



CASE STUDY

From 90% Admin Rights to Zero: How an American Manufacturing Giant Achieved Endpoint Application Control Across 70 Sites Without Slowing Production.

The PU foam manufacturer – one of the largest in the world – eliminated local admin rights to stop ransomware, pass audits, and unburden their IT helpdesk, using Securden.

Customer Profile

This world's largest vertically integrated manufacturer of polyurethane foams produces polyurethane chemical solutions, polyester fibers, and insulation materials for a diversified global marketplace.

With a range of research and production facilities across 70+ locations, employing a workforce of over 6500 people - the company establishes itself as a large manufacturing enterprise.

90%

FEWER ADMIN ACCOUNTS

2 min

MTTR FOR ACCESS TICKETS

Quick facts

INDUSTRY

Manufacturing

LOCATIONS

70+ Worldwide

HEADQUARTER

North Carolina, United States of America

CHALLENGES

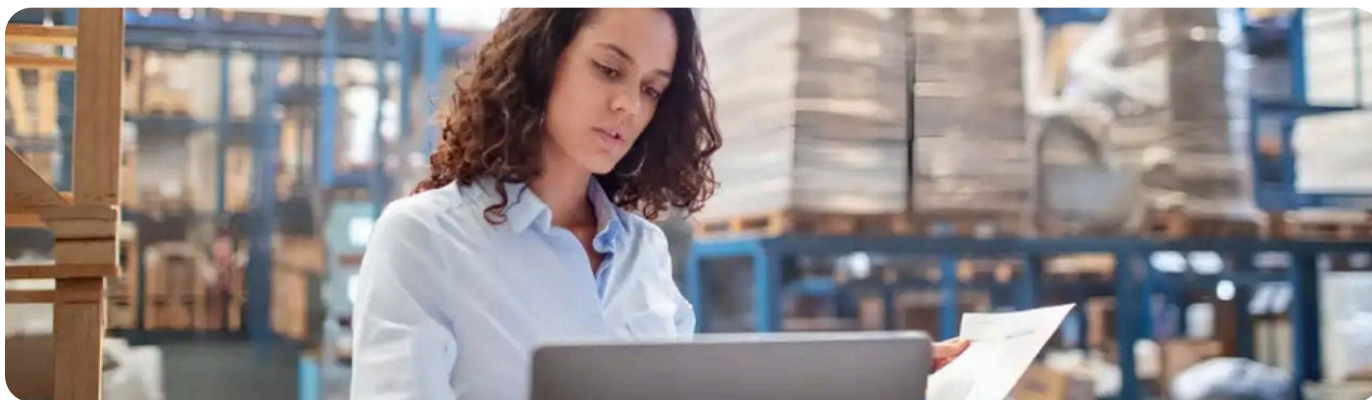
- Overprivileged users downloading files over the internet.
- Users using unauthorized USB sticks.
- Unregulated local admin rights on endpoints across geographical locations posing risk to overall organizational security

SOLUTION

Deployed the on-premises version of **Securden Endpoint Privilege Manager** across locations through a distributed deployment model.

RESULTS

- Reduced the number of admin accounts by 90%.
- Reduced MTTR for admin access tickets to two minutes.
- Enforced least privilege across 70 locations.
- Improved audit readiness and compliance posture.



Challenges Faced

The manufacturing industry is being increasingly targeted by threat actors globally. Being a pivotal player in the B2B manufacturing sector, the company is a prime target for cyber criminals.

It was imperative for them to adopt strong security measures and become resilient towards phishing, malware, and ransomware attacks.

Apart from protecting critical IT infrastructure, they needed to adopt robust security on user endpoints scattered across multiple locations.

Initially, employees, regardless of their role, had local administrator privileges on their workstations.

The IT team was quick to realize that local admin rights open up the IT network to a plethora of threats and vulnerabilities.

While the simplest solution was to manually remove local administrator rights across all endpoints by moving the users out of the local administrator group, the IT team realized right away that this manual approach was neither scalable nor sustainable.

