QSC24

Qualys Threat Research Unit: The ‘TRU’ Power Behind Qualys Solutions

Sandeep Potdar
Senior Director, Product Management, VMDR
Oct 10, 2024

Threat Research Unit (TRU): What Powers Qualys

Award Winning Research Team

✓ **Two**
Pwnie Award Wins

✓ **12+**
Pwnie Award Nominations

✓ **120+**
Strong Research Team continuously monitors new threats

Examples of Qualys TRU Discoveries

CVE Identifier	CISA KEV	Named Vulnerabilities	Component Affected	Description
CVE-2023-6779	No	NA	glibc	Off-by-one heap-based buffer overflow in the _vsyslog_internal (function).
CVE-2023-6780	No	NA	glibc	Integer overflow issue in the _vsyslog_internal (function).
CVE-2023-4911	**Yes**	**Looney Tunables**	**glibc (ld.so)**	**Local Privilege Escalation.**
CVE-2023-38480	No	NA	OpenSSH (ssh-agent)	Remote Code Execution in forwarded ssh-agent.
CVE-2023-33865	No	NA	RenderDoc	Local symlink vulnerability allowing attackers to gain RenderDoc user privileges.
CVE-2023-33864	No	NA	RenderDoc	Integer underflow causing a heap-based buffer overflow, exploitable remotely.
CVE-2023-33863	No	NA	RenderDoc	Integer overflow leading to a heap-based buffer overflow, potentially exploitable remotely.
CVE-2023-41974	No	Leeloo Multipath	multipathd	Authorization bypass and symlink attack.
CVE-2023-41973	No	Leeloo Multipath	multipathd	Authorization bypass and symlink attack.
CVE-2023-44731	No	Oh Snap! More Lemmings	snap-confine	Local Privilege Escalation Vulnerability.
CVE-2021-4034	**Yes**	**PwnKit**	**polkit's pkexec**	**Local Privilege Escalation Vulnerability.**
CVE-2021-33910	No	NA	systemd	Denial of Service (Stack Exhaustion).
21 CVEs/Vulnerabilities	No	21Nails	Exim Mail Server	Multiple Critical Vulnerabilities.
CVE-2021-33909	No	Sequoia	Linux's Filesystem Layer	Local Privilege Escalation Vulnerability.

regreSSHion CVE-2024-6387: Risk is Across Hybrid Infrastructure

14 Million

Potentially vulnerable OpenSSH server instances exposed to the Internet, based on searches using Censys and Shodan.

700k

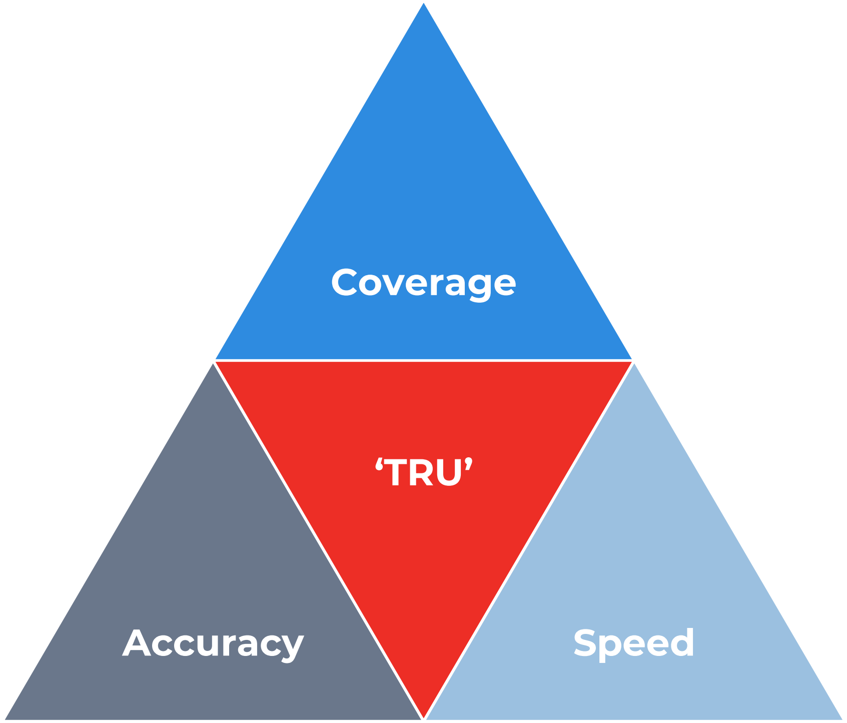
External internet-facing instances are vulnerable based on anonymized data from Qualys.

Why Critical

Unauthenticated remote code execution, Grants full Root Access and Poses a Significant Exploit Risk.

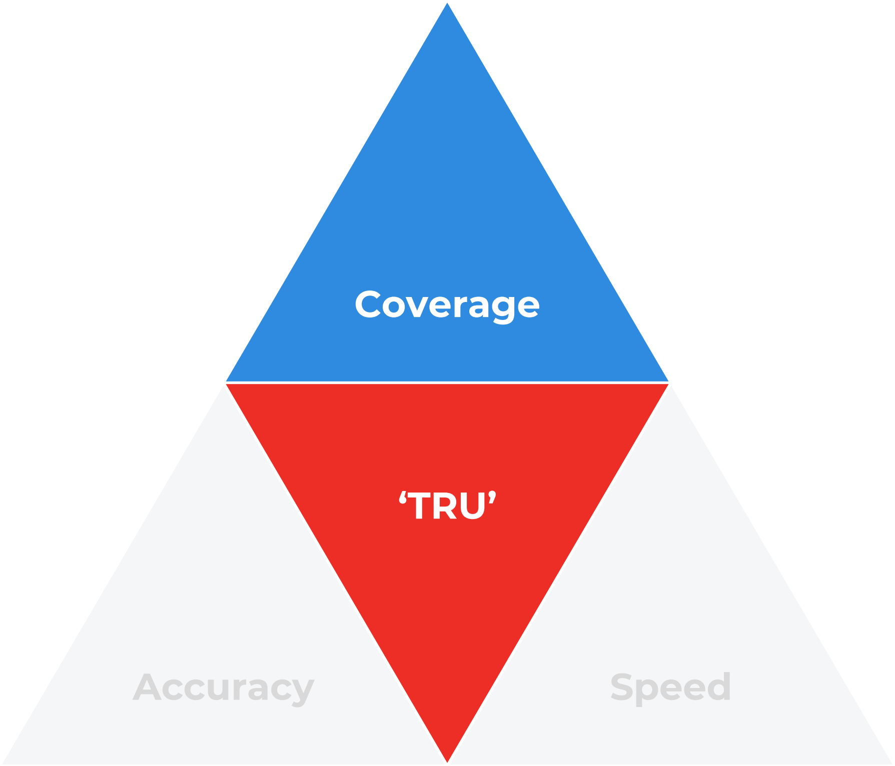
The Unbeatable Trifecta

The **fastest**, the most **accurate**, and the most **comprehensive**



- Most Comprehensive Coverage
- Fastest Response Time
- Six-sigma Accuracy

The Unbeatable Trifecta



Most Comprehensive Coverage

Fastest Response Time

Six-sigma Accuracy

Unmatched Product Support and Technological Coverage

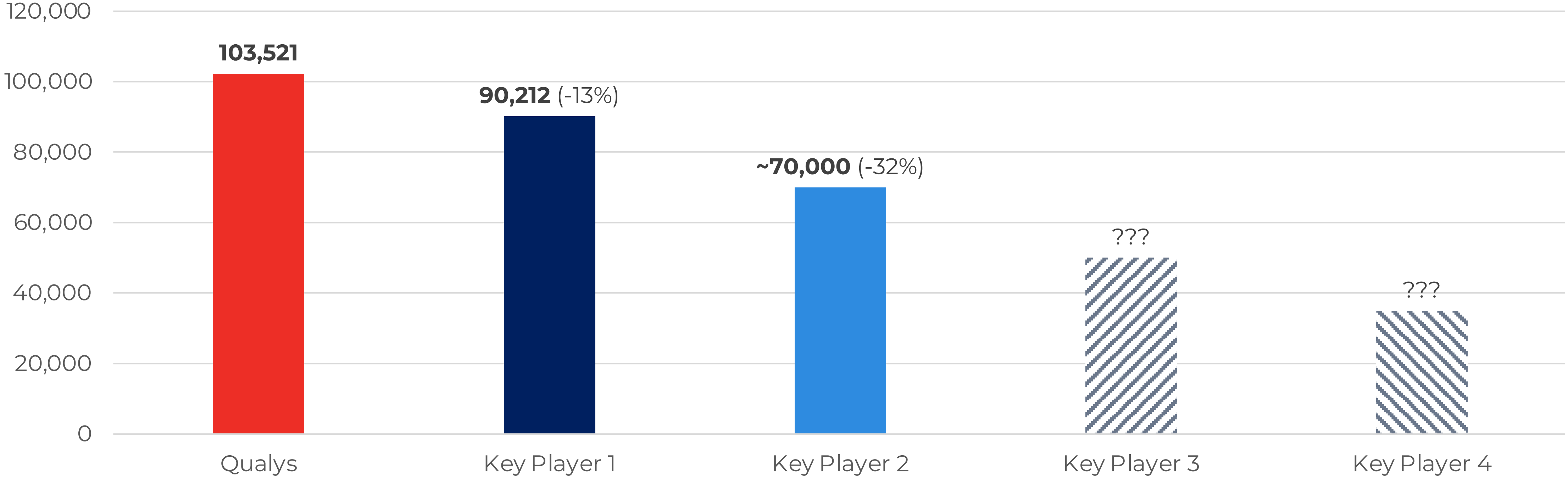
Broad Technology Spectrum

We cover various technologies, including operating systems, network devices, web servers, productivity suites, and security software, offering tailored security solutions for diverse environments.

