Closing the Last Blind Spot in Enterprise Vulnerability Management

Bringing HPE Nonstop into Qualys & Tenable workflows

Steve Tcherchian | CEO

XYPRO®
Mission Critical Security

About XYPRO

Trusted by global banks, payment networks, and governments for 40+ years

Global 24x7 Operation

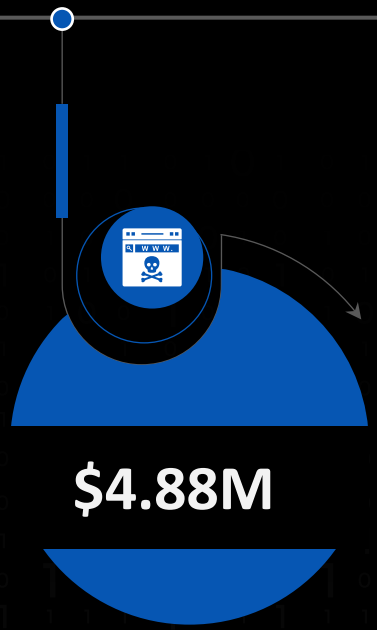
Fluent in over 25 languages, we provide personalized, region-specific expertise.

Your Cybersecurity Partner

XYPRO is the trusted leader in cybersecurity and regulatory compliance for complex workloads and environments.

Hewlett Packard Enterprise | XYPRO Mission Critical Security

Why This Matters



$4.88M

Global average cost of a breach

Prioritized vulnerability management is the most cost effective control you own

~296k CVEs tracked
~25k awaiting analysis

1,350 exploited CVEs in CISA's KEV today

up from 1,199 in Aug 2024 (~+12% YoY)—with new entries added this week; prioritize KEV first.

