Qualys.

ROCon 25

The Risk Operations Conference

AMERICAS

App-solutely Secure: Managing Application Security Posture in the Age of AI

Asma Zubair

Director, Product Management
Qualys

Joe Moore

Cybersecurity Architect
Siemens

AI Adoption is Surging — and Exposing Critical API Security Gaps

- Nearly 99% of AI-related vulnerabilities are tied to API flaws
- 89% of AI-powered APIs lack secure authentication
- AI models add another dimension to an already complex application attack surface

AI is Transforming Web Apps, Too

- Applications are rapidly evolving
  - Integrating LLMs, embracing new architectures, standards (e.g., WebMCP), and protocols (e.g., MCP)
- Fewer forms, user input fields. More intent-Driven Interactions (“book a flight”, “summarize email”)
- **Applications are turning into a network of APIs**

What Does Growing AI Adoption Mean For AppSec?

Increase in attack surface

Greater **need for comprehensive inventory of applications and APIs**

Greater risk

Assess an applications or API's **risk holistically and efficiently according to its underlying tech stack**

Need for faster remediation response

To keep up with **faster release cycles** powered by AI generated code

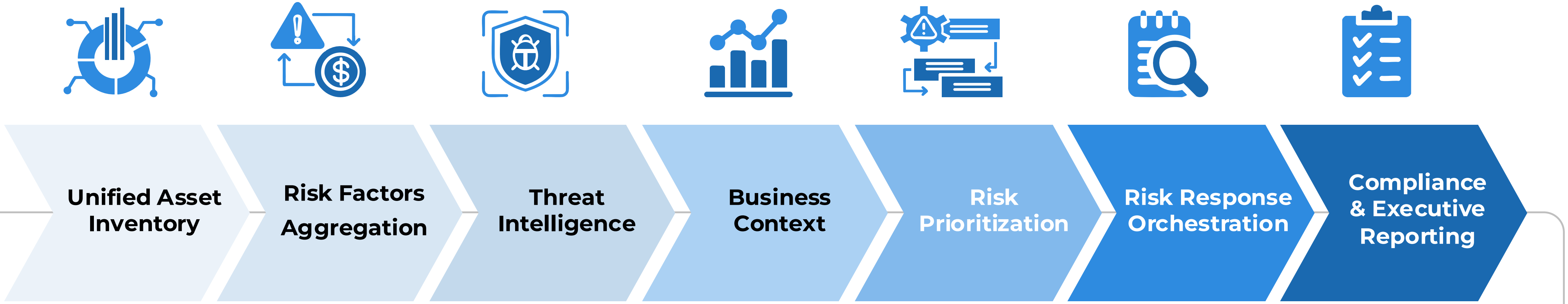
Greater need to manage application security posture

Manage application security risk holistically across the development lifecycle

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

Operationalize

The Risk Operations Center (ROC)