Extensive OS and Architecture Coverage

Robust support for multiple operating systems such as Windows, Linux, BSD, IBM AIX, and Apple MacOS across various architectures, ensuring superior compatibility and comprehensive security.

CVE Coverage Comparison & Transparency



Updated: Sep 18, 2024

CISA Known Exploited Vulnerabilities - Catalog Coverage

Rapid identification of critical vulnerabilities from the CISA KEV Catalog.

We safeguard the enterprises with coverage for **1166** out of **1181** CVE items in the CISA KEV, amounting to **98.7%*** coverage.

We set the industry standard with the most **comprehensive coverage** of CISA KEV.

21.74%

of CVEs are for actively exploited network and perimeter devices.

*The remaining 1.3% are predominantly vulnerabilities in outdated services, off-market products, or products with minimal enterprise value.
Updated: Sep 18, 2024

Breadth vs Depth

Exploit-based checks provide customers with attacker view of vulnerabilities.

Extensive coverage across operating systems, middleware, network device, web servers, productivity, and security software.

Provides enhanced contextual details *(impact, severity, conditions)* for better risk prioritization.

Deep checks that go beyond NVD CPE information resulting in better accuracy.

Competitive Advantage in Handling Non-CVE Vulnerabilities and Information Gathered QIDs

01

Extensive Coverage

Specializes in detecting non-CVE vulnerabilities, misconfigurations, detailed network insights, that set Qualys apart in the industry.

02

Advanced Vulnerability Detection

Qualys identifies non-CVE vulnerabilities and Information Gathered QIDs, offering insights into overlooked security risks.

03

Proactive Security Approach

Our strategy empowers organizations to tackle emerging threats preemptively, moving beyond traditional CVE-based responses.

12,900+ Non-CVE QIDs

Supply Chain Attacks:

A Growing Cyber Threat

The 2024 Verizon DBIR highlights a significant rise in breaches tied to third-party software and supply chain attacks, now accounting for 15% of all data breaches — **a 68% increase from the previous year.”**

2024 Data Breach Investigations Report

verizon business

SCA - Now Fully Integrated in VMDR

Complete Software Coverage:

Bundles SCA with VMDR for comprehensive vulnerability detection.

Detect More Vulnerabilities:

Activating SCA uncovers 15,830 additional vulnerabilities.

SCA helps mitigate Log4j-like vulnerabilities:

SCA identifies open-source components, detects specific security flaws, and accelerates remediation with streamlined updates.

Expand Coverage with Qualys
Custom Assessment & Remediation (CAR)

Bring Your Own QID
Write your own vuln custom detection scripts to measure your risk

Run Your Own Remediation Scripts
Qualys agents run your custom scripts

Fully Integrated Into VMDR
Measure and communicate custom risk as part of VMDR

PowerShell

python™ Perl

Lua vbscript

AI/LLM Security

AI/LLM Security Excellence:

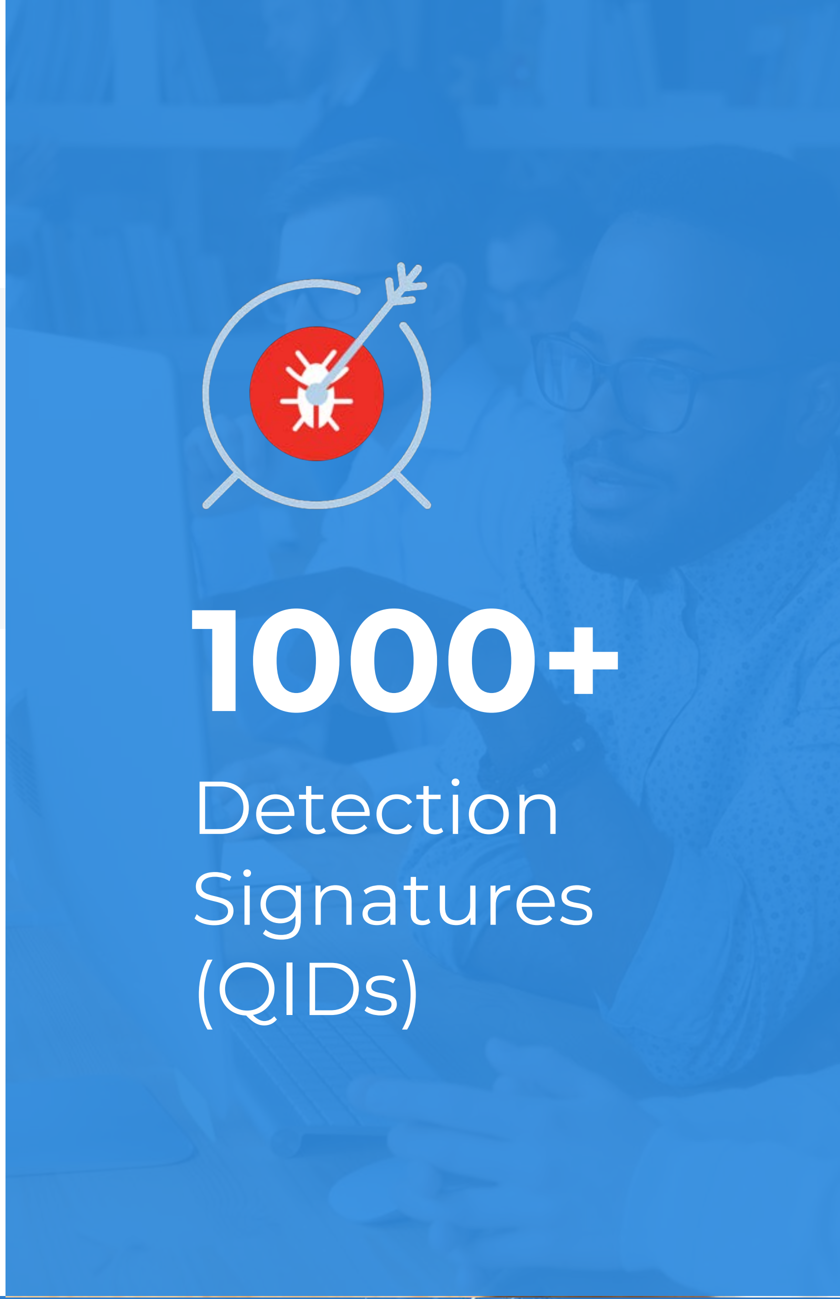
We proactively monitor sophisticated AI threats and identify vulnerabilities, from poisoned data sources and malicious pre-trained models to compromised dependencies and manipulated build processes, leveraging security to protect AI infrastructure.

Comprehensive AI Software Coverage:

- **Machine Learning Frameworks:**
  Extensive QID coverage for major tools including **TensorFlow** (496 QIDs), **PyTorch** (13 QIDs), and **Scikit-learn** (3 QIDs).

- **Development & Deployment Tools:**
  Support for **Jupyter Notebook** (52 QIDs), **OpenCV** (47 QIDs), **Mlflow** (33 QIDs), among others.

- **Emerging Technologies:**
  Includes coverage for **Anyscale Ray, ONNX, Apache MXNet, and Hugging Face** Transformers.



