



Managing Cyber Risk at the Speed of Business

Bridging Gaps to Manage and Eliminate Business Risk



Sumedh Thakar

President and CEO, Qualys



The Great Divide

Security

Business

The Deepening Divide



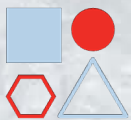
Too Many tools

Many larger organizations operate with **over 70 security and IT management tools**



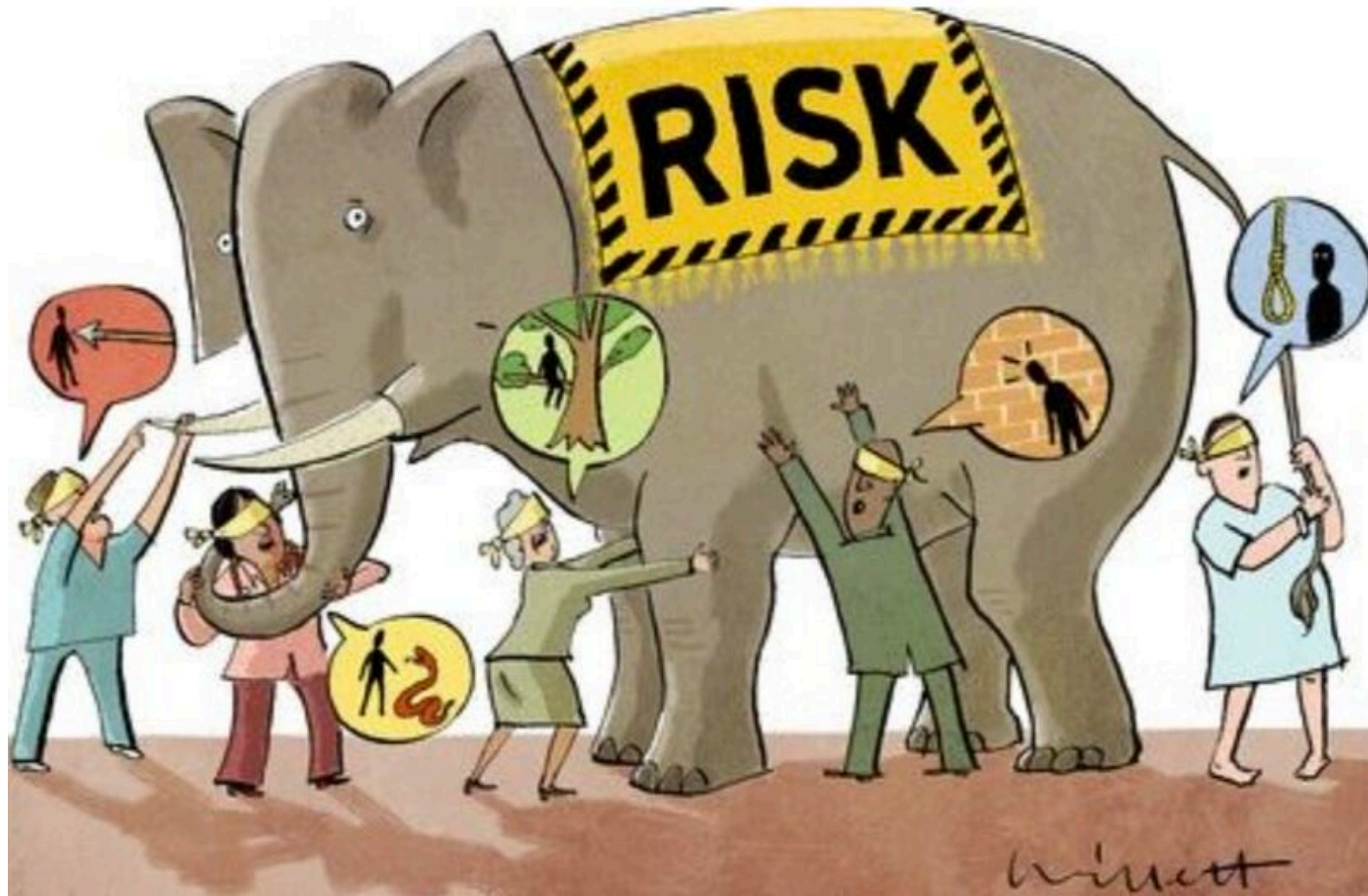
Speaking different languages

Communication with business & IT stake holders is broken



Slow/No remediation

No value in security spend if right issues not fixed in time



Types of RISK



Types of RISK



If Everything is Critical, Nothing Is

