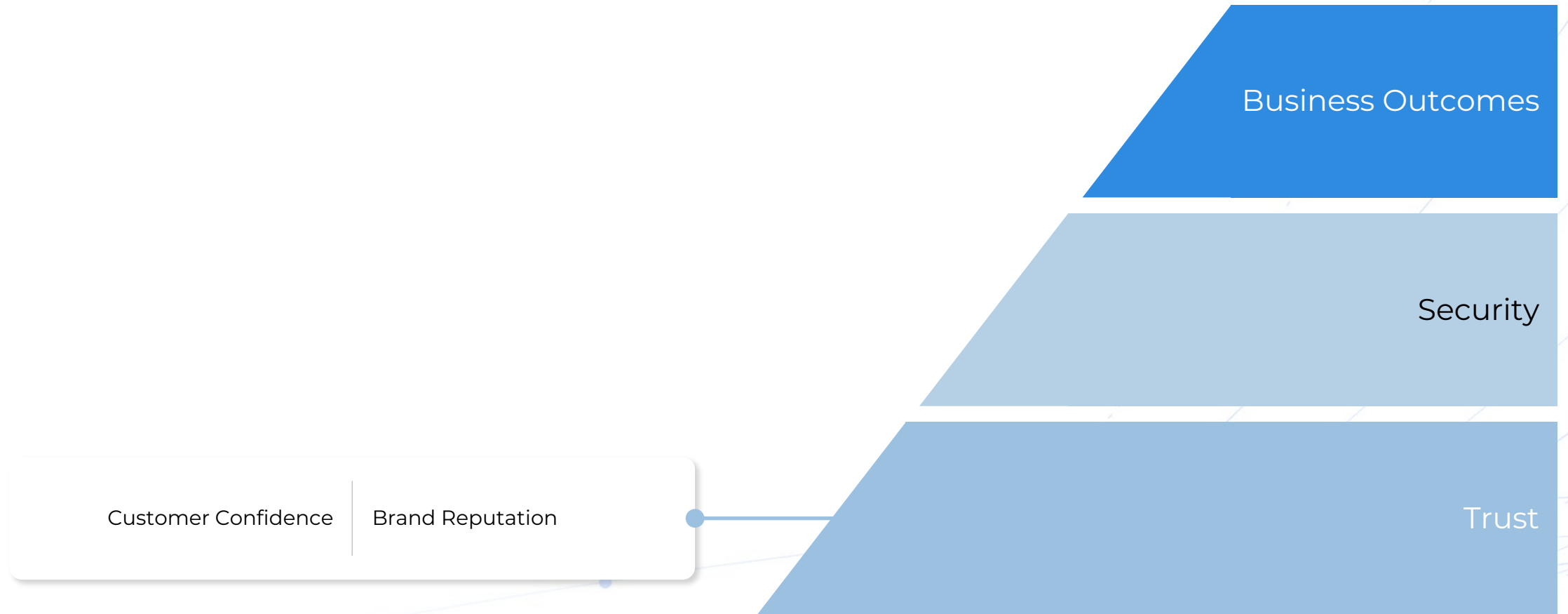# The Power of TruRisk: Building Business Value, and Trust

Joe Petrocelli
Vice President, Product Management
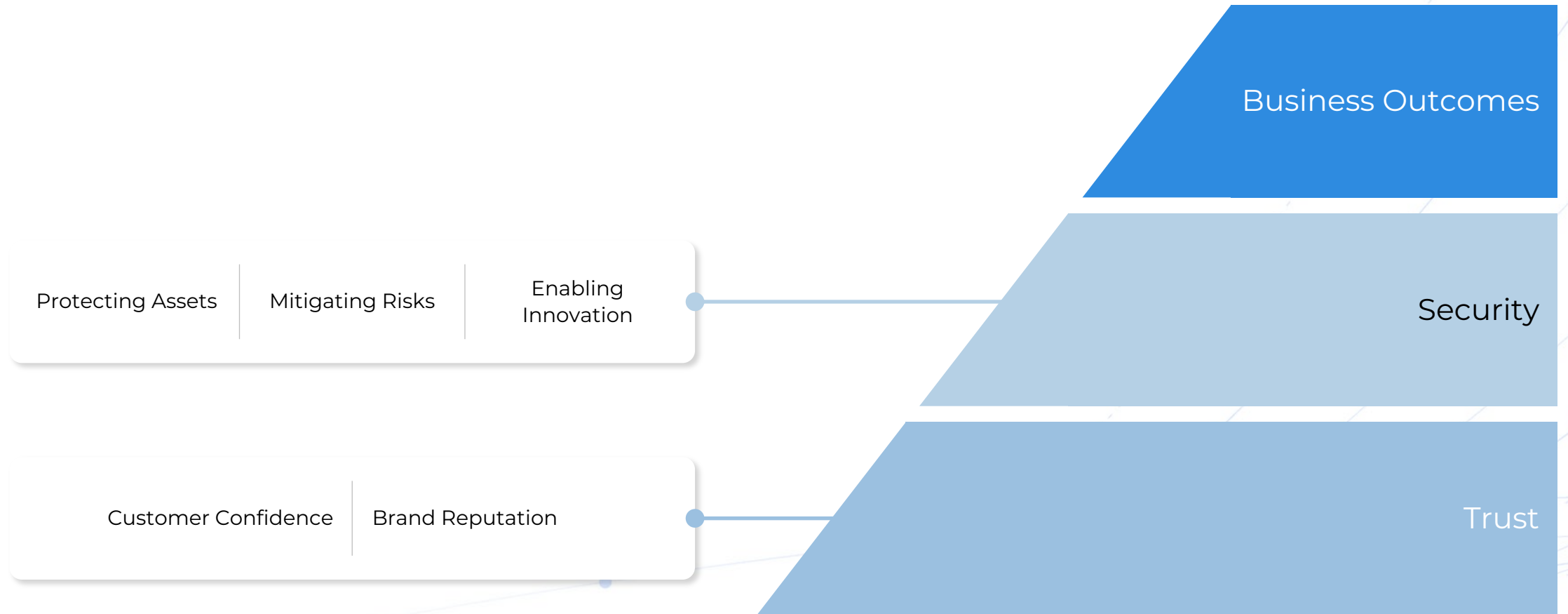
Trust, Security, Business Outcomes

A Virtuous Cycle

Business Outcomes

Security

Trust

Customer Confidence | Brand Reputation

Qualys.

Trust, Security, Business Outcomes

A Virtuous Cycle

Business Outcomes

| Protecting Assets | Mitigating Risks | Enabling Innovation |

Security

| Customer Confidence | Brand Reputation |

Trust

Qualys.