1000+

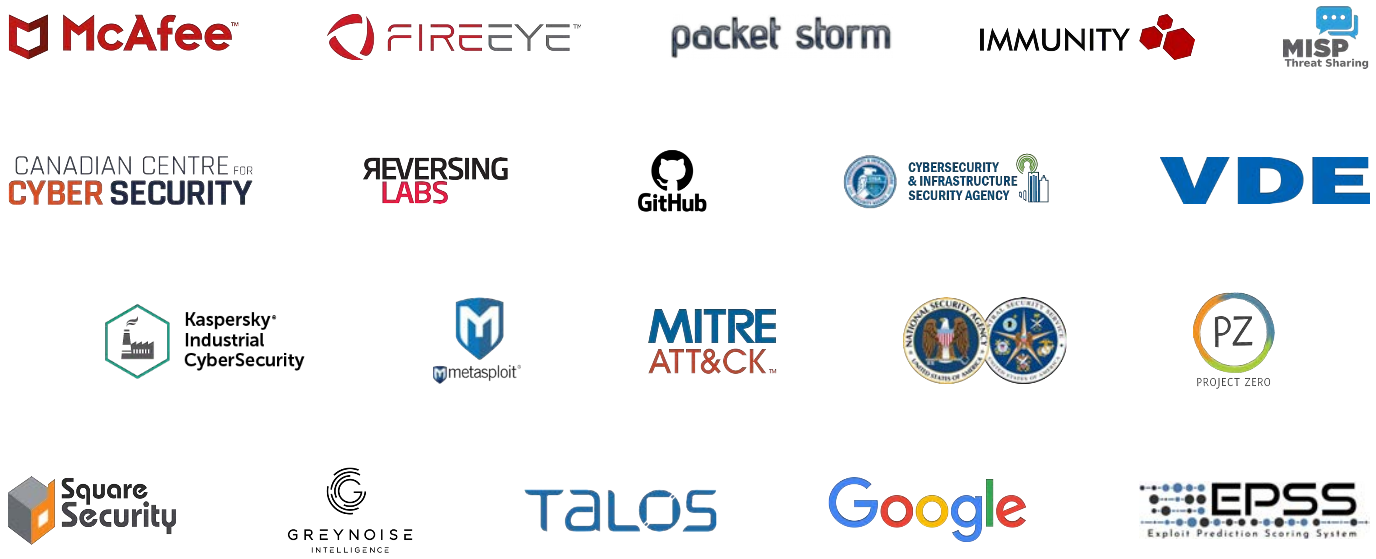
Detection Signatures (QIDs)

Real-time Threat Indicators (RTI)

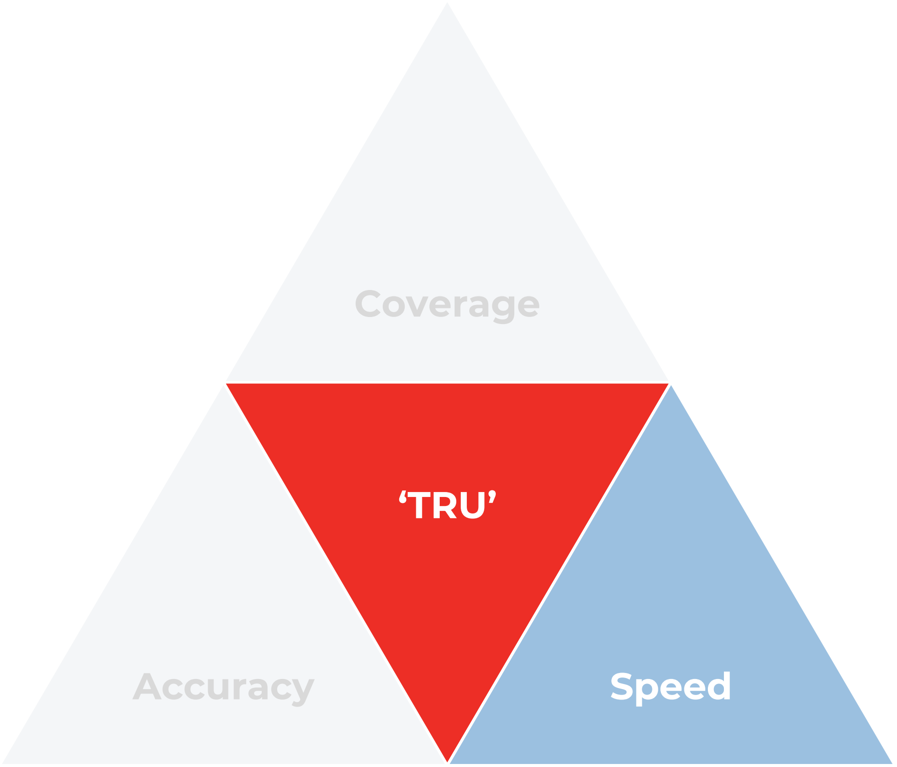
Best-In-Class Threat Intelligence Included

Leverage insights from over 200k vulnerabilities sourced from over **25+ threat sources** to get best-in-class threat intelligence with the Qualys Cloud Threat DB

25+ Threat & Exploit Intelligence Sources



The Unbeatable Trifecta



Most Comprehensive Coverage

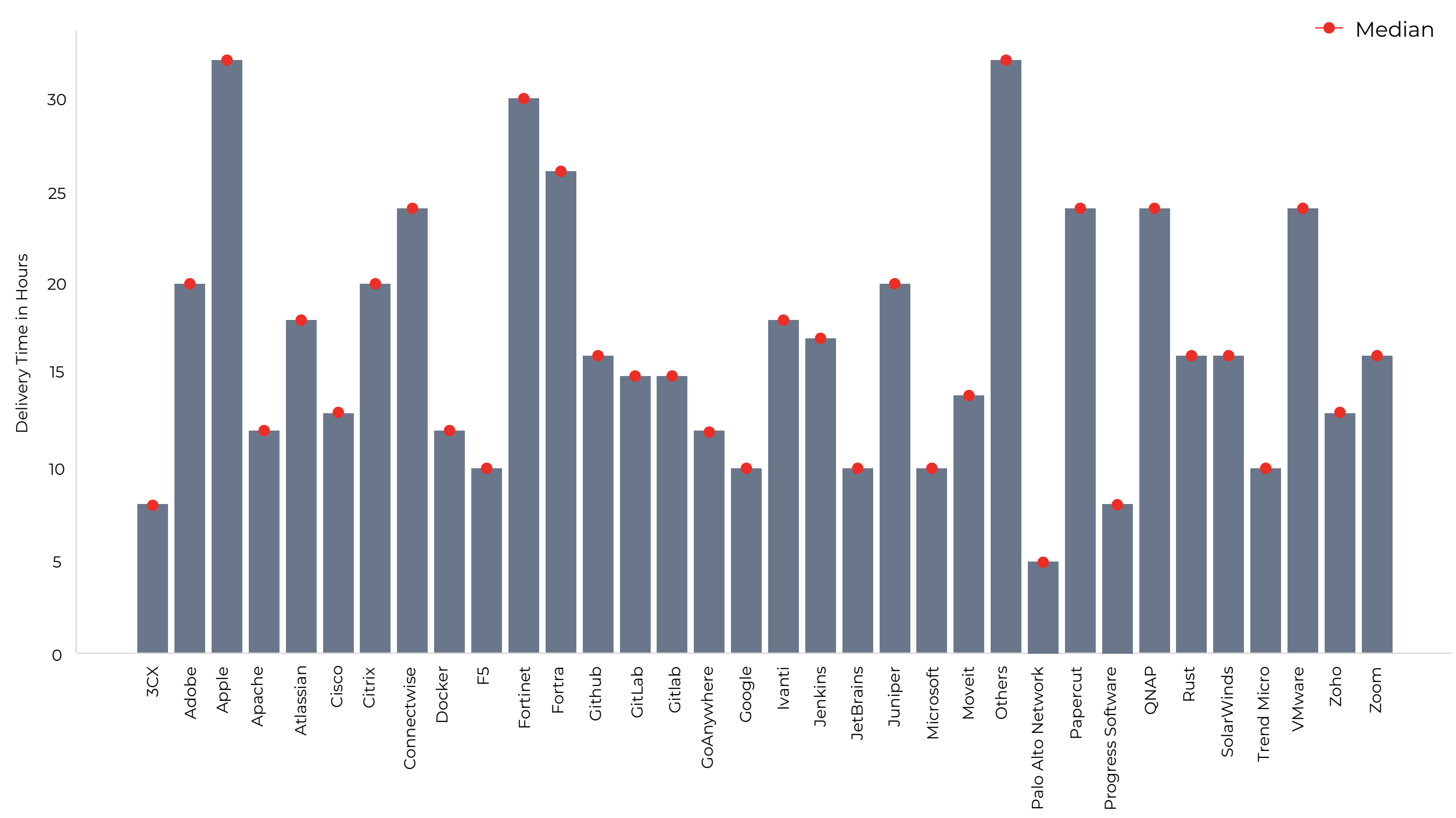
Fastest Response Time

Six-sigma Accuracy

Vulnerability Detection Times by Vendor (2023-2024)

This chart shows Qualys' median detection times

for Zero-Day and Critical vulnerabilities in 2023 and 2024, with a median response time of 16 hours.