Of **2.6 Billion** vulnerability detections analyzed, **2.1 (81%)** were deemed **'high-risk'** or **'critical'** according to CVSS

With TruRisk, only 603 Million were **'high-risk'** or **'critical'**

87 Million high risk vulnerabilities were found that CVSS missed

What's my True Risk Anyway?

2.6B
Vulnerabilities

With CVSS

2.1B / 81%

692M / 26%

With
Qualys
TruRisk

603M / 23%

87M / 3.3%

How Can Calculate Risk?

Know Your Cyber Risk From Disparate Inputs and Tools

Over 30% of Assets Aren't Visible

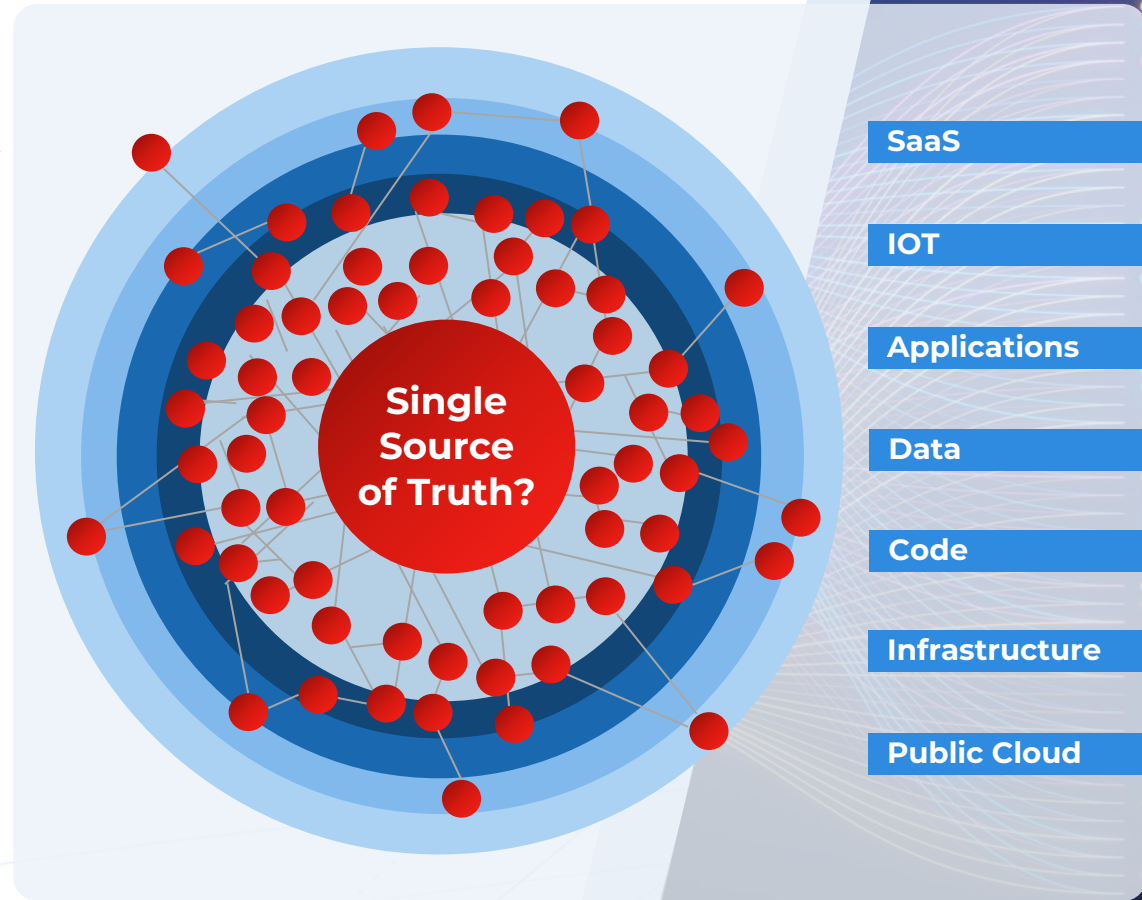
Most organizations **do not** have complete visibility to external and internal assets

