



ManageEngine
Patch Manager Plus

CUSTOMER SUCCESS STORY

How Aequs Limited keeps **its servers and endpoints patched and audit-ready** with **ManageEngine Patch Manager Plus**

About the organization

Aequs Limited is an aviation and aerospace component manufacturing organization based in India. Its IT team looks after about 1,800 Windows servers and endpoints, spread across several locations. In an industry where systems support day-to-day operations and security is closely watched, keeping those machines up-to-date is a constant job.

INDUSTRY

Aviation and aerospace

LOCATION

India

ORGANIZATION SIZE

Medium-size organization

ENDPOINTS MANAGED

1,800

COMPETITORS EVALUATED

SolarWinds Patch Manager

Microsoft WSUS

KEY BENEFITS



Reduced compatibility issues after patch updates with patch testing and approval workflows.



Faster patching of critical and zero-day vulnerabilities, reducing the impact on user's productivity.



One console for patch status and SLA-based reports, helps achieve compliance.



Business challenges

Before ManageEngine Patch Manager Plus, patching at Aequs was a time-consuming process. IT administrators had to find out what each machine was missing, decide what to deploy, and push it out with very little automation to lean on.

	No clear view of patch status	It was hard to see where every server and endpoint stood at any given moment. Without one place to check, the team could not say with confidence which machines were missing which patches. Getting critical security patches deployed on time was a regular struggle.
	Remote locations and patchy connectivity	Aequs operates from different locations, and network connectivity was not the same everywhere. That made remote patching difficult. Some systems stayed unpatched for longer than the team was comfortable with, which raised security risk and made patch compliance uneven from one site to another.
	Audit reports built by hand	Every audit meant pulling patch status together manually. It took extra effort and a fair amount of coordination between people, and it took time away from other work. With ISO 27001 requirements and internal IT security policies to meet, the team needed that evidence to be easy to produce.



Evaluating the market

Before choosing Patch Manager Plus, the team looked at SolarWinds Patch Manager and Microsoft WSUS. They compared all three against what the environment needed: automated deployment, control over when users are affected, and reporting that works for audits. Patch Manager Plus came out ahead for the reasons described below.

	Automated patch management	Cut down the manual effort of finding, approving, and deploying patches across servers and endpoints.
	Minimal user disruption	Flexible scheduling and reboot control let patching happen without getting in the way of production work shifts.
	Ease of use and deployment	The IT team could set it up and run it day-to-day without a steep learning curve.
	Cost and value	The feature set covered what the team needed at a price that held up against the other options.

The Patch Manager Plus solution

With Patch Manager Plus in place, Aequs moved from a slow, cumbersome patching routine to a central, automated process covering deployment, testing, scheduling, and compliance reporting for both servers and endpoints.

	1. Automated patch deployment	Patch Manager Plus detects missing patches and deploys them across the managed servers and endpoints, so administrators no longer work through machines one by one. Patches go out the same way each time, which has made the patching cycle faster and far more consistent.
	2. Patch testing and approval	Business applications at Aequs do not always react well to a new update. Testing and approval workflows let the team try patches on a small set of systems first and approve them for wider rollout once they are confirmed safe for the business applications. This has kept compatibility problems from reaching production machines.



3. Scheduling and maintenance windows

Earlier, due to lack of scheduling, patches were rolled out during work hours, which often impacted user productivity. Now, since deploying Patch Manager Plus, the IT team schedules patches around planned maintenance windows, so it can roll them out without affecting user productivity.



4. Critical and zero-day patching, with compliance reporting for ISO 27001

When a critical or zero-day vulnerability is disclosed, the team can find the affected systems and deploy the fix quickly instead of working through them by hand. This has shortened the time systems stay exposed.

The compliance side is just as useful. Patch Manager Plus monitors patching against SLAs and produces audit reports from one central place. These reports give the team a clear view of patch status and support ISO 27001 reviews and internal audits, without requiring any extra effort.



“Testing and approval workflows help us avoid compatibility issues with our business applications, and scheduling lets us patch during planned maintenance windows with minimal impact on users. The compliance reports give us clear visibility of patch status and make internal audits much easier.”

Manoj Kumar, Deputy Manager, Aequs Limited

Time savings and the ROI across every workflow

The biggest gain at Aequs has been the drop in time spent on patching. Finding missing patches, deploying them, and preparing reports used to require hands-on work from administrators. Centralized automation now handles most of it, which has saved IT administration time and made day-to-day operations run more smoothly.

Patch compliance has improved because systems are no longer left waiting on someone to address issues. The team also reports lower vulnerability exposure, and patching systems on time has helped prevent security incidents that can result from unpatched machines.

“Patch Manager Plus has reduced our manual patching effort, saved IT administration time, and improved patch compliance. With automated and centralized deployment, we have reduced vulnerability exposure and helped prevent security incidents related to unpatched systems.”

Manoj Kumar, Deputy Manager, Aequs Limited

Looking ahead

Aequs now has a dependable patching process built on ManageEngine Patch Manager Plus. Automated deployment, patch testing and approval, maintenance-window scheduling, zero-day response, and audit reporting all run from one platform.

As Aequs Limited grows and more systems come under management, the IT team continues utilizing Patch Manager Plus to fix critical vulnerabilities sooner and more efficiently. The manufacturing organization is ensured its IT patching plans stays on schedule, that users are disturbed less during the process, and that audit reports are generated promptly when requested.



See it on your estate.

Bring patch detection, testing, deployment, reboot control, and compliance reporting under one console.

[Request a demo →](#)