POLYVERSE

PRODUCT BRIEF

RE

Power Of Defense

DEFINE

Today's cybersecurity solutions are often complicated and expensive requiring companies to invest copious time and resources into securing their business. While each solution claims to be the "silver bullet" that will solve the security problem, each solution has failed to do so. Instead of building complex tools that attempt to constrain DevOps systems, Polyverse creates simple and intrinsic protections that works with innovation, not against.

Due to the fast-paced nature of modern development, company's software stacks are increasingly convoluted and include more and more components that originated elsewhere, for which there is little control. Even with having implemented multiple security tools, a single open-source vulnerability can take down organization at a global scale. Among common vulnerabilities, memory-exploiting zero-day attacks are the most difficult to defend against. This is the kind that gave us WannaCry, Spectre, and Equifax.

Why Should You Care?

7,217 CVEs in 2017 are of high or medium severity

80% involve memory exploitation

>50 person hours to patch a single vulnerability

Today, over **90%** of Fortune 1000 companies are late on patching

You do the math.

Polyverse's Moving Target Defense solution, Polymorphic Linux, is the **only cybersecurity product proven by the U.S. Department of Defense to stop 100 percent of zero-day memory exploits.**

Polyverse breaks industry complexity with Polymorphic Linux

Polyverse Polymorphic Linux randomizes and hardens open source Linux distributions using Moving Target Defense technology. By randomizing memory specifics of an application—crafted exploits targeting a specific memory vulnerability simply will not work, even when the application is left unpatched.

In addition, Polyverse leverages continuous deployment so you can receive new scrambled binaries every 12 hours. No patch? No problem. You are already protected.

Polyverse shifts power back to the defense

How does it work?

Instead of using the open source project, simply point to the Polyverse repo, and deploy with one line of command line code.

```
curl https://sh.polyverse.io | sh -s install <authkey> [<node_id>]
```

No change to the program functionality, performance, and interoperability. Get installed in under 2 minutes and stop memory-exploiting zero-day attacks immediately.

Supported Distributions	CentOS	Alpine	Ubuntu	Fedora

Do I still need to patch?

Patch for hygiene. Do not patch for security. No race against the clock. No risk for your business.

Talk is cheap, show me the code

https://polyverse.io/purchase/

RE
Power Of Defense
DEFINE