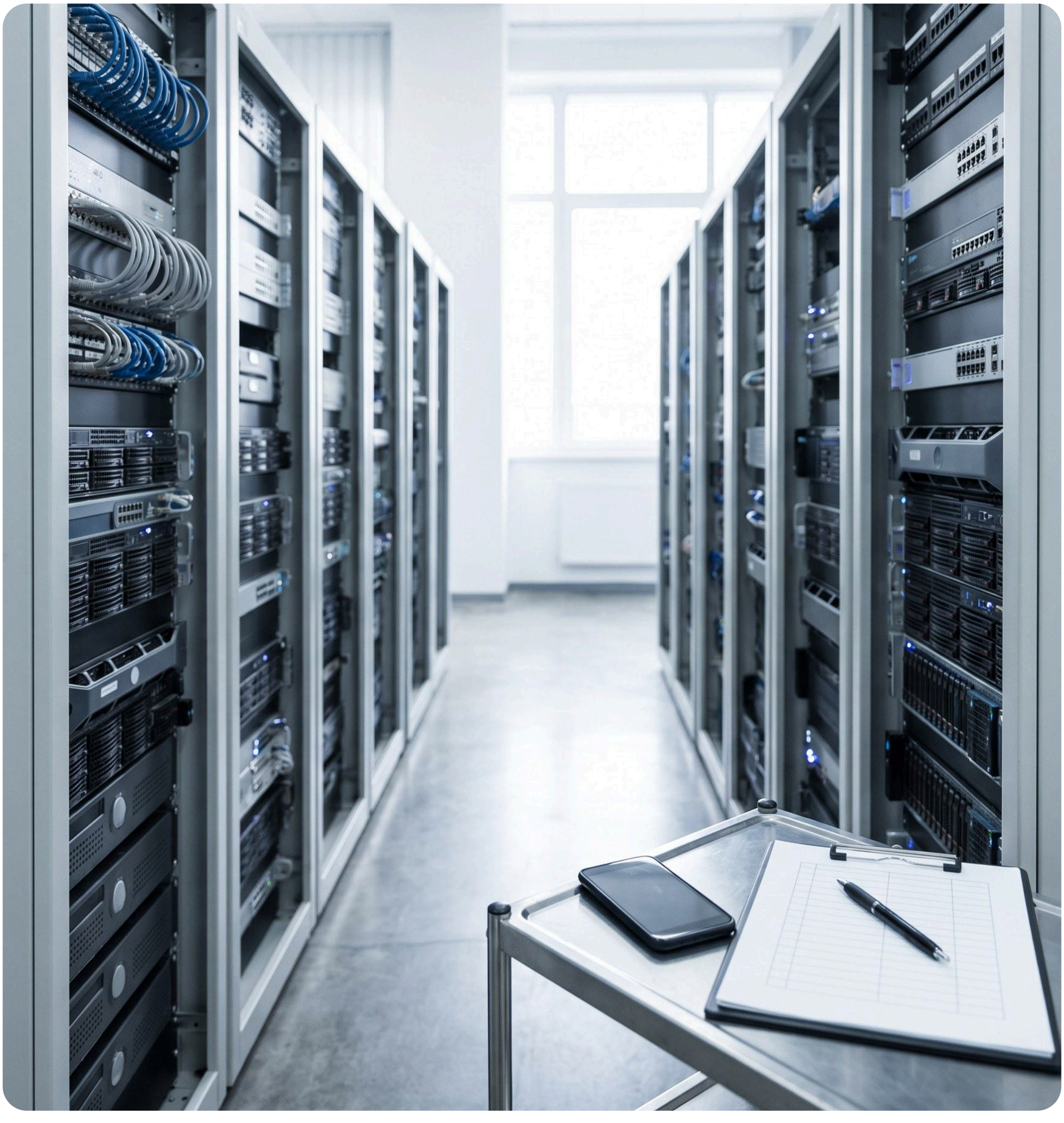
ManageEngine
Endpoint Central

BFSI endpoint estate is stranger than what EUC can see

www.manageengine.com/endpoint-central

Executive summary

Behind every core banking app and DR site sits a Unix server that no EUC team signed up to patch. In front of every branch, BYOD and company-owned mobile fleets keep relationship managers, and field agents running. At 10,000-plus endpoints, Indian BFSI IT is scrambling for visibility into both, split across 7+ fragmented tools, each run by its own team, held together by spreadsheets and SQL queries.