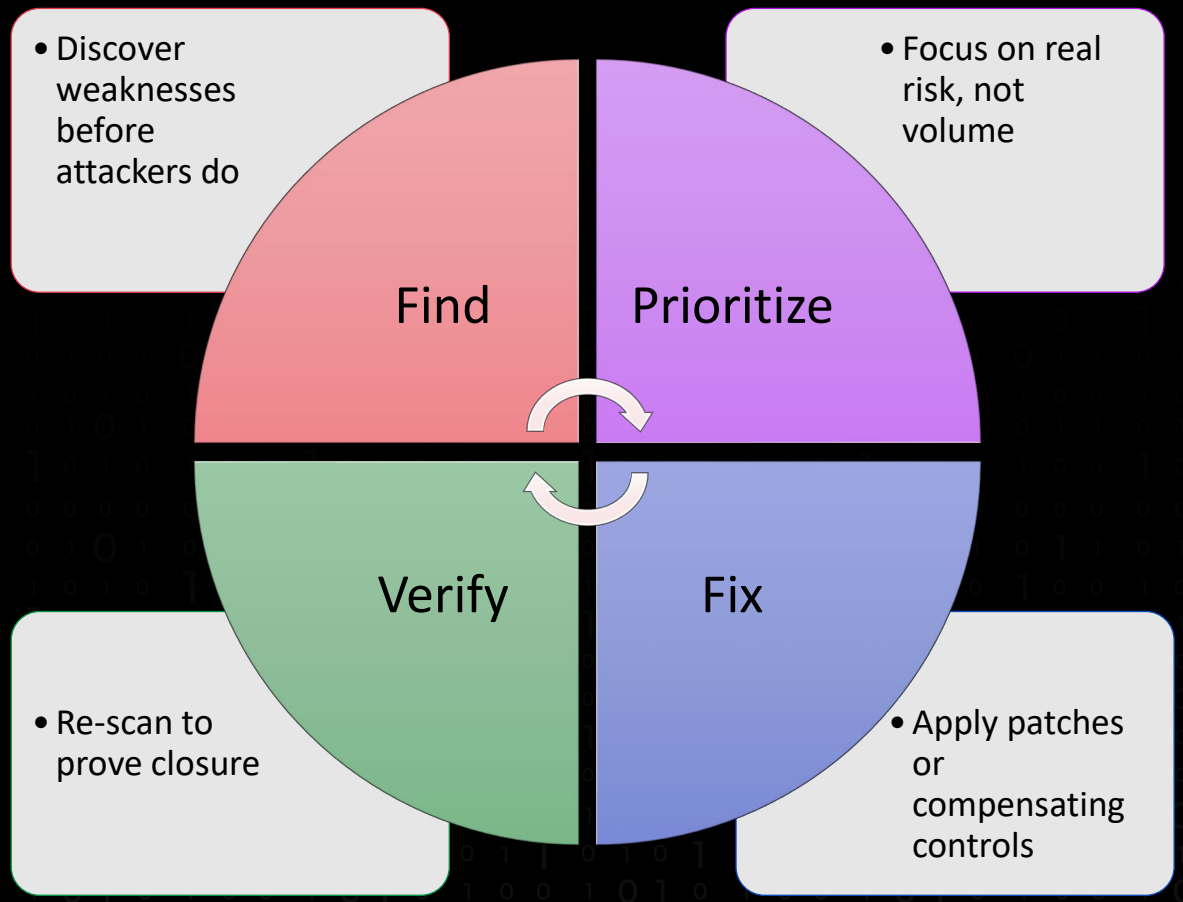
Compliance

PCI DSS 4.0.1

Requires regular authenticated vulnerability scanning (quarterly+)

Vulnerability Management

If you can’t prove you scanned it, you didn't



Why pay attention

