MORPHISEC KNIGHT FOR LINUX

The Best Protection to Stop Advanced Cyberattacks Against Linux Servers

Morphisec Knight for Linux protects bare metal and virtualized servers across on-premise and public, hybrid, and private cloud environments against supply chain, data theft, ransomware, and other advanced attacks.

MORPHISEC
Breach Prevention Made Easy

INTRODUCTION

With ever more workloads, processes, and systems moving online, threat actors are zeroing in on the Linux servers that power 90 percent of the cloud and 70 percent of the web. Linux threats were once relatively rare. But today cybercriminals use Linux-focused cryptojacking, code injection, spyware, in-memory, and zero-day threats for supply chain attacks, data theft, extortion, and ransomware. Few organizations have implemented the measures required to stop these threats.

threat actors are zeroing in on the Linux servers that power 90 percent of the cloud and 70 percent of the web

Cybercriminals have ported advanced tactics and techniques from Windows to Linux targets and created new customized threats. The volume of advanced attacks targeting Linux servers increased over 35 percent in 2021. Today, Linux servers face as many exploit vulnerabilities as their Windows counterparts, including a new wave of polymorphic, fileless, in-memory, and code execution attacks. Linux-specific threats such as ExtraBacon exploits, Golang-based spreader, QNACrypt ransomware, and Silex malware use techniques like shellcode injection and remote code execution to bypass signature- and behavior-based security controls.

Few defensive solutions meet the demands of real world Linux operations. Some are not optimized for dynamic server workload or cloud workload protection platform (CWPP) environments. Many endpoint detection and response (EDR) agents are too resource intensive for high uptime and workload environments. And the negative impact of EDR on server performance causes significant user disruption, particularly with legacy systems. Gartner warns that "Enterprises using endpoint protection platform (EPP) offerings designed to protect end-user devices for server workload protection are putting their data and applications at risk."

To keep end users productive, EDR and similar solutions are typically “tuned” to lower alert and performance settings, or simply not used at all. Doing so dramatically increases the risk of security breaches, data theft, audit failures, and lawsuits.

Many EDR agents:

ARE BLOATED

USE EXTENSIVE MEMORY

USE EXTENSIVE CPU RESOURCES

NEGATIVELY IMPACT PERFORMANCE

Key Benefits

Protect Linux servers from advanced threats

- Prevents supply chain, cryptojacking, spyware/data theft, zero-day, polymorphic, and ransomware attacks

Eliminate workload performance and downtime issues

- Lightweight cloud and server workload agent needs no reboot or downtime to deploy or maintain, and doesn’t impact performance

Slash alert overload and SOC OPEX costs

- Set-and-forget application runtime protection reduces EDR alerts and false positives to reduce staff needs

Harden virtual and physical server security

- Augments or replaces EDR/RASP/AV for bare metal, cloud, on-premise, VM, AWS, Azure environments

Eliminate patch vulnerability risks

- Next-gen virtual patching alternative prevents zero-day attacks prior to patching—far superior to WAF or IPS

Proven results against Linux attacks

- Independent penetration tests validate Knight’s effectiveness against common MITRE ATT&CK tactics and techniques

Supported Linux Distributions

- Amazon Linux 2, CentOS 7 / 8, Debian 9 / 10, Oracle 7 / 8, RedHat 7 / 9, Rocky 8, SUSE 12 / 15, Ubuntu 14 / 16 / 18 / 20 / 21

MOVING TARGET DEFENSE FOR LINUX SERVERS

Morphisec Knight for Linux employs a revolutionary, patented technology called Moving Target Defense (MTD). It uses morphing logic and runtime traps to create a dynamic attack surface threat actors can't penetrate. Knight shuts down attack chains early and stops threats before they can execute and cause damage. Uniquely in the marketplace, Knight employs runtime kernel morphing to provide system-wide protection for bare metal and virtualized servers. It also provides detailed forensics on prevented attacks, enhancing threat intelligence and hunting.

Knight's lightweight agent can be installed in less than an hour, and uses less than one percent of server CPU or memory to ensure zero performance impact

In contrast to EDR agents which take days or weeks to deploy, Knight's lightweight agent can be installed in less than an hour. It requires little to no maintenance, and uses less than one percent of server CPU or memory to ensure zero performance impact.

Knight protects mission-critical Amazon Web Services (AWS), Microsoft Azure, and other Linux servers from advanced attacks that evade EDR and endpoint protection platforms (EPP), whether on-premise or in public, private, or hybrid cloud environments.

