Sandfly®

Close Critical Linux Security Gaps Without Compromising Operations

Sandfly Security delivers an agentless Linux security platform designed specifically for mission-critical systems. Instantly deployable with advanced threat detection, incident response, and forensics capabilities, Sandfly eliminates the operational risks and poor visibility that's associated with traditional agent-based approaches.

Linux Security Challenges

Linux powers everything from massive cloud infrastructures to embedded systems and critical infrastructure, yet securing these environments presents distinct challenges:

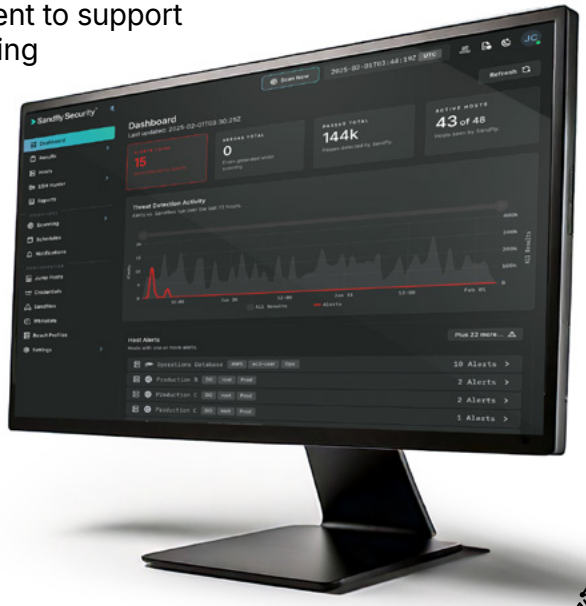
Securing Diverse Environments: From massive cloud clusters to embedded devices, Linux environments require universal protection that traditional solutions struggle to provide.

Reducing Operational Risk: Traditional agent-based solutions can compromise stability and slow critical systems, leaving gaps in coverage and introducing unnecessary complexity that raises costs and security risks.

Overcoming Expertise Shortages: Specialized Linux expertise is limited, leaving security teams overstretched and blind to potential threats across the enterprise.

Sandfly: Agentless Linux Security, Drama Free

Purpose-built for Linux, Sandfly goes beyond traditional Endpoint Detection and Response (EDR) solutions with instant deployment to support mission-critical workloads. It uncovers attackers using active tactics hunting vs. traditional signatures.



Key Features

- Custom Threat Hunting
- Drift Detection
- Deep Linux Forensics
- Endpoint Detection and Response
- Password Auditing
- SSH Key Tracking
- SSH Security Zones

Sandfly®

Competitive Differentiation

Sandfly	Competitors
Agentless approach with instant deployment	Risky agent-based deployment
No kernel integration, eliminating downtime and performance risk	Suffer from impacts to performance and stability
Comprehensive security beyond traditional EDR	Just EDR
Widest Linux support	Narrow Linux support
Supports network appliances, devices, and embedded systems	Do not support network appliances, devices, and embedded systems
Works in cloud, on premises, air-gapped and hybrid environments	Often cloud-dependent
Widest CPU architecture support	Limited CPU architecture support

Integration & Automation

Rapid Deployment at Scale: Agentless approach can cover thousands of hosts in minutes giving instant visibility without downtime risks

Secure Secrets & Access: Compatible with key vaults, password managers, key rotation, signed certificates, and PAM-ready

Robust API: Automate everything, provide instant actionable SIEM/SOAR alerts, enable cloud correlation, and create comprehensive dashboards

Close the Security Gap

Sandfly delivers agentless Linux security instantly across all Linux systems without traditional endpoint agent risks. Sandfly automatically hunts for intruders, discovers SSH key abuse, and finds suspicious activity from common and novel exploits. Built by Linux experts, Sandfly gives visibility where EDR agents fail, and does it with compatibility, performance, and safety where it matters most.

Visit sandfly.com to explore our scalable licensing models.

Customers & Use Cases

- Telecommunications
- Service Providers
- Auto & Robotics Manufacturers
- Higher Education
- Financial Institutions
- Critical Infrastructure
- Embedded System Deployments
- Air-Gapped & Sensitive Networks