Attackers iterate faster than change control.
Regulators expect evidence, not intentions.

What “good” looks like

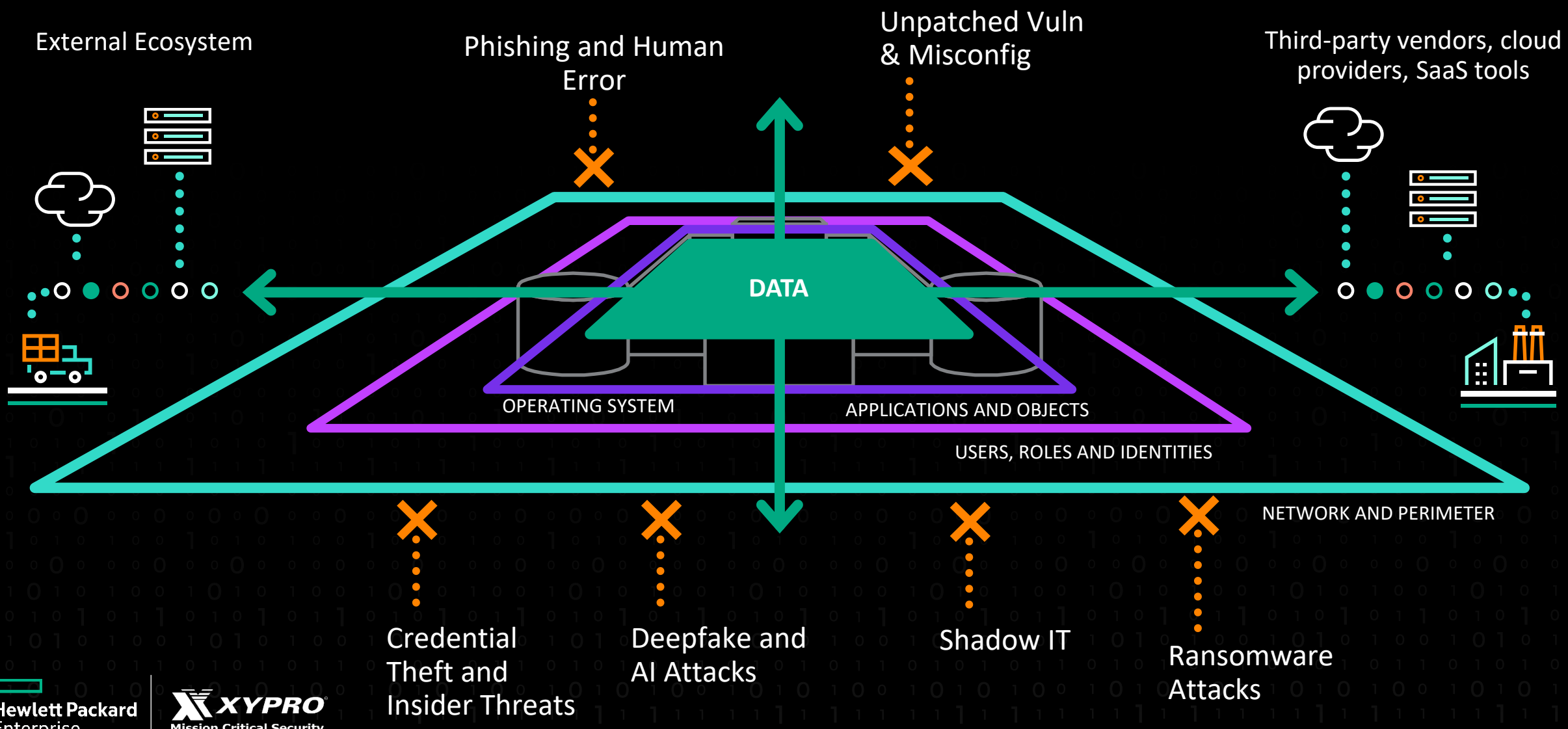
Authenticated scans (incl. Nonstop), KEV-first triage, clear owners/SLA, re-scan to prove closure.

