Vulnerability Management

Strategy & Execution Samples

PAGE 1 The Executive Brief (FAIR-Driven Strategy)

Monthly Vulnerability Landscape – Q1 Infrastructure

Objective

Translate technical exposure into measurable business risk, enabling executive-level decision making and optimized resource allocation.

Key Metrics

- **1,200 vulnerabilities identified** across infrastructure assets
- **Reduced to 12 critical priorities** using FAIR-based risk quantification
- **~99% noise reduction**, enabling focused remediation

Strategic Insight

Risk concentration analysis revealed that **70% of the total exposure** was tied to **legacy systems nearing end-of-life**.

Instead of allocating resources toward short-term patching cycles with low ROI, a **strategic pivot** was executed:

- Mapped vulnerable assets to the **Decommissioning Program**
- Eliminated redundant remediation effort on soon-to-be-retired systems
- Prioritized high-impact, business-critical exposures

Business Outcome

- **40% reduction in infrastructure team workload**
- Improved alignment between **security operations and IT strategy**
- Shift from reactive patching to **risk-informed decision making**

Executive Dashboard (Placeholder)

[RESERVED SPACE — EXECUTIVE DASHBOARD SCREENSHOT]

The Technical Ticket (The Remediation Standard)

[CRITICAL] RCE in OpenSSL (CVE-2023-XXXX)

Objective

Demonstrate operational excellence by delivering **actionable, low-friction remediation guidance** that reduces Mean Time To Remediate (MTTR).

Technical Context

- Vulnerability: Remote Code Execution (RCE) in OpenSSL
- Scope: **14 internet-facing load balancers**
- Exposure: Port 443 (HTTPS)
- Risk: High likelihood of exploitation with significant impact on service availability and data integrity

---

Remediation (Execution-Ready)

Instead of generic guidance, remediation is delivered as **directly executable action**:

yum update openssl

- No ambiguity
- No additional research required by infrastructure teams
- Immediate applicability across affected assets

Validation Strategy

To ensure closure integrity and eliminate manual follow-ups:

- Created dynamic tag: **"Scan on Demand – Critical Assets"**
- Automated validation workflow:

- Infra team applies patch
    1. Scan triggered automatically
    2. Vulnerability status verified
    3. Ticket closed based on evidence

Operational Impact

- Reduced MTTR through **clarity and automation**
- Increased trust between Security and Infrastructure teams
- Standardization of remediation lifecycle

Patch Management Evidence (Placeholder)

[RESERVED SPACE — QUALYS PATCH MANAGEMENT SCREENSHOT]

The CSAM Insight (Visibility & Shadow IT)

Asset Intelligence & Cloud Visibility

Objective

Demonstrate advanced capability in identifying and securing **unknown and unmanaged assets (Shadow IT)**.

Discovery Scenario

Through continuous asset discovery and correlation:

- Identified **22 instances running Python 2.7**
- Located within **isolated AWS VPCs**
- Assets were:
    - Not onboarded to security tooling
    - Missing Cloud Agents
    - Invisible to standard vulnerability scans

Risk Implication

- Unsupported runtime (Python 2.7 EOL)
- High exposure due to lack of monitoring
- Potential lateral movement entry points

Remediation Strategy

1. Visibility Enablement

- Integrated AWS environment via **AWS Connector**
- Enabled continuous synchronization of cloud assets

