# Sandfly Security™

AGENTLESS LINUX SECURITY
AND INCIDENT RESPONSE

## Revolutionizing Linux Security with an Agentless Approach

Sandfly protects Linux systems **without endpoint agents**, ensuring unmatched compatibility and performance.


### Agentless Security

Instant deployment without compromising system stability or needing endpoint agents.

### Threat Detection

Actively hunts for malware and intruders across all Linux systems, including cloud, on-premises, appliances and embedded environments.

### Widest Coverage

Industry-leading Linux coverage that protects modern systems to those a decade+ old. Covers Intel, AMD, Arm, MIPS and Power CPUs without modifications.

### SSH Key and Password Monitoring

Monitors SSH keys and conducts password audits to identify credential theft and lateral movement attacks.

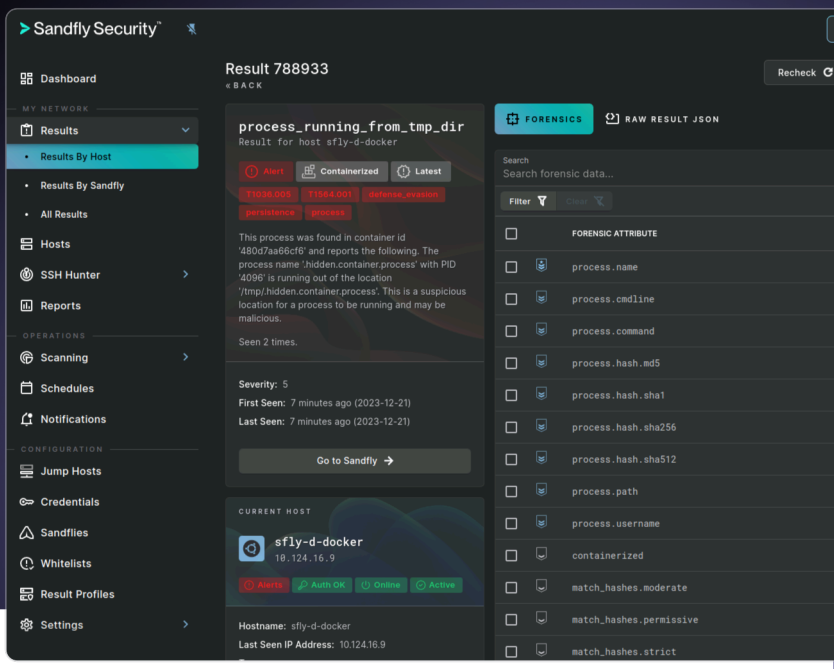
### Drift Detection

Agentlessly detects changes to all protected systems, including embedded devices and custom applications.

# Sandfly Security™

AGENTLESS LINUX SECURITY
AND INCIDENT RESPONSE

## Protects critical Linux infrastructure without impacting performance or stability.




## Comprehensive Protection for Linux

### Automatic Attack Detection
Over 1,000 modules to identify sophisticated Linux attacks.

### SSH Key Auditing
Track and monitor SSH keys to detect breaches.

### Custom Detection
Create new threat hunting modules instantly.

### Drift Detection
Instantly detect changes to any system, including embedded and appliance applications.

### Incident Response
Rapid compromise detection without compatibility risks.

### Privacy
Sends no telemetry outbound and works on isolated networks.

### Cross-Platform Defense
Works across nearly all Linux distributions, ensuring protection for modern cloud systems and those up to a decade+ old.

redhat · ubuntu · debian · fedora · CentOS · Rocky Linux · openSUSE · + many more

### Widest Hardware Support
Works on servers, embedded devices and custom hardware.

intel · AMD · ARM · MIPS · IBM

> "Sandfly is the first product I've seen that accurately and quickly detects thousands of signs of compromise on the Linux platform. Its unique method automates tasks which would be manually impossible. Automation is key with detection, and Sandfly completely fits this and other requirements. If your organization is using Linux, this should be part of your cybersecurity toolset."

Ken Kleiner University of Massachusetts Senior Security Engineer Adjunct Faculty Instructor in Digital Forensics

www.sandflysecurity.com

Get your free license and protect your Linux systems instantly.