Add Threat Context

Most security programs are missing context from threat intelligence

Layer Business Context

45% of assets misclassified for business criticality



How Can I Articulate Risk?

Briefing Executive Stakeholders that are now Cyber Risk Stakeholders

New Executive Stakeholders

47% of CISOs now report directly to the CEO, and nearly all brief the Board of Directors

Risk without Business Impact

CVEs do not provide the business context of cyber risk posture at any moment in time

Quantification of Cyber Risk

Cyber response statistics do not translate to cyber risk quantification

INFO-TECH RESEARCH GROUP

Vulnerability Management Policy

Introduction: How to Use This Template

Read the template, which includes the most common information understood by your organization. Other variables, values of vulnerability or severity or priority or risk are all remaining to be filled per your discretion.

| Policy Name | For the Information of the user |
|------------------|---------------------------------|
| Policy Approved | |
| Policy Purpose | |
| Policy Review | |
| Storage Location | |
| Revision Date | |
| Next Review Date | |

Purpose

Describe the factors or circumstances that motivate the existence of the policy. Also, state the policy's basic objectives and state the policy's scope of action.

Scope

Describe the system or systems that are covered by the policy. List the systems required to comply or specify include all if all are included. Also indicate any exclusions or exceptions. In this template, identify an address that are not covered by the policy or where special provisions apply.

Governing Laws and Regulations

Identify the laws or regulations that govern the policy or with which the policy must comply. Specify the legal jurisdiction that the law is from. Place an X in a position governing law or regulations, when applicable.

INFO-TECH RESEARCH GROUP

| Question | Org vulnerability | Application vulnerability | Network vulnerability | Vendor patch release | Vulnerability S |
|----------|-------------------|---------------------------|-----------------------|----------------------|-----------------|
|----------|-------------------|---------------------------|-----------------------|----------------------|-----------------|

Vulnerability Management Risk Assessment Tool

This tool is designed to assist you in prioritizing changes according to the level of risk, as defined by impact and urgency.

Instructions:

On Tab 2, Questions, enter the questions you will use to measure both impact and urgency. Assign a weighting to each question based on the importance of that measure factoring into overall impact and urgency. Ensure they add up to 100% for each of impact and urgency.

Define criteria for a Critical (4), High (3), Medium (2), and Low (1) risk for each of the questions through the dropdowns. (Note: If the labels for dropdowns are not correct, you can edit the Labels tab and modify them there.)

Enter up to 13 vulnerability types from columns A to P. You can also modify the rows from column D to I if they don't suit your environment. Assign a risk level on a scale of 1-5 for each question. The total impact and urgency for each change will automatically be calculated based on weighting and responses to each question.

Tab 3, Risk Matrix will plot your changes onto a 2x3 risk matrix (with a Critical square for the maximum Critical risk) based on impact and urgency. Identify low, medium, high and critical risk vulnerabilities.

For acceptable use of this tool, refer to Info-Tech's Terms of Use. These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply locate the Info-Tech information in the header and Footer fields of this document.

Tool

The Vulnerability Tracking Tool can be used to provide a document of your vulnerabilities and track the agencies as well as the remediation efforts. This tool will allow you to document:

- The list of vulnerabilities.
- The assigned agencies of the vulnerabilities.
- Any Out-of-Cycle Remedies performed for vulnerabilities.
- The testing of any remediation options.
- The remediation of the vulnerability including system owners and verification of the remediation.

