ManageEngine
Endpoint Central

Case Study

Port Townsend-based community care organization improves IT efficiency, secures PHI, and reduces clinical disruptions with Endpoint Central

About the organization

This community care organization, perched on the cliffs of the Port Townsend peninsula in Washington, serves over 29,000 residents of the county. With a 25-bed critical access hospital, 19 specialty clinics, and eight primary care clinics, the facility handles over 90,000 patient visits annually.

What keeps the pulse of this scene throbbing is a lean IT team that manages 1,100 Windows workstations, 100 servers, and 120 iOS devices from behind the scenes. This case study is about these unsung heroes and what they have achieved with our partnership, featuring insights from network systems administrator and help desk administrator.

What's inside?

IT overhaul project: The case against KACE

This community care organization takes the trust of its community seriously. Instrumental to this trust is their commitment to information security. To bolster cybersecurity and IT efficiency, a new director of IT was hired in August 2021.

Before the new IT directors' leadership, the network system administrator inherited nearly 150 unpatched Windows 7 systems when she joined the community care organization. When the new IT director came on board, he recognized the urgent need for change and rewrote most of the security policies. Bringing in Endpoint Central was a key focus of this overhaul.

The network system administrator recalls her experience with KACE before the community care organization switched to Endpoint Central:

> *"The patching using KACE just didn't work. We set it up with their support, but when the schedule came up, none of it actually patched. After three to six months, I decided I couldn't do it anymore."*

The help desk team also needed a new ticketing system, and the tight integration and license bundling of ManageEngine ServiceDesk Plus and Endpoint Central were very appealing. On why the team chose Endpoint Central, the network system administrator says:

> *"This solution featured a nice sandbox demo that I could get in and play around with. I liked that it seemed user-friendly enough for me to come in and build it out without needing full professional services."*

Reducing time and complexity in EHR client app distribution

Challenges

- Client apps interacting with Epic's EHR needing special scripts during installation
- Manually running the scripts on every machine using the Command Prompt

Solution

- With Endpoint Central, the company configured 11 post-deployment automations in sequence to customize software deployment, like changing registry keys, setting up the client to point to the server, and auto-populating desk icons.

Feature used

- Software deployment

"Software deployment was a challenge when I was using KACE. Customizing deployments for applications like Imprivata and Citrix that interact with our Epic was crucial for me if we were going to switch from KACE. But Endpoint Central enables me to run 11 post-deployment scripts in sequence to customize software deployment, like changing registry keys, and setting-up the client to point to the server. This saves me a lot of time."

—Network system administrator, Port Townsend-based community care in Washington, U.S.

For client apps that interact with Epic's EHR, the IT team had a special script that needs to be run on physician devices during installation.

The most complex use case comes for deploying Imprivata clients. Imprivata offers physicians badge-based access to workstations across the wards in a hospital.

This community care organization has a parent healthcare organization (HCO) as the EHR host, that supports its use of Epic EHR. To allow apps deployed on the physician devices to interact with Epic, the parent HCO offers Satellite along with special keys to install it. Satellite is a launcher used to manage third-party app integration with Epic. When installing Satellite on clinicians' devices, the IT team runs a script with this special key. This key tells Satellite what it's being downloaded to manage and what apps can interact with Epic, in this case Imprivata. This allows the Imprivata clients deployed on the end-users systems to interact with the parent HCO's Epic systems, so that it can pass credentials into the EMR and provide badge-based access to clinicians across workstations in the hospital.

Being able to manipulate post-deployment actions with a greater degree of control, in their case with almost 11 sequential automations, was a game changer for the IT team. The inefficient alternative was to copy the whole key from a text and paste it into an elevated Command Prompt on every individual computer utilized in the community care organization's network.

Patching playbook for the hospital staff devices and the server infrastructure

Challenges

- Managing patching across various hospital departments with both staff devices and server infrastructure
- Testing patches to ensure they don't break clinical or mission-critical systems
- Manual interventions required to stop and restart server during patching

