POLYVERSE

RE
Power Of Defense
DEFINE

Product Brief

In the CyberSecurity space, every defender struggles with the great power asymmetry. Without solving this asymmetry and shifting more power to the defense, we are losing the cyber war, one of the most important wars that we will fight in this modern era. So what is the asymmetry?

The great power asymmetry: To defend your system, you need to protect **every** application, eliminate **every** vulnerability, **every** minute of the day. Attackers only need to get through **1** app, **1** vuln, **1** time.

The problem is exacerbated by the proliferation of open source software. Not only a company’s software stack is getting more complex; it also includes more and more components originated elsewhere, for which you have little control.

A single open source vulnerability can take down organizations at a global scale. Amongst those, memory-exploiting zero-day attacks are the most difficult to defend against. This is the kind that gave us Wannacry, Petya, and the Equifax breach.

Polyverse Polymorphic Linux is the only solution that **protects you against 100% of the memory-exploiting zero-day attacks.**

Polyverse breaks the asymmetry with Moving Target Defense

Polyverse Polymorphic Linux uses Moving Target Defense to strategically randomize memory layouts of the target application to stop memory exploitation attacks. With Polyverse, crafted exploits targeting a specific memory vulnerability simply will not work, even when the application is left unpatched.

In addition, Polyverse can leverage continuous deployment to periodically reset the system back to a known good state. Continuously re-deploying clean images is cyber defense’s secret weapon - No patch? No problem. Just reset.

Why is this interesting?

7217 CVEs in 2017 are of high or medium severity

80% involve memory exploitation

>**50** man hours to patch a single vulnerability

You do the math.

Today: over **90%** of the Fortune 1000 are late on patching.

With Polyverse: 80% of the new vulnerabilities are simply not relevant, with or without patching. You are COMPLETELY protected against memory exploitation attacks.

Polyverse shifts power back to the defense

Start with open source applications today.

Polyverse Product	Techniques	Benefits
Polymorphic Linux	Randomizes the memory layout for the full Linux stack -- all 10,000+ open source projects in the Linux ecosystem.	Stops memory exploiting zero-day attacks from the get-go. No patching? No problem. Polymorphic Linux protects you intrinsically.
Advanced MTD	A set of sophisticated Moving Target Defense techniques that continuously reset the system back to a known good state	Makes threats/compromises non-persistent. Completely disables multi-stage attacks.

How does it work?

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

No change to the program functionality, performance, interoperability, and scale.

Do I still need to patch?

Patch for hygiene. Don't patch for protection.

No race against the clock. No patching compatibility risk.

Talk is cheap, show me the code

https://info.polyverse.io/free-tier

RE

Power Of Defense

DEFINE