



CASE STUDY

How Western Aircraft Stopped A Ransomware Attack with CyberFOX® AutoElevate

Background:

Western Aircraft is a full-service aviation company based in Boise, Idaho, supporting corporate and general aviation with maintenance, avionics, aircraft sales, and FBO services.

The IT team, led by Senior IT Manager Steve Jackson and IT Systems Administrator Jeremy Graham, supports nearly 400 employees and 500-600 endpoints across the organization.

Western Aircraft has been a **CyberFOX AutoElevate** customer for about a year, and has since also adopted **CyberFOX Password Manager** and **CyberFOX DNS Filtering**.



Industry:
Aviation Services



Headquarters:
Boise, Idaho



Product Used:
CyberFOX AutoElevate

The Problem:

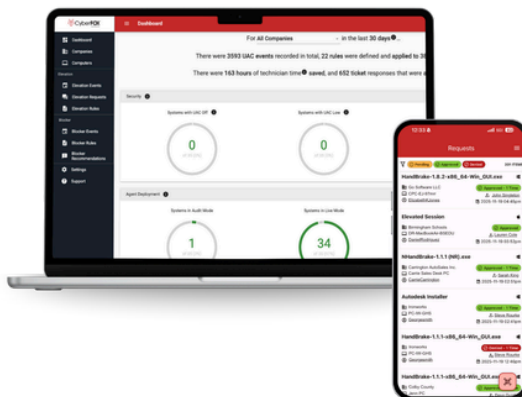
Before CyberFOX AutoElevate, Western Aircraft had no real alternative to giving nearly every employee local admin rights. It was the only way people could install the software they needed to do their jobs.

That was a problem the Western Aircraft team knew they couldn't ignore forever.

"We needed to make almost everybody in the company a local administrator so they could do their jobs, which was of course a big security vulnerability for us."

– Jeremy Graham, IT Systems Administrator,
Western Aircraft

As the threat landscape kept evolving, Steve and Jeremy wanted to lock down desktops without slowing the business down. They needed a way to remove standing admin rights without leaving users stuck waiting on IT for every request.



The Solution:

Western Aircraft first learned about CyberFOX through a former employee who championed the product internally. After evaluating other privileged access management vendors, CyberFOX AutoElevate stood out for the flexibility it offered.

With AutoElevate in place, Western Aircraft removed local admin rights across the company. Now, when an employee needs to install software, an alert routes straight into the IT team's ticketing system. Steve and Jeremy approve or deny it in minutes, no site visit required.

That setup was tested recently against its first real attack. An employee was contacted on Microsoft Teams by someone posing as internal IT support. Believing the request was legitimate, the employee let the caller into a remote session. It lasted nine minutes.

Western Aircraft's managed Endpoint Detection and Response (EDR) solution flagged the endpoint as high risk. The AutoElevate audit logs revealed that the attacker had disguised file-transfer software as a Windows update and installed it on the machine. AutoElevate's **Blocker** rules stopped it from ever running.

"So without the combination of the two systems in play there, I really think we would have been looking at probably a ransomware attack."
– Steve Jackson, Senior IT Manager, Western Aircraft

Organizational Impact:

Between the EDR solution isolating the endpoint and AutoElevate blocking the malicious software, Steve and Jeremy are confident the attacker never got the chance to steal anything.

The incident also became a launching pad. It pushed the team to close additional gaps in their Microsoft environment and sparked new user security training.

Day to day, AutoElevate gives Steve and Jeremy peace of mind across nearly 600 computers. Routine tasks, like adding a printer, run on approved rules. Anything outside those rules gets stopped automatically and routed through a ticket, whether the risk is an outside attacker or an internal one.

"I think **AutoElevate gives us that peace of mind** that if somebody does get onto a computer, whether through a cyber event or some type of disgruntled employee scenario, they're not going to be able to execute and do malicious things in the environment."
– Steve Jackson, Senior IT Manager, Western Aircraft

Conclusion:

For Western Aircraft, AutoElevate wasn't just a policy fix. It was a frontline defense during a live attack, and it held up because Steve and Jeremy had the visibility to catch what happened and the software to block it in real time.

They didn't have to choose between letting people do their jobs and keeping the company secure. AutoElevate gave them both, and in the nine minutes that mattered most, it protected them against a malicious attack.

"It's really two tools in one because there's the PAM side of it, but then there's the blocker rules that are built in that automatically stop things that are nefarious or potentially used by hackers to get into your environment."

– Jeremy Graham, IT Systems Administrator, Western Aircraft

Worried about social engineering and ransomware attacks at your organization?

Start a trial of CyberFOX AutoElevate today.