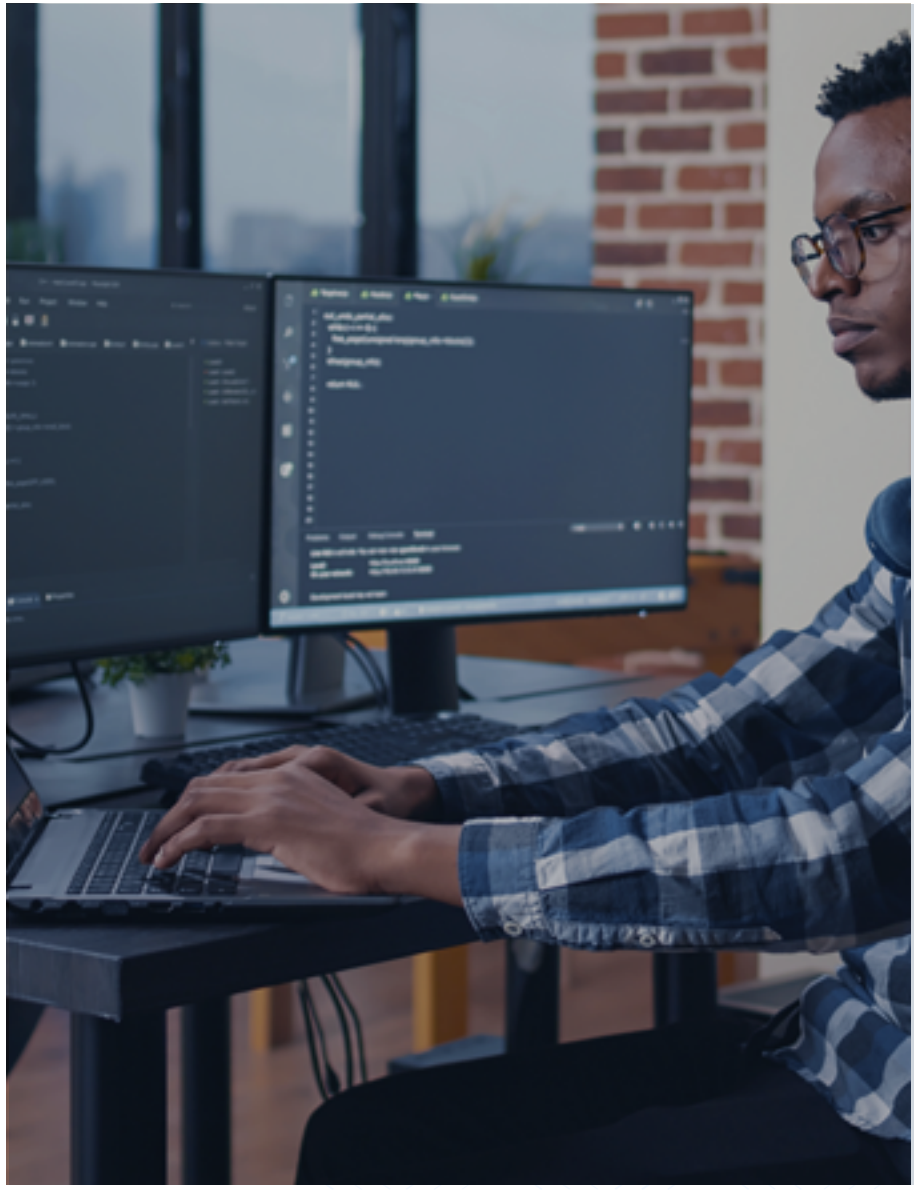
Solution

- Endpoint Central's test group feature allows patches to be tested in different environments, involving volunteers from different departments.
- The test and approve feature offers manual control to review patches before they are deployed.

Endpoint Central enables scripts to automate stopping and restarting server applications during patching, eliminating manual intervention

Feature used

- Patch management



Example patching playbook for data center servers and point-of-care devices

Week/Actions	Testing	Approval	Patch deployment	Automation	Reboot
Patch Tuesday (PT) week	**UAT** (Create test cohorts to simulate patch behaviour in different environments) **EUC** test group (Representatives from all departments- Diagnostics and imaging, clinical informatics, etc) **Servers** test group				
Week 1 after PT		Automatic patch approval For **EUC** Manual patch approval for **servers** based on change control	**EUC** is patched		Reboot initiated for EUC
Week 2 after PT			**Server patching** Multiple deployments with predictable schedules for different server cohorts based on their maintenance windows **Tuesday, morning** Data backup servers (ex: Veeam) are patched since they take backups at night **Wednesday** On-prem Exchange, utility, and Azure AD servers are patched **Friday** Research lab device are patched. Labs demand high compute resources. Downtime on specific days/times to avoid system slowdown.	Push scripts as part of the deployment process to stop apps before rebooting and restart them once the machine is up.	Reboot excluded for servers
Week 3 after PT					
Week 4 after PT			Production servers are patched in Week 4 to ensure maximum uptime, split by departments like Radiology and Data Analytics.		

The network system administrator uses the test group feature in Endpoint Central for almost all cohorts of endpoint users to simulate how patches play out in different environments before the actual patching process is initiated. She had colleagues in every department, from Clinical Informatics to Radiology, volunteer for testing. There were also test groups specifically for servers.

Patching the devices of end users is simple. Once the patches are tested, they are deployed to a large group of workstations while excluding the servers. And for healthcare-specific apps, Satellite on end-user devices reports back to the EHR server at the parent HCO about the apps that interact with the EHR and need updates. The parent HCO schedules updates, and the network system administrator's team uses Endpoint Central's remote wake-on-computer feature to ensure devices are online to receive updates.

