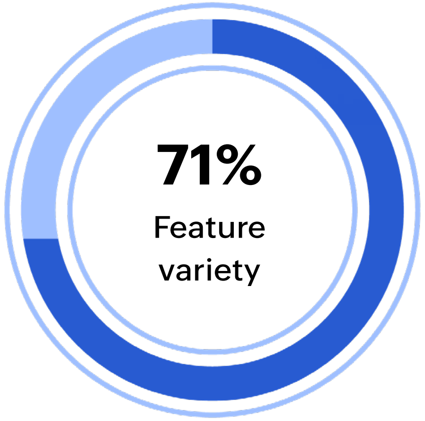
Compliance

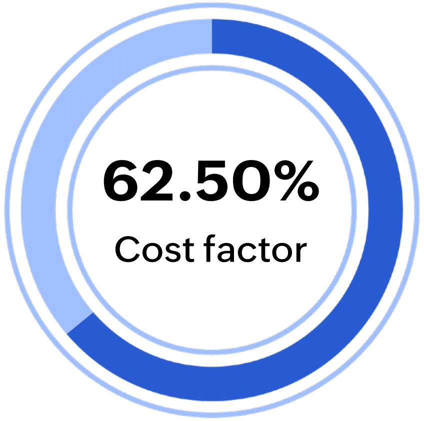
With increasing regulations around data privacy and security, we help you meet your compliance requirements like HIPAA, FERPA, GDPR, NIST and CIS with dedicated features.

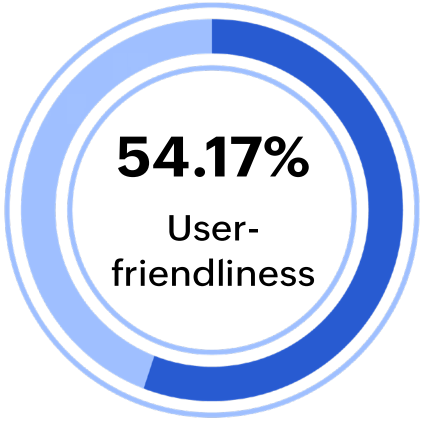
Independence

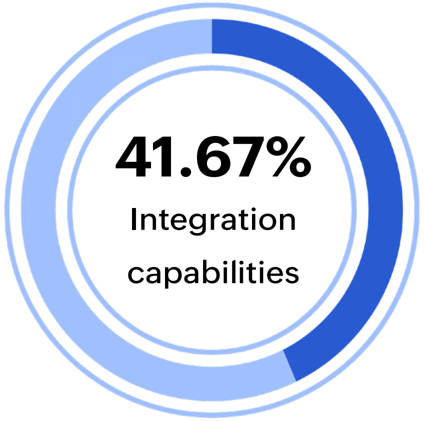
We stand against the headaches of system integration, new vulnerabilities, scrappy UI and user retraining when one company acquires another company.

Why our education customers chose us:









*In our survey of **2344** organizations

Let us help your technology and teaching go hand in hand

About Endpoint Central

Having been a key player in the market for more than 18 years, ManageEngine Endpoint Central offers IT management and security solutions for any possible requirement you'd have for keeping tabs on a company's endpoints. Endpoint Central centrally manages devices like servers, desktops, laptops, and mobile devices across multiple OSs from a single console. Crafted for SMBs and enterprises alike, Endpoint Central simplifies and automates routine IT tasks while securing your network against cyberattacks.

REQUEST A DEMO

TRY IT FOR FREE

Follow us on

Find us on Gartner

sales@manageengine.com | +1-925-924-9500