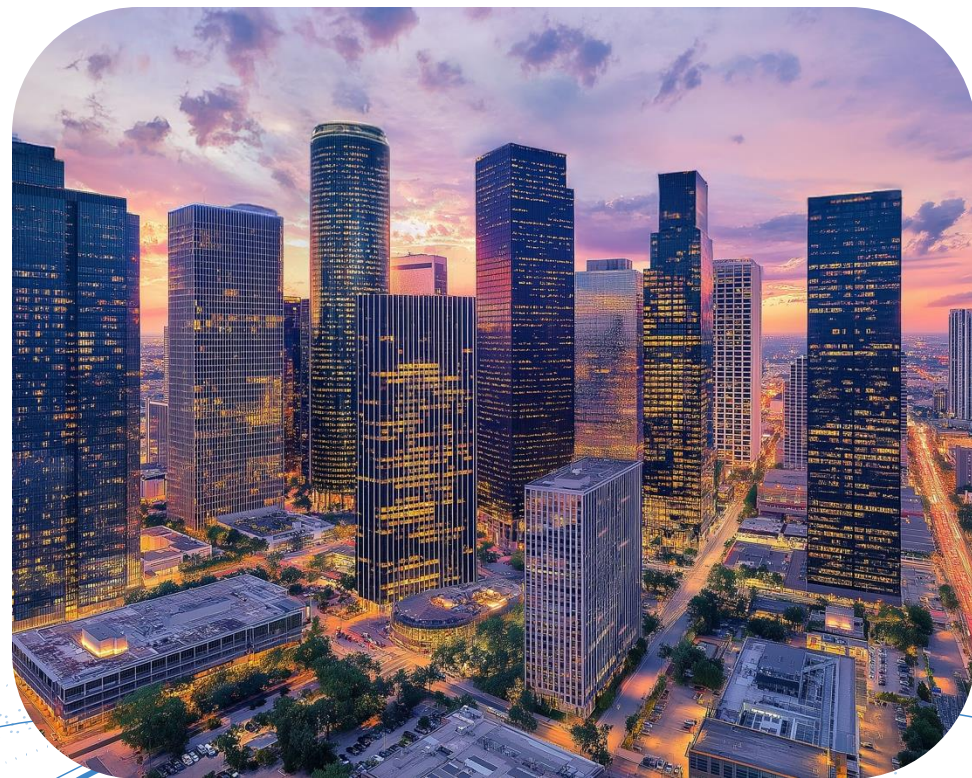


Eliminate the Risk of Audit Failure



Anu Kapil

Senior Manager,
Product Compliance Solutions



The Two Core Risks Every Organization Faces



Risk of Audit Failure

33%+ organizations face audit gaps each year



Risk of Misconfiguration

60% of breaches stem from misconfigs (Verizon DBIR)

One stops your business. The other exposes it.

Cost of Maintaining Compliance is too high

14B



Global fines for
non-compliance
hit **in 2024**

230



Workdays/year
spent on Audit
prep

2x



Audit fees have
doubled over the
last 5 years -
Gartner

Cost of non-compliance - Business comes to a halt

Staying Audit Ready is challenging



Staying Audit Ready is a Moving Target

- ✓ Evolving mandates – NIS2, PCI 4.0, and more
- ✓ In-scope technologies tend to increase with increased attack surface



Manual Compliance Efforts Can't Keep Up

- ✓ Increased Audit Frequency
- ✓ Mapping security exposures to compliance requirements



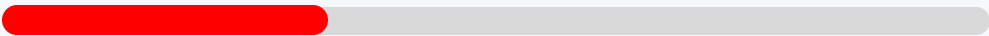
Non-Compliance has consequences

- ✓ Non-compliance costs 2.7× more than compliance — \$14.8 M vs. \$5.5 M per year on average
- ✓ Reputation Damage, loss opportunities, disruption

Top Audit Gaps in US

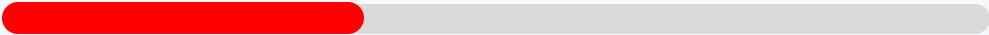


33.15%

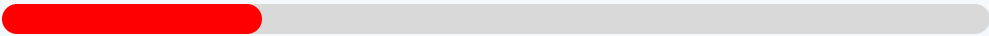


NIST

36.72%



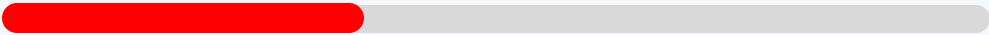
24%



49%



36.2%



36.18%



Risk of Misconfigurations

60%

of breaches stem from
Misconfigurations

99%

of cloud failures are caused
by user error (Gartner)

4.4M

Average cost per
misconfiguration-related
breach

58%

Enterprise network with at
least one critical
misconfiguration

**“One in every
three
configuration
checks reveals
a potential
weakness.” –
Verizon DBIR
2025**

Two Sides of Risk — One Unified Solution **Policy Audit**

Run Cyber Program as a ROC



How will you be
ROC Ready from Day 1

Qualys Policy Audit



Continuous Audit Readiness

Automated compliance monitoring always keeps organizations audit-ready



Proactive Gap Analysis

Identify and address compliance gaps early to avoid last-minute issues.



Risk Based Prioritization

Ensure audit-readiness by adhering to regulatory requirements requiring continuous risk analysis.



