MICRO FOCUS | POLYVERSE

On Point to Secure Vulnerabilities

"Houston, we have a problem."

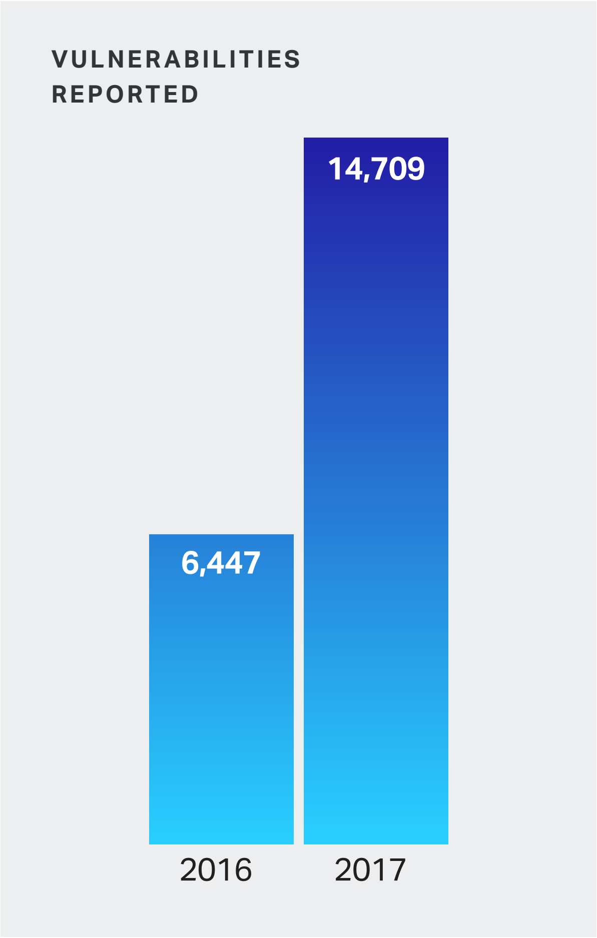
Securing your security information and event management (SIEM) software with polymorphic Moving Target Defense (MTD) technology

You don’t need to look further than the latest cyber breach headlines to see that securing code is an extremely difficult challenge to address, a challenge that shows no signs of easing. In 2016, the national vulnerabilities database reported 6,447 vulnerabilities. The following year, it smashed that record when more than double the number of Common Vulnerabilities and Exposures (CVEs) were reported, coming in at 14,709.

Some argue that securing code is simply not a priority in this fast-paced market where code has to be released in weeks instead of months. Others argue the monumental complexity of our code base is proportional to the number of security flaws lurking in the code.

It only took 400,000 lines of code to orbit earth in the space shuttle. But today, Microsoft Windows has 39 million lines of code. A typical new car now has over a 100 million lines of code. While these numbers are staggering, when one considers that one million lines of code is equivalent to 18,000 pages of printed text, it’s obvious that securing this code is no easy task and perhaps just not possible.

The question becomes, “Now what can you do to safeguard code?“ First, there are fundamental best practices that DevOps teams must follow. One is to employ a quality source code analyzer like Fortify SCA and Fortify WebInspect, which are invaluable in identifying high-priority flaws that may need remediation. For applications already in production, Fortify Application Defender can provide continuous monitoring, perform deep security scans, and protect applications in real time. Moving from a reactive security posture to a proactive one is the necessary first step. Our adversaries won’t go down that easy. This is where Polyverse and the theory of Moving Target Defense (MTD) enters the world of software security.


VULNERABILITIES REPORTED

SO MUCH CODE—SO MANY VULNERABILITIES

Orbiting Earth
400,000
lines of code

Microsoft Windows
39M
lines of code

Typical New Car
100M+
lines of code

Adding MTD to Your Defensive Strategy

The Department of Homeland Security stated, "MTD assumes that perfect security is unattainable. Given that starting point, and the assumption that all systems are compromised, research in MTD focuses on enabling the continued safe operation in a compromised environment and to have systems that are defensible rather than perfectly secure."

If every deployed operating system or application could be unique in their binaries, function locations, CPU registers, and memory layouts, it would be incredibly difficult for attackers to deconstruct that uniqueness to compromise their targets. This is due to the fact that many modern attacks are fully automated -- spraying the internet with discovered vulnerabilities on the assumption that all of their intended victims run identical code. Enter Polyverse, one of the only companies in the world that has successfully implemented the MTD theory on an enterprise scale.

Polyverse's Moving Target Defense solution stops 100 percent of zero-day memory exploits because it is powered by the Polyverse polymorphic version of Linux, which constantly scrambles unique location instructions. For example, their polymorphic version of Linux randomizes and hardens open source Linux distributions creating a constantly changing attack surface that is extraordinarily difficult for attackers to penetrate. Using their polymorphic compiler, they can dynamically change register usage, function locations, import tables, and so on to produce individually unique binaries that are semantically equivalent. When this strategic entropy is introduced to each and every production system, the attacker's window of opportunity is reduced or eliminated. And all of this can be deployed on a typical Linux stack in less than 5 minutes.

Polyverse provides the only Moving Target Defense cybersecurity product proven by the U.S. Department of Defense to stop 100 percent of zero-day memory exploits (buffer overflow, etc.).

STOPS

100%

of zero-day memory exploits

ArcSight ESM: The first MTD Fortified SIEM

Micro Focus, a recognized leader in the security space, has collaborated with Polyverse to bring the first MTD-protected SIEM to market with ArcSight running on a Polyverse MTD platform. SIEMs are the foundation for today's intelligent security operations centers (SOCs). The ArcSight ESM SIEM collects logs from across the enterprise and processes those events in real-time through its ArcSight Correlation Engine. To facilitate data analytics and the identification of indicators of compromise (IOCs), it's essential to have all logs centrally located and secured. Micro Focus and Polyverse are announcing the first integration of SIEM technologies with Polyverse's code scrambling and polymorphic MTD technologies to protect those organizations with the highest security requirements, such as those within the intelligence community and the Department of Defense.

Protecting against the unknown is difficult. When you are up against nation state actors with vast resources, you often need to take extra measures in building the layered defenses required to protect critical enterprise applications. Our collaboration with Polyverse is leading the way to new best practices and defensive strategies in protecting our largest businesses and our nation's security.

To learn more about how you can enhance your defensive layers with an MTD-secured SIEM, contact your Micro Focus ArcSight sales representative.

1. Dragan Radovanovic and Kif Leswing. "Google's services are powered by 5000 times more code than the space shuttle." Business Insider. Jul. 21, 2016. http://www.businessinsider.com/google-runs-on-5000-times-more-code-than-the-space-shuttle-2016-7

2. Doug Newcomb. "The Next Big OS War Is in Your Dashboard." Wired. December 3, 2012. https://www.wired.com/2012/12/automotive-os-war/

3. U.S. Department of Homeland Security, https://www.dhs.gov/science-and-technology/csd-mtd