ManageEngine
Endpoint Central

Case Study

A decade-long partnership with a Global Manufacturer: Battling Ransomware to securing production lines

ABOUT THE CUSTOMER

As we prepare for the post-pandemic world, how we navigate the planet remains a key interest among businesses and consumers alike. Integral to this mobility is modern automobiles. From wiring harness to vision system - behind every part that makes automobile possible - sits this world's leading automotive components manufacturer. We have accommodated their request to anonymize all names and places for this case study.

 Manufacturing Industry

 Managed endpoints - 25,000

 Based out of India

From **1** Location

Endpoint Central helps them oversee

Over **25K** Endpoint

Across **350** Facilities

In **41** Countries

To manage, help and secure

End-user computing enviroments

Server infrastructure on the production lines

WHAT DID WE HELP THEM ACHIEVE?

01

Optimized software spend on expensive software used for their product and concept designs by observing usage patterns.

02

Reduced risk across EUC and production servers without impacting production timeliness

03

Visibility into user logon schedules across time zones and extensive power management to meet ESG goals.

04

In 2012, the manufacturer deployed Endpoint Central, unify endpoint data across decentralized AD environments and workgroups, across divisions and time zones.

05

In 2016, during the global Wannacry outbreak, they patched their entire fleet, including servers, in just 36 hours.

06

Safeguarded confidential designs and production documents on executive and remote worker laptops.

07

Replaced point solution with unified platfrom, reducing management overhead and Total Cost of Ownership.

08

Platform's extensibility allowed them to extend capabilities at their own pace, and offers intergration potential with their tech stack to maximize value from existing investments (Edited)

What's inside?

IT ALL STARTED WITH VISIBILITY

For the case study, we interviewed the **practice lead - ITAM and security** of this automotive manufacturing company. They came to us 10 years ago looking to solve their asset management challenges. The customer was expanding across the globe to support customers by setting up greenfield plants wherever they needed them. This was borne out of various acquisitions and joint ventures. These divisions operated independently and so did their IT. However, as the company expanded, this decentralized approach proved increasingly inefficient. To tackle this, the company established the technology and industrial solutions division to provide centralized IT support each division.

The ITAM and security lead's team deployed ManageEngine Endpoint Central as a part of this transformation. Endpoint Central continually aggregated asset data from decentralized AD environments and workgroups, providing real-time updates whenever a site admin adds or removes a device. Today, the ITAM and security lead and their team oversee over a **25,000 endpoints across 350 facilities**—including servers on their manufacturing plants, end-user compute (EUC), and work-from-home environments.

"Today, as we speak, five new laptops have been added to a site's workgroup. Seeing and documenting what's changing across our dynamic endpoint fleet is paramount from the governance, risk and compliance perspective."

This newfound visibility translated into tangible value. This manufacturing organization relies heavily on expensive software for their concept and product designs. Leveraging ManageEngine's platform, they implemented effective license position (ELP) programs to optimize their software expenditure. This involved real-time analysis of design software usage patterns among their employees to identify license shortfalls or overages. They also efficiently managed unused licenses and proactively tracked contract renewals. Endpoint Central enabled this manufacturing organization to maintain a real-time inventory of both hardware and software, complete with installation history for audit purposes. Additionally, their commitment to compliance was reinforced through security audits like the ISO audit, which required them to represent all their processes. With role-based access control, auditors were granted view-only access to data collected from their assets, including insights into endpoint exposure and security posture. This coincided with their adoption of the platform's mobile device management (MDM) capability. Centralizing endpoint information, including mobile devices, servers, and desktops, in one place significantly boosted auditor confidence, particularly for audits conducted in Europe and the US.

"The level of awareness and responsiveness we have with Endpoint Central, help our team stay confident of upcoming audits and maximize the value of our technology investments."

THE 36-HOUR WAR ROOM

2016 was a pivotal period in our partnership with this manufacturing organization. This was also the time when WannaCry had the IT world in fear. It was early in the morning when the ITAM and security lead received a call from their CIO, which would forever change their approach to patching. Their entire IT team huddled in a war room, drafting an action plan to mitigate the threat to their environment. The ITAM and security lead proposed that since Endpoint Central's client was running on all endpoints, they could use the existing infrastructure to patch their network. The team initiated a trial on a few machines, which went smoothly.

What followed was an intense 36-hour marathon for this manufacturing organization's IT team. They huddled in a war room, using Endpoint Central to patch their remote sites spread across the globe.

> "We didn't leave the room for 36 hours. When we finally saw a complete green chart on the patch compliance widget by the end of two days, we had a moment of respite. That was the first time we patched our entire fleet using Endpoint Central, including servers. It was a monumental achievement considering the scale and complexity of our operations."

The team's strategic thinking, coupled with Endpoint Central's scalability, not only combated a global threat but also turned the crisis into an opportunity for growth. The success with Endpoint Central inspired the IT team to create a dedicated unit for expanding its use in patching EUC and server infrastructure across their production lines.