Streamline Audit Operations

Fix audit issues with ServiceNow Integration and accelerate time to value with seamless onboarding and end-to-end operationalization



Automated Audit-ready reports

Reduce manual efforts with always audit ready reports



Audit-Ready Reports

Why: Maintain Continuous Compliance



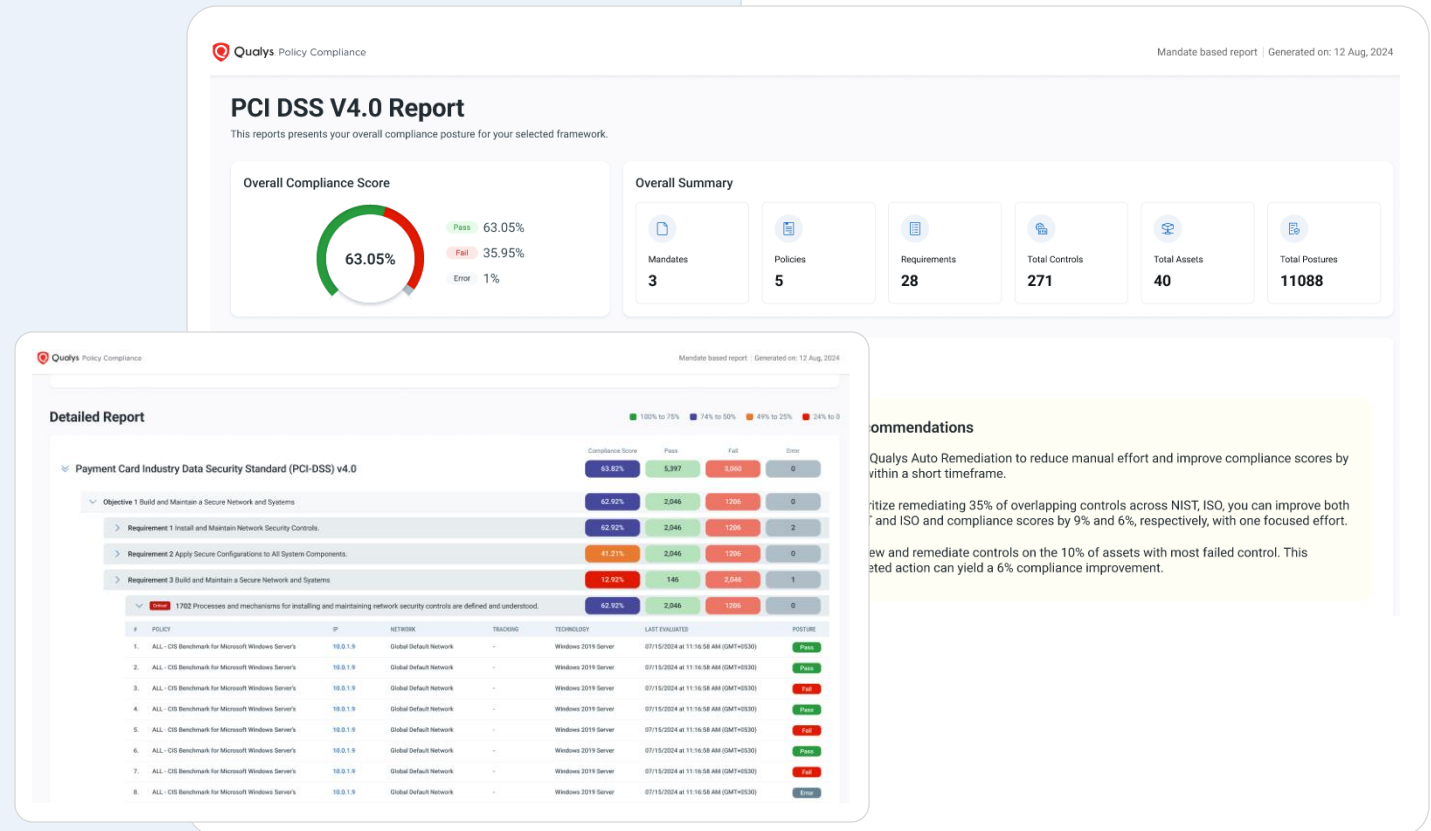
Effortless audit ready reports with Pre-built library of 100+ mandates mapped to controls

Automatically generate multiple reports from a single data collection

Custom reports for on-demand audits

Executive level and audit stakeholder ready reports to **prove compliance**

Reduce audit resources and costs by 50%



Executive Audit-Readiness Report



Audit-ready awareness with insights into gaps

Detailed Stakeholder Reports

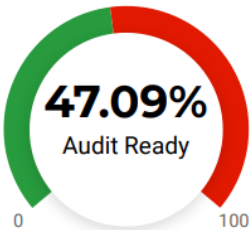
View a **high-level summary of your audit** and security posture.