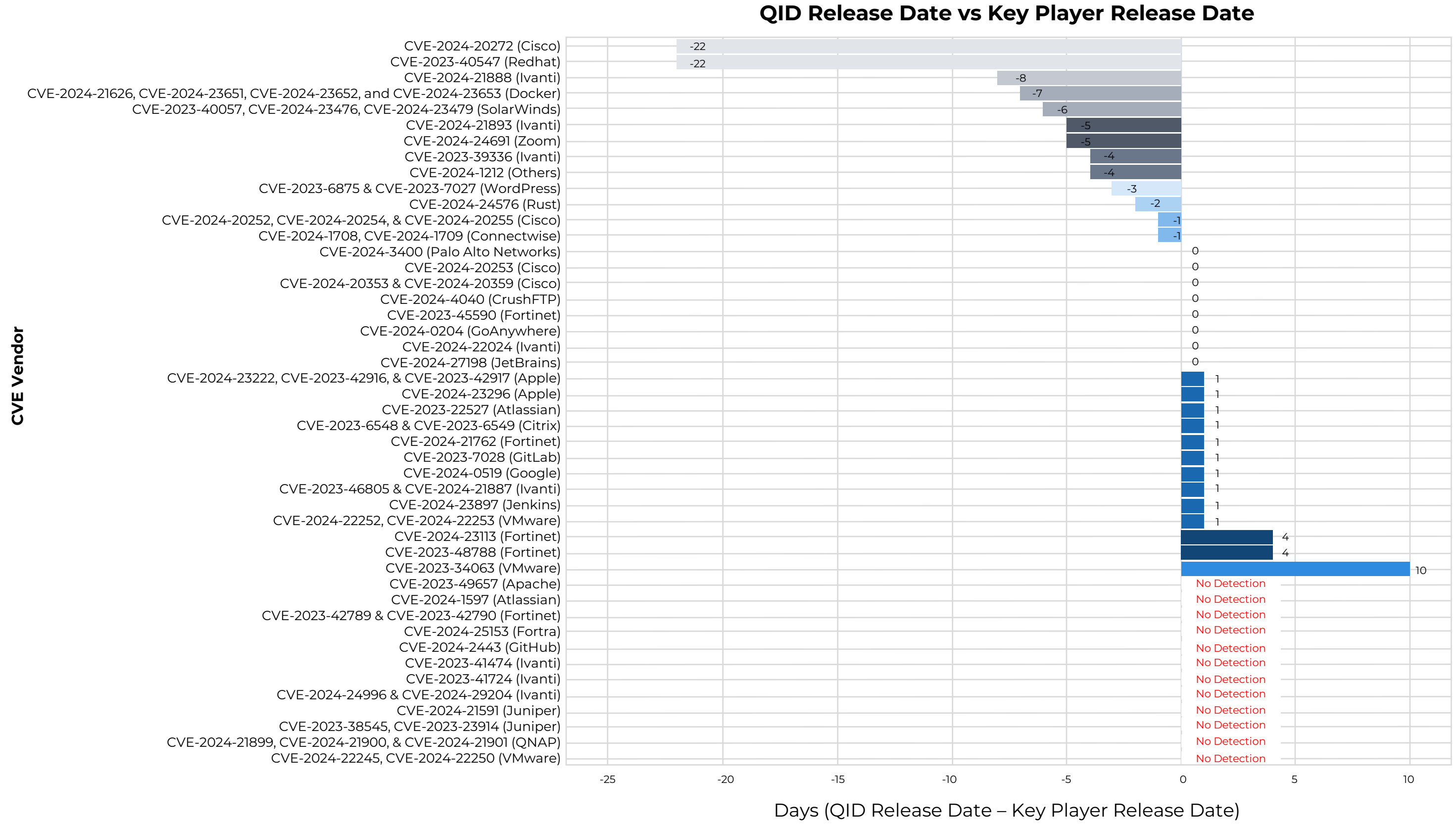
Zero-Day/Critical Vulnerability Detection Delivery Time by Vendor (Median Response Time of 16 Hours)

Comparative Detection Times for Critical Vulnerabilities

This clustered chart illustrates the comparative detection times for key Zero-Day and Critical CVEs between our system and a major competitor.

Key Points:

- ✓ Negative values indicate instances where we detected vulnerabilities up to 22 days before our competitor.
- ✓ Zero values represent cases where both vendors released detections simultaneously.
- ✓ Positive values show when the competitor detected vulnerabilities before us.



Proactive Threat Intelligence

Showcasing our foresight in identifying emerging threats before they are recognized by national cybersecurity authorities.

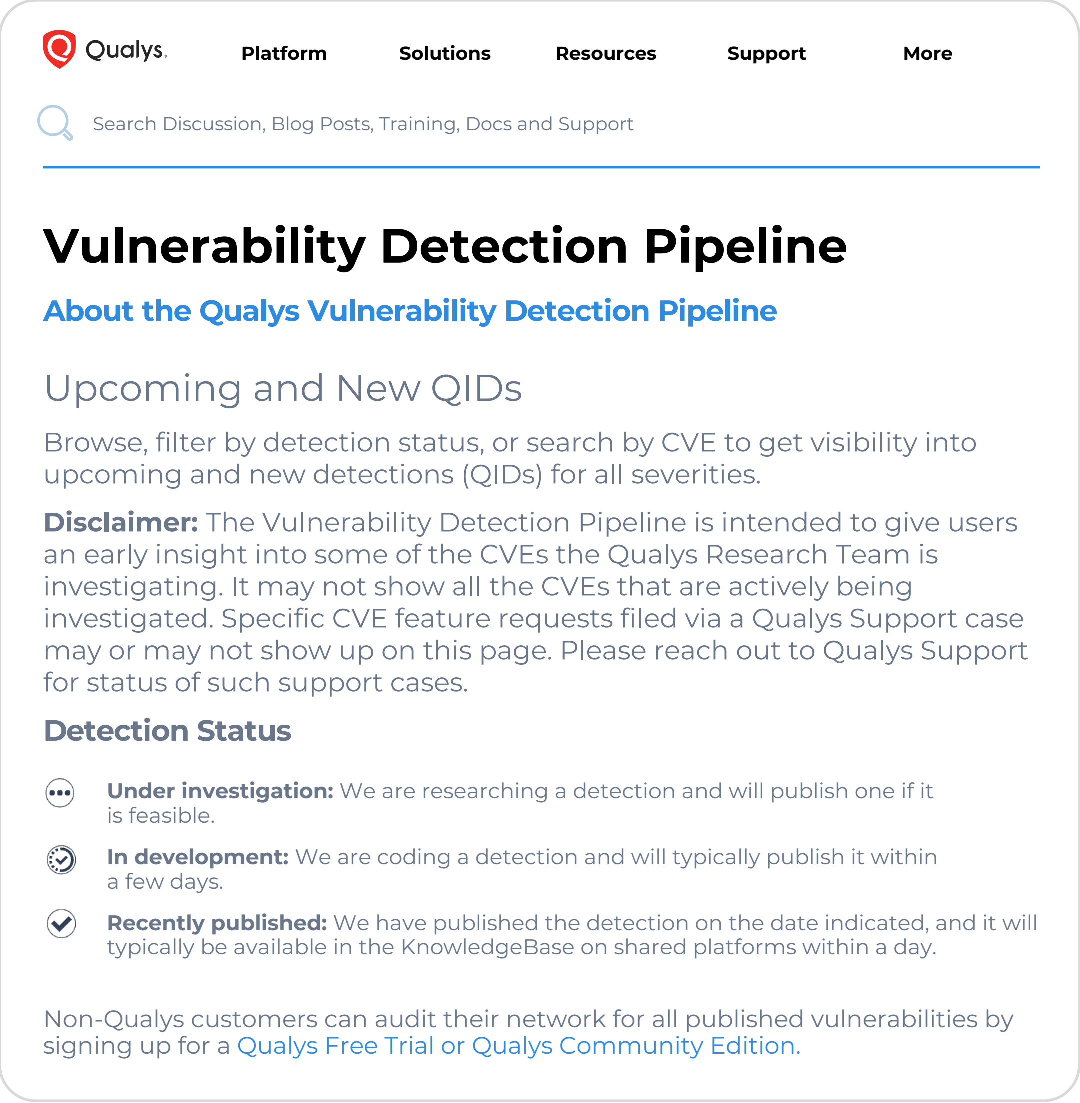
Spotlight:

CVE-2024-23897

Jenkins Core

Recognized by Qualys in the 2024 Midyear Threat Landscape Review, this vulnerability was added to CISA's KEV two weeks after our initial identification among the Top 10 Exploited Vulnerabilities.