This tool will provide a document that can assist in tracking all the vulnerabilities within the system, while identifying the testing and implementation of remediation.

For acceptable use of this tool, refer to Info-Tech's Terms of Use. These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply locate the Info-Tech information in the header and Footer fields of this document.

How Can I Remediate Risk?

Reducing Cyber Risk Effectively According to Business Impact

Break Internal Silos

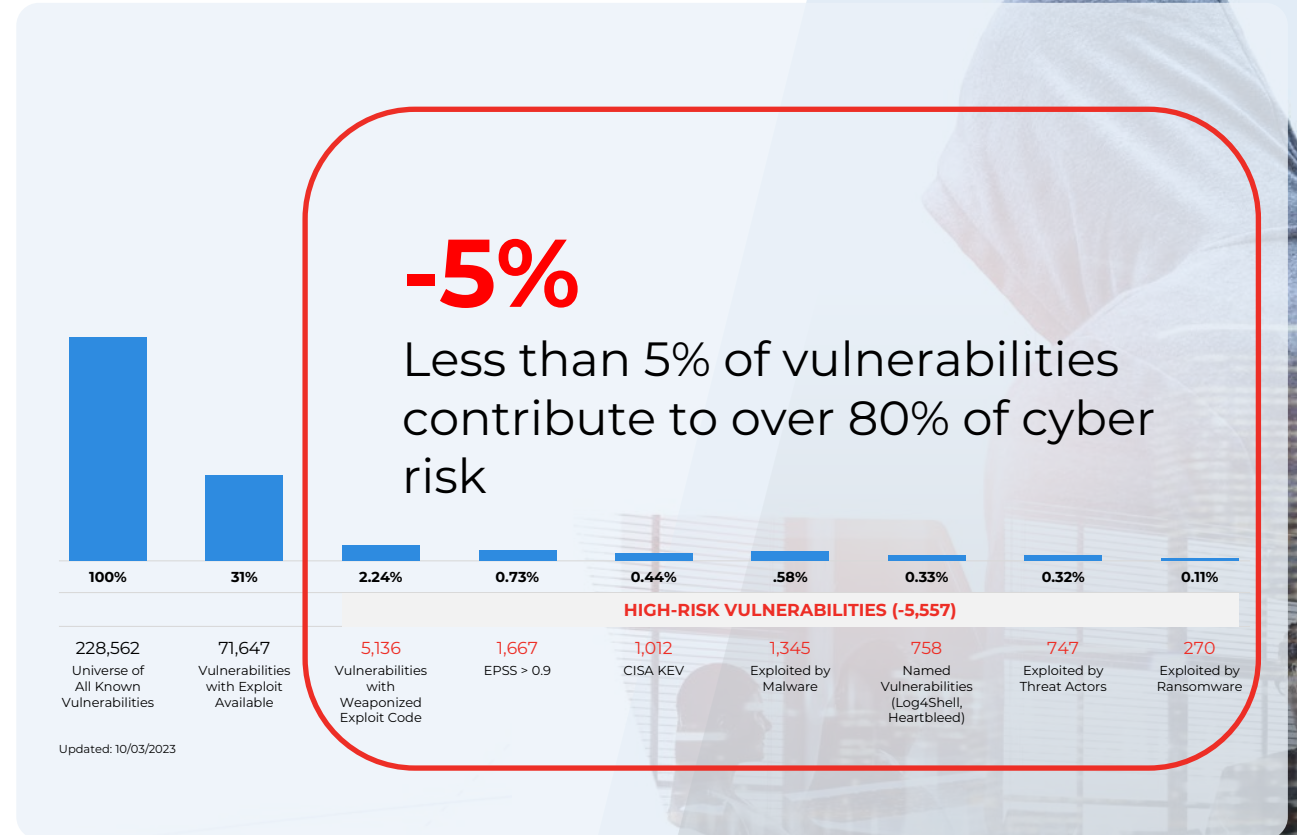
Misalignment between Dev, IT, and Security teams leads to **slow MTTR**