Trust, Security, Business Outcomes

A Virtuous Cycle

Financial Performance	Strategic Opportunities	Compliance and Competitive Advantage

Business Outcomes

Protecting Assets	Mitigating Risks	Enabling Innovation

Security

Customer Confidence	Brand Reputation

Trust

Qualys.
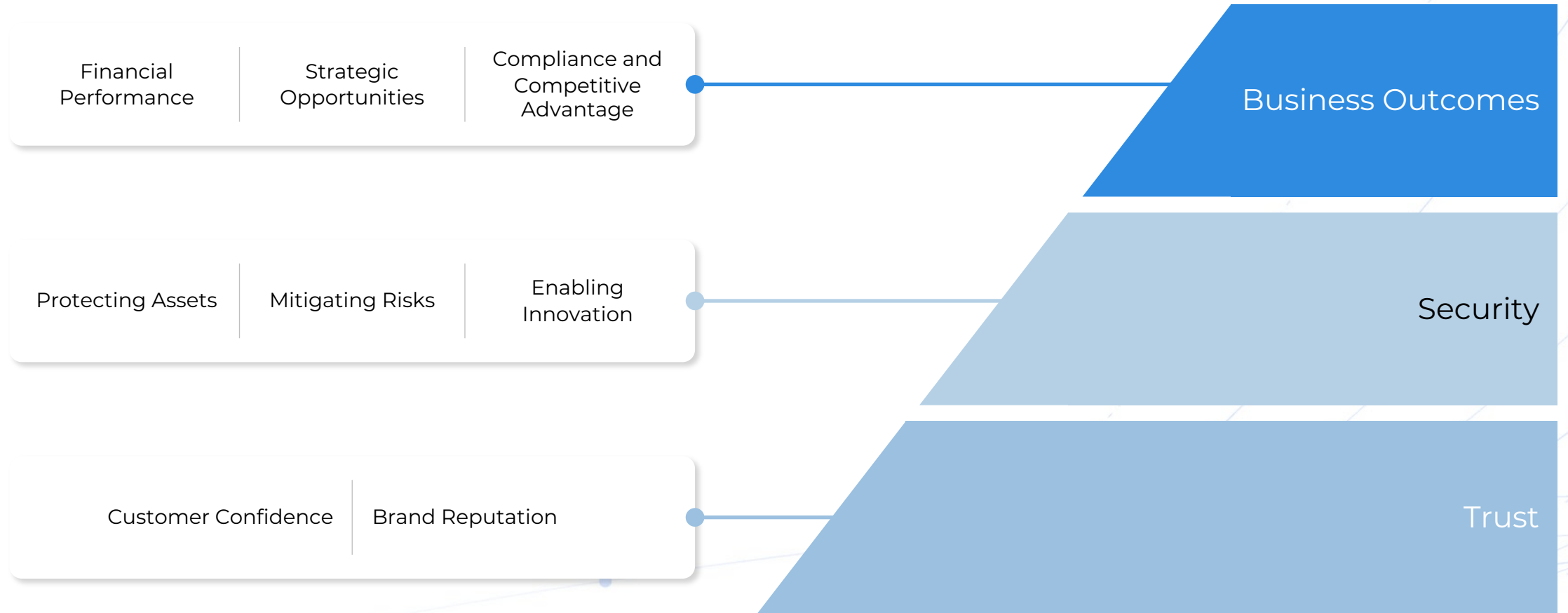
Security is Hard

The hits keep coming, and the adversary is getting smarter

2.5% — **Less than 2.5% of vulnerabilities contributed the highest risk** and were regularly exploited.
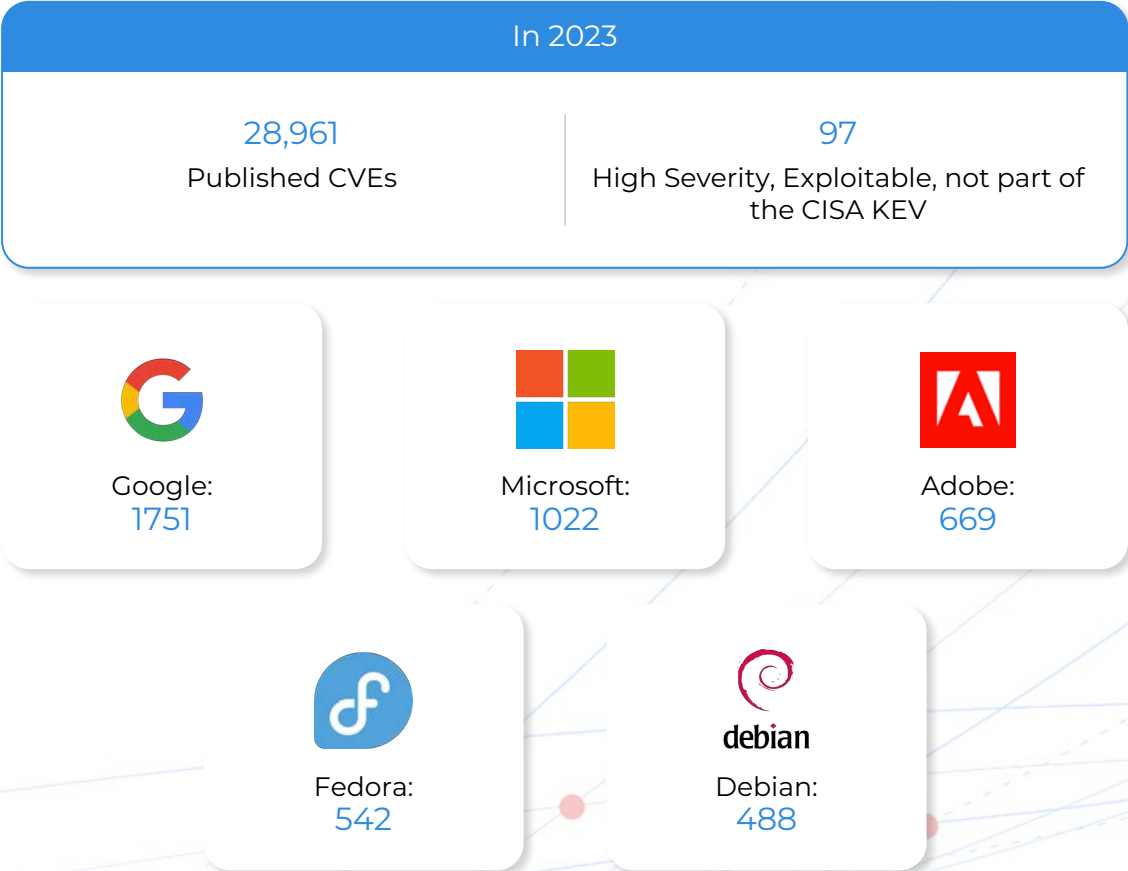
25% — **25% of known exploits were created within 24 hour**s of vulnerabilities being publicly disclosed.