For HPE Nonstop

Close the blind spot—plug Nonstop into your existing VM/ITSM. Same queue, same metrics, less exception debt and manual process)

Hewlett Packard Enterprise | XYPRO Mission Critical Security

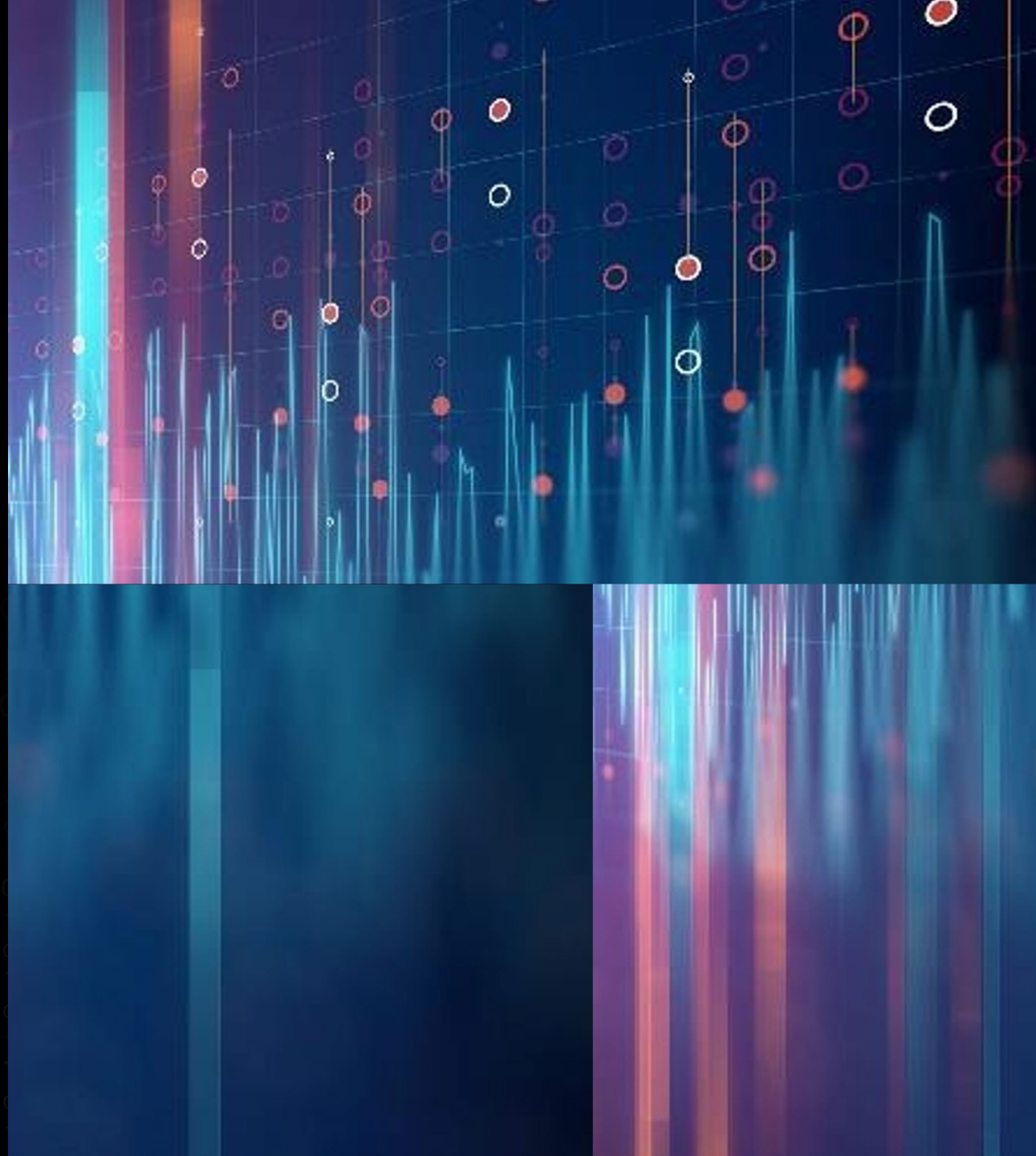
The Shift: From Perimeter to Zero Trust



Hewlett Packard Enterprise | XYPRO Mission Critical Security

Vulnerability Management for HPE Nonstop

XYGATE Aegis Scan



Hewlett Packard Enterprise | XYPRO Mission Critical Security

What “Good” Vulnerability Management Looks Like

1. Know

See it, Secure it

Map every OS, HPE component, version, owner, and business criticality.

2. Shrink

Harden Before You Hunt

Harden configs, secure baselines, remove EOL/EOS software, and patch routinely.

3. Find

Continuous Eyes, Zero Gaps

Run authenticated scans to uncover vulnerabilities and misconfigs

4. Fix

Cut Time, Contain Impact

Prioritize by exploitability and business risk, act fast, and prove closure with re-scans.

5. Prove

Evidence Beats Excuses

Generate auditable proof for regulators and leadership that issues are fixed, risks reduced, and systems hardened.