SECURING THE PRODUCTION SERVERS: A BALANCING ACT BETWEEN SECURITY AND AVAILABILITY

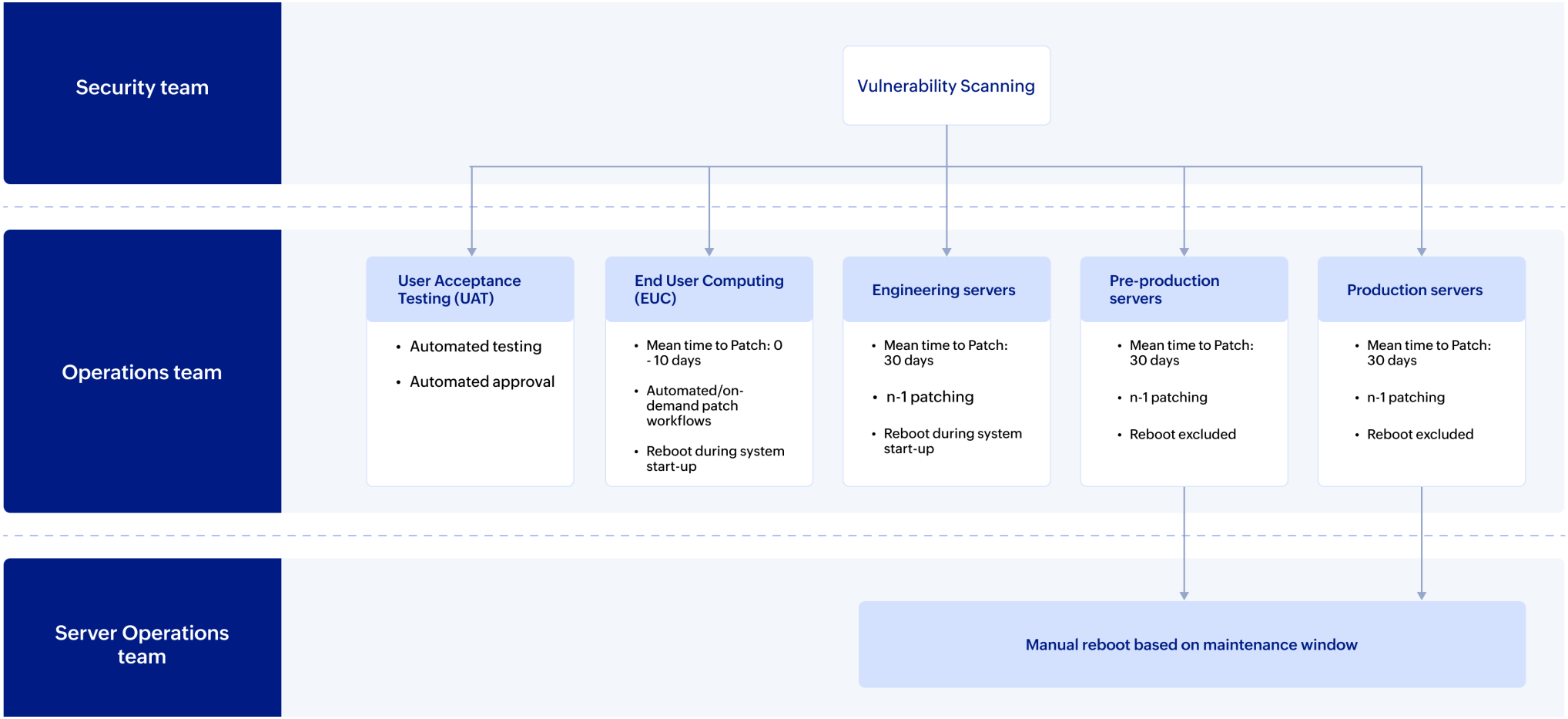
In their manufacturing plants, production machines are the backbone of their operations. These machines are controlled by servers, which store confidential designs for new vehicles expected to be launched by OEMs, production planning documents, and other intellectual property. Their experience in 2016 drove home the importance of fixing vulnerabilities on these servers to prevent ransomware attacks.

On the other hand, the availability of servers remained a deterrent to their security operations. The software and databases on these servers play a crucial role in feeding designs and workloads to the production machines, and monitoring their operations. Patching these servers was a challenge because they couldn't reboot them easily. If a server goes down, production comes to a halt. For this manufacturing organization, that was unacceptable considering their strict manufacturing timelines.

> "To put things in perspective, if we're to deliver a product within a week and experience a downtime of just a couple of hours, it affects our production costs and timelines. Getting production machines up and running again takes time. So, the challenge is that they couldn't reboot servers in our production environment based on our convenience."

The organization adopted NIST 800:40 as its playbook for their enterprise-wide patching, but to it required the right tools, strategy, and stakeholder communication across different environments.