33% — **33% of High Severity vulnerabilities were found in network infrastructure** or web applications.

4/5 — **4 out of 5 of the most exploited vulnerabilities** of 2023 are not in this list.

In 2023

28,961	97
Published CVEs	High Severity, Exploitable, not part of the CISA KEV

Google:
1751

Microsoft:
1022

Adobe:
669

Fedora:
542

Debian:
488

Qualys.

Too Many Tools

46   Average number of Cyber Security Tools in Enterprise > 5K employees in 2023

18%   Increase in tools from 2019 to 2023

Qualys

Too Much Data – Few Insights
Too Many Reporting Tools that Don't Scale

No Actionable Insights

VULNERABILITY MANAGEMENT

PEN-TESTING & BUG BOUNTY

Dataflows

Processing / ML

Data Collection

Data Storage

Data Cleaning

Data Analysis

Visualization

Reporting

Elimination

Feedback Loop

External Threat Intel

Goal

- **Blindspots?**
- **Anomalous behavior?**
- **Proactive measures?**
- **Attack paths?**
- **How's my current threat protection strategy working?**

Qualys.

No Single Source of Truth
Too Many Reporting Tools that Don't Scale

Expensive to build, manage, maintain, or buy
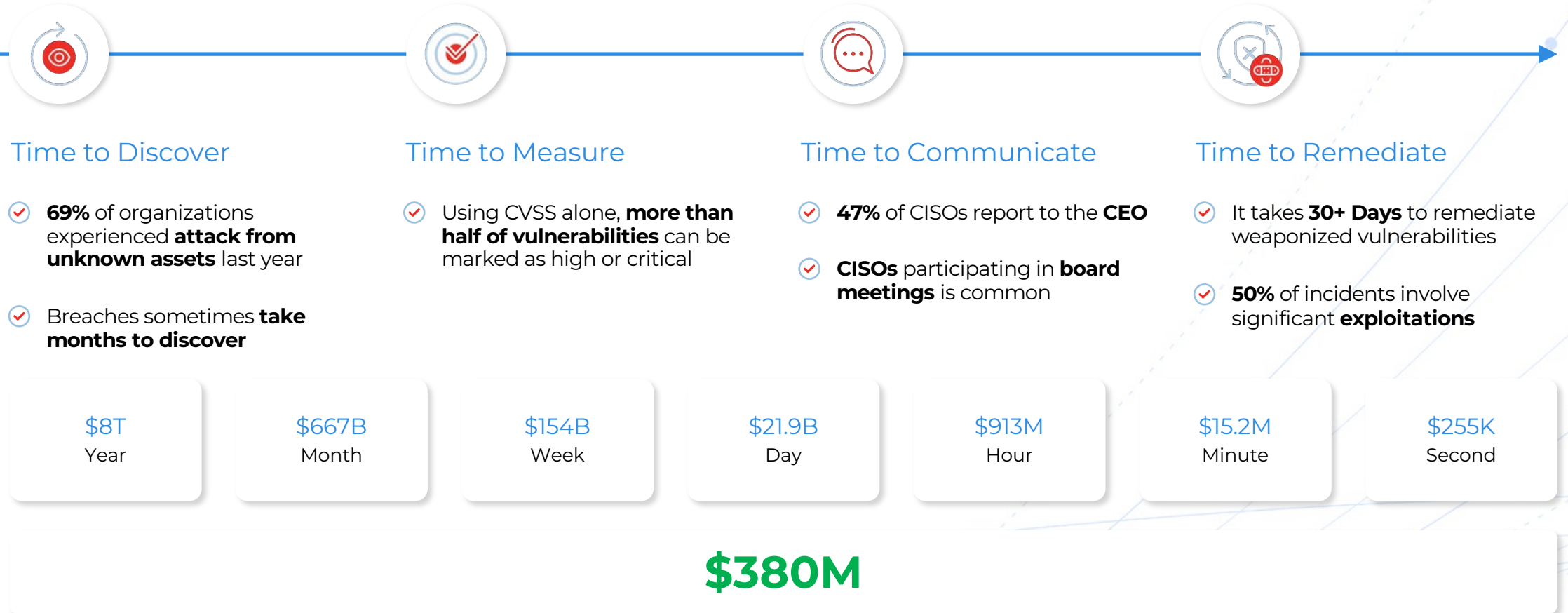
Do not provide a unified view of risk

Waste resources and distract business focus

Which tools should we use to communicate cyber risk?

Power BI

DOMO

+ableau

Qualys.

How does this impact your risk?

It's all about time.

Time to Discover

- ✓ **69%** of organizations experienced **attack from unknown assets** last year
- ✓ Breaches sometimes **take months to discover**

Time to Measure

- ✓ Using CVSS alone, **more than half of vulnerabilities** can be marked as high or critical

Time to Communicate

- ✓ **47%** of CISOs report to the **CEO**
- ✓ **CISOs** participating in **board meetings** is common

Time to Remediate

- ✓ It takes **30+ Days** to remediate weaponized vulnerabilities
- ✓ **50%** of incidents involve significant **exploitations**

$8T	$667B	$154B	$21.9B	$913M	$15.2M	$255K
Year	Month	Week	Day	Hour	Minute	Second

$380M

Qualys.

