ManageEngine
Endpoint Central

BANK ON ENDPOINT CENTRAL FOR YOUR BANKING IT

Did you know

That financial firms are **300 times** more likely than other institutions to experience **a cyberattack?**

INTRODUCTION

Banks are crucial for the world economy to run smoothly. IT has played a significant role in revolutionizing the banking industry. But it has come with its own set of challenges. A cyberattack could threaten a bank's existence and erode its brand value. Not staying abreast of the latest technologies can also result in decreased customer and employee satisfaction.

Consider ATMs, for instance. They still use four-digit PINs (although a few European and American banks use six-digit PINs) with no alphanumeric values despite the modern world developing more efficient forms of password authentication, reason?

A bad memory!

Though the inventor of the ATM planned for a six-digit PIN, his wife watered down his idea and persuaded him to go with four digits because it was difficult for her to remember numbers.

But that is not the actual reason. At the time of invention (in 1967), the inventor might have had the luxury of preferring convenience over security. But with modern biometrics and multi-factor authentication techniques, is the time still not ripe to migrate to better security practices?

Expanding this philosophy to banks and other financial institutions, the immediate question that arises is: **Are banks safe and efficient?**

Enter Endpoint Central—a comprehensive unified endpoint management and security (UEMS) suite that can supercharge your IT and secure your bank.

As passionate product makers, we at ManageEngine strive to evolve based on our customers' needs. We have analyzed the requirements of the financial sector across Asia, the Pacific, the Middle East, Europe, and North America.

Here is a list of a few must-have UEMS features that the financial sector requires:

- Effective patch management with vulnerability assessments
- Server management
- Linux support
- Real-time visibility into hardware and software assets
- Remote troubleshooting of endpoints
- Compliance with the PCI DSS, CIS Controls, and regional data protection regulations

Guess what? Endpoint Central meets almost every feature requirement of the financial sector. No wonder we are its most sought-after IT solution.

Read ahead to realize how we truly understand your IT needs and how Endpoint Central is an all-in-one solution that caters to those needs.

WINDOWS, APPLE, ANDROID, OR LINUX— ENDPOINT CENTRAL HAS GOT YOU COVERED

Banks generally have heterogeneous OSs, but with a looming economic crisis and negative business outlook, it doesn't make sense for them to invest in disparate IT tools for managing their endpoints. While most UEMS solutions cater to Windows, Apple OSs, and Android, they do not have a good Linux management capability. Secure IT is paramount for banks and financial institutions, so they prefer servers and endpoints that run on Linux.

Endpoint Central supports various flavors of Linux and has a comprehensive management capability. In addition to Linux, we also have broad management capabilities for Windows and Apple OSs. Thus, our solution could be your single pane of glass for managing various OSs and devices. It is also worth mentioning that only a few UEMS solutions have extensive server management capabilities like Endpoint Central.

RAMP UP YOUR FIRST LEVEL OF SECURITY BY PATCHING

Ransomware attacks and insider threats bewilder us with their frequency and scale. Of all the organizations that have suffered ransomware attacks, 68% didn't have an effective vulnerability and patch management process in place. Often, having a robust cyber hygiene policy can prevent these mishaps. Patching is a crucial practice as it is the first line of defense guarding your bank against cyberattacks.

However, patching is not easy. First, the IT admins need to know which endpoints need to be patched. After fetching the patches, it is imperative to test them before deployment as banks need to render their services without interruption to earn more customer satisfaction. IT admins also need visibility into the deployment status for patch compliance. If a patch causes applications or endpoints to crash, there must be a provision to roll it back to mitigate the productivity damage.

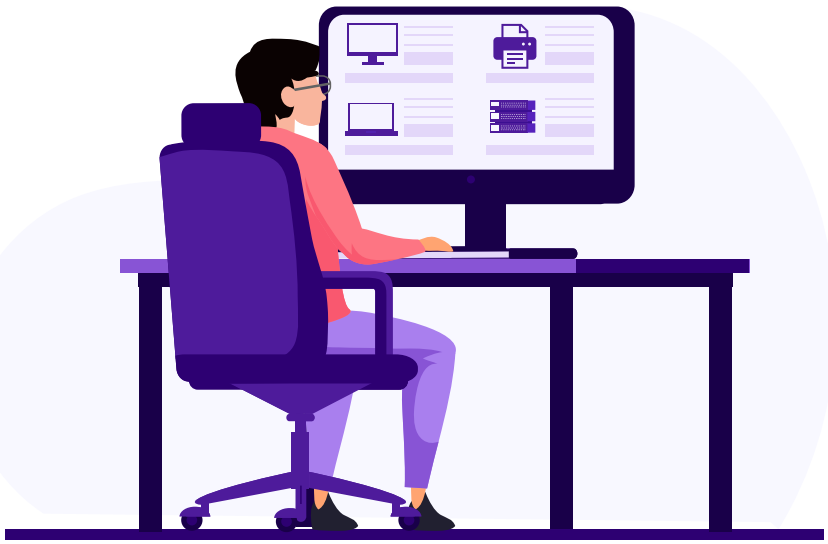
Endpoint Central is your smart IT assistant that diligently meets the above requirements and helps you patch your endpoints seamlessly with its automated, flexible deployment workflows. Our solution also reduces risks to the IT environment by constantly assessing vulnerabilities for various risk factors (like CVSS scores, exploit types, and patch availability) and prioritizing the response to highly critical vulnerabilities on the verge of exploitation.