HERE'S AN OUTLINE OF THE ADOPTED PATCH MANAGEMENT STRATEGY



Patching the EUC environment was a no brainer. They could handle emergency OS updates on demand within 2-5 days SLA worldwide, and standard patching cycles in just 10 days, thanks to our Endpoint Central's automation.

They adopted a ring-based rollout approach to test patches on a smaller scale, followed by automated approvals and phased roll-outs across EUC. All user devices were rebooted within a couple of days.

When it comes to servers, it's a whole new ball game. Having centralized, high-fidelity data from 25,000 endpoints, proved to be the foundation for planning their patching strategy. The asset information from Endpoint Central was regularly ingested into their in-house CMDB. This information was enriched through collaboration with site admins across all their production plants. With their help they added tags to every server extensively—indicating whether it belonged to engineering, preproduction, or production environments. For production servers, they needed information about server operators, running applications or databases, and noted down their owners. This CMDB information proved invaluable for planning preventive maintenance, including patching, and helped them understand who to collaborate with to take down maintenance windows.

Their standard practice was to maintain a N-1 software version for production and preproduction servers, with N-1 representing a software version that's a month old. With our platform, which can retain up to the last three months of superseded patches. They monitor the behaviour of the latest patches on the EUC for 30 days before they roll them out safely to production servers.

Endpoint Central's deployment policy configurations allowed them to identify servers autonomously and exclude reboots specifically for them. Server operators then manually performed the reboots during their scheduled downtime.

> "A good security programme requires striking a balance—that is, setting an acceptable level of risk to pursue business objectives."

The security team runs a monthly routine audit with Tenable to verify that the systems are no longer vulnerable, and consults with ITOps on the results. In an effort to leverage their existing investments and streamline vulnerability response, the IT team is exploring Endpoint Central's integration with Tenable.

While Endpoint Central's security edition includes a proprietary vulnerability management module, our platform's interoperability empower customers like this manufacturing organization to extract maximum value from their current investments, ultimately reducing their total cost of ownership.

While Endpoint Central's security edition includes a proprietary vulnerability management module, our platform's interoperability empower customers like this manufacturing organization to extract maximum value from their current investments, ultimately reducing their total cost of ownership.

NAVIGATING THE PANDEMIC : SUSTAINABILITY, SECURITY, AND BEYOND

During the pandemic, the organization's designers and engineers faced the challenge of remote work. They left their desktops at the manufacturing facilities and other sites, making it necessary to connect to these office-based desktops from their personal laptops. To facilitate this, they adopted ManageEngine PAM 360, an affordable solution that offered secure remote connectivity.

However, there was also a need to address energy conservation at the manufacturing sites during periods of inactivity to align with their ESG goals. To tackle this, the IT team effectively used Endpoint Central to gather user logon reports from all 350 locations. This data was crucial for planning power management schedules. Leveraging the remote control capabilities of the platform, they efficiently hibernated inactive desktops and initiated bulk computer boot-ups, synchronized with each time zone's logon and work schedules. This contribution strengthened the organization's commitment to becoming a globally preferred sustainable solutions provider.

Before the pandemic, the organization stored most of its sensitive data on production servers and central storage systems, which were air-gapped from the internet. Only a minority of executives ventured beyond the corporate network to meet with clients. As the pandemic threw majority of the employees to remote workstyles, directly exposed to the internet, their attack surface expanded largely. It became challenging for them to connect to network-attached storage always, leading to the local storage of confidential vehicle designs and production planning documents on their devices.To address this, Endpoint Central played a crucial role by enabling BitLocker encryption to protect sensitive data on their devices across diverse locations. Even when employees were on holidays or offline for extended periods, our platform securely backed up BitLocker recovery keys for over a year, simplifying the decryption process.

THE ROAD AHEAD

In ManageEngine's 20+ years in the industry, this manufacturing organization's journey with us has been a substantial part of our existence. When they initially partnered with us, they quickly recognized that we were in it for the long haul. With a fully homegrown approach, we've developed all our capabilities on a single platform, without resorting to acquisitions. This unique approach allowed them to adopt capabilities at their own pace and mature their processes as they expanded.

Through our partnership, they successfully consolidated their siloed tools and processes. They replacing multiple tools, such as WSUS for patching, OS deployment, mobile device management, and remote control (where TeamViewer was utilized). This move substantially reduced management overhead and their overall total cost of ownership.

With the increasing threat of ransomware and data breaches, which account for over 70% of cyberattacks today, the organization found reassurance in our next-gen antivirus capabilities. In our ManageEngine user conference, held in Delhi, 2023, they saw a demo of our ransomware detection and advanced data loss prevention features, all integrated into the Endpoint Central platform.

Looking ahead, they are considering further evaluation of these capabilities, highlighting their trust in us as a long-term partner capable of addressing their needs today and for the days to come.

Talk to us

Together, let's build a brave new world, where our people can work safely from anywhere, on any device, with a rich experience across all their workplace services.

REQUEST A DEMO