

MORPHISEC

Threat Protection for Linux

Linux powers the world's most critical infrastructure. Morphisec Protection for Linux is built to guard it from the most damaging cyberattacks—including zero days, fileless attacks, and in-memory exploits. With Morphisec in the security stack, vulnerabilities are virtually patched before fixes get released and memory structures are morphed to preserve valuable assets.



Protect Linux Servers from Sophisticated Targeted Attacks and Zero Days

With Linux powering the servers that run 96.5 percent of the top one million domains in the world, the Linux kernel, once considered secure, has increasingly been the target of zero days and sophisticated cyberattacks. Attacks targeting the platform are becoming more frequent, more sophisticated and more dangerous. However, as quickly as security researchers discover and publish indicators for Linux threats, attackers change their tools and techniques.

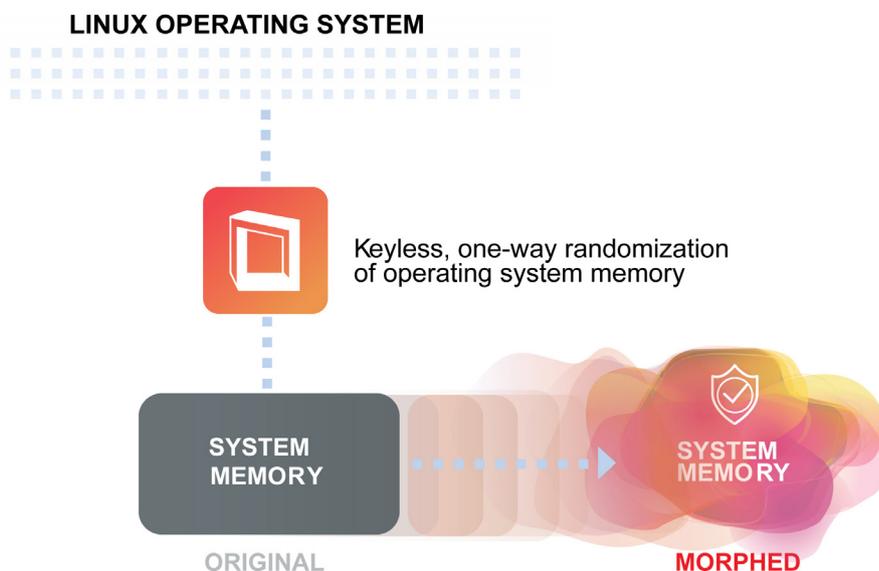
To reduce the risk to their Linux servers, companies of all sizes have protected themselves with client-grade endpoint security technology. Rather than reduce risk, this has created a false sense of security and still left the organization open to attacks. This is why Morphisec has extended its Moving Target Defense technology to the Linux OS with Morphisec Threat Protection for Linux.

Get the Power of Moving Target Defense for Your Linux Servers

With Morphisec Threat Protection for Linux, your servers are protected from advanced persistent threats and targeted zero-day attacks, including shellcode injections, fileless malware, and exploits.

All Protectors, Windows and Linux, connect to the Morphisec Management Server and are centrally managed in the Console. Attacks are displayed in the Management Dashboard for visibility across your Windows and Linux deployments.

How It Works



KEY BENEFITS

POWERFUL PROTECTION

Preemptively prevents unknown evasive attacks, exploits, fileless attacks, and zero days targeting your Linux servers.

ONE UNIFIED PLATFORM

Morphisec operates as one unified protection platform across organizational endpoints and servers running Windows and Linux operating systems.

LIGHTWEIGHT AGENT WITH ZERO PERFORMANCE PENALTY

Morphisec for Linux uses a slim agent that does not impact endpoint performance or disrupt user operations.

SUPPORTS A WIDE RANGE OF LINUX PLATFORMS

Morphisec runs on 64bit 4.x kernel versions of Linux on various distributions.

CUT SECURITY OPERATIONAL COSTS

Does not generate false positives, no need to investigate, analyze or remediate. Blocks attacks pre-breach, before they can do any damage.



Morphisec works by morphing the system memory in your Linux operating system. This changes the memory structure of your operating system and turns it from a known entity into an unknown landscape.

By doing this, Morphisec protects your Linux applications from zero days, fileless attacks, in-memory exploits, and evasive malware.



Attacks Morphisec Blocks

Morphisec blocks Linux attacks such as:

- The Linux-targeted ExtraBacon exploit
- The Google Project Zero Linux kernel bug CVE-2018-7182
- The Golang-based Spreader recently used in a cryptojacking campaign
- The QNAPCrypt ransomware attack that targeted Linux-based file storage systems (NAS servers)
- Silex malware
- New Mirai variants
- Attacks on Monero and various cryptocurrency mining malware such as Skidmap
- Botnets such as Roboto and Mozi (Hajime), a DHT botnet
- Rats such as Dacls
- Backdoors such as ACBackdoor

Simplify Your Security and IT Operations

Morphisec for Linux deploys quickly and easily with no configuration needed, does not require updates and provides the same level of protection whether online or off. Morphisec stops attacks deterministically, with no false positives, substantially reducing remediation and forensic analysis requirements and costs.

About Morphisec

Morphisec delivers an entirely new level of innovation with its Moving Target Defense-powered Unified Threat Prevention Platform – placing defenders in a prevent-first posture against the most advanced threats to the enterprise, including APTs, zero-days, ransomware, evasive fileless attacks and web-borne exploits. Morphisec provides a crucial, small-footprint memory-defense layer that easily deploys into a company's existing security infrastructure to form a simple, highly effective, cost-efficient prevention stack that is truly disruptive to today's existing cybersecurity model.

Schedule a demo: demo@morphisec.com