Using the network access control feature, admins can quarantine the endpoints and applications that do not meet their tailor-made requirements, such as unpatched endpoints and old versions of applications. Most UEMS vendors forget the need to provide patching support for third-party applications. Endpoint Central supports patching for over 850 third-party applications.

ATTAIN NEVER-BEFORE-SEEN VISIBILITY

One of the biggest challenges for IT admins in a bank is asset management. Banks may have multiple regional offices and branches, and it is crucial for them to maintain visibility into their inventories. Endpoint Central has a **robust architecture** precisely to meet this need. Asset management is also necessary for auditing purposes and to understand what is happening in the IT environment, which is made up of many types of hardware, software, files, and more.

To that end, our UEMS solution's asset management capability does more than just provide visibility. IT admins can configure alerts for when users add hardware or software, remove hardware or software, add prohibited software, and more. Admins can also leverage software metering to track usage and trim costs if the software is underutilized. Our solution also generates out-of-the-box reports on the hardware and software inventory, system details, and warranties, which banks can use for auditing purposes.

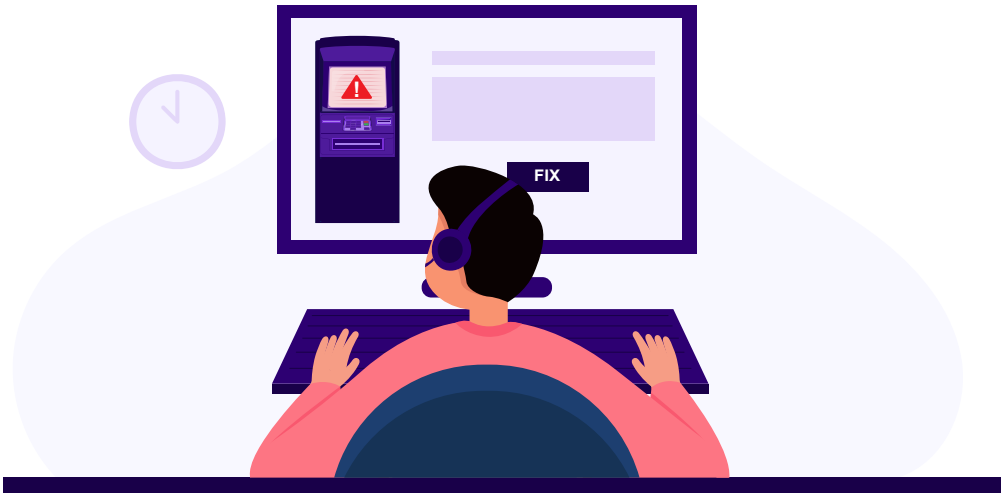


NO, WE DIDN'T FORGET YOUR ATMS, CASH DEPOSIT MACHINES, AND SELF-HELP KIOSKS

Banks aim for last-mile delivery of services and therefore provision ATMs, cash deposit machines, and passbook printing kiosks in remote areas. With over 40 configurations for Windows, Linux, and macOS, Endpoint Central can help IT admins configure a firewall and manage power for these devices so that they can be turned

off when idle, lowering power bills. In addition to patching and deploying software on these machines from their work locations, admins can schedule a program or script to run at a specific time.

IT admins can also use our modern management capabilities for managing these specialized devices. Kiosk mode helps you enable single-app or multi-app lockdown mode to ensure that only the banking apps are available to the public. You can also customize the device by restricting the hardware buttons and the network and security policies.



MAKE YOUR IT SERVICES AVAILABLE ANYTIME FOR WHEN YOUR ENDPOINTS GO HAYWIRE

Since financial services are customer-centric, banks cannot afford to have an IT breakdown. It is hard to imagine a cashier or a customer-facing attendant having a faulty device while customers are bombarding them with more requests. Here, both customer and employee satisfaction take a hit.