Prescriptive guidance on how to **improve audit-readiness scores**

Audit Readiness for NIST 800-53 (Special Publication)

Selected Asset Tags:

Unassigned Business Unit | Cloud Agent | Asset Groups | AZURE-SD-CAP | GCP-SD-CAP



Total Assets
2925



Unique Controls
8070

Audit Gaps

50.43%

1538.9k of 3051.3k
Total Audit Gaps

44.49%

684.6k of 1538.9k
Critical Audit Gaps

Critical

Asset Summary

72.03%

2.1k of 2.9k
Assets with Audit Gaps

99.95%

2.1k of 2.1k
Assets with Critical Audit Gaps

Critical

Comprehensive visibility across your Asset landscape

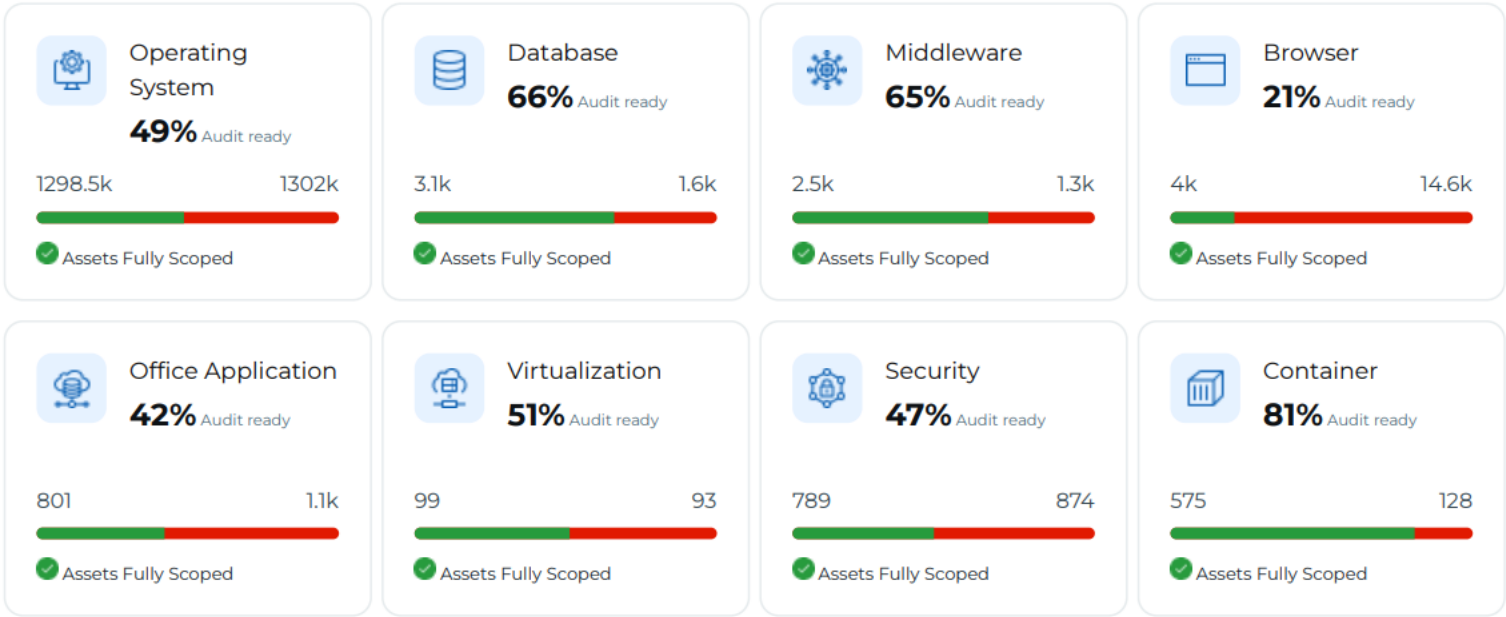


