POLYMORPHING FOR LINUX

STOP CYBERATTACKS IN THEIR TRACKS

In our increasingly interconnected and digitized world, cybersecurity is a hot topic. Cyberattacks and data breaches are constantly in the news. These attacks are growing at an alarming rate and becoming more ingenious and aggressive.

Polymorphing for Linux stops these attacks before they start. It makes your operating system impervious to zero-day, code-execution, overflow and memory-based attacks. A comprehensive multifaceted cybersecurity defense strategy is imperative for all modern organizations. By including Polymorphing for Linux, your cyber-protection is advanced to a whole new level.

At a Glance

Key Benefits

+ *Fast and easy installation*
+ *No runtime overhead or performance impact*
+ *Zero-day detection and reporting*
+ *100% protection against memory-based cybersecurity attacks*
+ *Patch for hygiene, not for security*
+ *Enables enhanced compliance*
+ *High return on security investment*

Linux Distros Supported

+ *CentOS*
+ *Red Hat Enterprise Linux*
+ *Fedora*
+ *Alpine*
+ *Ubuntu*
+ *SUSE (2020)*
+ *Debian (2020)*

Product Overview

Polymorphing for Linux is a ground-breaking technology that hardens open source Linux distributions by scrambling the binary code to create a unique version of the operating system.

This is accomplished by running the source code of your chosen Linux distribution through an advanced polymorphic compiler to scramble the low-level machine code. The result is a Linux stack that has a unique binary makeup (including CPU registers, function locations, memory layouts and instruction sets) that still functions, performs and operates in exactly the same way but is completely impervious to memory-based attacks.

When attacking an operating system with randomized and unique resource mapping, hackers are unable to craft exploits and attacks that target specific memory vulnerabilities, even when the OS or applications remain unpatched for known issues.

Each Polymorphed Linux OS deployment is effectively immunized against everything in the code-execution, overflow or memory corruption attack categories. This includes the memory-exploiting zero-day attacks that make up over 80 percent of all common vulnerabilities and exploits (CVEs) and are the most difficult to defend against. The protection level is ramped up even further by recompiling the OS every 12 to 24 hours, rendering any customized or specifically targeted assault infeasible and futile.

Polymorphing for Linux is also ideal for delivering enhanced and comprehensive protection during any security-patch gaps. A patch gap is the time period from when a vulnerability is discovered until security patches are made available and applied to fix the issue. This is vitally important because valuable systems can often go unpatched and exposed for up to a year or even longer in some cases (see figure 1 on next page).

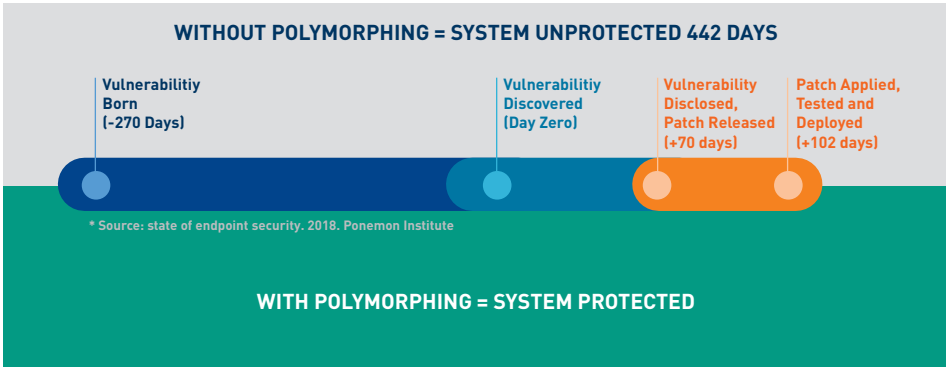

Figure 1

Business Benefits

Closes the door on attackers. Creating a unique resource map for each OS safeguards against 100% of attacks aimed at zero-day memory exploits, as well as everything in the code-execution, overflow and memory corruption categories.

Removes the panic and scramble to apply security patches. Unpatched systems are safeguarded without additional administration overhead or costly resources. Patches can be efficiently and pragmatically applied when it is most appropriate to the business, freeing up valuable IT resources to focus on innovation.

Maintains security compliance. Enables adherence to strict security compliance frameworks with an incremental, robust, and innovative cybersecurity barrier.

Outstanding Return on Security Investment (ROSI). Polymorphing for Linux delivers superior, high-caliber protection at a substantially lower cost than more traditional solutions. This makes it easier for each organization to balance its specific security risk profile and budget.

Key Features

- **Zero changes to anything that matters.** No changes are made to the source code, only to the binary layout of the compiled OS image. There are no changes to program functionality, performance and interoperability; no impact on developers or users; and no changes to OS logging, debugging or any other functional behavior.
- **Fast and easy installation.** Polymorphing for Linux is simple to deploy with a single command-line of code and can be deployed in a matter of minutes
- **No runtime overhead or performance impact.** No CPU cycles are required to protect the OS.
- **Zero-day attack detection and reporting.** The Polytect Agent provides insight into the nature of an attack.

Installation and deployment

Deployment can be carried out in a matter of minutes using a simple one-line Linux installation command that points to the repository for the polymorphed version of your chosen distribution.

Polymorphing for Linux is available in three forms:

- AWS or Azure ready technology
- As an on-premise build farm behind your organization's own firewall
- As an embedded Linux image distribution for devices

"Polymorphing is hands down the highest ROI cybersecurity tool on the market. There is nothing easier or more effective to protect your systems from remote cyberattacks. With a one-click, 'fire and forget' installation process, Polymorphing eliminates 100% of memory-based cyberattacks."

Paul Weidow
President and Founder
Plex Corporation

Contact Us at:
sales-us@polyverse.com
sales-emea@polyverse.com
sales-apac@polyverse.com

or visit our website
https://polyverse.com