Why Most VM Programs Fail

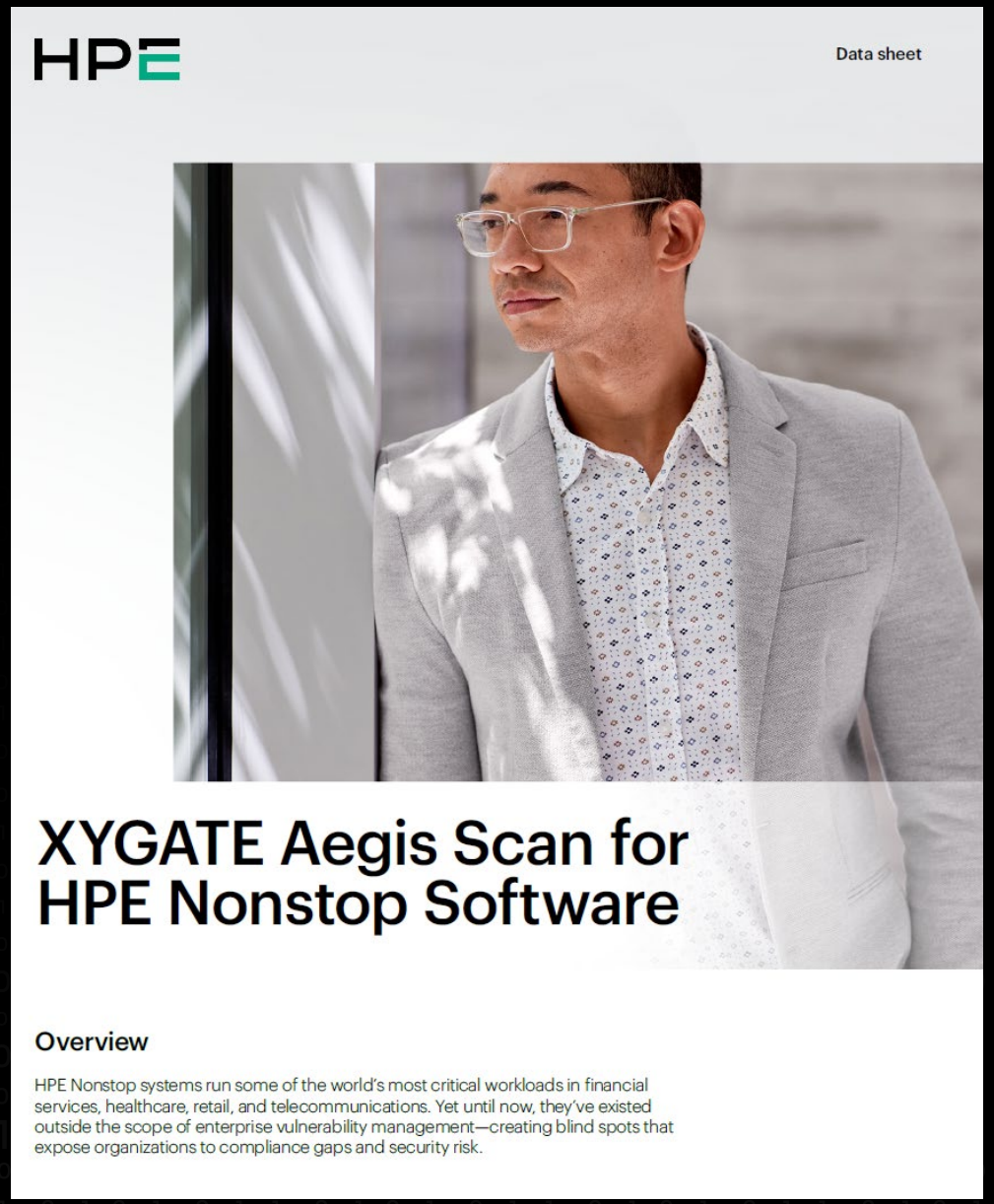
(and what you should do different)

1. Too Many Tools
   - Duplicate findings
   - False positives

2. No Risk Context
   - CVSS ≠ Business Risk
   - Wrong prioritization; without context, teams chase the wrong work.

3. Technical Debt
   - EOL/EOS systems
   - No patch path

Teams spend more time managing tools than reducing risk



Closing the Gap with XYPRO and HPE

- Purpose built for HPE Nonstop
- Lightweight, agent-based scanner
- Scans Nonstop OS + HPE-provided software and maps to CVEs
- Outputs in standard formats (CSV / XML / JSON)
- Seamless integration with Qualys and Tenable (coming soon)
- Designed with HPE – optimized performance, secure by default