Speed up Threat Response

Top Attacks of 2021, 2022 & 2023 used **Exploitable, Ransomware-Exploited** or CISA catalogue provided vulnerabilities, **not patched**

Operational Risk vs. Security Risk

Fear of **operational impact** outweighs fear of security impact





UK defenders are faster, but still not fast enough

Internal vulnerabilities are **43.6 times more prevalent than external vulnerabilities**

According to NCSC, **remediation must be 7 days for internal assets and 5 days for external assets**

Internal Vulnerabilities

Global

23 Days

UK

15 Days

External Vulnerabilities

24 Days

17 Days

Every Next-Gen Cybersecurity Expert

Must become a **Cyber Risk** expert



Next-gen cyber risk expert

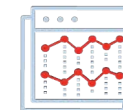
Stakeholder to help reduce Business Risk



Measure known and unknown cyber risk and **quantify that risk in business terms**



Eliminate cyber risk by **unifying security and IT efforts**



Communicate your cyber risk posture across your organization **beyond cyber risk enumeration to quantification**



Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.

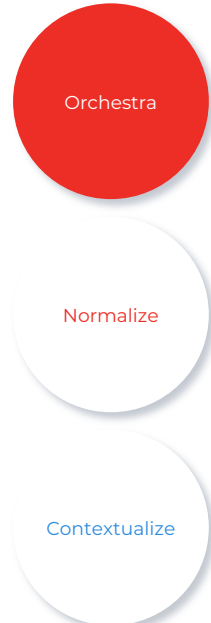
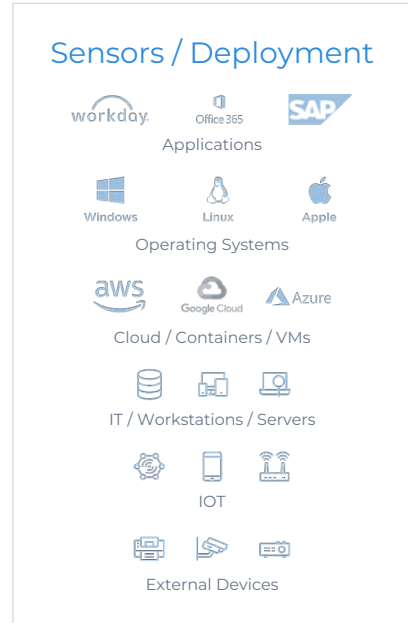
Enterprise TruRisk Platform