Unified Asset Inventory

Risk Factors Aggregation

Threat Intelligence

Business Context

Risk Prioritization

Risk Response Orchestration

Compliance & Executive Reporting

How will you be

ROC Ready from Day 1

Elevate Your AppSec Program to ASPM

TotalAppSec: From Attack Surface to Risk Surface

Operationalize Application Security Risk to Reduce Noise, Cost, and Time

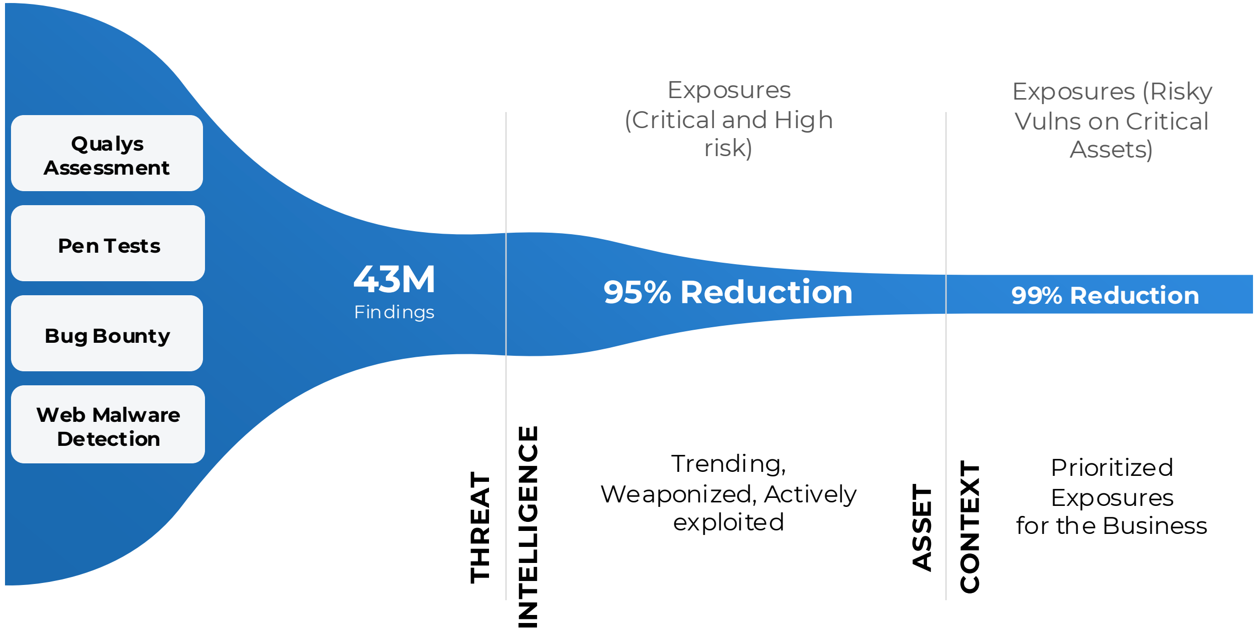
Discover Your Full Application Attack Surface

Comprehensive Discovery From:

- ✓ Cloud environments
- ✓ API gateways
- ✓ Web application scans
- ✓ Internal and internet-facing scans

456K
Assets

Assess and Prioritize Risk With Multi-Dimensional Context



Qualys Assessment
Pen Tests
Bug Bounty
Web Malware Detection
43M
Findings
THREAT INTELLIGENCE
Exposures (Critical and High risk)
95% Reduction
Trending, Weaponized, Actively exploited
ASSET CONTEXT
Exposures (Risky Vulns on Critical Assets)
99% Reduction
Prioritized Exposures for the Business

Integrated Remediation Response

- ✓ Automatic Real-Time **Prioritization**
- ✓ Automatic Real-Time **Triaging**
- ✓ Automatic Real-Time **Retesting**

TotalAppSec: Make Your AppSec Roc-Ready

Unified Asset Inventory

Covering known and unknown APIs and web applications, their correlation

Ability to spot AI usage in apps and APIs

Risk Assessment

OWASP Top 10 risks

Web malware detection

OAS v3 testing

Custom signatures

Testing of components

AI-powered scans

Risk Response Orchestration

TruRisk^{TM} prioritization

Automated triaging & remediation

CI/CD integrations to retest

Application Security Posture Management

Unified and correlated view of findings from different sources

Automatically generated application graph demonstrating application and API correlation