Undesired Outcomes

Endless Cycle of Failed Results

Organizations **don't have accurate inventory, stale CMDB,** leading to a breach

Security Teams **focus on remediating inconsequential vulnerabilities,** which **don't reduce risk**
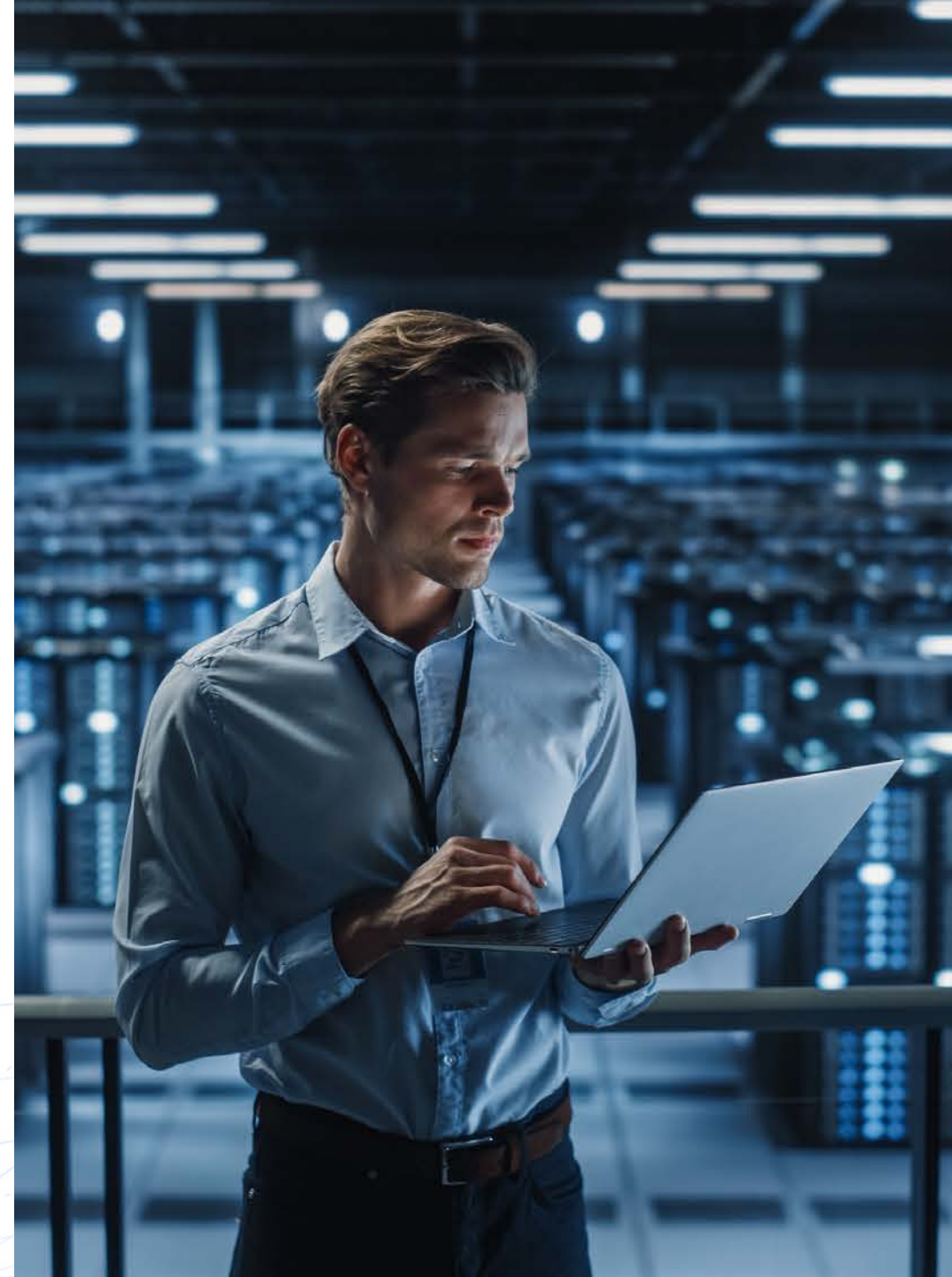
IT Teams miss SLA's for high-risk vulnerabilities

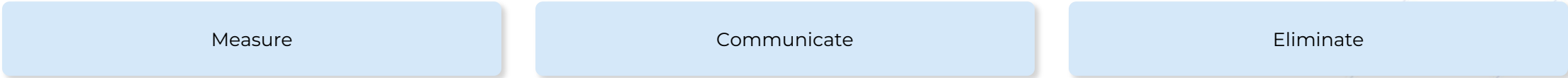Security & IT Teams **waste countless hours communicating risk through spreadsheets, reports & manual processes**

Failures expose organization to unnecessary risk

Qualys.

Qualys Enterprise TruRisk Platform

Qualys
TruRisk™

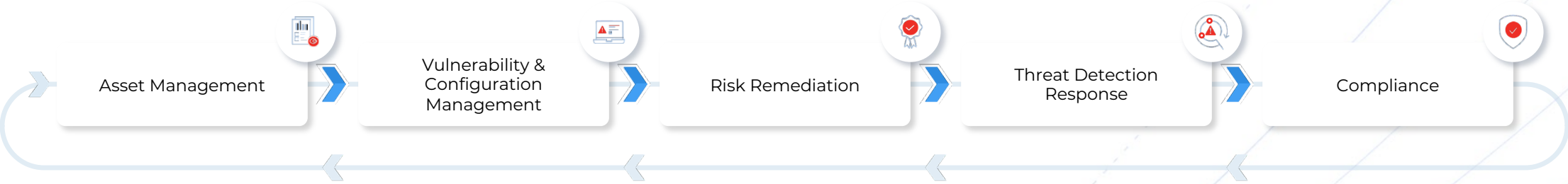| Measure	Communicate	Eliminate

Internal & External Attack Surface Risk Management with Business Context

Detect, Prioritize, manage vulnerabilities, misconfigurations

Map Remediate vulns, miconfigs with Remediation Automation and intelligent workflows

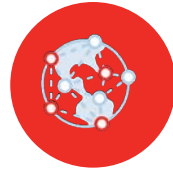**Monitor, detect & respond & Prevent threats** with Risk, business context

Drive compliance Monitoring, Reporting for Industry mandates, standards

Asset Management → Vulnerability & Configuration Management → Risk Remediation → Threat Detection Response → Compliance

API

Lightweight Agent

Platform Services

Sensors

First-Party OSS ◄ · ► **3rd Party Data**

Applications

Operating Systems

Cloud / Containers / VMs

IT / Workstations / Servers

IOT

External Devices

workday. Office 365 SAP

Windows Linux Apple

aws Google Cloud Azure

Qualys.

Measure TruRisk, Comprehensively

Asset Critically	Location of the Asset	Infra Vulnerabilities	Infra, DB misconfigurations/control failures
Certificates	Open-source software vulns	EOL Software	Web Application vulnerabilities
Cloud Misconfigurations	Unauthorized software, Absence of security tools	External Attack Surface/Exposures – ports, services	

Threat mapping: Exploitation, CISA, EPSS-augmented, Ransomware, Darkweb (with VMDR)

Business Asset Context: Criticality, Ownership, role, exposure (Enhanced with CSAM) + Compensating controls