For servers, her team has a clear patching schedule.

> ***"My main goal was to test and automate everything as well as to retain control to ensure nothing breaks. I've separated healthcare staff devices from servers using RBAC so the help desk doesn't interfere with server patching. All servers have a specific patching day each month,"***
> - the network system administrator explained.

The test and approve feature allows the network system administrator to approve patches manually, ensuring nothing goes through without her review.

> ***"I feel better manually picking what I'm approving,"*** she noted.

> ***"For certain servers, I have to manually stop applications before rebooting, which means waking up at 5:30am once a month, which was a pain. But missing this means those servers stay vulnerable for longer,"***
> - the network system administrator explained.

She needed a way to stop services automatically. Her IT team found that Endpoint Central's patching workflow allows uploading scripts as part of the predeployment process to stop applications before rebooting and restart them once the machine is back up.

Reducing help desk calls when EHR is down

Challenges

- Help desk gets barraged with calls when Epic goes down

Solution

- Pop-up announcements to keep the clinicians informed about Epic downtime

Feature used

- Announcements

Whenever Epic went down, the help desk was flooded with calls, and the help desk administrator struggled to get the message out. With Endpoint Central, the IT team had a simple pop-up announcement appear on our clinicians' computers, informing them that Epic was down. This significantly reduced help desk calls.

Empowering Clinical Informatics and Imaging teams to troubleshoot securely

Challenges

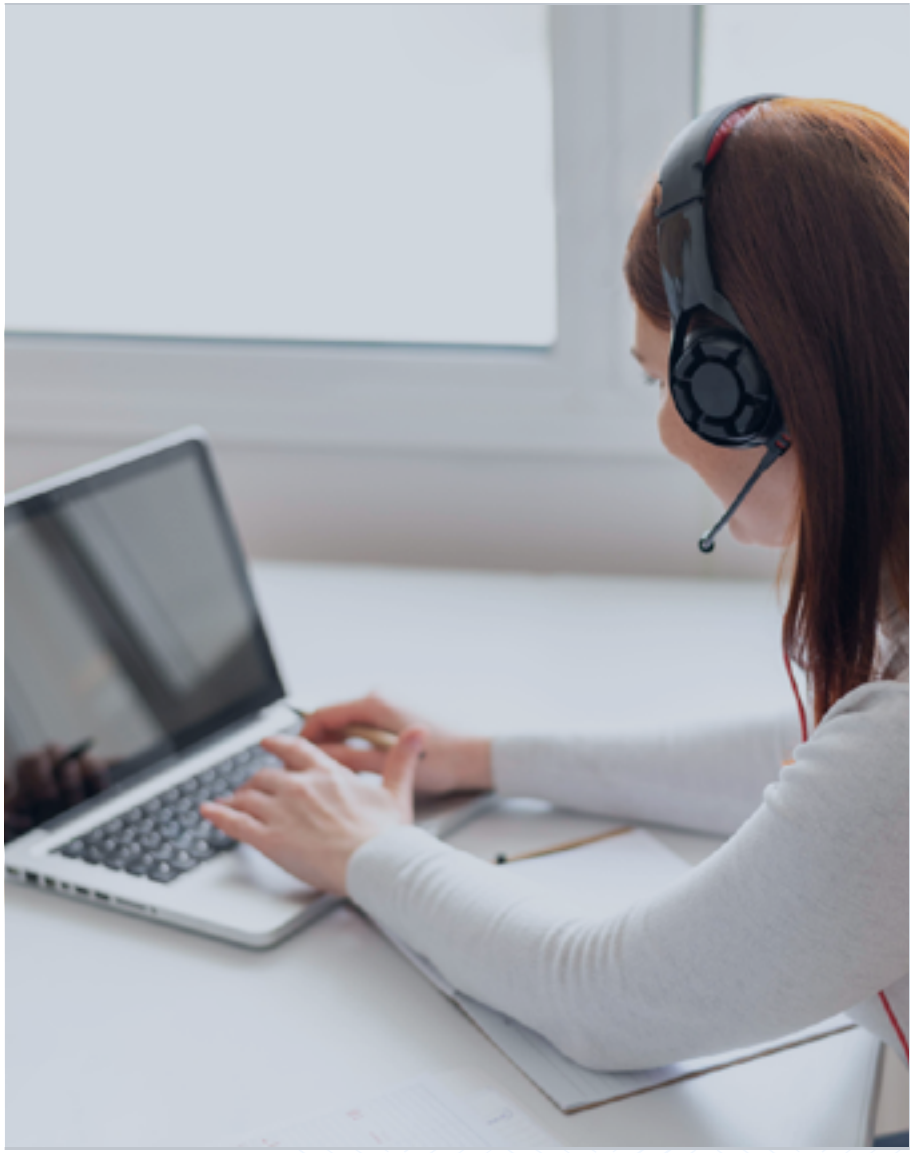
- Limited IT bandwidth to resolve issues across the entire organization
- UltraVNC used for remote control posed a significant security risk

Solution

- Endpoint Central provides HIPAA-compliant native remote control.
- Role-based access allows Clinical Informatics and PACS teams to troubleshoot their specific issues.

