



Manufacturer Relies on Teramind for Insider Threat Detection, IP Protection and Data Loss Prevention

“We use Teramind to protect our IP and trade secrets from insider threats. The User Activity Monitoring is a great feature that automatically detects potential threats and even blocks dangerous behavior. Teramind’s support team was great in helping us setup and running in no time”

Chief Security Officer (CSO)

CASE STUDY



Business Challenges

The alarming trend of insider threats in the industrial sector made the Manufacture realize that it was only a matter of time before it too became a victim unless it took appropriate measures. It needed to:

- ✔ Protect its production and shop floor from growing insider threats:: sabotage, industrial espionage and IP theft.
- ✔ Prevent data leaks of its: industrial designs and blueprints, R&D secrets, supplier and customer information, contract information and other trade secrets.

Success Factors

Standard ICS based security measure wasn't enough to protect its IP and customer information from malicious employees and suppliers who were already inside the network. It needed a way to weed out those dangerous insiders and establish a data loss prevention and rapid response policy to handle this pervasive risk.

Company Profile

A global manufacturer and assembler of industrial automation components, automotive electronics and other parts.



Solution

Monitor and Prevent Suspicious Insider Activity :

- ✔ Monitor abnormal employee behavior like frequent late shifts or sick calls, unusual hours, etc.
- ✔ Track non-compliant vendor activities like login attempt during off-hours or after the completion of a project.
- ✔ Block downloading and opening of files and email attachments from unauthorized sources.
- ✔ Restrict access to external drives or sensitive network resources.
- ✔ The intelligent behavior rule engine could even identify subtle indicators that might lead to future issues such as, angry sentiment in emails.

Live View and Session Recording:

- ✔ Live view and recording of all user activities and session logs to pinpoint the exact time and user for any data breach incident.

Teramind DLP

Endpoint Data Loss Prevention with UAM Built-In

Teramind's endpoint-based Data Loss Prevention solution goes beyond traditional DLP approaches by adding intelligent behavioral analysis, OCR, fingerprinting and advanced risk and compliance management features.



Solution

Limit Exposure of IP Related Information:

- ✓ OCR, fingerprinting and tagging to discover employee exposure to sensitive data.
- ✓ Limit and segregate access to the production systems, design servers, supplier and customer databases on a need to know basis.

Risk Analysis and Reporting:

- ✓ Identify high risk employees, vendors, system components and policies with unique Risk Scoring system.
- ✓ Easy reporting and trend analysis of vulnerabilities, frequency violation by severity, departments and groups.

Employee Education & Training:

- ✓ Train employees why IP should be protected and how to safeguard against mistakes with custom rule violation messages.

About Teramind

Teramind is a leading, global provider of employee and user activity monitoring, workforce productivity optimization, user behavior analytics, insider threat detection, forensics and data loss prevention solutions.

Over 2,000 organizations in finance, retail, manufacturing, energy, technology, healthcare and government verticals across the globe trust Teramind's award-winning platform.



Result

Manufacturer was able to get the following benefits soon after implementing Teramind:

- ✔ Was able to identify and stop several data exfiltration attempts by insiders.
- ✔ Supported by the forensic data supplied by Teramind, the HR and legal teams were able to take action against the perpetrators.
- ✔ As an additional benefit, the Manufacturer was able to optimize productivity from the visibility gained into employee activity and how they spent their work hours.

hello@teramind.co

Live dashboard demo