A brief for CIOs, CTOs and IT Directors at Indian banks, NBFCs and insurers above 10,000 endpoints.

The devices your EUC count doesn't include

Ask what an Indian bank's estate looks like and you will usually be told a number of computers. Ask what that number covers and the answer narrows. One small finance bank customer came to ManageEngine because they were "managing patches only for end user systems and not servers." Nothing in that sentence is careless. It is an accurate description of a scope that the end-user computing team was funded, and staffed for. It is also roughly half the estate an IT audit examiner will ask about.

> **Two populations sit outside the count. One is behind the branch, in the data centre and at the disaster recovery site. The other is in front of it, in a bag on a motorbike.**

The servers behind core banking and DR

A distinct endpoint population appears in the estate of 9 of our large BFSI enterprise customers - Unix or Linux distributions such as Red Hat, Ubuntu, CentOS, Rocky, SUSE, Solaris and AIX. These are not test boxes. In one public-sector bank they are described as core banking infrastructure, DR sites and legacy Unix systems in the same breath.

A global financial services came to us with an intent to bring server patch management into the same platform as branch workstations, moving off the incumbent, SCCM. But, should the server be a separate track, on a separate tool?

The same tool can serve both teams, but each team focuses on it differently. When working from an end user's perspective, an admin's priorities are the user's experience, productivity, and ease of use. When working with server infrastructure, the priorities are entirely different.

End user computing: balancing SLA and experience

For end user devices, the admin has to balance two things: SLA compliance and user experience. The goal is to meet the SLA while giving users the best possible experience.

End user notifications and self-service capability to deny or postpone patching or reboots help manage this balance. But if push comes to shove and SLA is the priority, experience takes a back seat, and patches has to be enforced.

Server infrastructure: balancing upkeep and downtime

For servers, the balance is between downtime and upkeep. Server owners only grant a limited window to run patching activity, for example once every three months for one or two hours. Within that window, the admin has to work in bursts, taking a bulk approach: how many patches can be processed quickly and correctly, so the system stays up to date, and the work can be handed off to the next team.

Maintaining a server involves multiple teams, and patching or endpoint security is just one part of that chain. Once patching is done, the DevOps team attaches the load balancer. After that, the SecOps team audits, and re-audits, to confirm the patches were applied correctly. Only after all of this is complete does the server return to the owner, who is accountable for uptime, since a net banking application, for instance, needs to stay live for customers.

Besides, server patching has to follow a strict order: for example, the application server first, then the database server, then the file server. Bringing systems back up follows the reverse order. Across a cluster, this means one server at a time, in a defined sequence of operations, not in parallel.

For servers, real-time visibility matters most: the tool needs to be reliable and give real-time updates, since the work happens under time pressure. If the tool is reliable, the team uses it directly. If not, they fall back to manual steps. If a hiccup comes up during the assigned window, the team pitches in and solves it, giving full focus to that system or set of systems for the duration of the window. It is effectively a race against time, which is why a robust, real-time tool matters.

