OWN YOUR SOFTWARE SUPPLY CHAIN

Providing enterprises 100% supply chain integrity and accountability

THE PROBLEM

Enterprise companies are using Linux from any one of 15,000 or more servers, controlled by various entities, in multiple countries around the world.

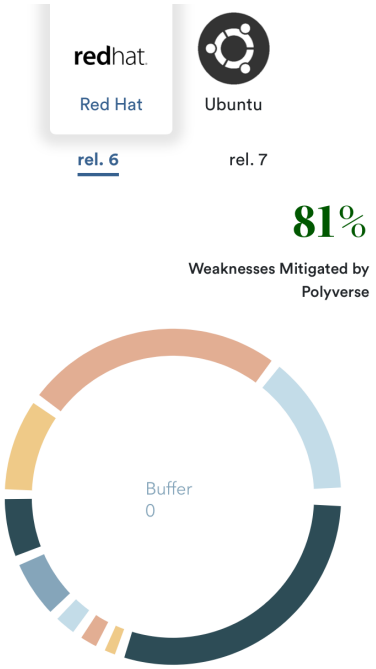
This means that there is no integrity or control over the supply chain, or visibility and accountability for what operating system (OS) or patch level is running on any given system.

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 companies 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 providence
- 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 that is 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 enterprises 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	FEDRAMP
CIS Security Controls "Sans Top 20"	FFIEC v2016
CMS Information Security ARS	HIPPA
Cyber Resilience Review V2016	HITRUST Framework v1
CSA Cloud Controls Matrix v3.01	NIST SP 800-53 R4
State of Nevada - SPI (NRS 603A)	COBIT
PCI DSS	ISO 27799:2008 7.7.4.1
TX Health Services Code (TX HB 300)	NIST Critical Infrastructure v1
Massachusetts Data Protection Act	ISO/IEC 27002:2013
CAQH CORE	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 one most dangerous software error to date.

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