Sandfly® x AUTO INDUSTRY

Automotive Manufacturer Achieves Complete Linux Security Visibility Without Production Risk

Sandfly's agentless security platform delivers reliable threat detection across thousands of Linux servers supporting critical assembly line systems - with no production impact

Customer Profile

An international automobile manufacturer operating critical manufacturing systems that manage just-in-time global assembly line operations alongside corporate infrastructure. Security solutions must deliver threat visibility without disrupting production.

Technology Environment

Approximately 1,600 Linux servers distributed across nearly 20 North American facilities supporting corporate and production line systems. Linux runs production operations, including automated guided vehicles (AGVs) moving inventory autonomously between assembly lines.

Background & Challenges

The customer's Security Operations Center (SOC) had almost no Linux visibility, leaving teams with blind spots in detection and triage that a Windows-heavy toolset couldn't address. Agent-based EDR systems introduced performance and stability risks that threatened production lines. The SOC team also lacked deep Linux expertise and had no visibility into password security. They wanted visibility without the drama of endpoint agents.

COMPETITIVE TESTING RESULTS

During competitive testing, an agent-based solution crashed test servers, exhibited progressive memory growth, and sustained 80% CPU usage - proving that the customer's concerns about production impact were well-founded.

KEY RISK FACTORS

Safety & Operational Risk: Security tools that impact performance or stability could topple critical servers and shut down manufacturing operations company-wide

Visibility Risk: Insufficient Linux visibility reduced the SOC's ability to reliably detect and triage security events across the fleet

> *"We needed visibility into the systems, but it also could not impact production. We could not be toppling servers, we could not be causing production issues. Sandfly proved that it would not cause problems in evaluation, and it has held up in production."*
>
> **SENIOR SECURITY ENGINEER, Automotive Manufacturer**

REQUIREMENTS

No Impact to Production: Agentless deployment to eliminate stability and performance risks on critical manufacturing systems in touch-averse environments, where traditional agent-based EDRs caused system failures during testing

Demonstrable Threat Detection: Detects all customer-defined test cases based on real issues observed in their environment, where alternative solutions did not meet detection criteria in the customer's evaluation

SOC-Ready for Non-Experts: Low false-positive alerts with human-readable descriptions and seamless SIEM integration, enabling SOC teams to act on alerts without deep Linux expertise

Minimal Maintenance Overhead: Automated upgrades and straightforward management without custom tooling or ongoing administrative burden

Sandfly® x AUTO INDUSTRY

Solution: Sandfly Agentless Linux Security

The customer selected Sandfly's agentless Linux EDR after competitive testing that included performance monitoring and customer-designed test cases. Sandfly was the only option that met the requirements for detection coverage and no performance impact. The agentless architecture provided comprehensive Linux visibility without endpoint agents, and enabled rollout across critical manufacturing servers where agent-based tools require extensive change control approval.

Sandfly's infrastructure was stood up in minutes. The customer leveraged existing Ansible automation to create accounts and deploy SSH keys across the fleet. Tag-based grouping enabled efficient baseline and whitelist development. Sandfly integrated into SOC workflows through JSON alerts to Microsoft Sentinel. Human-readable descriptions enabled the Windows-heavy SOC team to act on Linux alerts without deep Linux expertise, no custom tooling, and minimal ongoing maintenance. Upgrades, certificate renewals, and whitelisting are all handled through built-in automation.

> *"Sandfly is designed to not require a lot of maintenance and a lot of handholding. It works as you expect it to work."*

The team plans to expand Sandfly coverage to embedded Linux devices supporting vision-based quality assurance in manufacturing facilities.

Results

16x **Expansion in Linux security coverage**

> *"I stood up containers for node-runners and the Sandfly server in minutes and had everything running the way I wanted it to run basically. Shortly after that, it was less than a day. It was fantastic."*

SOC Visibility: The SOC gained wide visibility into security events across a fleet that previously had limited Linux coverage

Security Hygiene: Sandfly surfaced password and configuration issues outside Active Directory's reach, enabling targeted, actionable remediation conversations with application owners

Safe Fleet-wide Coverage: Deployed broadly in touch-averse environments without requiring disruptive changes to production systems