> **Given this chain of handoffs, the priority is to keep downtime as short as possible.**

The tooling can be shared across both domains, but the operating model cannot. **End user computing management is about experience versus SLA, supported by notifications, self-service, and approval-based rollout. Server infrastructure management is about downtime versus upkeep, driven by strict sequencing, cross-team handoffs, and time-boxed maintenance windows.**

None of this is exotic infrastructure. It is the layer directly beneath the systems an examiner cares most about, core banking and DR, owned by IT infrastructure teams who currently run their own tools on their own schedule, separate from that of EUC. But the banking sector bank customers who come to us ask explicitly in a single line item: patching of RHEL, Windows and CentOS, written as one requirement rather than three.

The field fleet on BYOD and company-owned devices

Mobile devices appear to outnumber the branch workstations across Indian BFSI. Three characteristics make this device population harder to manage.

01 **It turns over constantly.**

A private bank reports roughly 500 users leaving and 500 joining each month against a base of 10,000 endpoints they manage. At that rate, the enrolment and de-provisioning workflow is not just an onboarding task. It is a monthly re-inventory of a tenth of the fleet, and every device that misses that stays attached to someone who has left the org. But regulatory bodies have a stricter policy on having a single device associated with a single user on its IT inventory.

02 **Personal and corporate hardware share the same fleet.**

BYOD and company-owned devices coexist among field worker fleets. Banks face two problems that show up as mirror images of each other. A small finance bank found that strict corporate proxy and firewall policy, applied uniformly across BYOD and corporate handsets, blocked the store the device enrolment flow depended on, and described the result as a “showstopper” on app deployment. A microfinance NBFC shows the opposite failure: with controls loosened enough to let enrolment through, field staff bypassed the web filter and BYOD users’ groups were able to install any application on a device that still had access to bank’s sensitive data. The approach we usually recommend to banks is having a standard set of network-level controls and bringing more nuanced, stronger controls onto device management so that it can accommodate diverse device deployment use cases (such as BYOD and COPD) and make policies tailor-made for different personas, departments, and device types.

03 **The hardware is chosen by procurement, not by policy.**

A small finance bank buys corporate Samsung handsets through a reseller for relationship managers and field operators. A second small finance bank runs diverse Android devices in kiosk mode for tellers and field staff, but flags a real leakage path where personal and work profiles mix on certain OEMs. When it comes to Android devices our recommended approach is to have a stricter policy to onboard only devices that are Android Enterprise recommended, which have a strong container to segment work resources on BYOD.

> **Neither device population is unmanaged by choice. But both sit outside the boundary general UEM vendors are capable of managing.**

But IT needs an answer before regulatory audits

A gap in visibility is tolerable until a date is set by someone other than IT. Most of our BFSI customers either name an audit or M&A as the event that forced action.

The regulatory event

An audit date comes from the regulator, not the bank, so it can't be pushed back the way an internal deadline might be. And crucially, a bad finding this cycle doesn't disappear, it becomes a committed fix date that has to be closed before or during the next cycle.

Consider this example from one anonymised IT Examination tracker at a banking customer above 10,000 employees when they reached out to us:

OBSERVATIONS	
01	Server patching ran through a management tool, but no tracker was maintained, and patching for Red Hat, Solaris, Oracle and CentOS servers was performed manually with no record kept
02	Of 400 servers visible in the patching tool, 102 had agent failures, with no action taken
03	Solaris, Oracle and CentOS servers had not been patched since the core banking migration
04	No patching tracker was maintained for the core banking Solaris servers, which were being patched manually
05	The patch management SOP was silent on turnaround time between UAT, DC and DR
06	Turnaround time for keeping DC and DR patch levels identical was undocumented, and undefined entirely for manual patches
07	All patch types were not tested in a dedicated UAT environment before production deployment

> **Read as a set, these are not seven findings. They are one finding stated seven ways: the servers behind core banking were being patched by hand, by a team whose work left no exportable record. The obligation to keep DC and DR configurations and patch levels identical is a specific supervisory expectation.**

The workstation fleet is usually already enrolled, already scanned and already reported on, because it is what the endpoint count was built to cover. The servers and the field fleets are the parts most likely to be partially inventoried when the date arrives, because they are the parts owned by teams who were not in the room when the count was agreed.

