Sandfly® x vay

Sandfly's Zero-Impact Agentless Linux EDR Secures Vay's Remote Driving Fleet

Innovative remote-driving technology company implements Sandfly's agentless security to maintain critical performance standards while ensuring fleet-wide safety and performance

Customer Profile

Vay pioneers commercial remote driving technology that enables Remote Drivers to drive vehicles on public roads from afar. Their safety-critical service demands absolute reliability, near-zero latency, and compliance with stringent automotive cybersecurity standards.

Technology Environment

Hybrid Linux infrastructure including NVIDIA based embedded vehicle systems, on-premises servers, Remote Driving Stations, and cloud services. Sandfly integration via API; SIEM integration for alerts.

Background & Challenges

Vay's safety-critical technology required robust Linux security and system visibility across its rapidly scaling fleet. This highlighted a core industry challenge: securing high-risk Linux systems using EDR designed for desktops, where performance impacts are critical. Traditional agent-based tools would pose unacceptable latency, performance, and reliability risks on resource-constrained systems.

KEY RISK FACTORS

Safety & Operational Risk: Security tool performance hits could directly compromise vehicle control and safety

Compliance & Business Risk: Failure to secure the fleet would jeopardize ISO 21434 compliance, brand reputation, and ability to scale

Visibility Risk: Lack of monitoring created unknown vulnerabilities across an expanding attack surface

> *"From a high-level perspective, what Sandfly fundamentally brings us is visibility. For a growing company like ours, that's the first critical security issue that needs addressing — you can't secure what you can't see. Sandfly enabled us to have comprehensive monitoring and observability across our entire vehicle fleet, providing insights we simply couldn't get with other solutions."*
>
> **MEHDI ASGARI, Senior Engineering Manager, Vay**

REQUIREMENTS

Absolute Performance: No resource impact (latency, CPU/RAM) to ensure public safety and service reliability

Agentless Control: Full command over security scan timing to prevent operational interference during active remote driving

Robust Linux Security: Deep protection tailored for Linux to address unique threats and visibility gaps inherent in their environment

Compliance & Scalability: Features and visibility supporting compliance requirements and safe fleet expansion

Sandfly® x vay

Solution: Sandfly Agentless Linux Security

Vay selected Sandfly Security's agentless Linux platform – the only approach meeting their stringent needs. Sandfly provided deep Linux visibility without endpoint agents, eliminating performance risks and giving 100% control to the Vay team for securing a time sensitive, mission critical environment. Extensive testing validated its compatibility, minimal impact, and operational safety. Vay leveraged Sandfly's API for controlled, non-disruptive scanning during vehicle idle times.

Results

Security Without Compromise: Fleet-wide Linux security achieved with verified zero impact on remote driving performance

Complete Fleet Visibility: Gained essential monitoring and observability across vehicles and infrastructure

Baseline Enforcement & Risk Reduction: Established and maintained a "Golden Baseline," detecting drift and risks

Operational Efficiency Without Drama: Eliminated agent management overhead, saving valuable security team time and resources

Business Enablement: Supported ISO 21434 compliance needs, reduced endpoint security risk, and enabled safe operational scaling

"We frequently face questions about our security posture, such as how we handle vulnerability management or potential network issues caused by attacks like LTE spoofing, mobile data jamming, or GPS jamming. Sandfly directly addresses a key part of this: how we monitor for attacks across our vehicle fleet."

MEHDI ASGAR

"Sandfly's agentless Linux security gives us visibility without impacting our remote-driving systems where performance directly affects public safety. We can't compromise on either security or stability when lives are at stake. Sandfly's reporting, alerting, and scanning features operate without impacting our critical systems..."

EDGAR AVETISYAN, Senior Security Engineer

63% of the world's servers run Linux, but the operating system is the most attacked, accounting for **54% of all malware infections.** Securing critical infrastructure devices and embedded systems demands security without resource impact. Sandfly delivers zero impact EDR, extensive visibility, and **100% end–user control** to protect key systems without compromise.