From Enumeration to Elimination of Risk

Collect Data

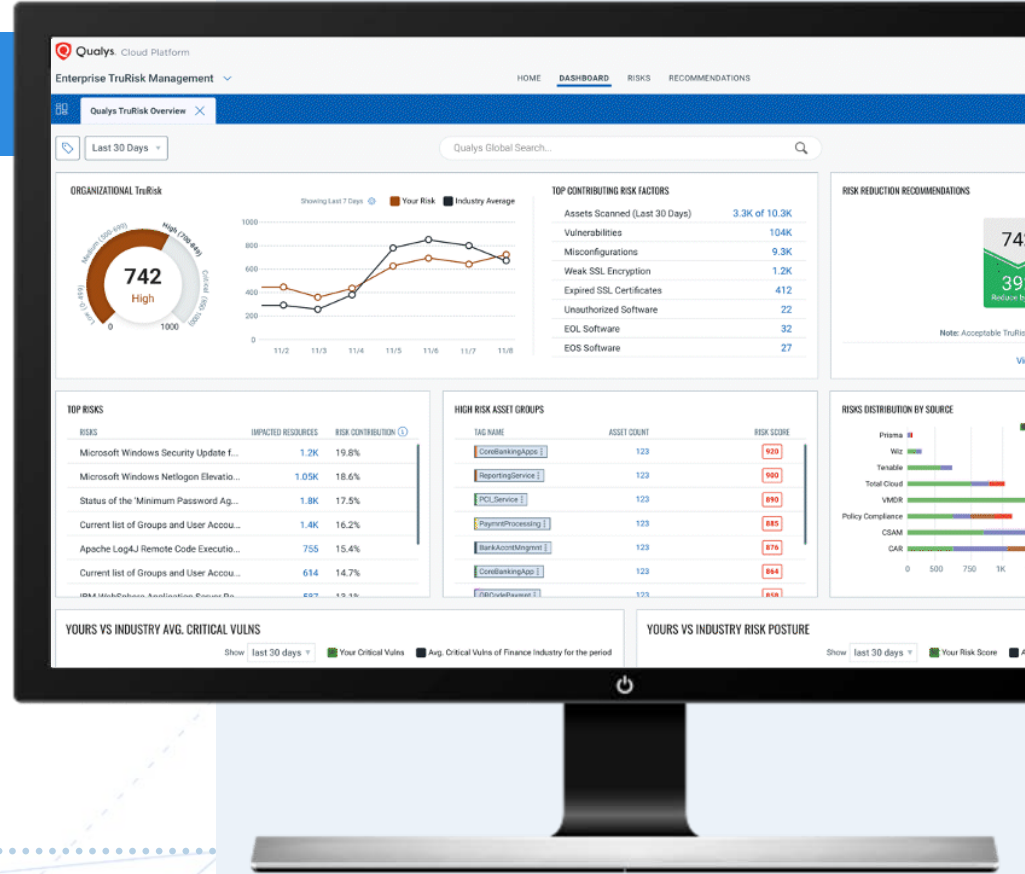
Apply Threat Intel

De-Risk Business

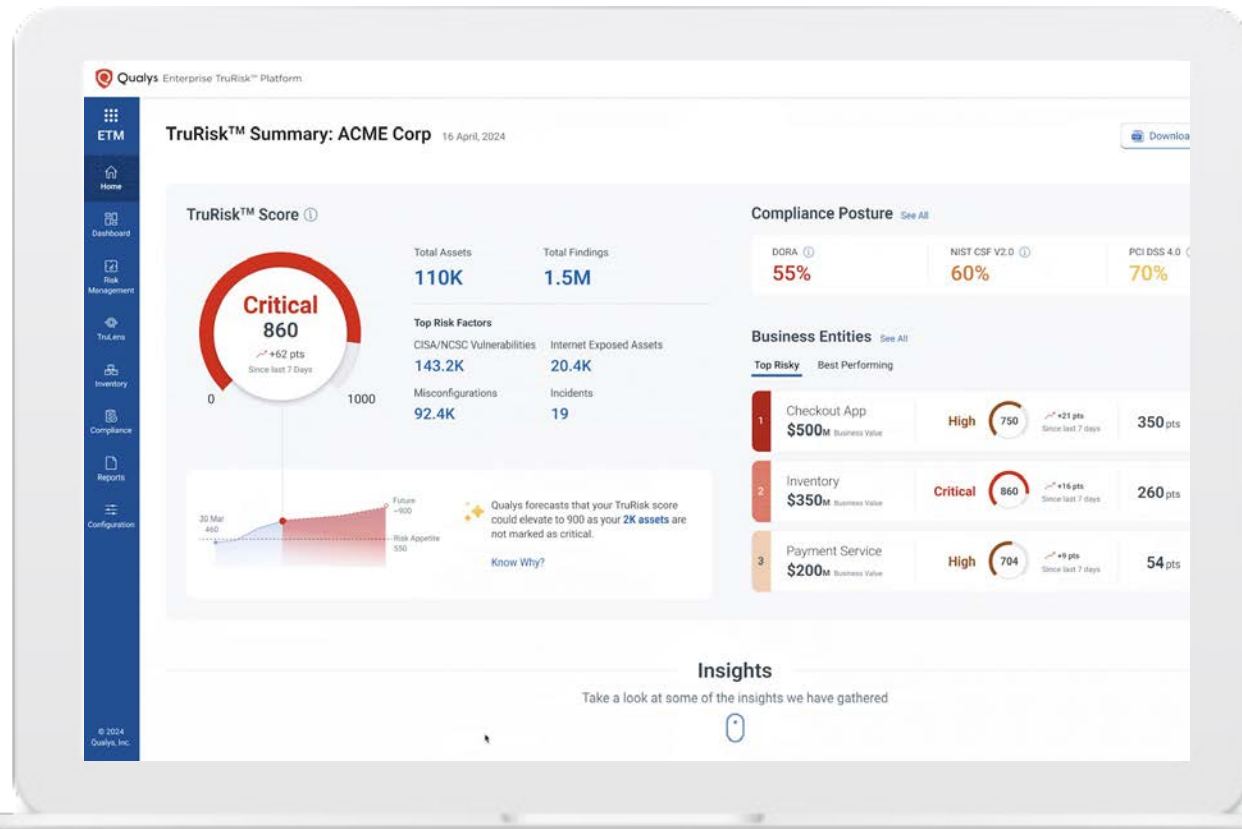


Measure:
External Ecosystem Risk Factors

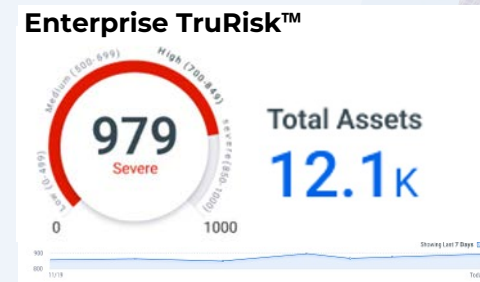
Communicate:
Specialized Reports



Measure Cyber Risk



Quantify risk across Qualys & non-Qualys tools



Contributing Risk Factors

| Contributing Factor | TruRisk | Sources | Contribution | Assets |
|-----------------------------|---------|---------------|--------------|--------|
| Vulnerabilities | 961 | VMDR/Defender | 36% | 8.2K |
| Misconfigurations | 961 | TC/Wiz/PC | 25% | 6.2K |
| Posture Risk | 961 | PC | 19% | 5.2K |
| Open Source Vulnerabilities | 961 | Snyk | 12% | 8.2K |
| WebApps | 961 | WAS/Veracode | 11% | 8.2K |

Communicate Cyber Risk

Quantified Cyber Risk with Business Impact



Eliminate Cyber Risk

Go beyond patch management

| CATEGORY | ASSETS | REMEDIATION | MITIGATION |
|---------------|--------------------------------------|---|---|
| Vulnerability | pro-v14-sp1-u9 625800550 | ⚠ Servicing stack update... Patch | Registry Key change Mitigation |
| Vulnerability | pro-v14-sp1-u9 625800550 | ⚠ Security Update for Adobe Patch + Conf. Change | Device Isolation Mitigation |