Qualys®

tenable™

Hewlett Packard Enterprise | XYPRO Mission Critical Security

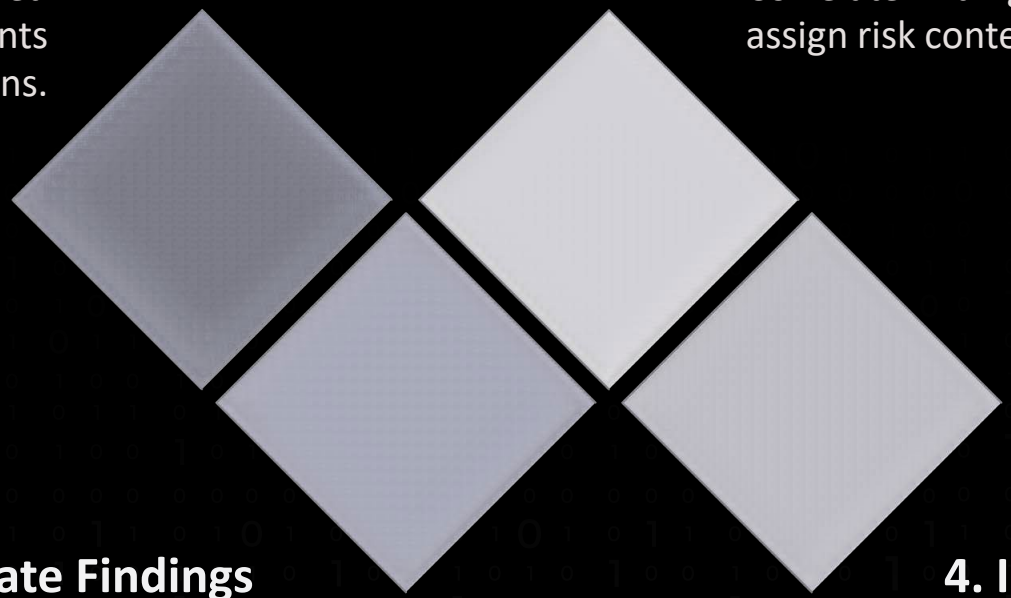
How XYGATE Aegis Scan Works

1. Scan Components

Scan OS and HPE-provided software components and versions.

2. Map to CVEs

Correlate findings to CVEs and assign risk context.



3. Generate Findings

Create report with remediation guidance in standard formats.

4. Integrate Results

Feed Nonstop results to VM platforms for resolution and compliance.

XYGATE Aegis Scan closes the HPE Nonstop blind spot by deploying a lightweight agent that scans the OS and HPE-provided software, maps findings to CVEs, and outputs structured data for seamless ingestion into your existing Qualys or Tenable vulnerability management workflows.

2
Total Assets

Search for assets...

All Time

TOP HARDWARE CATEGORIES

TOP OPERATING SYSTEMS CATEGORIES

QUICK FILTERS

MANUFACTURER
Unidentified 2

TAGS
Generic CSV 2

SOURCES
Generic CSV 2

Actions (0) | All | Managed | Unmanaged | Group By

1 - 2 of 2

NAME	CRITICALITY	TruRisk™Score	OPERATING SYSTEM	HARDWARE	LAST USER	SOURCES	MODULES	TAGS
\AEGIS1	3	197	L25.02.00	HPE Non...	-	4 more First Found: A... Last Seen: Sep 0...	CSAM	Generic CSV
\AEGIS2	3	376	L25.02.00	HPE Non...	-	3 more First Found: A... Last Seen: Sep 0...	CSAM	Generic CSV

← Asset Details: **\AEGIS2**

INVENTORY
- Asset Summary
- System Information
- Network Information
- Open Ports
- Installed Software
- Software Instances
- Traffic Summary
- Business Information

SECURITY
- TruRisk™ Score
- Threat Protection
- Certificates

SOURCES
- Summary
- Passive Sensor
- CAPS
- Alert Notification
- Generic CSV

Asset Summary

\AEGIS2 (edited)