But the answer doesn't come from 7 fragmented endpoint tools run by five different teams

The reflex under a deadline is to buy for the gap that was just exposed. Mobile turns out to be unmanaged, so a mobile tool is procured. Linux turns out to be unreported, so a Linux patching track is stood up beside it. Remote support for branches is slow, so a remote-control product is added. Each purchase is defensible on its own. But the accumulation is not.

One diversified financial services group's prior state before Endpoint Central names six incumbents before any consolidation began: SCCM for patching, a handset vendor's own container for mobile, a full-disk-encryption product, a Linux satellite server, a separate service desk and a second MDM, with manual scripts filling the gaps between them. Across the BFSI customers, most of them mention at least one incumbent being displaced, retained alongside, or evaluated against, and the tools named recur: SCCM, Jamf, AirWatch, Intune, a handset vendor's container, Nessus, Qualys, Tenable, BeyondTrust, BigFix, SOTI. The connective tissue is named too, and it is not a product. It is spreadsheets, custom SQL queries and manual reconciliation.

Team count follows tool count. In the third private bank's records, five separate teams appear against a single 15,000-endpoint estate: a mobile device management team, an infrastructure and server operations team, an Active Directory team, the CISO office, and branch operations escalating on behalf of the business. Each owns a real problem. None owns the consolidated answer.

What makes Endpoint Central a credible alternative is that it collapses all the data that's spread across diverse tools into one shared source of truth for all IT teams across the entire endpoint estate. What this consolidation looks like for BFSI organizations who folded all their endpoint fleet under us:

- **A global financial services firm is moving server patch management off SCCM and remote control off BeyondTrust, into the one platform already managing its workstations.**
- **A diversified financial services group is retiring Intune as its MDM, replacing a handset vendor's own container, and folding threat detection into endpoint management.**
- **A small finance bank is consolidating a 17,500-device mobile fleet off its standalone MDM into the platform that already manages its desktops.**
- **The second private bank is merging standalone patch management and a separate MDM into one console specifically so that application control, device control and encryption policy can be applied from the same place.**
- **A second microfinance NBFC is uninstalling a legacy asset-management agent as its estate moves onto a single inventory.**

> **The result is: fewer tools and fewer teams standing between a question from an examiner or a board and the answer.**

One console, one answer, Endpoint Central

See beyond your branch workstations

Servers. Patch and inventory management extends across Windows, macOS and Linux, including server operating systems, with test-and-approve before production deployment, decline and rollback, and customisable reboot behaviour. Hardware and software inventory covers workstations, servers and virtual machines in one asset record.

Mobile. Corporate-owned and BYOD enrolment, work-profile containerisation following the OS vendor's own model, multi-app kiosk, geofencing, web content filtering, remote lock and lost mode, and selective wipe of corporate data separate from personal data. Application management is available for handsets that cannot take full enrolment.

The proof

442%
ROI over 3 years (Forrester TEI)

$4.5M
Quantified benefits over 3 years

$913K
Saved from patch automation

95%
Patching efforts automated

Validated by experts. Championed by users

Gartner Peer Insights™

90% of Gartner Peer Insights™ 'Voice of the Customer' Reviewers recommend Endpoint Central

Gartner

A Challenger in the 2026 Gartner Magic Quadrant for Endpoint Management Tools

IDC

Leader in the IDC MarketScape: Worldwide Unified Endpoint Management Software 2025–2026 Vendor Assessment

AV comparatives

97.4% Protection Rate, with low impact on system performance

Next steps

Bring a set-up with a server group behind core banking, and five handset models your field teams actually buy. We will run them in a single session and show how you can manage them in a single console.

Or simply sign up for a free demo:

www.manageengine.com/products/desktop-central/request-demo.html

REQUEST A FREE DEMO

ManageEngine
Endpoint Central