Empowering proactive defenses with advanced threat intelligence from Qualys Threat Research Unit (TRU).



Vulnerability Detection Pipeline

About the Qualys Vulnerability Detection Pipeline

Upcoming and New QIDs

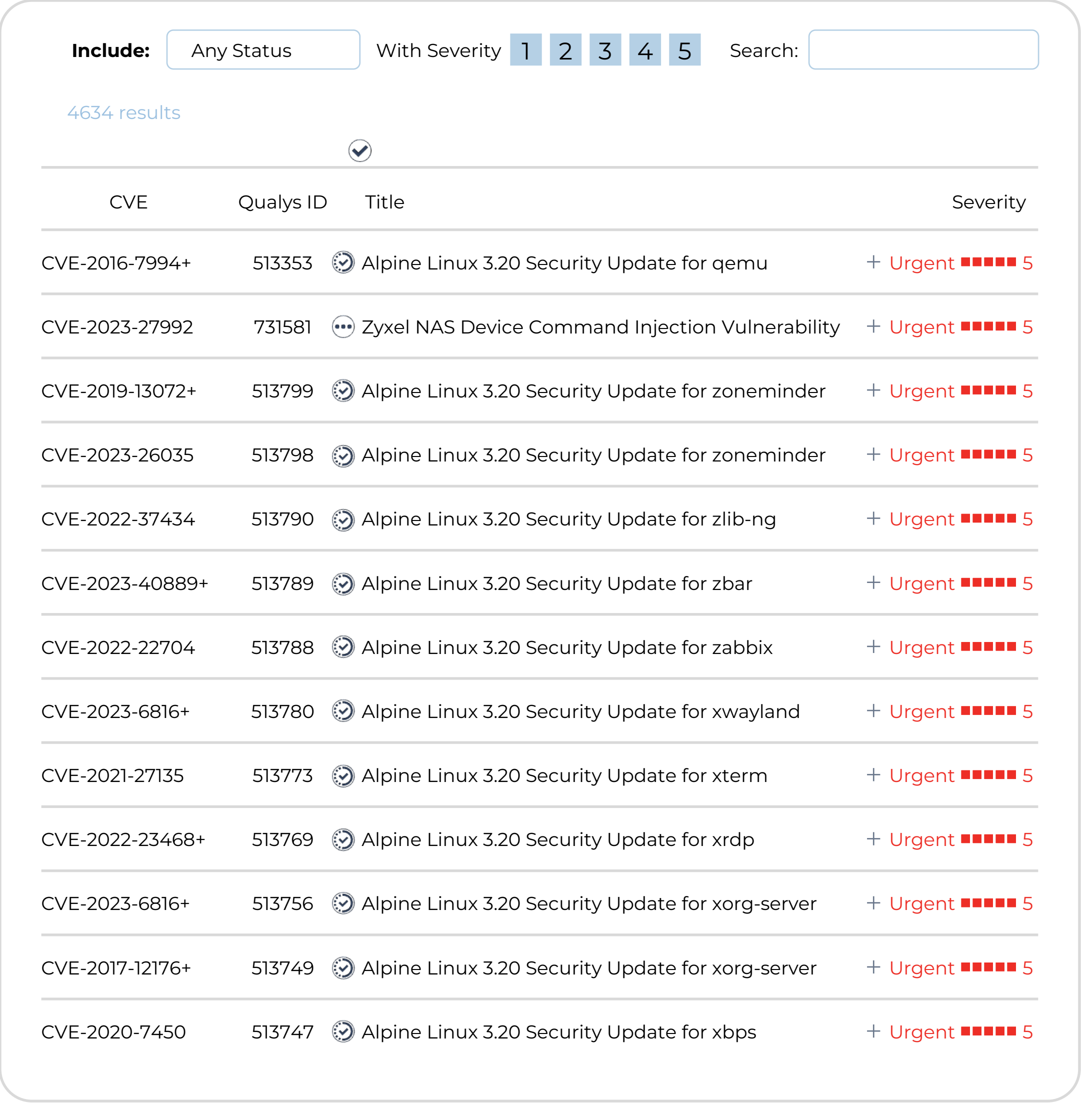
Browse, filter by detection status, or search by CVE to get visibility into upcoming and new detections (QIDs) for all severities.

Disclaimer: The Vulnerability Detection Pipeline is intended to give users an early insight into some of the CVEs the Qualys Research Team is investigating. It may not show all the CVEs that are actively being investigated. Specific CVE feature requests filed via a Qualys Support case may or may not show up on this page. Please reach out to Qualys Support for status of such support cases.

Detection Status

- ••• **Under investigation:** We are researching a detection and will publish one if it is feasible.
- ◷ **In development:** We are coding a detection and will typically publish it within a few days.
- ✓ **Recently published:** We have published the detection on the date indicated, and it will typically be available in the KnowledgeBase on shared platforms within a day.

Non-Qualys customers can audit their network for all published vulnerabilities by signing up for a Qualys Free Trial or Qualys Community Edition.

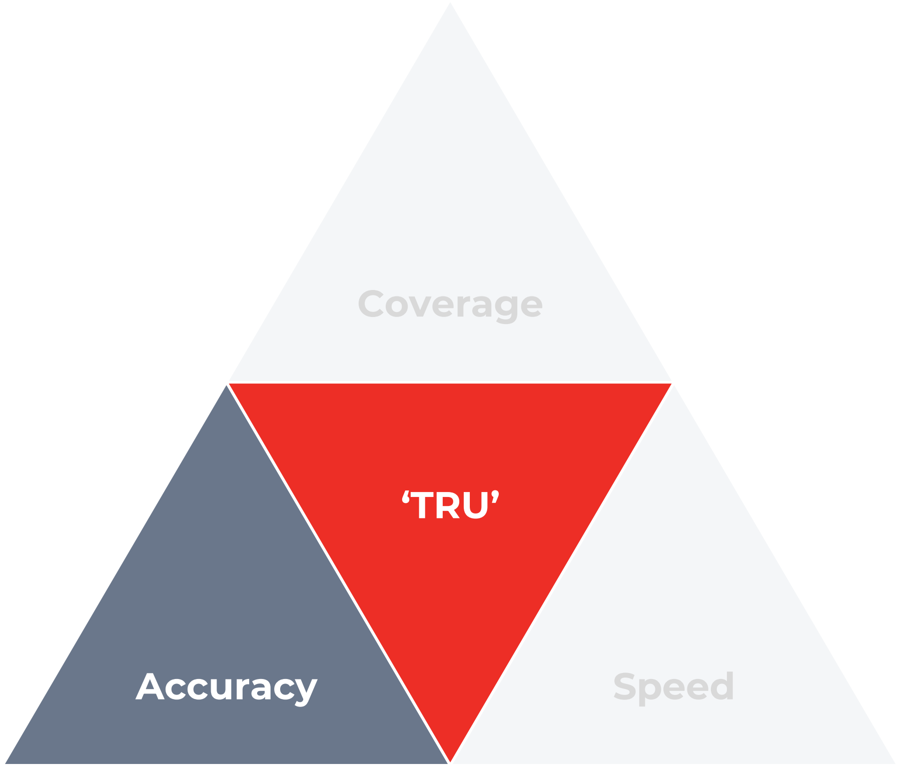


4634 results

CVE	Qualys ID	✓	Title	Severity
CVE-2016-7994+	513353	◷	Alpine Linux 3.20 Security Update for qemu	+ Urgent ■■■■■ 5
CVE-2023-27992	731581	•••	Zyxel NAS Device Command Injection Vulnerability	+ Urgent ■■■■■ 5
CVE-2019-13072+	513799	◷	Alpine Linux 3.20 Security Update for zoneminder	+ Urgent ■■■■■ 5
CVE-2023-26035	513798	◷	Alpine Linux 3.20 Security Update for zoneminder	+ Urgent ■■■■■ 5
CVE-2022-37434	513790	◷	Alpine Linux 3.20 Security Update for zlib-ng	+ Urgent ■■■■■ 5
CVE-2023-40889+	513789	◷	Alpine Linux 3.20 Security Update for zbar	+ Urgent ■■■■■ 5
CVE-2022-22704	513788	◷	Alpine Linux 3.20 Security Update for zabbix	+ Urgent ■■■■■ 5
CVE-2023-6816+	513780	◷	Alpine Linux 3.20 Security Update for xwayland	+ Urgent ■■■■■ 5
CVE-2021-27135	513773	◷	Alpine Linux 3.20 Security Update for xterm	+ Urgent ■■■■■ 5
CVE-2022-23468+	513769	◷	Alpine Linux 3.20 Security Update for xrdp	+ Urgent ■■■■■ 5
CVE-2023-6816+	513756	◷	Alpine Linux 3.20 Security Update for xorg-server	+ Urgent ■■■■■ 5
CVE-2017-12176+	513749	◷	Alpine Linux 3.20 Security Update for xorg-server	+ Urgent ■■■■■ 5
CVE-2020-7450	513747	◷	Alpine Linux 3.20 Security Update for xbps	+ Urgent ■■■■■ 5

