MORPHISEC

Data Sheet

For Linux

The Evolution of Linux Endpoint, Server & Workload

Linux is an ideal target for attackers due to its longevity, stability, and role in hosting critical organizational data and essential application services. Historically perceived as secure, many organizations have overlooked Linux security. However, its widespread use in cloud computing, virtual machines, and data centers has made it increasingly vulnerable. Attacks on Linux continued to rise between 2022 and 2023, accounting for 62% of attacks, more than 40% of all malware infections.

- Often used to host an enterprise's most critical data at rest and in motion , often used to host virtual machines
- Tend to be long living in a "set and forget" state which leave security vulnerabilities unattended
- NGAV, EPP, and EDR/XDR have security gaps due to being probabilistic, not deterministic. And they do not change the underlying system, so attackers can train and attack where and when they please
- Security gaps and misconfigurations are prevalent across an organization's entire infrastructure, which are harder to patch and harden once in production, especially mission-critical and legacy systems to stop at least three of the top 10 MITRE ATT&CK techniques—a critical 30 percent security gap.

Core Capabilities

- Leverages Adaptive Exposure Management for in depth software inventory and vulnerability visibility
- Continuously monitors critical runtime activity across the system
- Enforces strict trust boundaries to prevent unauthorized execution
- Observes application and process behavior in real time
- Deploys smart decoys to identify ransomware threats

Security Benefits

- Visibility into installed and running applications (e.g. Adaptive Exposure Management)
- Ransomware protection
- Capture keys for recovery
- Data exfiltration prevention

Results

- Protects virtual machine and bare metal servers across the infrastructure—including air-gapped servers
- No extra headcount needed– "install and forget"
- Ultra-low maintenance, no updates required

Key Benefits

- Stops ransomware
- Prevents data exfiltration
- Blocks evasive, early-phase MITRE ATT&CK tactics and techniques
- Stops supply chain and advanced attacks at runtime
- Detects and blocks polymorphic defense evasion
- Restores encrypted files and preserves forensic insights for fast, effective recovery

© Morphisec Inc.

Gartner states, “Preemptive cybersecurity technologies are crucial in enhancing organizations’ defense capabilities against threats like ransomware and zero-day vulnerabilities.” [1]

Gartner

The Next Evolution of Endpoint Security

Morphisec for Linux is a proactive security solution that shelters your most critical assets from sophisticated attacks by monitoring critical system functions, stopping supply chain attacks and other exploits at runtime.

Morphisec does this by implementing a unique combination of prevention capabilities, attack surface reduction mechanisms, and ransomware protection, exfiltration and recovery.

“Morphisec for Linux is an effective and comprehensive eBPF solution for mitigating native code-based attacks on the Linux platform.”

MDSec

Supports:

AlmaLinux 8.x, 9.x, Amazon Linux 2023, CentOS Stream 8.x, 9.x, 10.x, Oracle Linux 7.x, 8.x, Red Hat Enterprise Linux (RHEL) 6.x and above, Rocky 8.x, 9.x, SUSE Linux 12.x and 15.x, Debian 9.x and above, Ubuntu 14.04 and above. Bare metal or virtual machines using at least Intel x86 or AMD64 Architecture. For 64-bit ARM based architecture we support Debian 11 5.x and 6.x. Access the full matrix here: https://support.morphisec.com/hc/en-us/articles/26886470889490-Morphisec-Linux-Protector-3-x-Support-Matrix

Footnotes

1. Gartner® Report: Report: Emerging Tech: Build Preemptive Security Solutions to Improve Threat Detection (Part 2)

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

MORPHISEC

See Morphisec in action

Stop ransomware with our Preemptive Cyber Defense Platform

Get a demo

About Morphisec

Morphisec is the trusted global leader in prevention-first Anti-Ransomware protection, redefining cybersecurity with our industry-leading Automated Moving Target Defense (AMTD) technology. Our solutions are trusted by over 7,000 organizations to protect more than 9 million endpoints worldwide, stopping 100% of ransomware attacks at the endpoint and safeguarding businesses against the most advanced and dangerous threats, including zero-day exploits and ransomware.

At Morphisec, we don’t just fortify defenses – we proactively prevent attacks before they happen, delivering unmatched protection and peace of mind to our customers. With our Ransomware-Free Guarantee and commitment to Preemptive Cyber Defense, we set the standard for accountability and innovation in the fight against modern cybercrime.

As a rapidly growing company, we are dedicated to empowering security professionals and organizations to adapt, protect, and defend against ever-evolving threats. Join us in shaping the future of cybersecurity with prevention-first strategies and unparalleled expertise.

To learn more, visit morphisec.com/demo