Criticality Score: 3 | TruRisk™ Score ⓘ: 197

OS: L25.02.00 | Hardware: HPE Nonstop

Identification

Hostname \AEGIS2	FQDN aegis2.xypro.com	NetBIOS Name -
IPv4 Addresses 10.1.1.229	IPv6 Addresses -	Asset ID 946828738
Host ID 089481	Company XYPRO	Department -
Owner/Custodian -	Environment -	
Assigned Location Simi Valley, CA		

Activity

Last User Login xypro.aegis2	Last System Boot 21 Aug 2025, 14:49:47	Created On 7 days ago 04:00 PM
Last Updated a day ago 10:58 AM	Last Activity -	

Last Location

Tags Add Tags

Generic CSV ⋮

Asset Details: \AEGIS2

INVENTORY
- Asset Summary
- System Information
- Network Information
- Open Ports
- Installed Software
- Software Instances
- Traffic Summary
- Business Information

SECURITY
- TruRisk™ Score
- Threat Protection
- Certificates

SOURCES
- Summary
- Passive Sensor
- CAPS
- Alert Notification
- Generic CSV

Search Vulnerabilities...

Group By: ... | Filters (3)

1 - 50 of 61

TITLE	QDS	SOURCES	LIFECYCLE
CVE-2024-31227: Redis Denial-of-Service via Malformed ACL Select... Confirmed CVE-2024-31227	37		First Found: a day ago Active
Stack Buffer Overflow in Redis Lua 'bit' Library via Crafted Lua Script... Confirmed CVE-2024-31449	42		First Found: a day ago Active
OpenSSL Use-After-Free Vulnerability (CVE-2024-4741) in SSL_free_... Confirmed CVE-2024-4741	35		First Found: a day ago Active
CVE-2024-9143: High-Severity Vulnerability in OpenSSL Low-Level G... Confirmed CVE-2024-9143	30		First Found: a day ago Active
CVE-2023-41056: Critical Heap Overflow Vulnerability in Redis Allow... Confirmed CVE-2023-41056	35		First Found: a day ago Active
CVE-2023-45853: Critical Heap-Based Buffer Overflow in MiniZip (zli... Confirmed CVE-2023-45853	65		First Found: a day ago Active
CVE-2023-45145: Redis Improper Privilege Management - Unix Sock... Confirmed CVE-2023-45145	20		First Found: a day ago Active
CVE-2024-31228: Redis Denial-of-Service via Unbounded Pattern M... Confirmed CVE-2024-31228	30		First Found: a day ago Active
CVE-2024-51741: Redis Server Denial-of-Service via Malformed ACL... Confirmed CVE-2024-51741	30		First Found: a day ago Active
CVE-2023-45853 Confirmed No CVE Assigned	40		First Found: 6 days ago Active
CVE-2024-0397	40		First Found: 6 days ago

Business Impact

Eliminate Exceptions and Manual Effort

Before XYGATE Aegis Scan

- ❌ Manual tracking
- ❌ No visibility or evidence
- ❌ Audit challenges
- ❌ Slow/No remediation

After XYGATE Aegis Scan

- ✅ Full visibility
- ✅ Automated workflows
- ✅ Audit-ready reporting
- ✅ Enterprise integration

Faster remediation | Reduced risk | Compliance

Hewlett Packard Enterprise | XYPRO Mission Critical Security

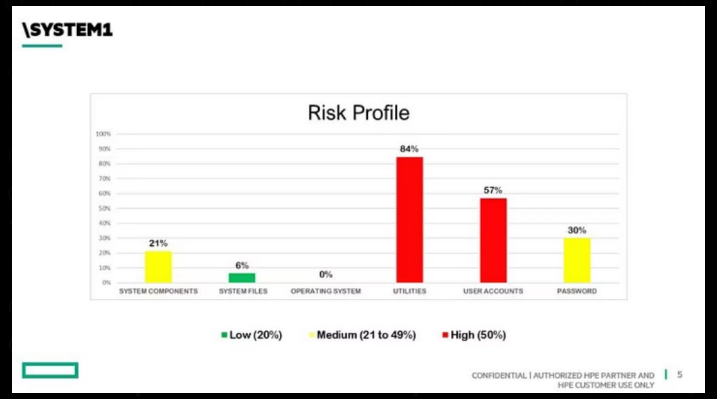
FREE Security Assessment!