Feature used

- Remote Contro



The network system administrator's team set up role-based access for different teams to troubleshoot issues with their own services. Now, when physicians have trouble with electronic medical records, the IT team transfers the call to the Clinical Informatics team. The Clinical Informatics team then logs into Endpoint Central, remotes into the user's desktop, and resolves the problem.

This approach saw a ripple in other teams, particularly data and analytics, which used Remote Control to help staff with Tableau reports, and diagnostics and imaging to help users with issues related to the picture archiving and communication system (PACS) PCs.

Despite the autonomy given to other departments, IT retained visibility. Endpoint Central helped the network system administrator's team keep logs of remote access, which UltraVNC lacked.

"Earlier, we used UltraVNC for remote control, but it posed a massive security risk, especially when resolving issues related to electronic medical records. We wanted something more secure. Endpoint Central's remote control is HIPAA-compliant and integrated natively into the existing agent. We love the role-based access control, which empowers Clinical Informatics and Imaging teams to troubleshoot EMR and PACS systems without relying on IT."

—Network system administrator, Port Townsend-based community care in Washington, U.S.

Tracking locations of home care workers to meet regulations by the Department of Health

Challenges

- Local laws require location tracking on home care staff devices.
- The help desk had to pull in every Apple device and manually enable the location tracking permissions.

Solution

- IT now turns on locations on devices in mass utilizing MDM.
- IT tracks the location and also wipes the device if it's determined to be stolen

Feature used

- Mobile device management
- Geo-tracking

Before using Endpoint Central's Mobile Device Management (MDM) feature, to enable location tracking on iPhones, the help desk had to get its hands on every single phone because of how Apple locks down permissions. Now, with the help of Endpoint Central, they can turn on location tracking in bulk. With MDM, the healthcare organization can not only track the location but also remotely wipe devices that have been found to be stolen.

"Starting 2024, in the state of Washington, the Department of Health requires that there be a traceable path that proves that the nurse did actually go to the patient's house for home health visits. Having the ability to turn on locations in bulk and track them with MDM and Epic Rover strengthens our commitment to patient and staff safety."

—Help desk administrator, Port Townsend-based community care in Washington, U.S

Preventing scareware from causing clinical disruptions

Challenges

- Devices infected with scareware disrupting both IT and clinician workflows

Solution

- Locking down browsers, URLs, and extensions to prevent scareware, save time, and reduce disruptions

Feature used

- Browser security

Frequently, their employees would visit news websites and get hit by scareware. The device would then need to be reimaged by the help desk, disrupting both IT and clinician workflows.

"When our clinicians got scareware on their devices, our only option was to reimage the computer. This took the help desk staff away from their important projects and disrupted clinical operations. With Endpoint Central's browser security, we can now lock down browsers, URLs, or extensions to prevent scareware from ever getting on users' devices."

—Network system administrator, Port Townsend-based community care in Washington, U.S.