Audit-readiness for your inventory

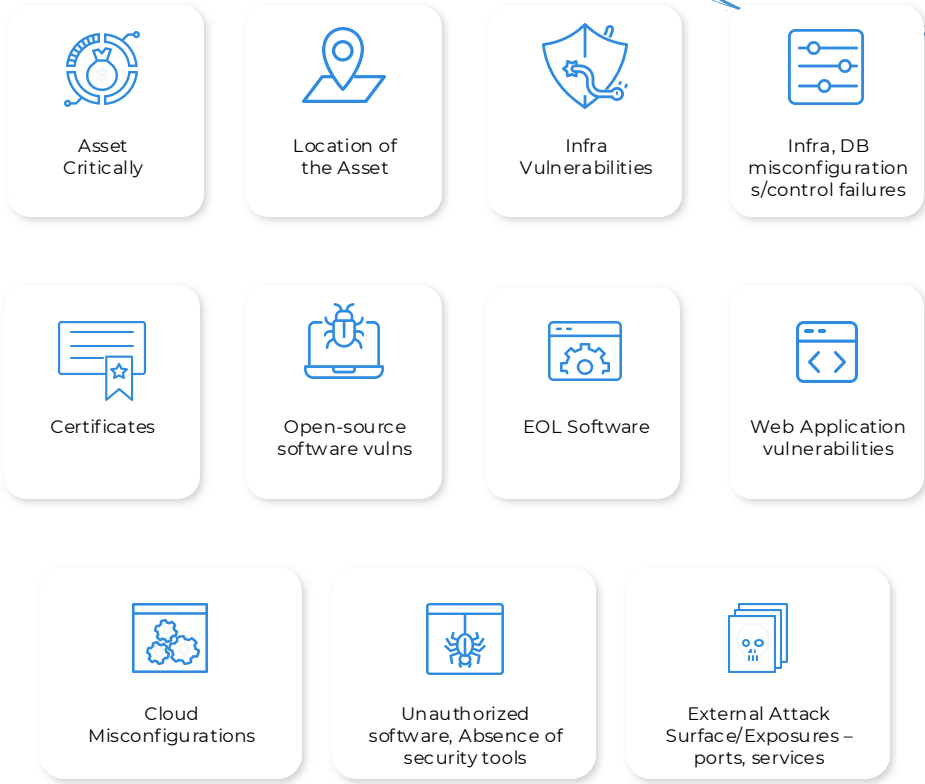
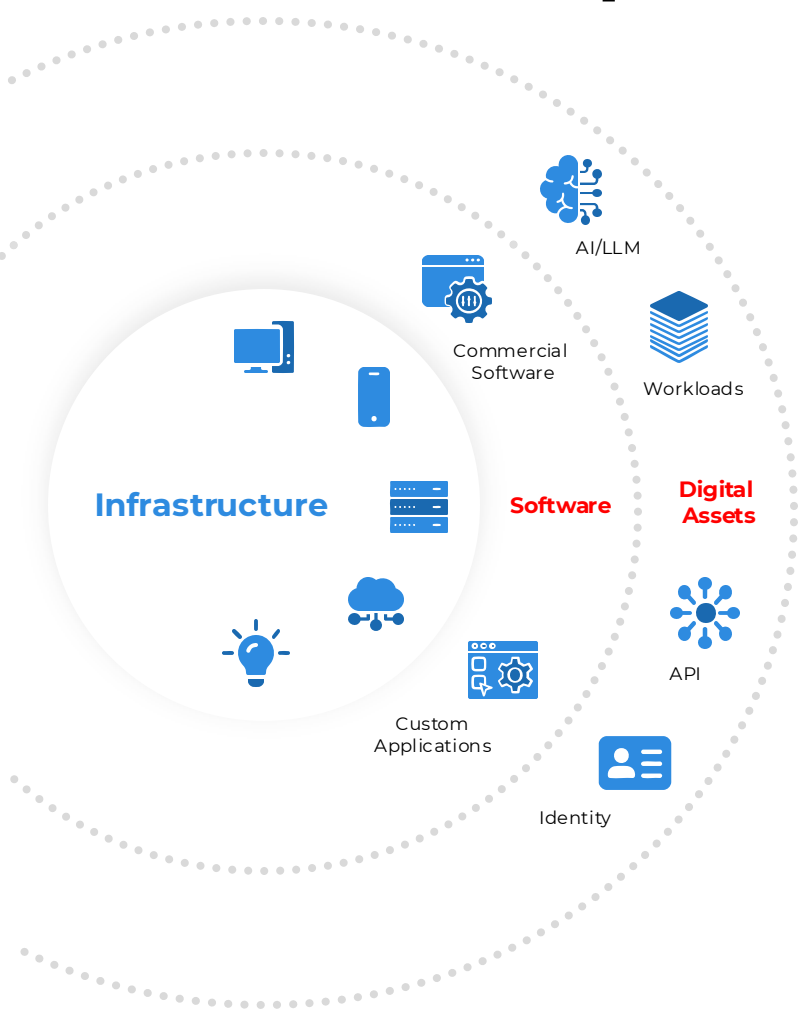
- Identify assets with EOL/EOS software
- Auto discover web servers, middleware, databases
- Classify mission critical assets for compliance

Audit Insights: Asset Landscape

Understand audit readiness across your asset inventory



Multiple SPM tools and Scattered exposures



*Enterprises have **70+ security tools on average**

Prioritize Compliance Risk with Enterprise TruRisk



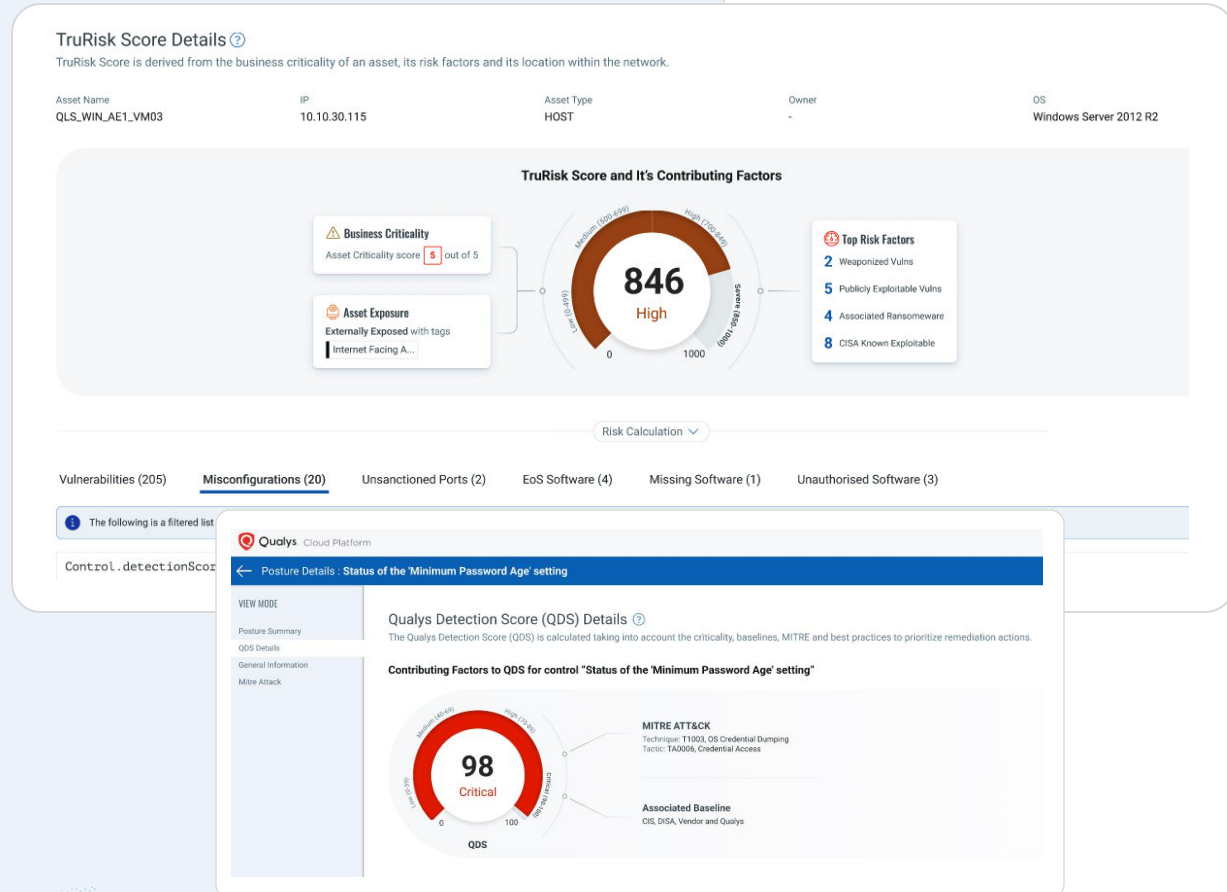
Identify findings with the biggest impact on **audit-readiness**