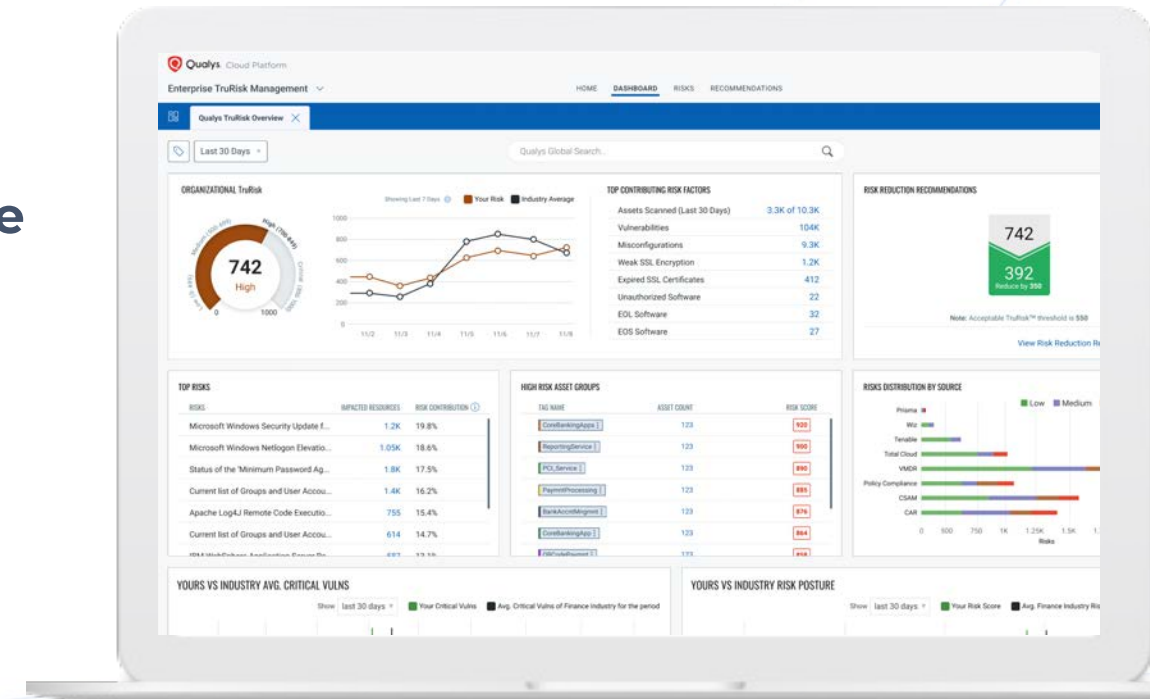**Quantified Score, transparent formula and weightages (comes with VMDR)**

25+ Threat Feeds

IMMUNITY · McAfee · FIREEYE · packet storm · REVERSING LABS · GitHub · MISP Threat Sharing · CANADIAN CENTRE for CYBER SECURITY · VDE · Google · EPSS · CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY · MITRE ATT&CK · GREYNOISE INTELLIGENCE · PZ PROJECT ZERO · Kaspersky Industrial CyberSecurity · TALOS · Square Security · metasploit

Asset Context – CMDB, AD, EASM

Selected Asset Tags
Production | Win-Servers | Database

840 ↑ 3.16% High

Contributing Factors
- 18K Weaponized Vulns
- 680K Publicly Exploitable Vulns
- 8.7K Associated Threat Actors
- 8K CISA Known Exploitable
- 330K External Facing Assets

900 / 850 / 800 — 08/02 · 08/18 · 09/04 · 09/19

Qualys

What Customers Are Asking For

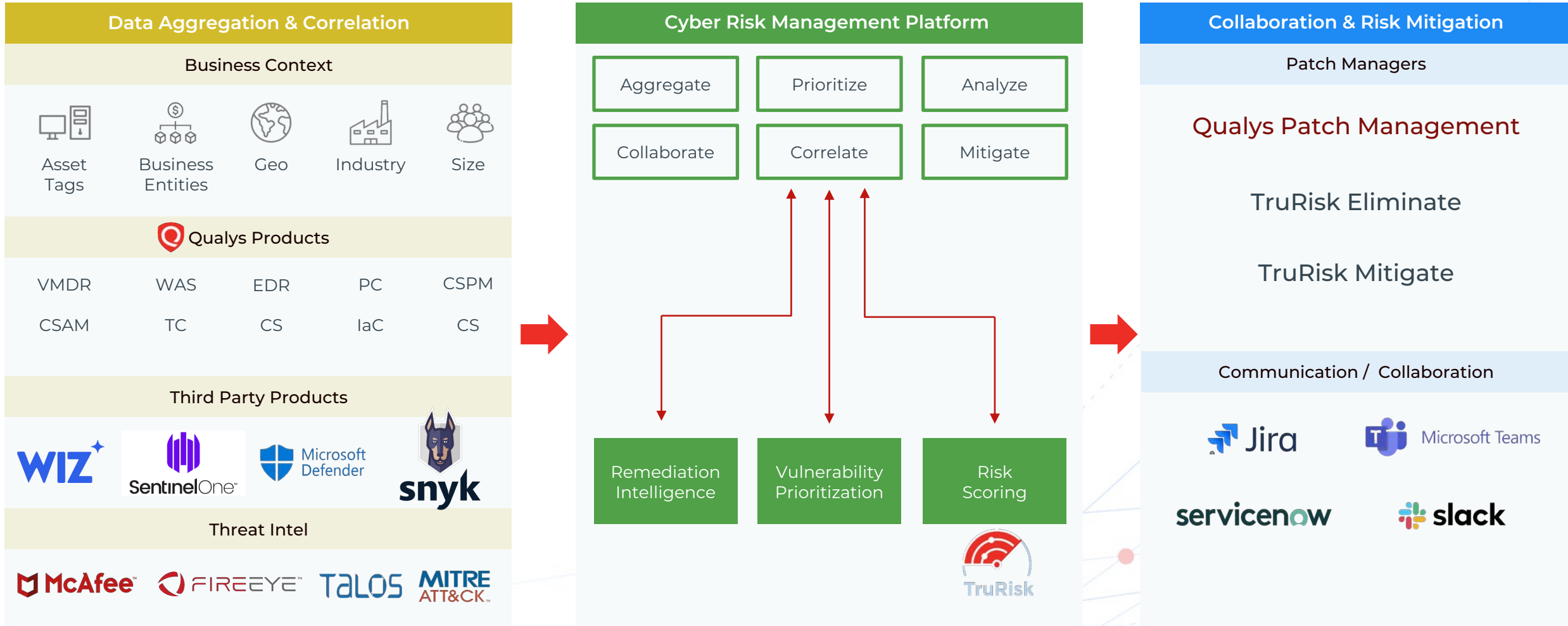## Unified Risk View

- **Aggregate cyber risk** across **Qualys & Non-Qualys Products** (cloud, application, infrastructure, etc)

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

- **Transition away** from difficult to manage in-house or expensive risk reporting tools

- Consolidate on **Qualys Cloud Platform for managing Cyber Risk**

Qualys.

Enterprise TruRisk Management

How does it work?