Preventing shadow IT and enabling healthcare staff with vetted software

Challenges

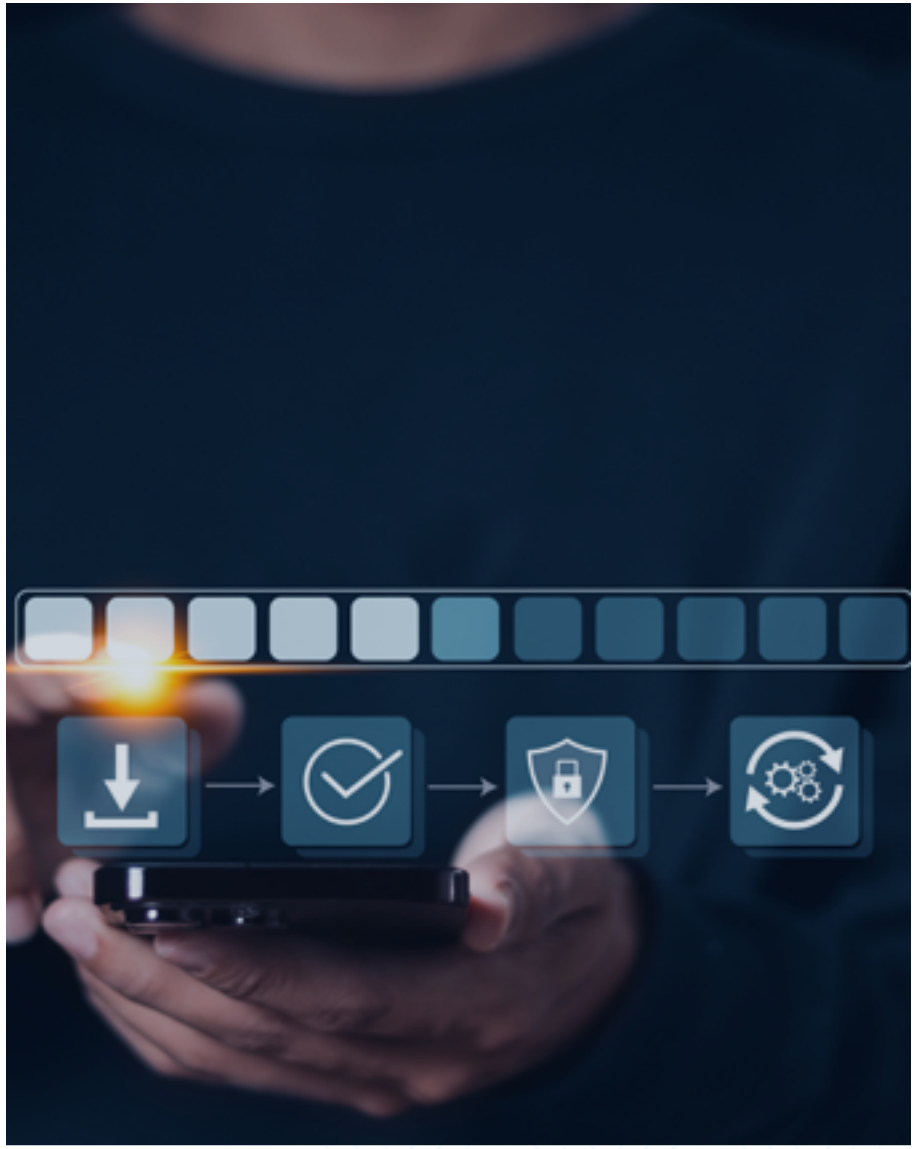
- Apps and files downloaded from the web introduce security risks

Solution

- Prevented file downloads on the web across browsers
- IT vets apps and files and shares them with employees through software deployment