ON-PREMISE | PUBLIC | PRIVATE | HYBRID

Knight leverages MTD to deterministically block known and unknown threats that use:

- REMOTE, UNAUTHORIZED, OR OTHERWISE WEAPONIZED CODE EXECUTION
- LIVING OFF THE LAND (LoTL) OR MAN-IN-THE-MACHINE (MiTM) TECHNIQUES
- PRIVILEGE ESCALATION
- POLYMORPHIC DEFENSE EVASION
- OTHER ADVANCED TACTICS, INCLUDING FILELESS MALWARE ATTACKS

Unlike the many Linux security solutions ported from workstations or Windows-focused platforms, Knight is purpose-built for Linux server and CWPP environments and threats. Knight can augment AV, EDR, XDR, and obsolete runtime application self-protection (RASP) solutions. Or it can replace them.

REDUCE ATTACK RISKS

More than 13 million attempted malware attacks on Linux systems were detected between January and June 2021 alone.[1] There are now at least nine major ransomware families targeting Linux systems, including Linux versions of REvil, DarkSide, BlackMatter, and Defray777. Cryptojacking is on the rise, with 89 percent of Linux cryptominers using Monero cryptocurrency XMRig-related libraries to tracelessly mine crypto using compromised Linux servers. Criminals are also doubling down on Linux vulnerability reconnaissance. There are now more than 14,000 active Cobalt Strike team servers, with almost 8,000 cracked or leaked, exposing them to crooks looking for vulnerable Linux instances. Knight combats these advanced, often polymorphic threats with polymorphic MTD.

Unpatched vulnerabilities account for over 60 percent of ransomware attacks.

Unpatched vulnerabilities are a major Linux server threat vector. Knight offers a next-generation virtual patching alternative for Linux applications that is faster, easier, more affordable and effective than web application firewalls (WAF) and Intrusion Prevention Systems (IPS). It blocks attack pathways without relying on network traffic or signatures, and reduces "patch panic" and risk from unpatched vulnerabilities.

Morphisec Knight for Linux is set and forget; one person can deploy and run it

LOWER EFFORTS AND COSTS

Most IT and security teams are lean and overburdened, spending 25 percent of their time chasing false positive alerts. EDR solutions are complex to deploy and manage and require a team of analysts to investigate alerts. Teams must create IT support tickets for each alert and downtune EDR policies to reduce alert overload. As a result, most firms ignore almost one-third of alerts, increasing attack risks.

Morphisec Knight for Linux is set and forget; one person can deploy and run it. It does not create false alerts and does not need a continuous online connection to protect Linux servers. This ensures no efficacy or efficiency degradation for air gap and completely isolated or disconnected conditions. Instead of reacting to threats, Knight's MTD proactively and automatically prevents attacks and provides alerts that are never false positives. If deployed alongside EDR, Knight allows you to use standard rather than aggressive EDR alert settings, eliminating alert overload and slashing IT support tickets, analyst investigation resources, and costs.

Source 1 | https://www.computerweekly.com/news/252505771/13-million-malware-attacks-on-Linux-seen-in-wild

ELIMINATE AUDIT FAILURES

Linux servers typically store and process client and employee data, so securing them is critical to avoid regulatory penalties. Whether international regulations or U.S. state civil codes, almost every organization faces severe penalties if it allows personally identifiable information (PII) to be exposed. You risk audit failure, fines, lawsuits, and brand damage for non-compliance.

Faster patching could have prevented security breaches or audit failures at 80 percent of firms

Although compliance is vital, most firms struggle to implement frameworks such as the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), recommended by leading analysts. NIST mandates meeting zero trust architecture (ZTA) guidelines for identity and access management (IAM), endpoints, devices, and servers.

Morphisec Knight is a zero trust solution. And it makes NIST compliance easier by providing enhanced alert and threat intelligence for audits and compliance reporting. Knight helps organizations meet the NIST CSF Five Steps and endpoint ZTA mandates by augmenting or replacing less effective application whitelisting solutions.

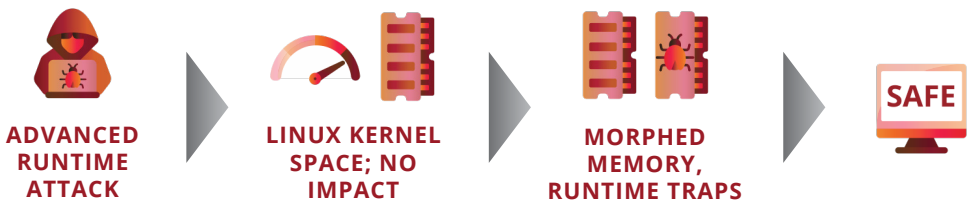
Faster patching could have prevented security breaches or audit failures at 80 percent of firms. Morphisec Knight's instantaneous virtual patching prevents zero-day attacks before a patch is available, enabling more time for patch implementation.