Data Aggregation & Correlation

Business Context

Asset Tags	Business Entities	Geo	Industry	Size

Qualys Products

VMDR	WAS	EDR	PC	CSPM
CSAM	TC	CS	IaC	CS

Third Party Products

WIZ · SentinelOne · Microsoft Defender · snyk

Threat Intel

McAfee · FIREEYE · Talos · MITRE ATT&CK

Cyber Risk Management Platform

Aggregate	Prioritize	Analyze
Collaborate	Correlate	Mitigate

Remediation Intelligence	Vulnerability Prioritization	Risk Scoring

TruRisk

Collaboration & Risk Mitigation

Patch Managers

Qualys Patch Management

TruRisk Eliminate

TruRisk Mitigate

Communication / Collaboration

Jira · Microsoft Teams · servicenow · slack

Qualys.

Supported Formats
Measure, Communicate, and Eliminate Cyber Risk Effectively

Manage Cyber Risk

Across the Enterprise Effectively

1.

Measure Risk Across The Organization

Get complete visibility across your organization from Qualys and Non-Qualys Tools
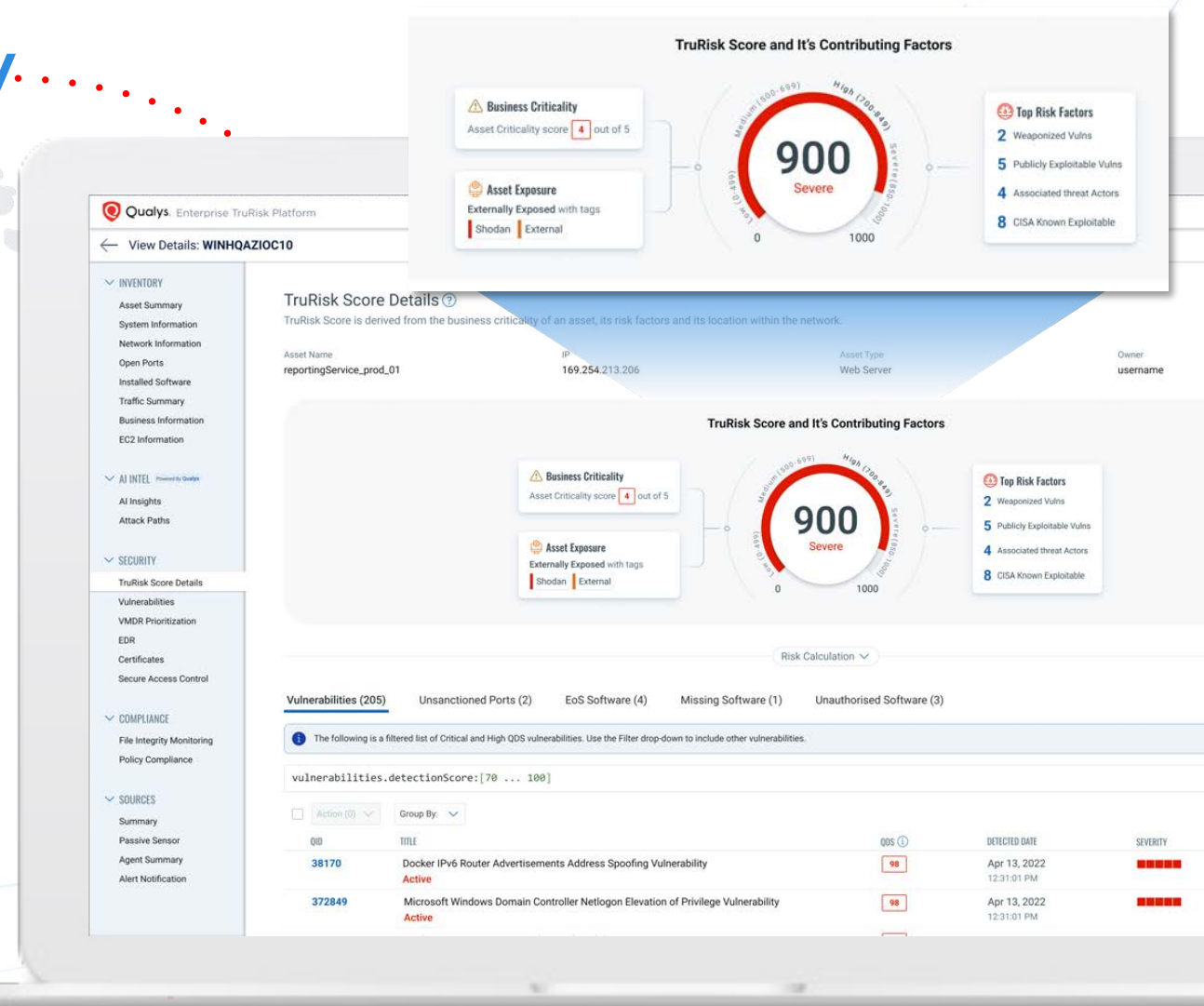
2.

Communicate Cyber Risk

Leverage unified risk scoring to communicate risk across the organization

3.