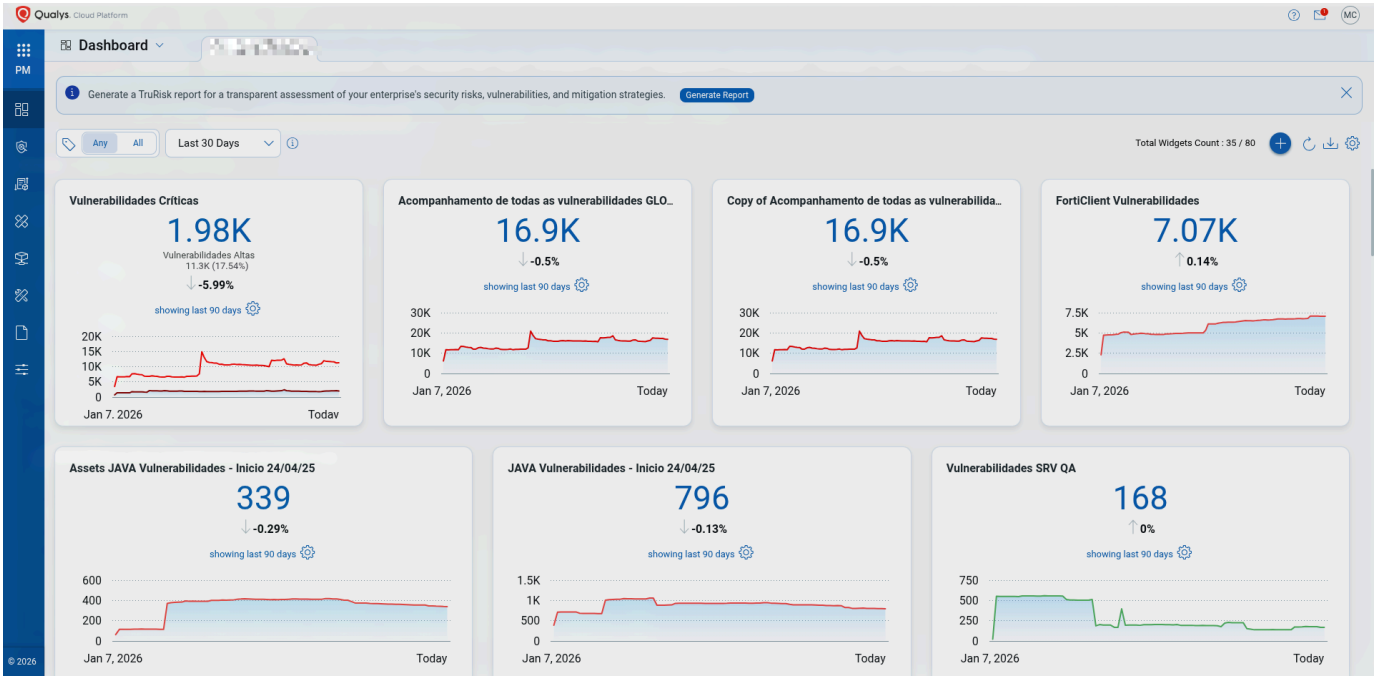
2. Control Enforcement

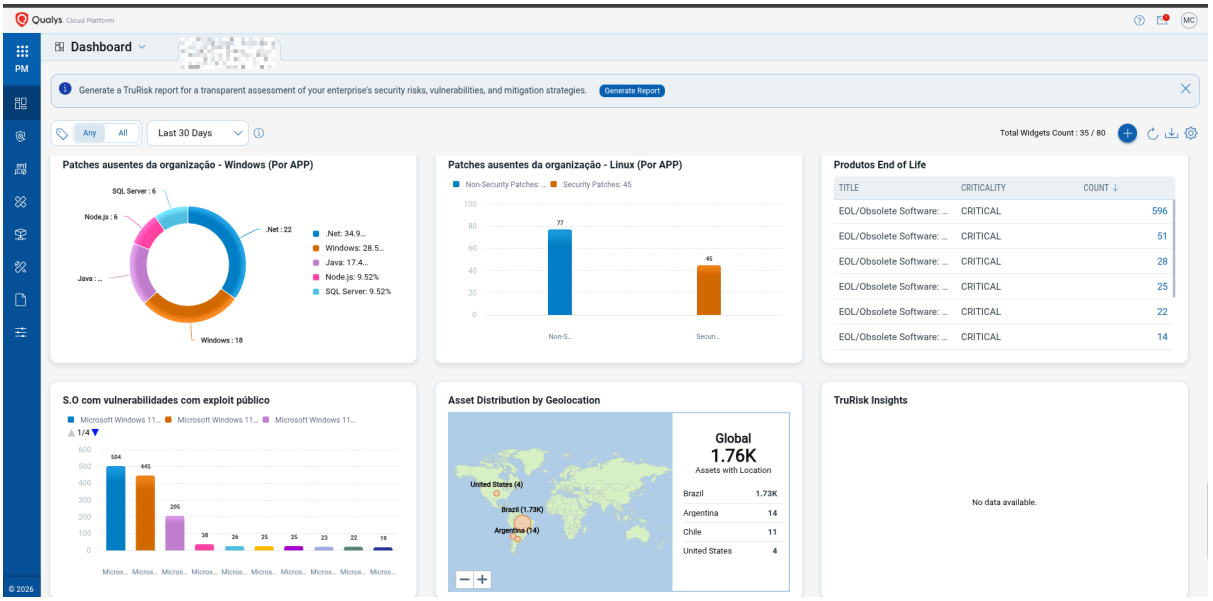
- Automated deployment of **Qualys Cloud Agents** using Terraform
- Standardized onboarding pipeline for all cloud resources

3. Continuous Monitoring

- Assets broug ht into centralized vulnerability management lifecycle
- Real-time visibility and compliance enforcement

Prints Dashboards




Qualys. Cloud Platform
Dashboard
PM
Generate a TruRisk report for a transparent assessment of your enterprise's security risks, vulnerabilities, and mitigation strategies.
Generate Report
Any
All
Last 30 Days
Total Widgets Count : 35 / 80
Patches ausentes da organização - Windows (Por APP)
SQL Server : 6
Node.js : 6
.Net : 22
Java : ...
Windows : 18
.Net: 34.9...
Windows: 28.5...
Java: 17.4...
Node.js: 9.52%
SQL Server: 9.52%
Patches ausentes da organização - Linux (Por APP)
Non-Security Patches: ...
Security Patches: 45
100
80
60
40
20
0
77
45
Non-S...
Securi...
Produtos End of Life
TITLE
CRITICALITY
COUNT
EOL/Obsolete Software: ...
CRITICAL
596
51
28
25
22
14
S.O com vulnerabilidades com exploit público
Microsoft Windows 11...
Microsoft Windows 11...
Microsoft Windows 11...
1/4
600
500
400
300
200
100
0
504
445
265
38
26
25
25
23
22
19
Micros...
Asset Distribution by Geolocation
United States (4)
Brazil (1.73K)
Argentina (14)
Global
1.76K
Assets with Location
Brazil
1.73K
Argentina
14
Chile
11
United States
4
TruRisk Insights
No data available.
© 2026