OWN YOUR SOFTWARE SUPPLY CHAIN

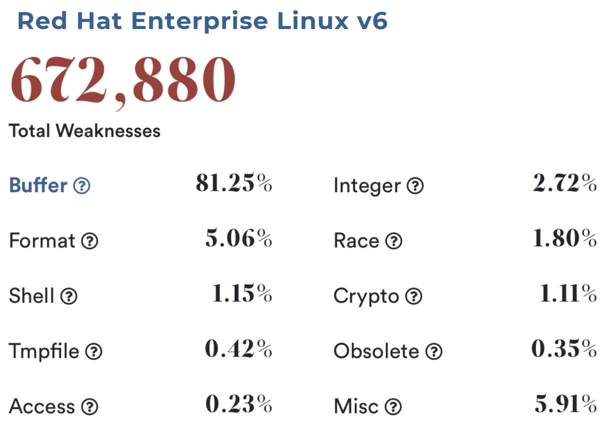
Providing DOD/NAVSEA 100% supply chain integrity and accountability

THE PROBLEM

The government is using Linux from any one of 15,000 or more servers, controlled by various entities, in countries around the world. This means there is little integrity or control over the supply chain, or visibility and accountability for what operating system (OS) or patches are running on any given system.

Today, the DOD procures operating systems from various vendors, often through third-party integrators or system manufacturers.

> **MULTIPLE TEST TEAMS REPORTED USING FREE, PUBLICLY AVAILABLE INFORMATION OR SOFTWARE DOWNLOADED FROM THE INTERNET TO AVOID OR DEFEAT WEAPON SYSTEM SECURITY CONTROLS.**
>
> THE GAO WEAPON SYSTEMS CYBERSECURITY REPORT



Red Hat Enterprise Linux v6

672,880

Total Weaknesses

Buffer	81.25%	Integer	2.72%
Format	5.06%	Race	1.80%
Shell	1.15%	Crypto	1.11%
Tmpfile	0.42%	Obsolete	0.35%
Access	0.23%	Misc	5.91%

THE SOLUTION

A build farm will provide the DOD with complete, end-to-end source code, and 100% guaranteed ability to create and update the entirety of those operating systems, as needed.

- ✓ Real-time vulnerability management
- ✓ Centralized distribution for all OSs
- ✓ Accountability of patching levels for all OSs
- ✓ Track and monitor software provenance
- ✓ Point-in-Time Caching (PTC): Lock in a configuration at a specific time and patch level for the life of the system, and rebuild it at any time with zero interdependency issues

POLYVERSE BUILD FARM

Polyverse currently runs the world's largest build farm built and maintained by senior engineers who ran infrastructure at Azure, Amazon, Microsoft, and Ask.

Polyverse.com | +1 855-765-9837 | info@polyverse.com

OWN YOUR SOFTWARE SUPPLY CHAIN

Providing DOD/NAVSEA 100% supply chain integrity and accountability

THE POLYVERSE BUILD FARM

Capability	With Polyverse	Without Polyverse
Central distribution for all operating systems (OSs)	✓	✗
Accountability of patching levels	✓	✗
Reliance on third-party vendors to update and patch	✗	✓
Polymorphic operating system	✓	✗
Real-time vulnerability management	✓	✗
Exact same software as adversaries	✗	✓
Point-in-Time Cache	✓	✗
Protections when unpatched	✓	✗
Track and monitor providence of software	✓	✗

POLYVERSE ENABLES THE FOLLOWING COMPLIANCE FRAMEWORKS

AICPA

CIS Security Controls "Sans Top 20"

CMS Information Security ARS

Cyber Resilience Review V2016

CSA Cloud Controls Matrix v3.01

State of Nevada - SPI (NRS 603A)

PCI DSS

TX Health Services Code (TX HB 300)

Massachusetts Data Protection Act

CAQH CORE

FEDRAMP

FFIEC v2016

HIPPA

HITRUST Framework v1

NIST SP 800-53 R4

COBIT

ISO 27799:2008 7.7.4.1

NIST Critical Infrastructure v1

ISO/IEC 27002:2013

ISO/IEC 27002:2005

THERE ARE NO SILVER BULLETS

However, with Polyverse, mitigate the entire class of memory-based attacks, which have been identified by MITRE's as the most dangerous software error to date. By implementing a build farm, we can win the cyber war and get 100% supply chain integrity and accountability.

Polyverse.com | +1 855-765-9837 | info@polyverse.com