

# Close Critical Linux Security Gaps Without Compromising Operations

## Bringing agentless Linux security to DigitalOcean's cloud platform

Sandfly Security delivers an agentless Linux security platform designed specifically for safety and performance on all Linux systems, now available as a Droplet 1-Click solution in the DigitalOcean Marketplace. Quickly deployable with advanced threat detection, incident response, and forensics capabilities, Sandfly significantly reduces the stability, performance, and compatibility risks that are 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 Complex 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 compromise stability and slow systems, leaving gaps in coverage and introducing complexity that raises costs and security risks.

**Overcoming Expertise Shortages:** 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 quick deployment to support all workloads. Sandfly uncovers attackers using active tactics hunting vs. traditional signatures.

### Key Features

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



## Competitive Differentiation

Sandfly	Competitors
Agentless approach with quick deployment	Risky agent-based deployment
No kernel integration, eliminates virtually all downtime and performance risks	Suffer from impacts to performance and stability
Security that goes 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

**Fast, Universal Deployment at Scale:** Leverage rapid, non-disruptive security that scales to thousands of hosts across workloads, VMs, network devices, appliances, IoT, OT, and more without downtime risks

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

**REST API:** Integrate with your existing tooling to provide actionable alerts, correlation, and create comprehensive dashboards

## Address the Security Gap

Sandfly automatically hunts for intruders, discovers SSH key abuse, and finds suspicious activity from common and novel exploits. Built by Linux experts, Sandfly delivers agentless Linux security across all systems without traditional endpoint agent risks.

Visit the [DigitalOcean Marketplace](#) to deploy Sandfly as a Droplet 1-Click App today for enhanced protection of your cloud infrastructure. Professional plans start at just 10 hosts.

## Customers & Use Cases

Telecommunications

Service Providers

Auto & Robotics  
Manufacturers

Higher Education

Financial Institutions

Critical Infrastructure

Embedded System  
Deployments

Air-Gapped &  
Sensitive Networks