Eliminate Risk
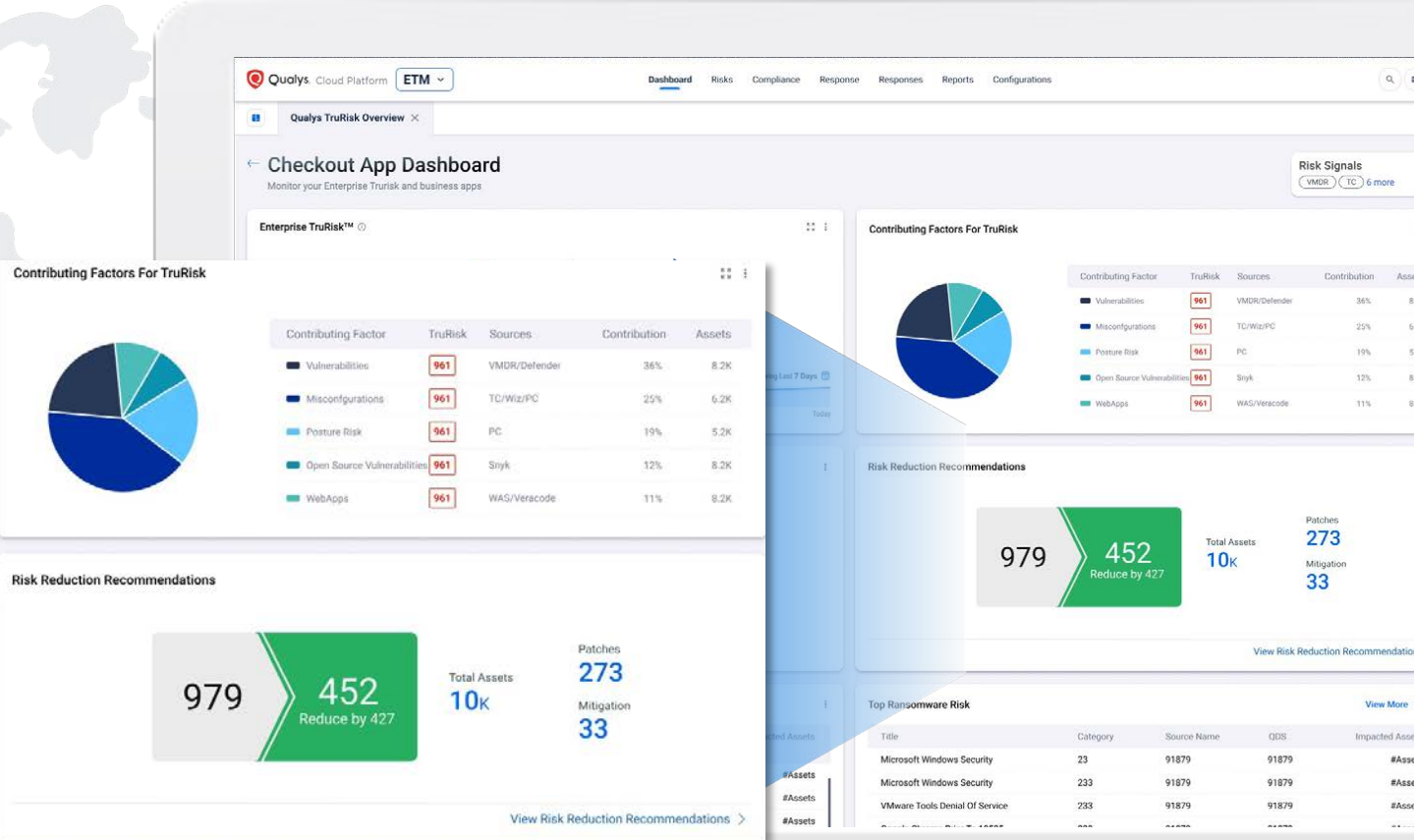
Leverage Qualys Intelligence to identify the top risks that will eliminate the most risk

Qualys

Communicate Cyber Risk

To All Stakeholders

1.

Measure Risk Across The Organization

Get complete visibility across your organization from Qualys and Non-Qualys Tools
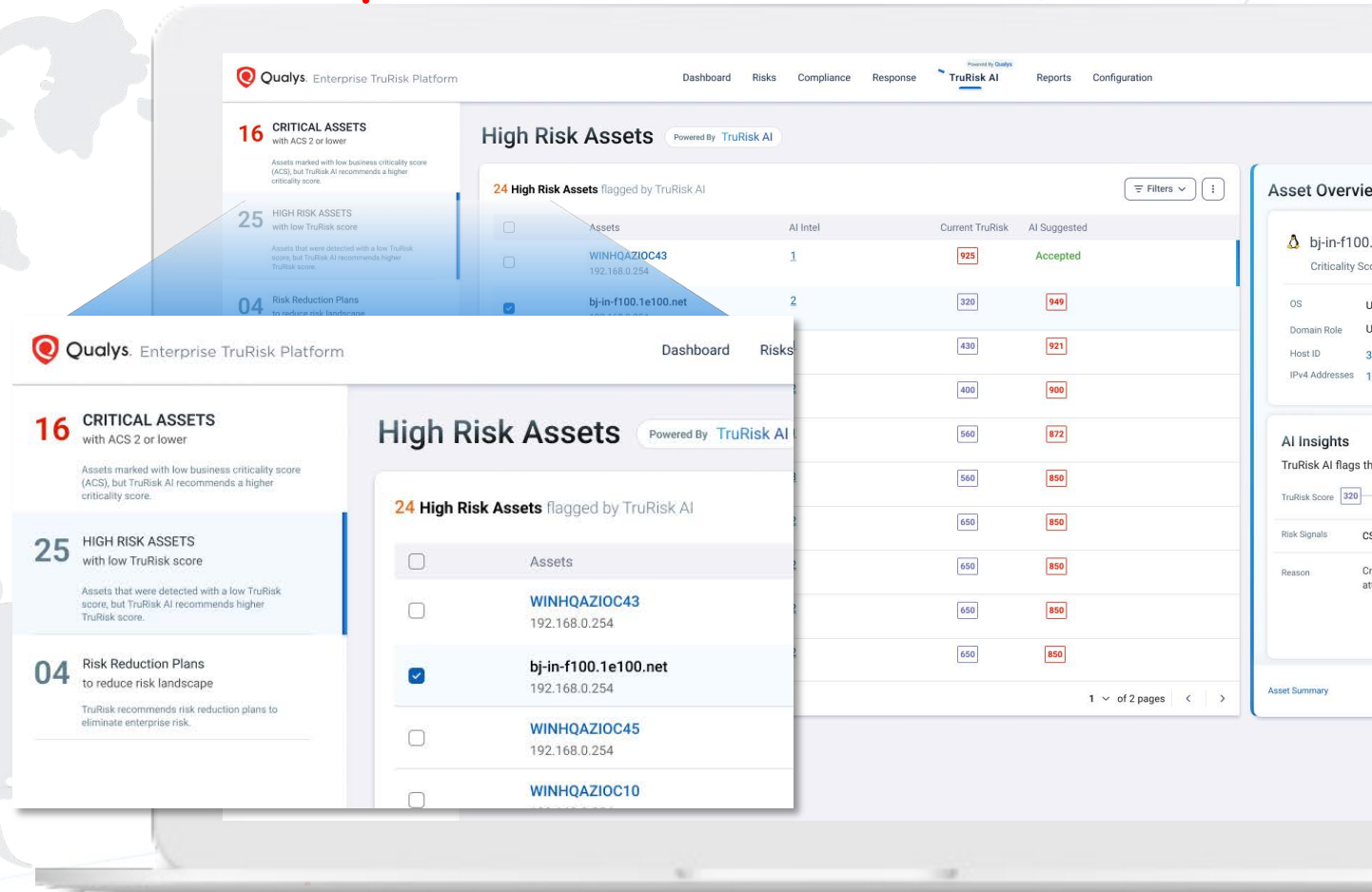
2.

Communicate Cyber Risk

Leverage unified risk scoring to communicate risk across the organization

3.