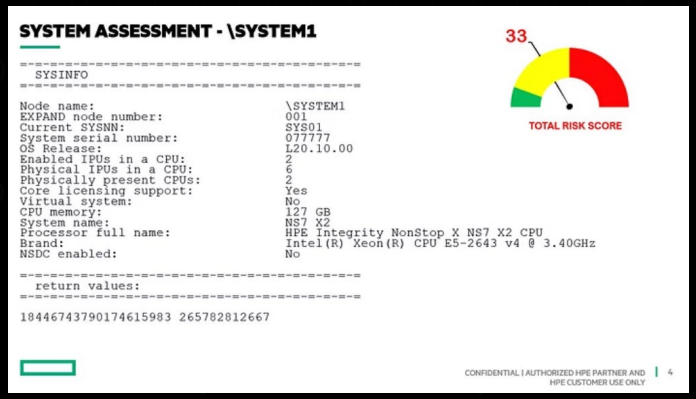
Understand Your Exposure – No Cost, No Disruption

RAPID SECURITY ASSESSMENT

xypro.com/free

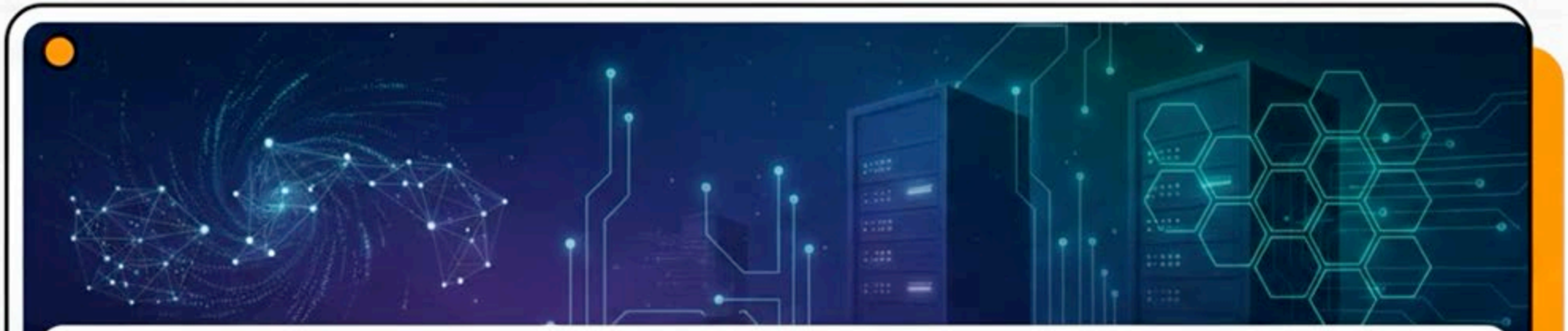
- Expose Hidden Risks – Identify vulnerabilities and misconfigurations
- 120+ different security vectors evaluated in 6 key categories
- No install, no delay – quick time to insight
- Get a prioritized roadmap to tighten your defenses
- **NO COST!**





Hewlett Packard Enterprise | XYPRO Mission Critical Security

Closing the Blind Spot



THANK YOU

Sign up for our free security assessment www.xypro.com/free

Visit XYPRO	www.xypro.com
YouTube	youtube.com/xyprotechnology
LinkedIn	linkedin.com/stevetch linkedin.com/xyprotechnology

Hewlett Packard Enterprise | XYPRO Mission Critical Security