Improve security and reduce risk exposure by identifying the most **critical risks**

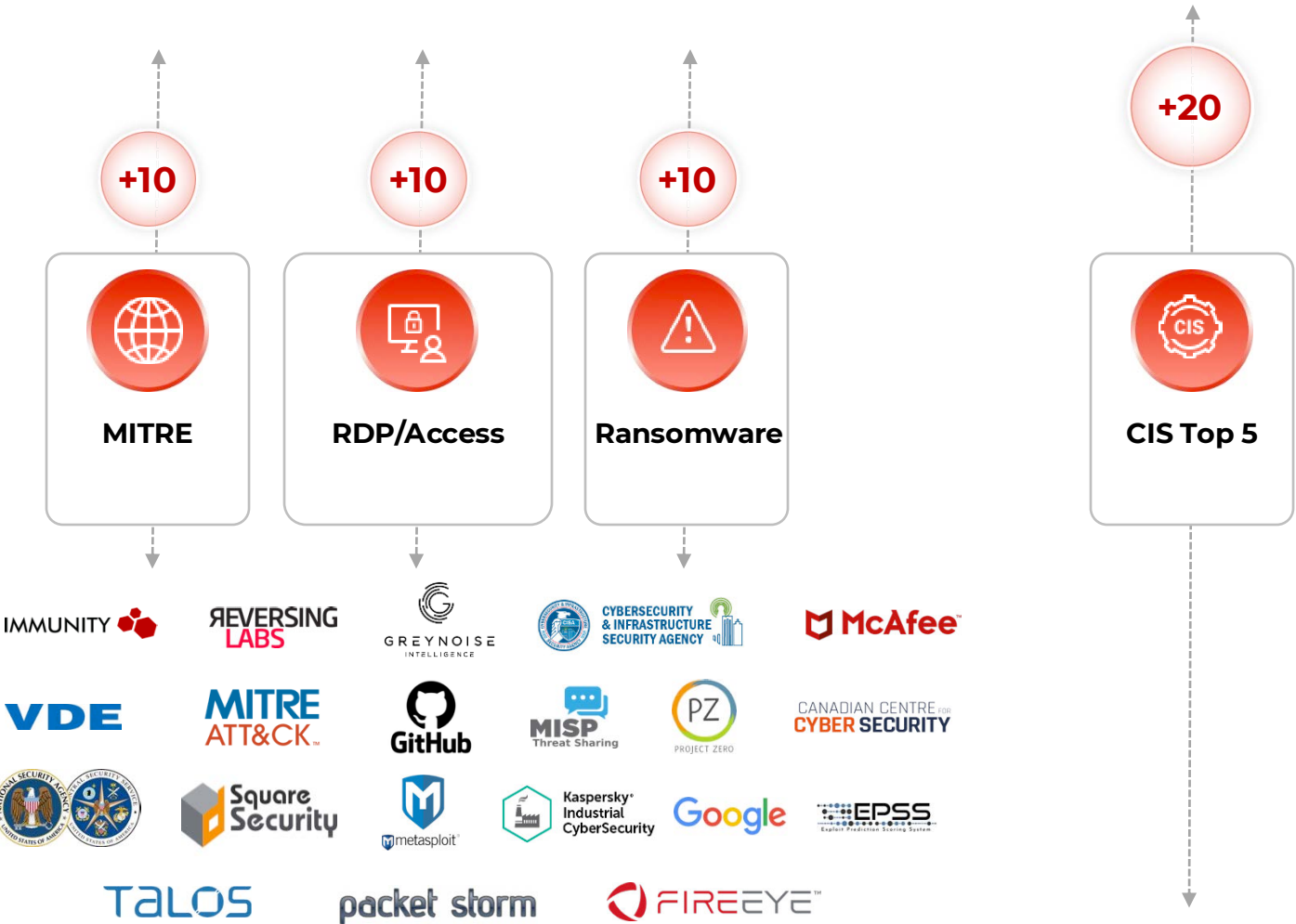
Meet compliance requirements for risk prioritization

Prioritize risk of your misconfigurations based on:

- Business and Mission Impact
- Asset Exposure
- Threat Exposure

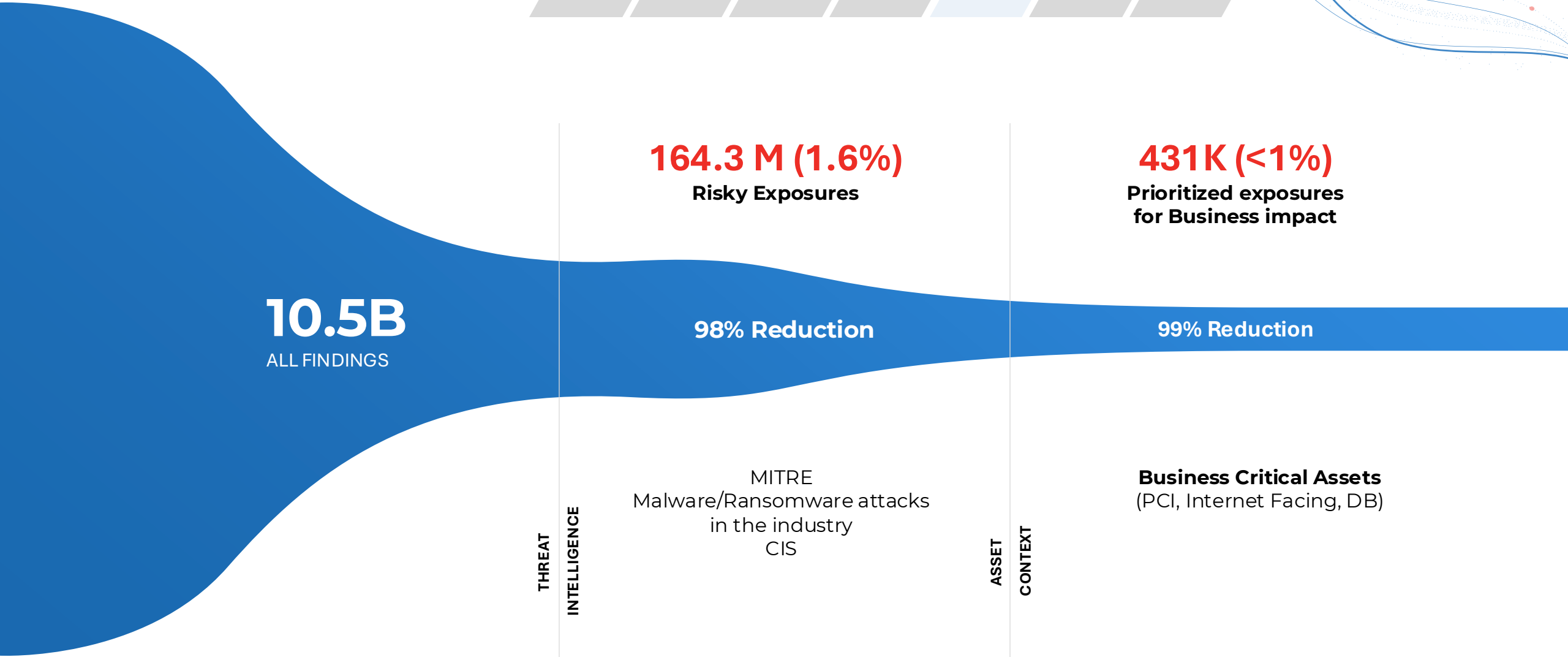


Measuring Risk of Misconfiguration



95
Critical

Prioritizing Risk of Misconfigurations



Custom Checks and Remediation

Why: Automate Evidence collection



Regulatory Alignment & Flexibility

Address unique compliance requirements Create custom scripts to assess proprietary configurations, ensuring full compliance with internal and external policies

Close compliance gaps proactively

Easily adapt to evolving regulations like DORA, ISO 27001, NIST, and CIS with custom checks.

Reduce risk of emerging threats

← Create New Script
STEPS 2/3

1 Basic Information
2 Script Details
3 Review and Confirm

Script Details

Type of Script *
Select
Custom QID
Custom Script

Platform *
Select

Scripting Language *
Select

Category *
Select

Timeout limit *
300 Seconds

Severity *
3

Scripts *
☒ Enter Script ☐ Upload Script ☐ Import from GitHub ☐ Select a Predefined Script

Define Script Parameters [Creating Parameterized Scripts? \[?\]](#)
This option allows you to define parameters to customize script behavior during execution.

Script

Cancel Previous Next

Audit Fix - Automated Remediation Workflows



Regulatory Alignment
& Flexibility

Fix your Audit findings before they become audit issues with Automated Remediation

Pre-defined library of out of the box scripts

Customizable remediation

Significantly Reduce
Breach Exposure

Qualys Cloud Platform

Policy Compliance

HOME DASHBOARD **POSTURE** POLICIES SCANS REPORTS EXCEPTIONS REMEDIATION ASSETS USERS

Posture

posture.status: "Fail" and criticality: "CRITICAL"

asset.operatingSystem: "Windows 10" and asset.trackingMethod: Agent

FAILURE BY CRITICALITY

4K 2K 0 CRITICAL

CRITICALITY

CRITICAL 3.91K

EXCEPTION STATUS

Actions (49)