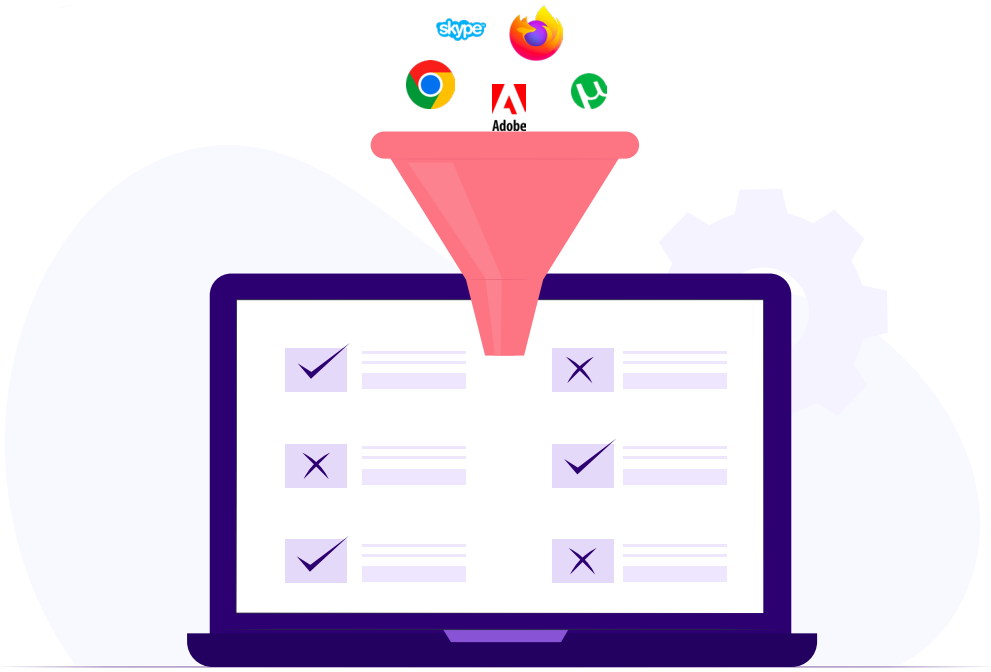
Remote screen sharing is just one aspect of our troubleshooting capabilities. Admins can transfer files and folders and access the Command Prompt, Device Manager, Registry, and Task Manager—all without screen sharing. Keeping the employees' privacy in mind, Endpoint Central empowers them by requesting user confirmation to establish remote sessions and access diagnostic tools.

Finding a technician to fix ATMs and kiosks in remote locations is cumbersome. Endpoint Central is a blessing in these scenarios because admins can troubleshoot these machines from their seats without needing to be physically present in those locations.

REDUCE THE ATTACK SURFACE AND LOCAL ADMIN PRIVILEGES

Banks have a myriad of applications, such as core banking systems, network OSs, databases, enterprise resource planning systems, and customer relationship management systems. Banks' employees usually access different systems and applications. Controlling access and ensuring the appropriate level of protection for these applications and their data is challenging.

Endpoint Central leverages the principle of least privilege, allowing IT admins to grant employees the ability to elevate their privileges for specific applications while limiting the creation of local admin accounts. Admins can also permit, restrict, or graylist applications in their banking environment. With just in time access implemented, users can access blocked applications within their organization for brief periods as needed.



HAVE CONTROL OVER HOW THE DATA FLOWS IN YOUR NETWORK

Banks deal with copious amounts of data, and there is always the risk of a data breach. Besides dragging the banks into lawsuits, these breaches erode their credibility. Banks also handle quite a lot of personal data for their customers. Thus, it is crucial to be vigilant about data protection.

Endpoint Central helps prevent data leakage via clipboards, cloud backups, USBs, and more. Our solution allows for quick identification and classification of data through techniques like fingerprinting, regular expressions, filtering by file extension, and keyword searching. In addition to these, Endpoint Central categorizes sensitive data based on factors like the source and format using a variety of predesigned and custom templates.

Our data loss prevention features also include measures to address false positives, ensuring that employees do not waste valuable time addressing nonexistent security threats.

ACHIEVE COMPLIANCE WITH REGULATIONS AND STANDARDS USING ENDPOINT CENTRAL

Endpoint Central helps banks comply with regulatory standards like the CIS Controls, the GDPR, the PCI DSS, the RBI, POPIA, the CCPA, and the AICPA's SOC 2 Type 2. You can find more about this here and here.

Conclusion

Banking institutions need their IT systems to function seamlessly like finely tuned machines to increase customer and employee satisfaction. They also need secure IT so that they can earn the trust of their customers and run their operations without any disruptions. Endpoint Central is the one-stop solution for banks, helping your IT admins run your IT efficiently and securely.

Envisioned as a client management tool nearly two decades ago, our UEMS solution now manages over 20 million endpoints and serves 25,000 customers worldwide. Excited yet? Manage and secure endless endpoints for free for 30 days.

TRY OUT NOW