Ref: https://www.qualys.com/vulnerability-detection-pipeline/

The Unbeatable Trifecta



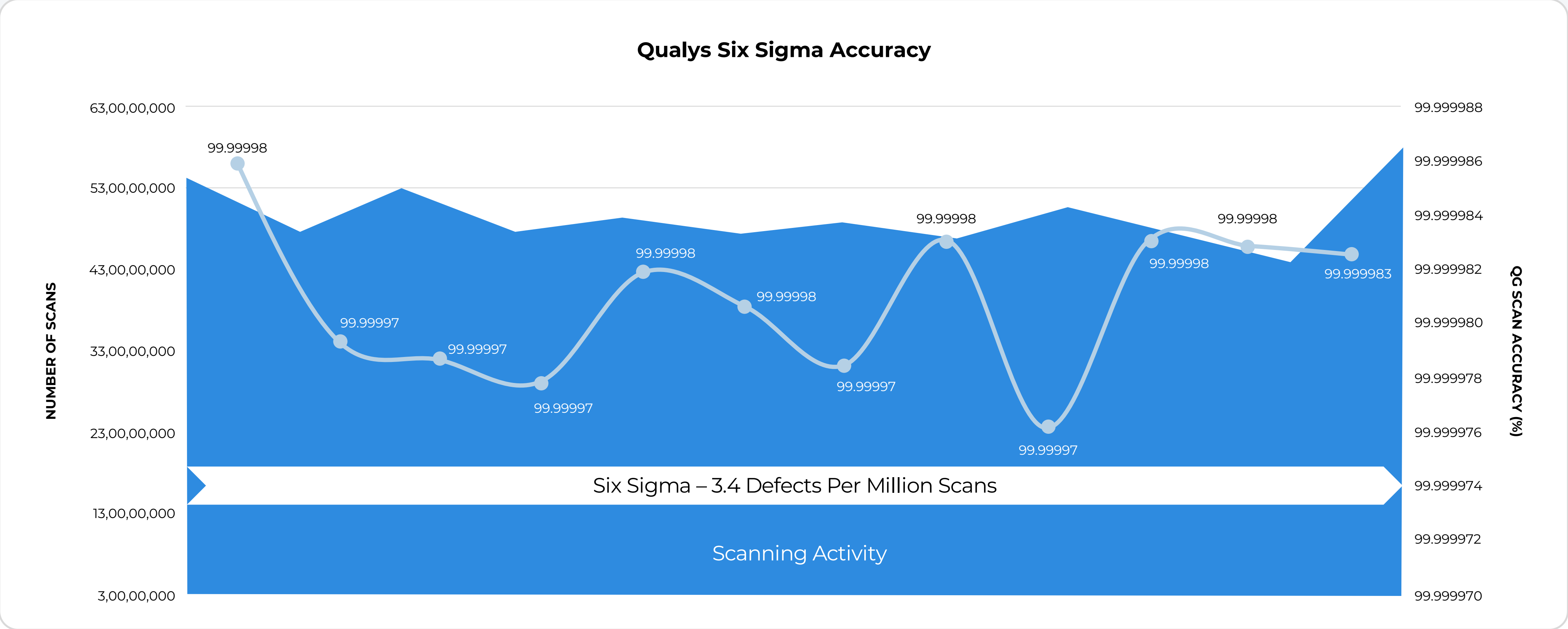
Most Comprehensive Coverage

Fastest Response Time

Six-sigma Accuracy

Detection Accuracy

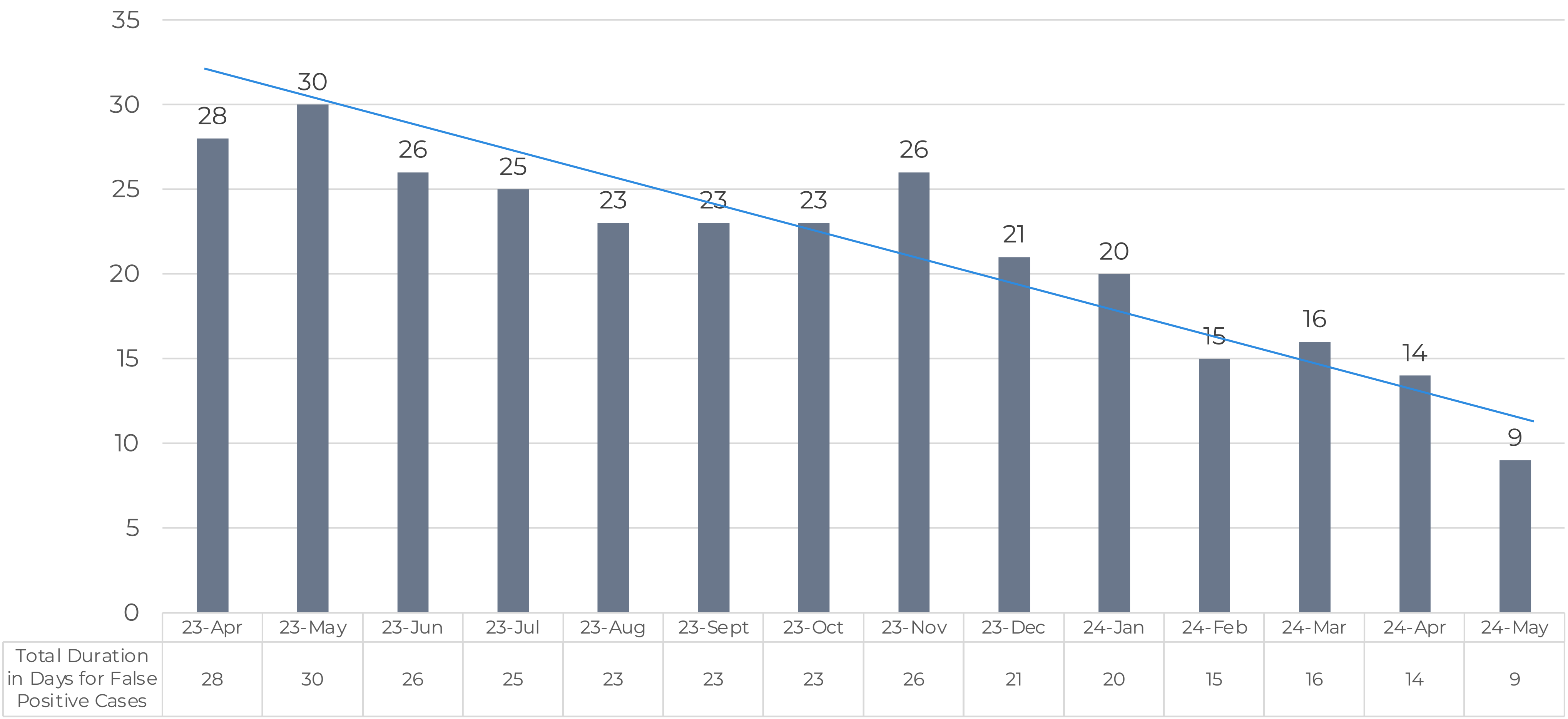
Over 10 Years Achieving Six-Sigma Accuracy in Detection