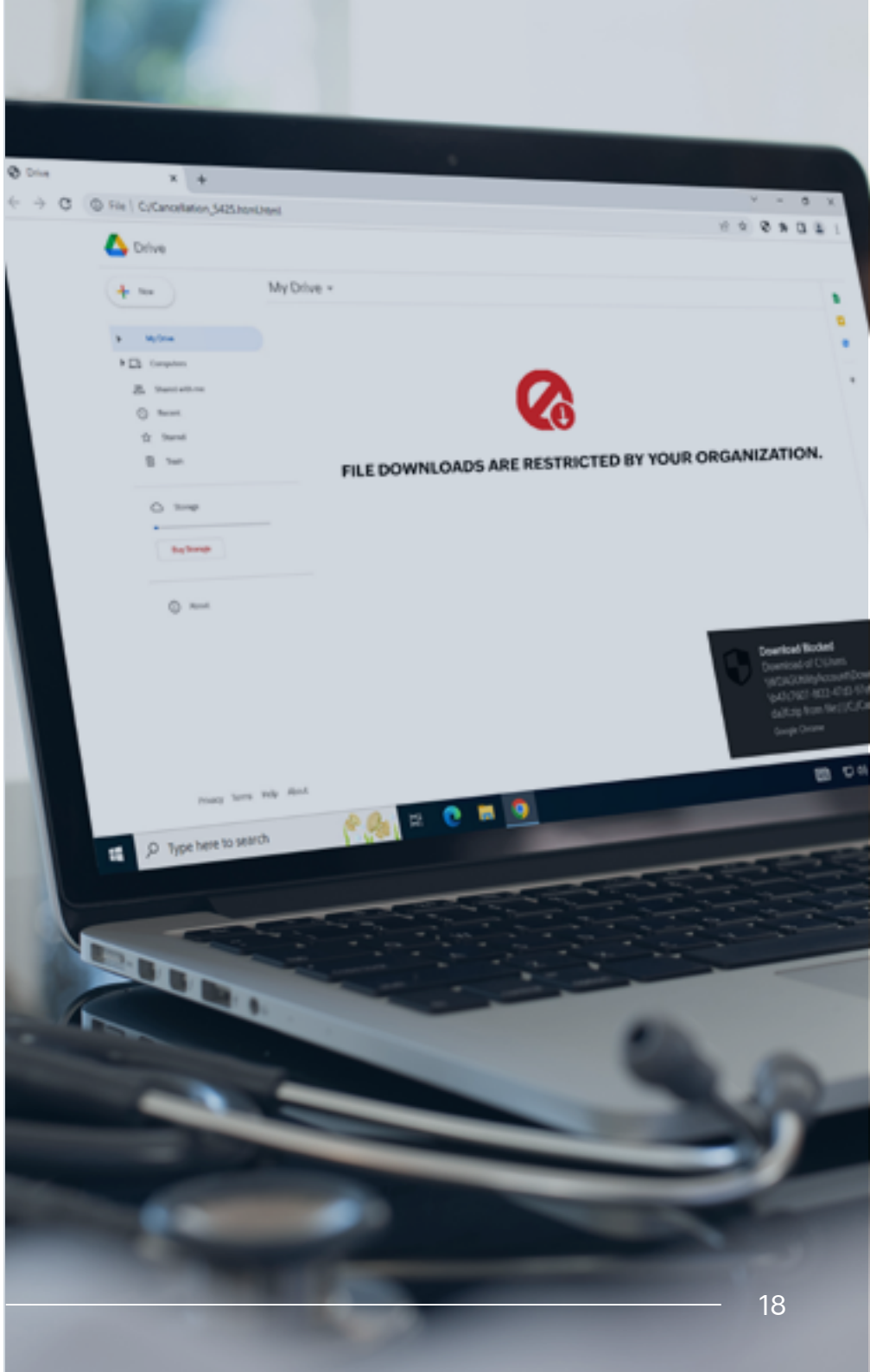
Feature used

- Browser security
- Software deployment
- Remote file sharing



Google Chrome allows user-specific installation of apps that don't require admin rights. The front desk staff and clinicians at the community care organization
like to download files quickly, and they require apps from the web to accomplish various tasks. This was something that the IT team wanted to prevent to reduce security risks.

Endpoint Central gave the network system administrator the flexibility to prevent file downloads from the web across browsers. This reduced the security risks and routed employees to IT for software requests. This way, IT can vet them and roll out apps and files to employees officially through Endpoint Central's Software Deployment module and file sharing capabilities of the Remote Control module.



Preventing patient records from leaking through personal Gmail accounts

Challenges

- Employees storing notes in personal Google Drives
- Blocking personal Gmail accounts would impact employees' bookmark storage

Solution

- Leadership buy-in: The IT director plans to create a detailed policy for approval by the chief patient health and quality officer.
- Operational alignment: The help desk will write guides for employees on how to migrate their bookmarks to their work profile.
- Technology enablement: IT will use Endpoint Central to remove personal Gmail accounts from all browsers.

Feature used

- Browser security

The community care organization's IT recently discovered a pharmacist storing notes in his personal Google Drive using Chrome. The IT team plans to block staff from signing into their personal account. Since physicians have their bookmarks saved to their personal account, blocking personal Gmail accounts would impact their workflow and naturally result in a blow back from them.

Changes that are disruptive need leadership buy-in and clear employee education. The director of IT is writing a policy to block Gmail accounts. The policy includes directives for the help desk to prepare employee education and procedures. This policy must be approved by the chief patient health and quality officer, Brandy Manuel, before implementation.

Employee education is the next crucial step. The community care organization would usually distribute a notice to the users prior to the change in policies. This is intended to advise employees to move their individual bookmarks to a work profile. The help desk also develops screenshots and how-to guides before implementations so it can avoid the flood of phone calls later.

To operationalize this requires the right alignment between people, processes, and of course, technology. That's where Endpoint Central comes into the picture. Its Browser module comes with endpoint security capabilities for comprehensive browser security, using which the company is planning to remove personal Gmail account access across all browsers used by employees.

Persona-based device and app provisioning

Challenges

- Ensuring department-specific iPads are restricted to relevant apps based on the users' roles

Solution

- Devices are put in kiosk mode using Endpoint Central's MDM to restrict iPads to department-specific usage

Feature used

- Mobile device management

Generally, any iPads shared among department users at the community care organization are put in kiosk mode. The help desk administrator has configured multiple profiles that lock the iPads to specific apps and use cases. For example, some iPads are set to access only Epic, translator services, or imaging apps, depending on the department or location.

> ***"I have a speech therapy iPad with only applications for speech therapy. I put Rover and other relevant apps on the home care workers' iPads. For imaging and diagnostics, devices are restricted to MiPACS, Nova PACS, or NOVA RADS based on job function. If an iPad is given to a director and not shared, it gets a different profile. Endpoint Central's MDM features help us distribute apps and devices and lock these devices based on the user personas,"*** the help desk administrator noted.