Remediate Now

ID	CONTROL STATEMENT	TECHNOLOGY/INSTANCE	ASSET	POLICY
10353	Status of the 'Turn off Microsoft consumer experiences' setting	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Imp Windows 10,V2R5 v.2.0
9009	Status of the 'Allow Microsoft accounts to be optional' setting	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Imp Windows 10,V2R5 v.2.0
10028	Status of the 'Turn on PowerShell Transcription' setting	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Imp Windows 10,V2R5 v.2.0
10593	Status of the 'Hardened UNC Paths' setting for Sysvol	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Imp Windows 10,V2R5 v.2.0
10592	Status of the 'Hardened UNC Paths' setting for Netlogon	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Imp Windows 10,V2R5 v.2.0
11281	Status of the 'SMB v1' protocol for LanManServer services on Windows	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Imp Windows 10,V2R5 v.2.0
13342	Permission set for '%ProgramFiles(x86)%' folder on Windows 64-bit systems	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Imp Windows 10,V2R5 v.2.0
11186	Status of the version of McAfee product extension 'Host Intrusion Prevention'	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Imp Windows 10,V2R5 v.2.0
3704	Status of the 'Base name of the installed	Windows 10	WYQ-HADLEY-0008	DISA Security Technical Imp


Powering your ROC with Agentic AI

- ✓ Automated, Continuous Evidence collection
- ✓ Natural Language Query Interface for Audit Insights
- ✓ Actionable insights for Prioritization



Build Your Own Agent

Train and build an AI agent with necessary skills to autonomously perform assigned tasks

Popular

Agent Chang ★ 4.6

Audit-readiness Assessment & Reporting
Keeps you audit-ready continuously with autonomous evidence collection for in-scope assets, mapping to compliance requirements, delivering audit-readiness reports that highlight gaps and prioritize fixes, improving success while reducing manu...

Core Skills
Compliance Management Audit Management +1

Projected Agent Impact

85% Less Time	22% Less Audit Gaps
-------------------------	-------------------------------

Employ

SCA vs Policy Audit

**Managing Risk of Audit Failures + Managing
Risk of Misconfigurations = Continuous Audit
Readiness**

**Basic CIS
Benchmark Checks**

SCA



PA



Demo

Operationalizing Configuration Compliance at Scale

Financial Firm Success with Qualys Policy Audit



Presenter

Joshua McDonald

Senior Policy Compliance Architect

Leading Financial Institution

- Extensive background in compliance and security
- Understanding of compliance frameworks
- Deep experience with numerous industry mandates



Compliance Context

Financial institutions under continuous audit pressure (Federal Review Bd)

Compliance = business trust, not just IT hygiene

Legacy systems & fragmented visibility made control accuracy difficult

Needed to standardize configuration compliance (measured & enforced)

Mission: Transform compliance from reactive reporting into op excellence

Challenges

Problem 1

- **Asset Identity Crisis** – inconsistent, inaccurate tagging
- Flawed inventory, misaligned policy mappings, wasted remediation effort