| Vulnerability | pro-v14-sp1-u9 625800550 | ⚠ Servicing stack update... Patch | Process stop Mitigation |
| Vulnerability | win2008-p-69-177 167659968 | Security Monthly Rollup ... Patch | ⚠ Proprietary script Partial Mitigation Change |
| Vulnerability | win2008-p-69-177 167659968 | ⚠ Security Update for .NET Patch | Block access to file attrib... Mitigation |
| Vulnerability | win2008-p-69-177 167659968 | KB5020439 (OS Build 1... Patch | ⚠ Registry Key change Partial Mitigation |


Enterprise **TruRisk™** Platform

The Business Value of Qualys

The ROI of investing in the platform according to IDC

 **5-Month** payback period

 **\$5.1M** in benefits on average

 **24%** more efficient security teams

 **24%** reduction in compliance fines

403% ROI?

Real Customers. Real ROI.



Fixing Cyber Risk at the Speed of Business

De-Risking Your Business
with the Qualys Enterprise
TruRisk Platform



Aggregate cyber risk across
Qualys & Third-Party Products,
and **their Risk Factors**



Share a **common language** to
communicate cyber risk to
key stakeholders



Leverage prioritization and
automation for **risk elimination**



Practice and be prepare for your
Value at Risk (VAR) response



Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.



Qualys[®]