The road ahead: Secure BYOD for clinicians

A lot of clinicians use personal devices to access Haiku or Canto and have free rein with these apps on their personal devices that IT currently has no control over when clinicians leave. These apps restrict screenshots and do not store data on the phone, but if a healthcare provider is accessing these apps on a personal device, they could open their camera up and take pictures of patient documents, then upload them into the app.

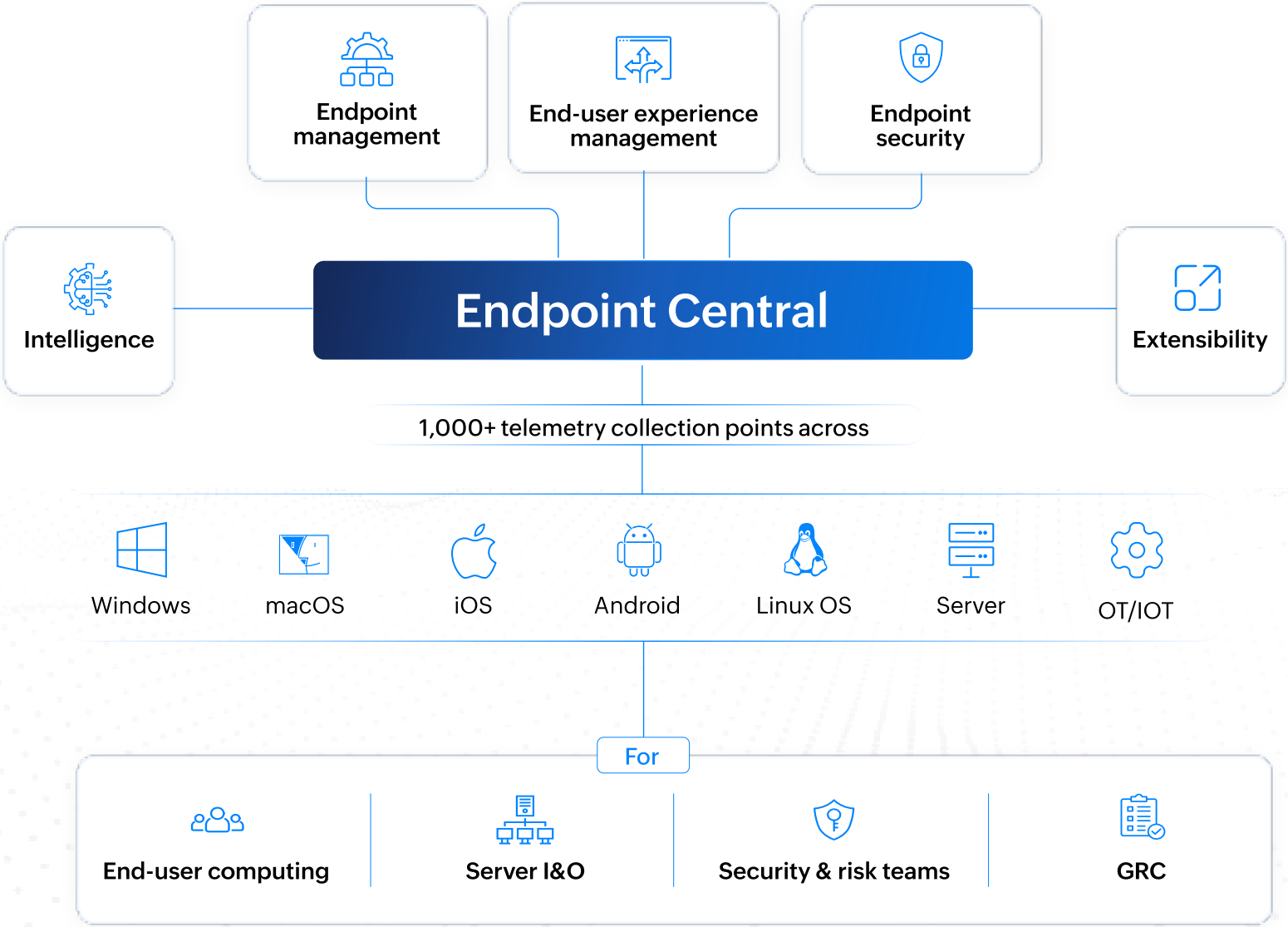
The community care organization is currently testing the platform's MDM capabilities to create BYOD containers that segment work apps from personal space.

To begin, the IT director is putting together a written policy detailing the scope of control for IT and privacy policies, requiring approval from top management before they can enforce them, because there is going to be backlash from people who don't want control over their devices.

"We do our best to train clinicians that they need to be taking the picture from within Haiku because then it's not storing anything on their device. But this doesn't prevent them from doing it. Previously, my biggest concern was not being able to wipe everything work related from their phone once they've permanently left the organization, and having that workspace container is great for that."