Challenges

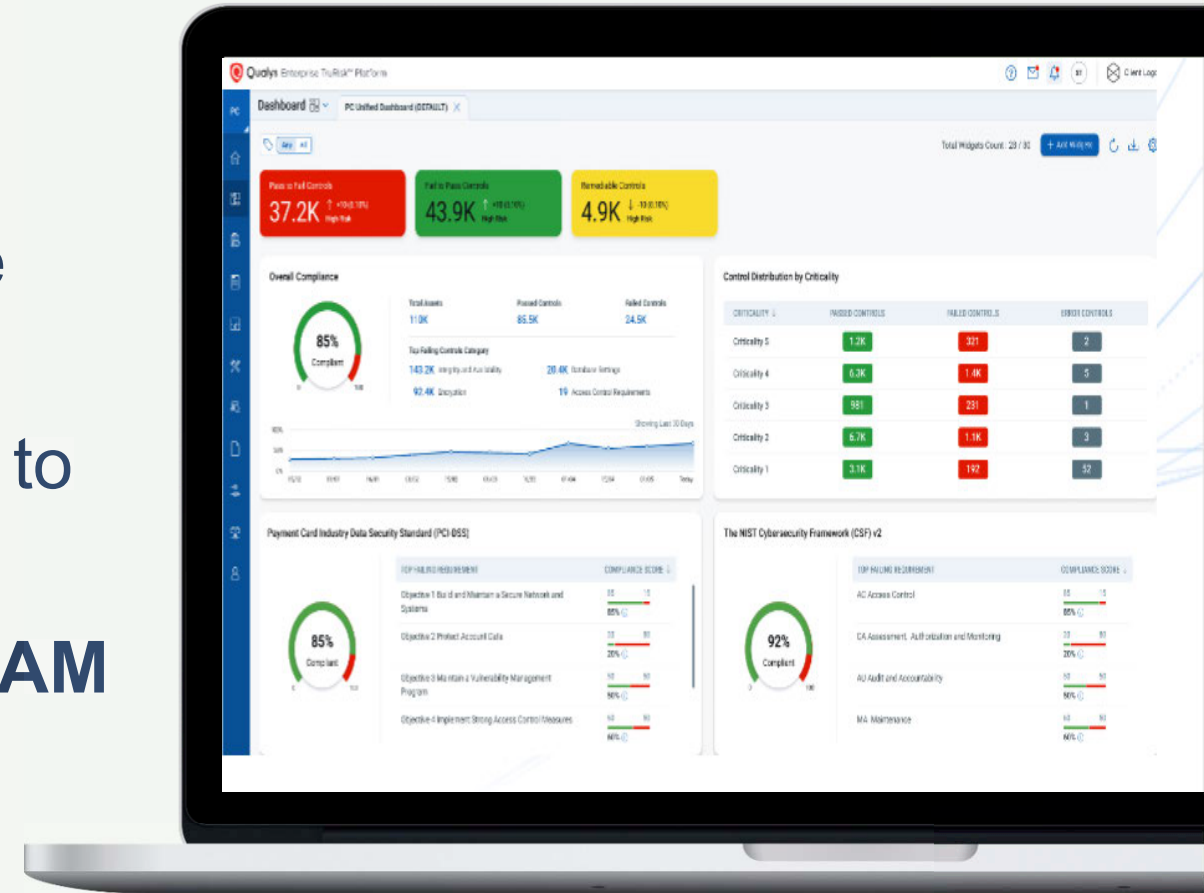
Problem 2

- **Weak Policy Engine** – outdated internal standards, lenient controls passing noncompliance

2

The Solution: Policy Audit

- Unified platform to design, deploy, validate configuration baselines
- Prebuilt **CIS/NIST policies** accelerate modernization
- Allow **custom regex-based controls** to enforce business intent
- Simplified tagging & mapping with **CSAM GUI** and **QQL automation**
- Clear, actionable remediation



Challenges

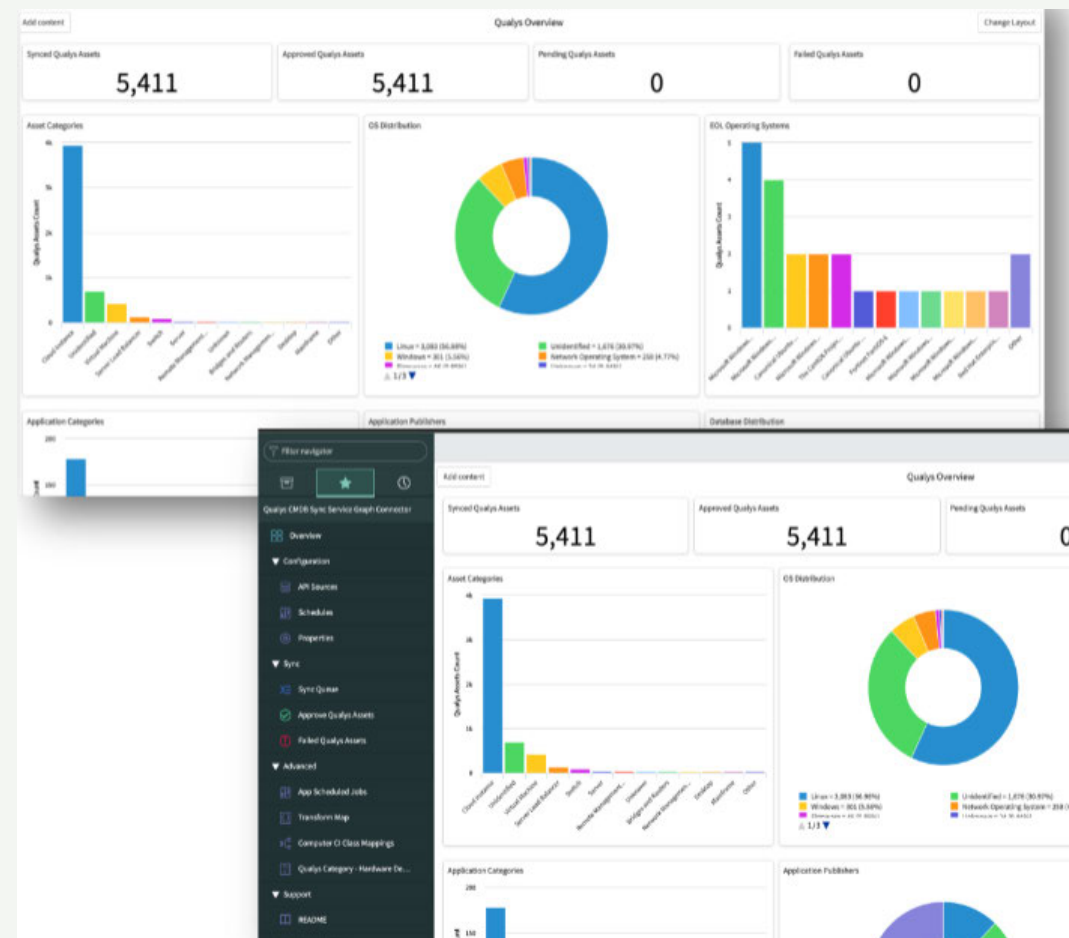
Problem 3

- **Prioritization Gap** –
overwhelming failures without
risk-based ranking
- Confusion, inefficiency, and audit
stress across team

3

Prioritization, Exceptions, SLAs

- Initial triage by raw failure count to identify “big rocks” for fast wins
- Qualys Detection Score (QDS) for dynamic, risk-based prioritization
- Remediation focused on true business impact, not just numbers
- ServiceNow integration to track exceptions & SLAs
- Risk-aligned SLAs = faster closure



Recommendations

- **Start with accurate tagging: you can't secure what you can't identify**
- **Leverage Policy Audit CIS templates for modernization**
- **Ensure regex precision: define “secure” in your environment**
- **Adopt QDS & automation for meaningful, risk-based prioritization**
- **Treat compliance as an operational foundation for resilience**



ROCon²⁵

The Risk Operations Conference

AMERICAS