Eliminate Risk

Leverage Qualys Intelligence to identify the top risks that will eliminate the most risk

Qualys

Manage & Reduce Cyber Risk

Go Beyond Patching Alone

1. **Measure Risk Across The Organization**
Get complete visibility across your organization from Qualys and Non-Qualys Tools

2. **Communicate Cyber Risk**
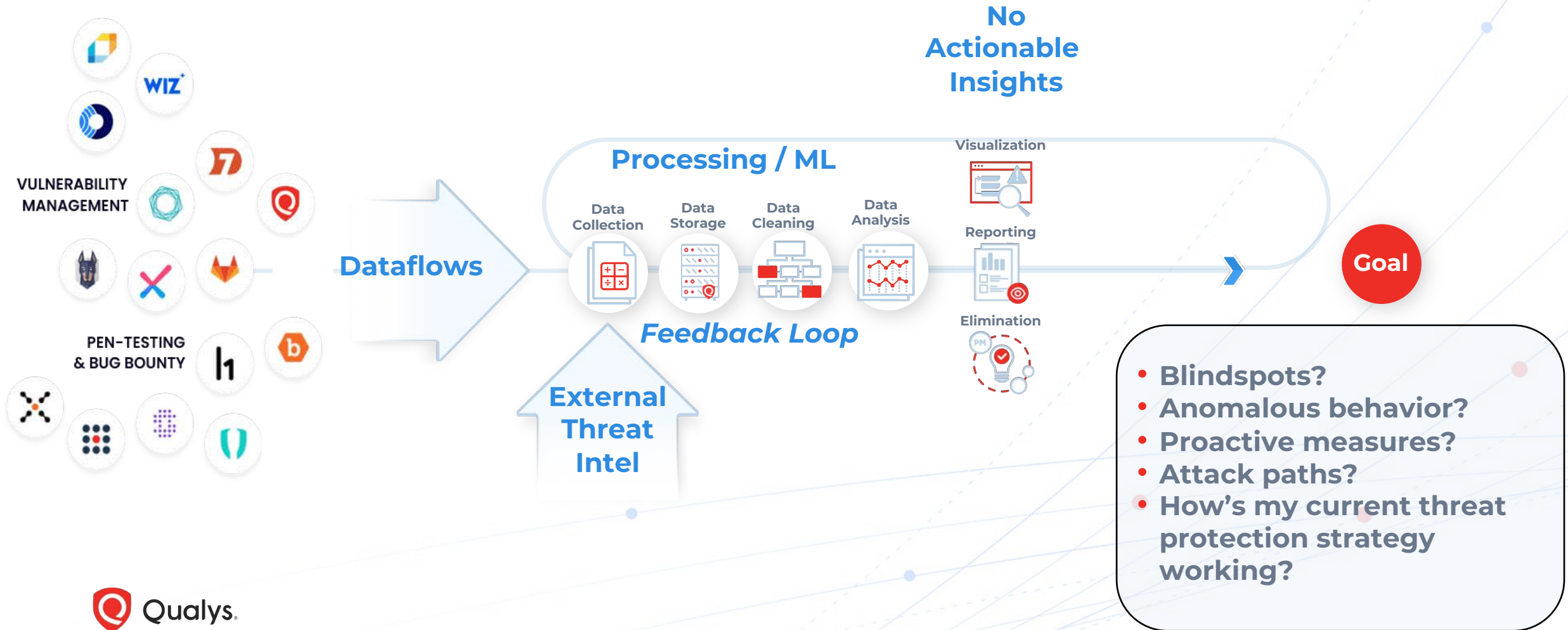Leverage unified risk scoring to communicate risk across the organization

3. **Eliminate Risk**
Leverage Qualys Intelligence to identify the top risks that will eliminate the most risk

Too Much Data – Few Insights
Too Many Reporting Tools that Don't Scale

VULNERABILITY MANAGEMENT

PEN-TESTING & BUG BOUNTY

WIZ

Dataflows

No Actionable Insights

Processing / ML

Data Collection

Data Storage

Data Cleaning

Data Analysis

Visualization

Reporting

Feedback Loop

Elimination

External Threat Intel

Goal

- **Blindspots?**
- **Anomalous behavior?**
- **Proactive measures?**
- **Attack paths?**
- **How's my current threat protection strategy working?**

Qualys

The Path to Cyber Risk Elimination

Measure, Communicate, and Eliminate Cyber Risk Effectively

Goal

The Qualys Solution set

- Cyber Asset Attack Surface Management (CSAM)
- Application & API security
- External Attack Surface Management (EASM)
- Vulnerability Management Detection and Response (VMDR)
- TotalCloud
- Patch Management (PM)
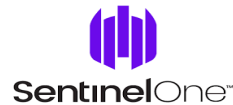- Policy Compliance (PC)
- **...and more**

IBM X-Force Red

+ TruRisk Quantification
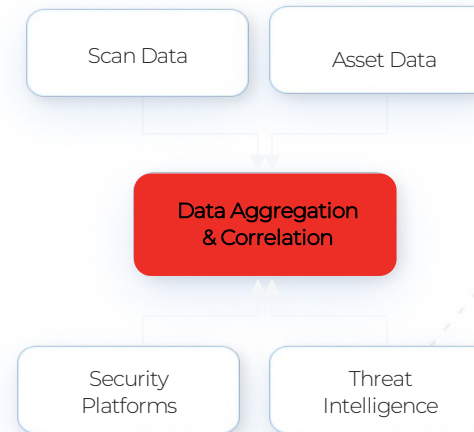
TruRisk

+ Non-Qualys Ecosystem

asimily

SYNOPSYS

SentinelOne

Security Scorecard

VERACODE

WIZ

SafeBreach

snyk

+ Aggregated Risk Signals

Scan Data	Asset Data

Data Aggregation & Correlation

Security Platforms	Threat Intelligence

Risk Elimination and Remediation Pathways

Patching

Configurations changes

Prescriptive Mitigation

Virtual Patching

Qualys.

Qualys Enterprise TruRisk Platform

Qualys
TruRisk™

Measure	Communicate	Eliminate

Internal & External Attack Surface Risk Management with Business Context

Detect, Prioritize, manage vulnerabilities, Misconfigurations

Map, Remediate vulns, misconfigs with Remediation Automation and intelligent workflows

Monitor, detect & respond & Prevent threats with Risk, business context

Drive compliance Monitoring, Reporting for Industry mandates, standards

Asset Management → Vulnerability & Configuration Management → Risk Remediation → Threat Detection Response → Compliance

First-Party OSS

API   LIGHTWEIGHT AGENT   PLATFORM SERVICES   SENSORS

3rd Party Data

APPLICATIONS   OPERATING SYSTEMS   CLOUD / CONTAINERS / VMs   IT / WORKSTATIONS / SERVERS   IOT   EXTERNAL DEVICES

workday.   Office 365   SAP   Windows   Linux   Apple   aws   Google Cloud   Azure