1 Loss of productivity after removing admin rights

The IT team tried removing admin rights in a small test group. The number of tickets and requests raised by

the users forced the IT team to give admin rights back to the users.

“After removing admin rights, some of our users started questioning their inability to access certain apps”

IT ADMINISTRATOR

Removing admin rights directly created more problems than it solved, as employees had to run applications with admin rights to complete their everyday tasks.

Without admin rights, user productivity dropped significantly

2 Roadblocks encountered in granting temporary admin rights

The IT team tried a workaround for this problem using Windows LAPS. They created separate local administrator accounts for endpoints and granted temporary admin access to users who needed higher privileges for their tasks.

For example, when users need to install an application, they would log in using the administrator account.

They would simply use their standard user accounts to perform their day-to-day tasks.

They tried to control the use of admin account by forcing users to raise tickets when they wanted to use the admin account.

The IT team had two concerns here.

- Granting full blown access to admin credentials for elevating individual applications
- Burdening the IT helpdesk with admin access tickets

They realized that any manual approach to endpoint privilege management is not scalable for an organization of their size and complexity. They must automate privilege management to enforce security measures sustainably.

3 Need for Operational Oversight Across Locations

Their global presence across 70+ locations gave rise to a new challenge. They needed to delegate the responsibility of managing privileges and retain central oversight on the operations on all the networks.

They wanted the solution to be scalable and robust enough to handle distributed deployment.

The Solution

Being a pivotal player in the manufacturing sector, the organization's IT and OT network is a prized target for cyber criminals. Protecting themselves from malware, ransomware, and phishing attacks by eliminating vulnerabilities from their system was of paramount importance.

After carefully evaluating multiple solutions available in the market based on capabilities, pricing, and value for money, the IT management team decided to go with Securden Endpoint Privilege Manager.

Initial Deployment

The IT team wanted to deploy the solution in a phased manner. They planned to deploy the Securden Agent on specific endpoints in location zero through PDQ.

During deployment, a few minor obstacles were encountered in configuring PDQ to deploy the agent. The Securden support team assisted their IT team to successfully overcome obstacles and deploy the agent on their endpoints.

“We faced some snags with our agent deployment. But you guys are just great. I hit the customer service up, one of the engineers walked me through PDQ and set that up. It has been going on ever since. No problem, no issue with the product at all.”

IT ADMINISTRATOR

After successfully deploying the solution in the pilot deployment, their IT team was confident of expanding the deployment to other endpoints in the same location.

Subsequent Expansion to Other Locations

The IT team rolled out Securden Endpoint Privilege Manager across different locations and delegated administration responsibilities locally while retaining central oversight. They achieved this by using the distributed deployment capabilities of Securden Endpoint Privilege Manager.

Automated Privilege Management on Endpoints

Once the agents were deployed, they fetched the applications users were running with admin rights and helps with policy creation. The IT team started designing policies for their teams with assistance from experts at Securden. Once the policies were in place, the IT team removed admin rights from the endpoints.

The request-release workflow helped them overcome requirements that were not covered through policies. When the team wanted to create a policy for these requirements, they were able to do that right from the request approval page.

“In rare scenarios where a new application request came through, we were able to add it to an existing policy or create a new one easily.”

IT ADMINISTRATOR

This dynamic privilege elevation and automation capability provided by Securden Endpoint Privilege Manager (EPM) proved to be of immense help to the multinational organization.

Complete Oversight with Privilege Elevation History

The endpoint privilege manager records all privilege elevation activities performed by users on their endpoints. It serves as a record of 'who' had elevated access to 'which' application on 'which' endpoint with appropriate time stamps.

They could maintain complete oversight over privilege elevation activities at any endpoint in their various locations centrally.

Securden Endpoint Privilege Manager helped the organization adopt the principle of least privilege at a justifiable cost (license cost, maintenance cost, and other miscellaneous expenses).