DE-RISK YOUR **BUSINESS**

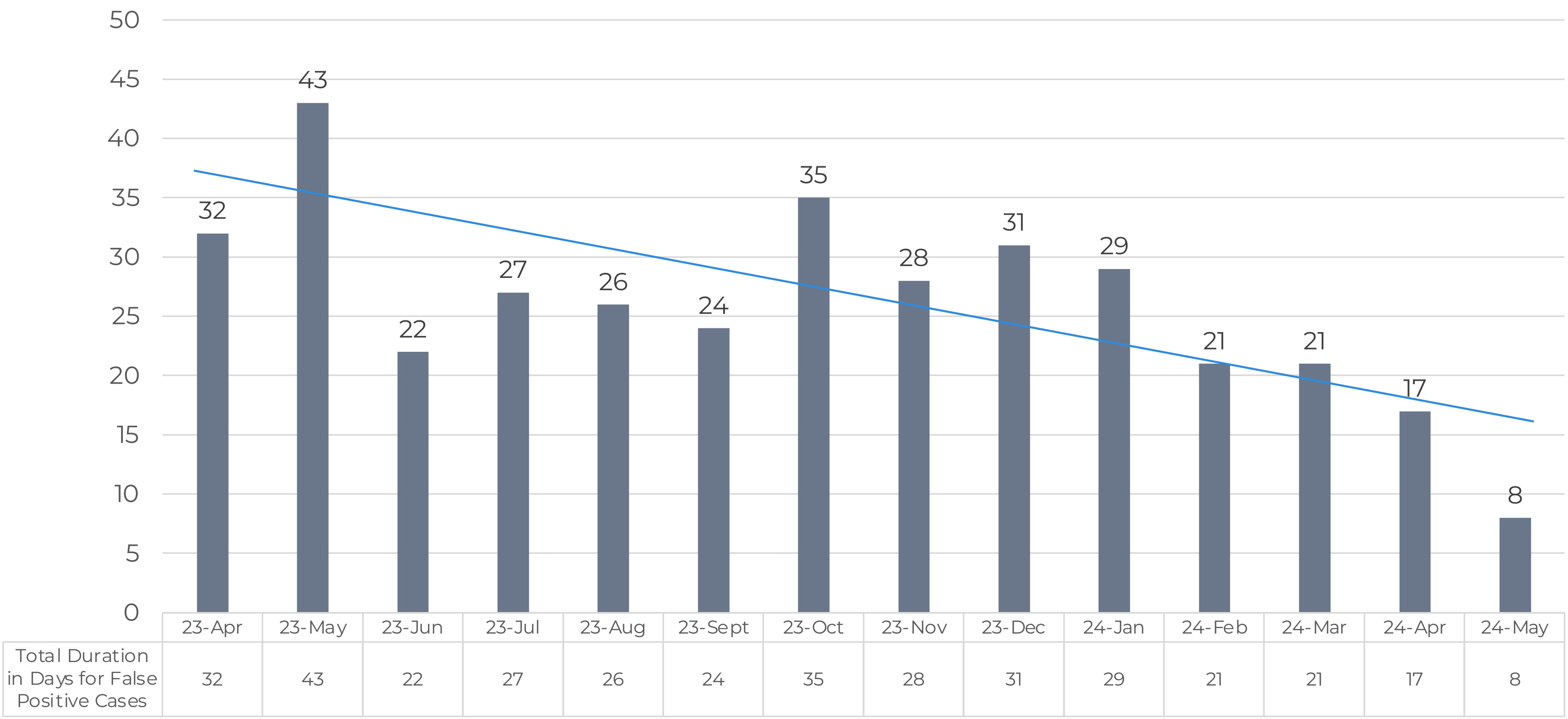
Qualys.

Total Duration in Days for False Positive Cases



	23-Apr	23-May	23-Jun	23-Jul	23-Aug	23-Sept	23-Oct	23-Nov	23-Dec	24-Jan	24-Feb	24-Mar	24-Apr	24-May
Total Duration in Days for False Positive Cases	28	30	26	25	23	23	23	26	21	20	15	16	14	9

Total Duration in Days for False Negative Cases



	23-Apr	23-May	23-Jun	23-Jul	23-Aug	23-Sept	23-Oct	23-Nov	23-Dec	24-Jan	24-Feb	24-Mar	24-Apr	24-May
Total Duration in Days for False Positive Cases	32	43	22	27	26	24	35	28	31	29	21	21	17	8

Advanced Detection Capabilities

13,000+

Signatures coupled with **active probing techniques** to precisely identify vulnerabilities.

Exploit-Based Risk Assessment:

We use exploit-based checks to assess risks, accurately minimizing false positives. This approach offers insights from an attacker's standpoint, effectively managing vulnerabilities like Log4Shell and BlueKeep.

Kernel Package Protection:

Our detection extends to all kernel packages, with capabilities to distinguish active from non-active kernels, ensuring focused and relevant vulnerability management.

Superior Detection Methods:

We employ dynamic evaluation for in-depth checks, which include verifying the actual presence of files, providing a more comprehensive detection than typical software inventory assessments.

Summary

103,521

Identified Vulnerabilities/ CVEs

187,113

Detection Signatures (QIDs)

120+

Threat Research Unit (TRU) Experts

16 hrs

Median Response Time

Qualys TruRisk™ 2.0

Qualys.

Measure Risk with TruRisk™

The most accurate way to **measure & prioritize cyber risk**

Measure Cyber Risk

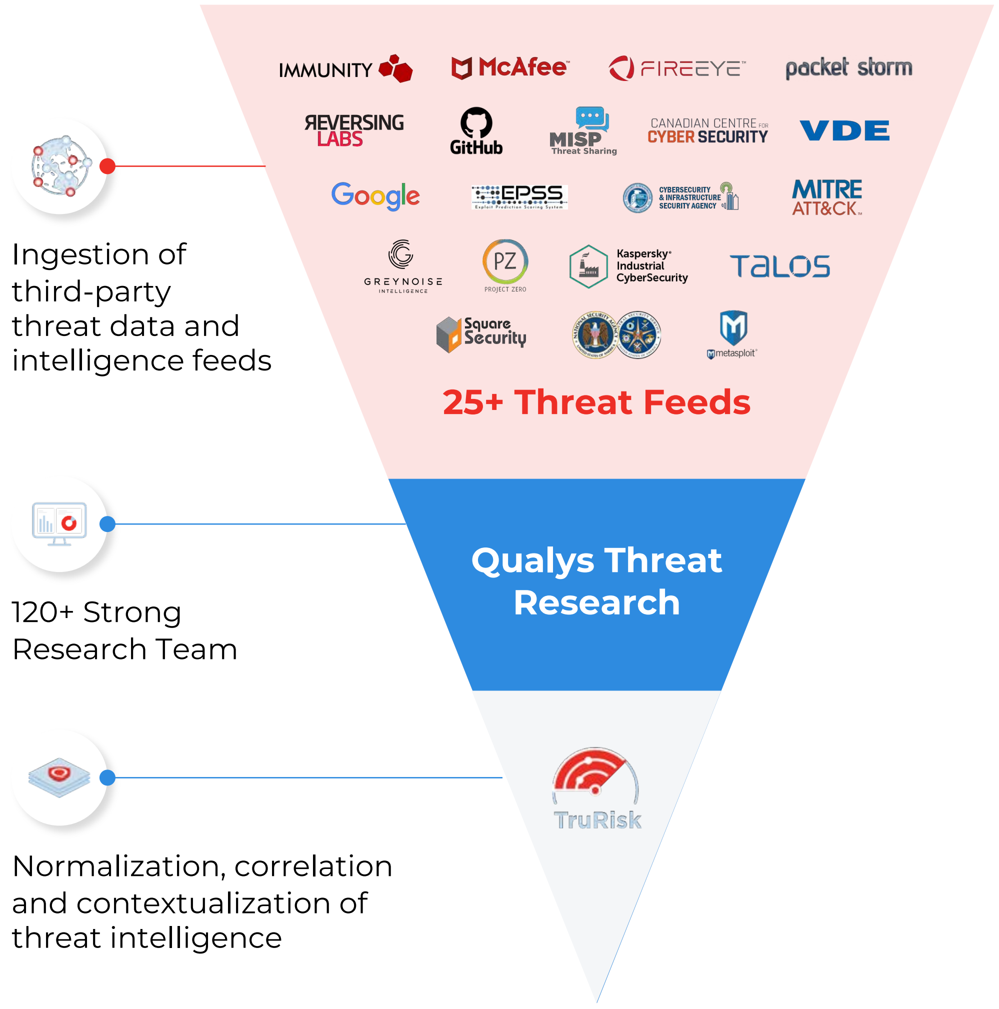
Quantify risk across vulnerabilities, assets, and groups of assets helping organizations proactively reduce risk exposure and track risk reduction over time with Qualys TruRisk

Prioritize Based On Real Risk

Prioritize based on context from the **4-E**s: **Exposure, Exploitation, Evidence,** & **Enterprise context**