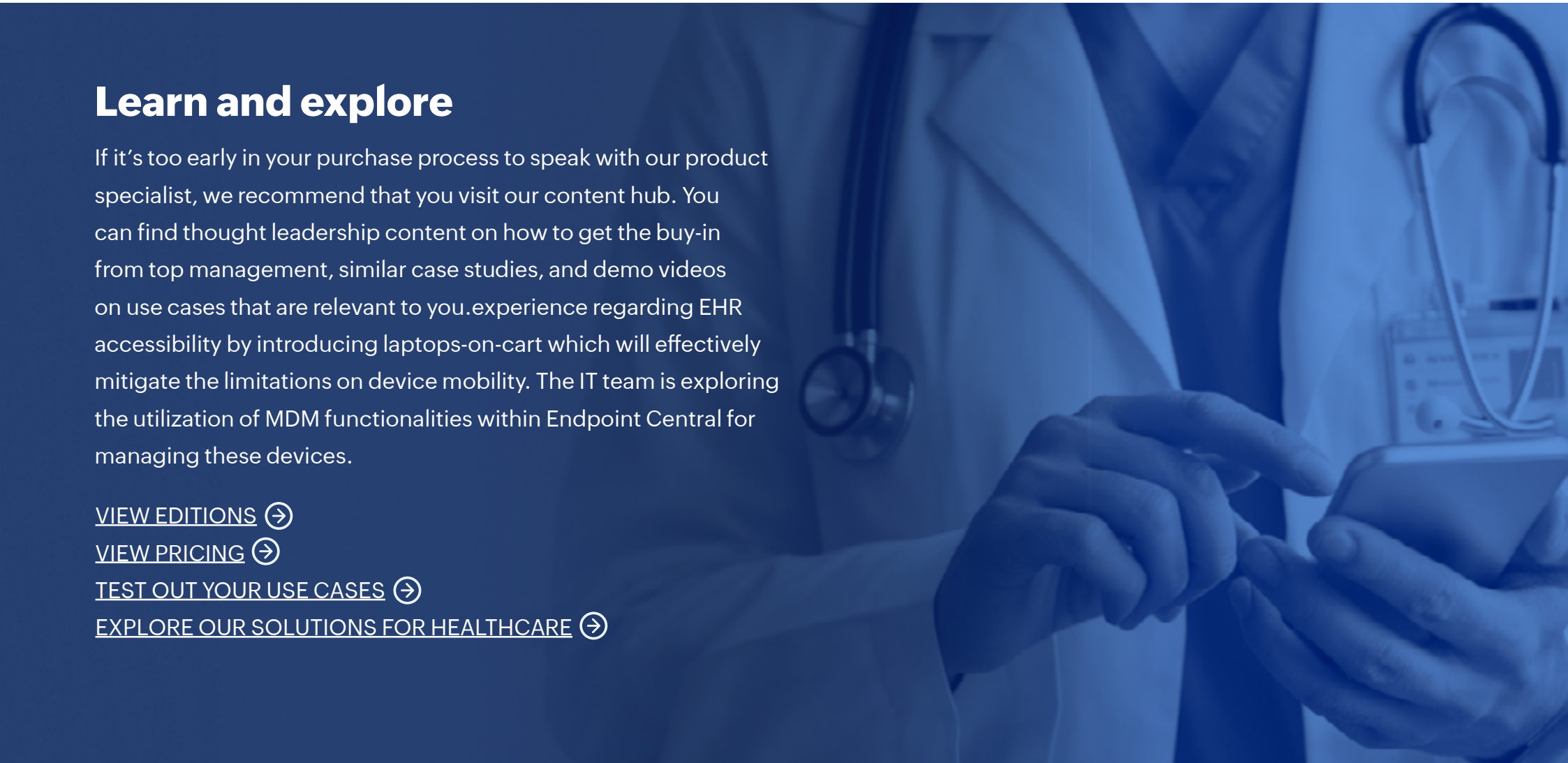
—Network system administrator, Port Townsend-based community care in Washington, U.S.

If you're a healthcare enterprise, learn what we can do for you.



If you’re a healthcare enterprise, learn what we can do for you.

Book a custom demo | Talk to sales



Learn and explore

If it’s too early in your purchase process to speak with our product specialist, we recommend that you visit our content hub. You can find thought leadership content on how to get the buy-in from top management, similar case studies, and demo videos on use cases that are relevant to you.experience regarding EHR accessibility by introducing laptops-on-cart which will effectively mitigate the limitations on device mobility. The IT team is exploring the utilization of MDM functionalities within Endpoint Central for managing these devices.

VIEW EDITIONS
VIEW PRICING
TEST OUT YOUR USE CASES
EXPLORE OUR SOLUTIONS FOR HEALTHCARE