Management feels more secure with Securden in place

The Securden Difference

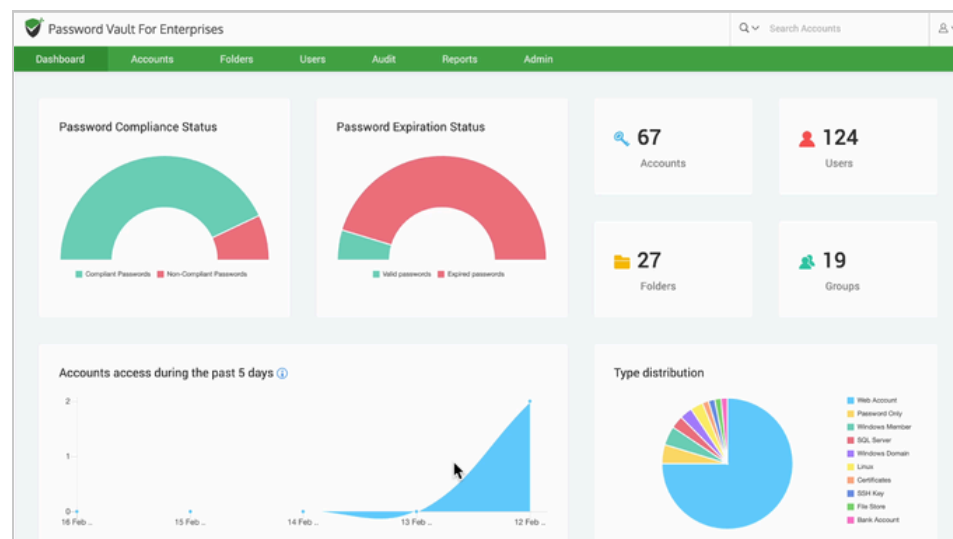
The simple and straightforward deployment model of Securden made this very large and complex deployment seamless and easy. Their IT team deployed the solution on 3900 endpoints across locations with relative ease.

With dynamic and comprehensive security controls, Securden Endpoint Privilege Manager helped them to:

- ✓ Restrict, control and manage admin rights without disrupting user experience
- ✓ Prevent unauthorized software installation on endpoints
- ✓ Automate privilege elevation and reduced IT helpdesk load
- ✓ Gain centralized oversight over operations across locations

The executives at the organization feel more secure with Securden as they have successfully fortified themselves against malware, ransomware, and phishing attacks.

Beyond the capabilities of the product, the IT team were delighted with the customer support offered by Securden.



Privilege elevation activity, tracked centrally across every location.

90%

FEWER ADMIN ACCOUNTS

2 min

MTTR FOR ACCESS TICKETS

3,900

ENDPOINTS SECURED

70+

LOCATIONS COVERED

“

I like the product, and I like the support. It is always great to have someone walk you through the steps, teach you, and inform you on things. I know if I have an issue, it is gonna get fixed. There is no time I have been sitting and waiting for a fix or a solution. I have no complaints at all.

IT ADMINISTRATOR

About Securden

Securden is a leading provider of privileged access governance solutions that holistically combines the principle of least privilege with other critical security principles such as zero-trust and provide visibility into privileged activities to continuously monitor cyber risk to effectively prevent cyberattacks, malware & ransomware propagation, and insider exploitation.

With simplicity and robustness in its core design, Securden offers a refreshing and intuitive panel of controls to govern privileged access across cloud, physical, and virtual environments. Here is a quick list of Securden's offerings:

- Password Vault for Enterprises
- Endpoint Privilege Manager
- Unified PAM
- Vendor PAM
- Unified PAM for MSPs
- Password Self-Service
- Secure Remote Access

The products have been built to be extremely scalable and secure. Securden is trusted by small businesses and large enterprises such as large banking and financial services, manufacturing companies, government agencies, healthcare organizations, managed IT service providers, educational institutions, and security service provider. To learn more, visit www.securden.com

