MORPHISEC

For Linux

The Evolution of Linux Endpoint, Server, Workload & OT Security

From an attacker's perspective, Linux is a perfect target. It's a long-living operating system, with a stable and reliable surface. It hosts organizations' most critical data at rest, and in application services needed to keep businesses running. Because it's historically been widely perceived as secure, many organizations haven't thought too hard about Linux security. But Linux malware attacks have escalated rapidly in recent years, growing by 50 percent in 2022 alone. Linux security risks include:

- Often used to host an enterprise's most critical data at rest and in motion
- 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 in the cloud and on-premises, which are harder to patch and harden once in production, especially mission-critical and legacy systems

CORE CAPABILITIES

- Periodically randomizes system-level APIs
- Kernel morphing: System-wide protection ensures nothing slips
- Only trusted code gets to run; everything else is trapped for forensic analysis
- Autonomously rewrites low-level trusted application code in memory at runtime

SECURITY BENEFITS

- Runtime exploit prevention
- Defense-in-Depth for trusted applications
- Attack surface reduction for legacy and under-protected systems
- Negligible false positive alerts

OPERATIONAL BENEFITS

- Protects virtual machine and bare metal servers on-premises and in the cloud—including air-gapped servers
- Negligible memory and CPU footprint. Can run on a Raspberry Pi, IoT device, and critical financial transaction management servers
- No extra headcount needed—"install and forget"
- Ultra-low maintenance, no updates required

RESULTS

- Stops a wide range of early-phase MITRE ATT&CK tactics and techniques
- Stops supply chain and other advanced attacks at runtime
- Blocks harder-to-catch Linux OS/native remote code execution (RCE) and privilege escalation (PE) without generating false positive alerts
- Identifies and blocks polymorphic defense evasion and other advanced tactics

Gartner states, “Automated moving target defense is an emerging game-changing technology for improving cyber defense.”[1]

Gartner.

Automated Moving Target Defense: The Next Evolution of Endpoint Security

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

Morphisec does this by implementing a unique combination of prevention capabilities via Automated Moving Target Defense (AMTD) technology and attack surface reduction mechanisms.

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

MDSec

About Morphisec

Morphisec provides prevention-first security against the most advanced threats to stop the attacks that others don’t, from endpoint to the cloud. Morphisec's software is powered by Automated Moving Target Defense (AMTD) technology, the next evolution of cybersecurity. AMTD stops ransomware, supply chain attacks, zero-days, and other advanced attacks. Gartner® research shows that AMTD is the future of cyber. AMTD provides an ultra-lightweight, Defense-in-Depth security layer to augment solutions like NGAV, EPP and EDR/XDR. We close their runtime memory security gap against the undetectable cyberattacks with no performance impact or extra staff needed. Over 5,000 organizations trust Morphisec to protect nine million Windows and Linux servers, workloads, and endpoints. Morphisec stops thousands of advanced attacks daily at Lenovo, Motorola, TruGreen, Covenant Health, Citizens Medical Center, and many more.

To learn more, visit morphisec.com/schedule

Footnotes

1. Gartner® Report: Emerging Tech: Security—The Future of Cyber is Automated Moving Target Defense

©Morphisec Ltd. 2023