AN INDUSTRY LEADING LINUX SECURITY SOLUTION

Morphisec Knight for Linux is a purpose-built Linux security solution that's lightweight, non-disruptive, and highly effective against advanced Linux attacks. Knight protects bare metal servers and virtual machine (VM) guests by leveraging MTD technology to prevent supply chain, data theft, ransomware, and other advanced attacks.

Traditional server security solutions

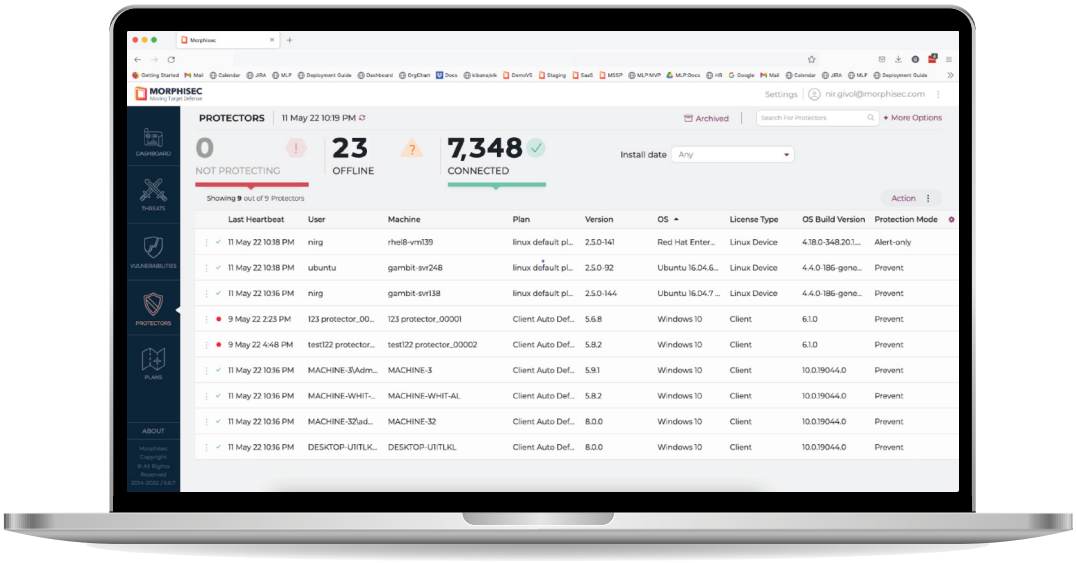
Morphisec Knight for Linux Moving Target Defense



For Linux user-space applications, Knight employs executable modifications in-memory and pre-execution. This ensures specialized handling for adversaries trying to exploit a trusted yet vulnerable application. These pre-execution in-memory changes stop an adversary being able to train in one place and reuse that approach on other servers.

Knight's lightweight agent uses less than one percent of server CPU or memory, and does not impact performance or create false alerts.

Morphisec Knight applies real-time, deterministic prevention while decreasing cost and complexity, and eliminating performance drag. It is isolated from backend systems, does not require updates, and leverages a command validation process—similar to CPU opcode—to determine if an action should be trusted or not.



Independent test lab MDSec validated that Morphisec Knight stops typical MITRE ATT&CK tactics and techniques used by threat actors. "Overall, MDSec found Morphisec Knight for Linux to be an effective and comprehensive solution for mitigating native code-based attacks on the Linux platform." Described by Gartner as easy to implement, complementary, and scalable, the MTD technology powering Morphisec Knight denies threat actors access to mission-critical Linux servers.

SCHEDULE A DEMO

ABOUT MORPHISEC

Morphisec is breach prevention made easy. We are a leader in providing prevention-first software that STOPS ransomware and other advanced and evasive attacks from endpoint to the cloud—augmenting next generation antivirus (NGAV) and endpoint detection and response (EDR) solutions. This defense-in-depth capability is powered by Morphisec's revolutionary Moving Target Defense technology that delivers automated, proactive, operationally simple, highly effective protection against advanced attacks. Morphisec secures nine million endpoints worldwide from ransomware, zero-day, fileless attacks, and other evasive threats at companies such as Motorola, Maersk, Citizens Medical Center, Yaskawa, and many more.

MORPHISEC
Breach Prevention Made Easy