Best-In-Class Threat Intelligence Included

Leverage insights from over 200k vulnerabilities sourced from over **25+ threat sources** to get best-in-class threat intelligence with the Qualys Cloud Threat DB



Ingestion of third-party threat data and intelligence feeds

25+ Threat Feeds

120+ Strong Research Team

Qualys Threat Research

Normalization, correlation and contextualization of threat intelligence

Industry Leading Prioritization with TruRisk™

Cut 52% to **<10% with TruRisk™**

CVSS

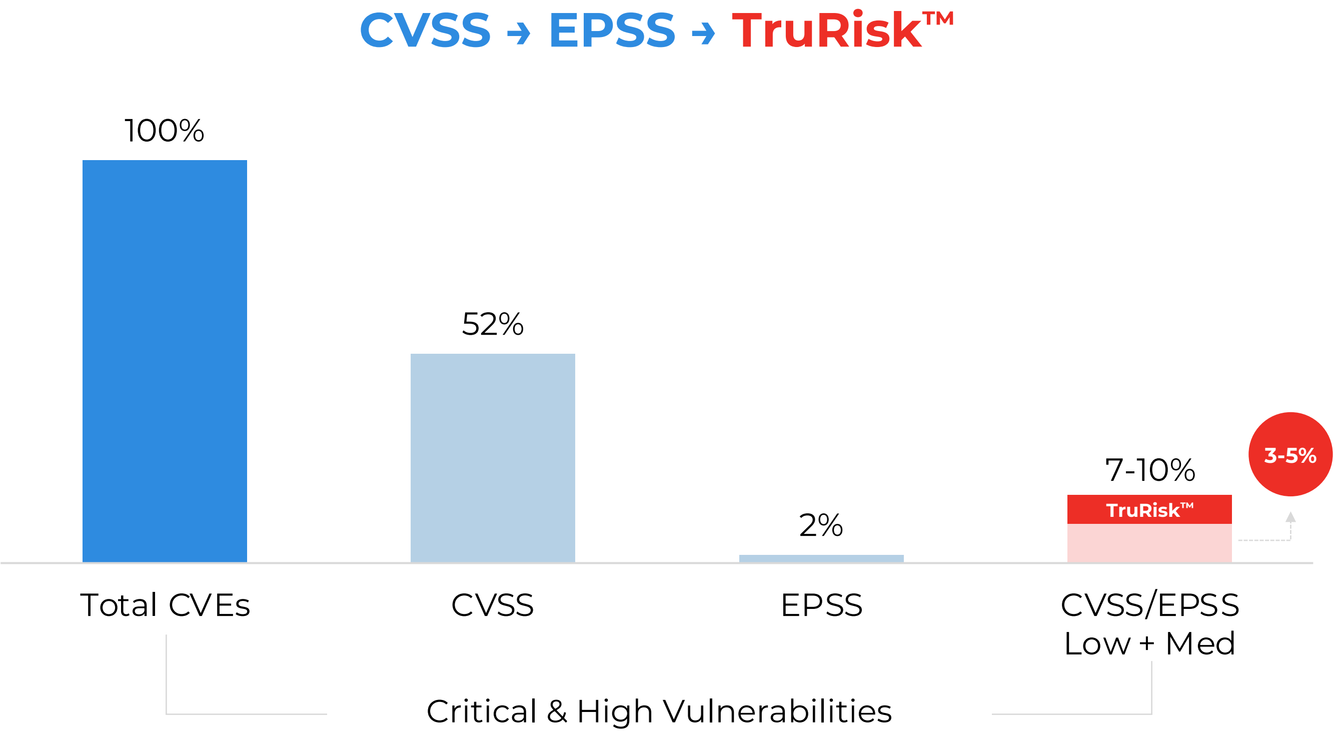
Too Many

EPSS

Too Few

TruRisk™

Just Right!



Enhancements to TruRisk™ 2.0

Expanded Risk Sources & Factors

- New Risk Sources
- New Risk Factors

CVE-centric Scoring

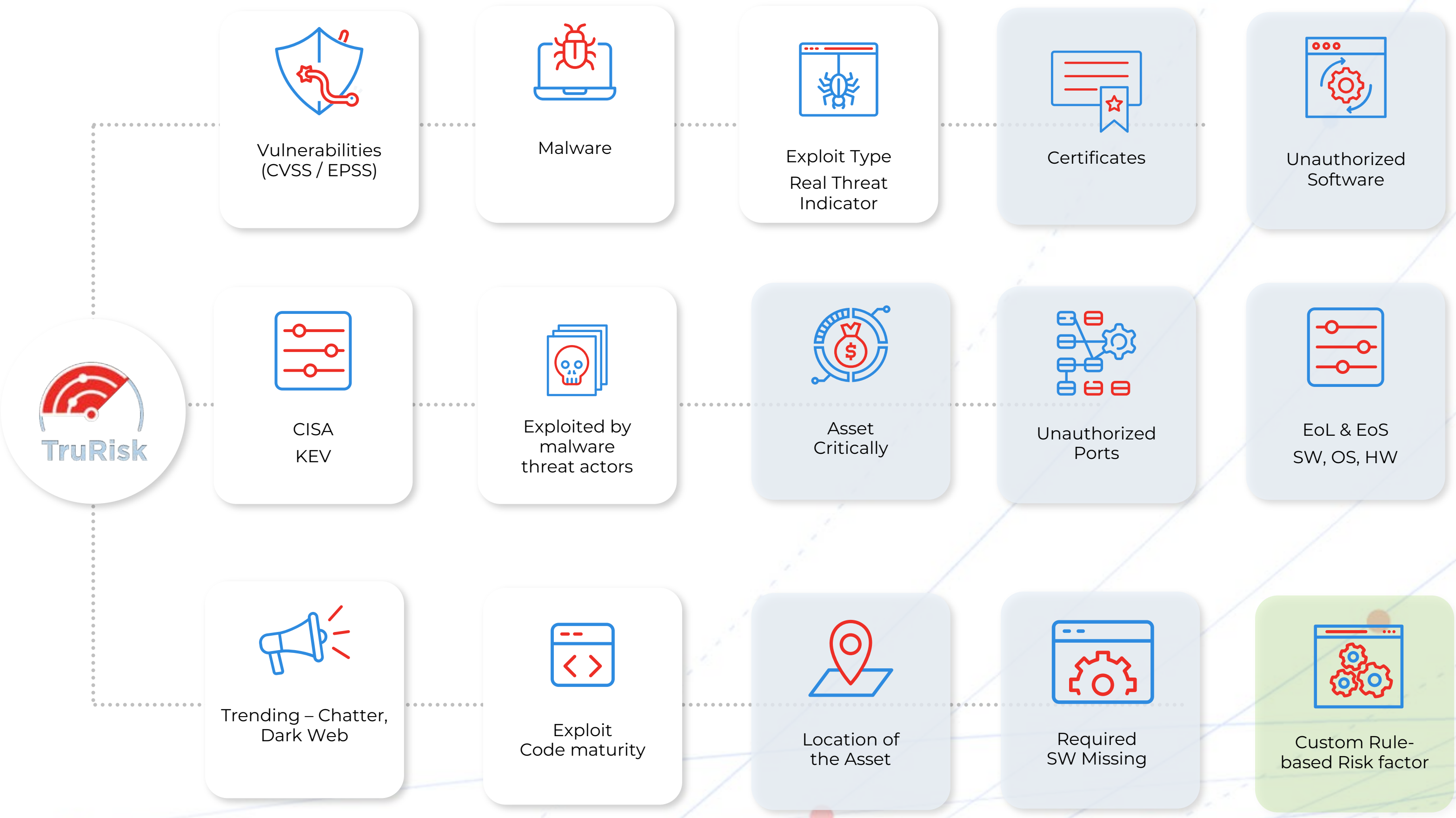
- Standardization
- Vuln Counts using CVE IDs

Enhanced Formula

- New Risk Sources
- New Risk Factors

Dynamic Scoring

- Standardization
- Vuln Counts using CVE IDs



TruRisk

Vulnerabilities (CVSS / EPSS)

Malware

Exploit Type Real Threat Indicator

Certificates

Unauthorized Software

CISA KEV

Exploited by malware threat actors

Asset Critically

Unauthorized Ports

EoL & EoS SW, OS, HW

Trending – Chatter, Dark Web

Exploit Code maturity

Location of the Asset

Required SW Missing

Custom Rule-based Risk factor

Qualys.

Advantages of Qualys QIDs over CVE IDs

Streamlined remediation

Contextual insights for effective prioritization

Comprehensive coverage

Streamlined mitigation with detailed guidance

Qualys®

Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.