1000+ organizations trusted us within the first year of launch

4.4*/5 Gartner Peer Insights™

4*/5 PeerSpot

Key Capabilities

Unified Asset Inventory of Known and Unknown Web Assets

Including the ability to discover AI usage in web applications and APIs

3rd Party Import

Swagger, Postman, Burp Suites

API Gateways

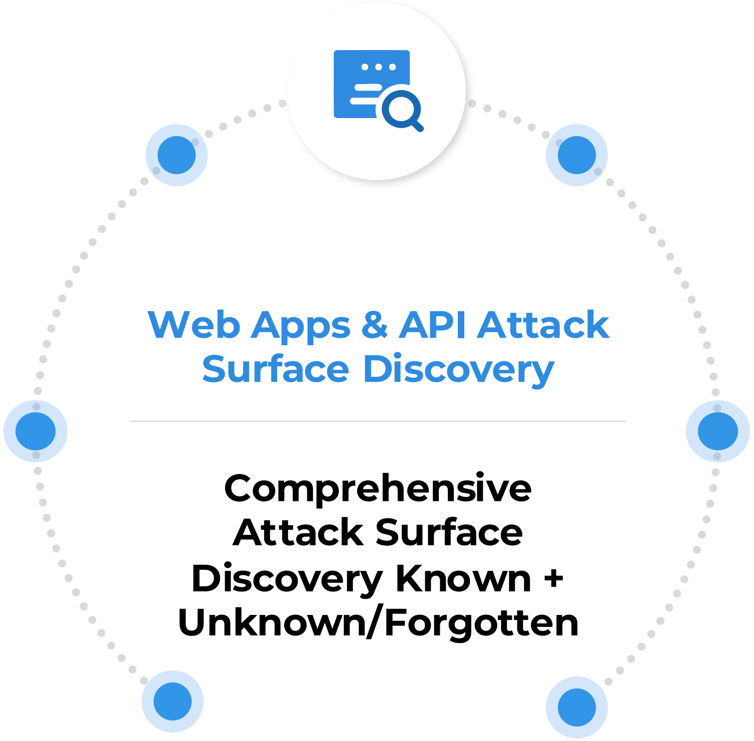
Discover APIs from Mulesoft, AWS API gateway, Azure APIM and APIgee

AI and API Discovery

Discoverer swagger files, API calls, and AI usage during web app scanning

Multi-cloud Environment

Web application discovery from AWS, GCP, Azure



Web Apps & API Attack Surface Discovery

Comprehensive Attack Surface Discovery Known + Unknown/Forgotten

Traffic Analysis

Discover APIs by analyzing traffic

Internet Exposed and Internal

Discover internet exposed and internal web apps and APIs from CSAM and VMDR scans

Source Code

Discover APIs from source code

Risk Assessment with API scanning

Plus, the ability to perform AI risk assessments as needed

- Test APIs for conformance to OAS V3
- OWASP API Security Top 10 testing
- Prioritization with TruRisk score
- Build a “Shift Left” & “Shift Right” security
- AI-powered scanning cuts scanning time in half

~600

QIDs for APIs

Including checks for OWASP Top 10 for APIs, Sensitive Data leakage and compliance to OAS

100%

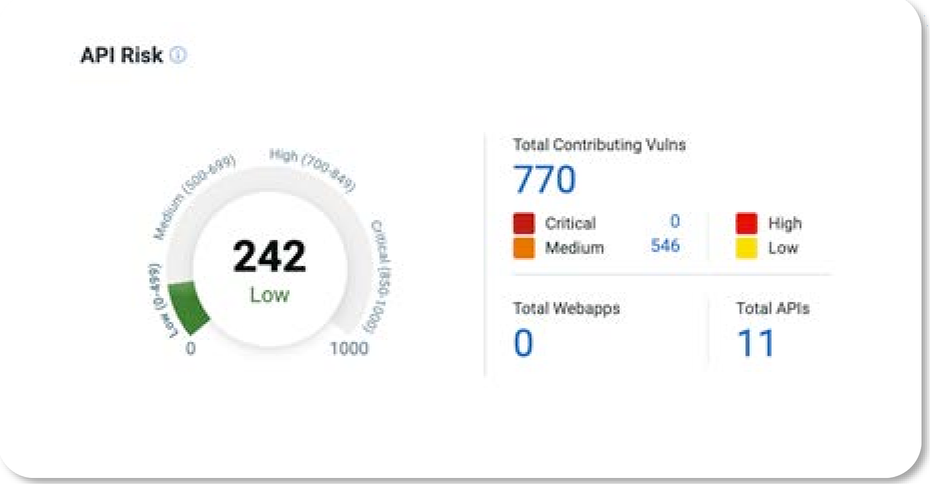
Coverage

of OWASP Top 10 for APIs

5000+

API Endpoints tested

within the first few quarters of launch



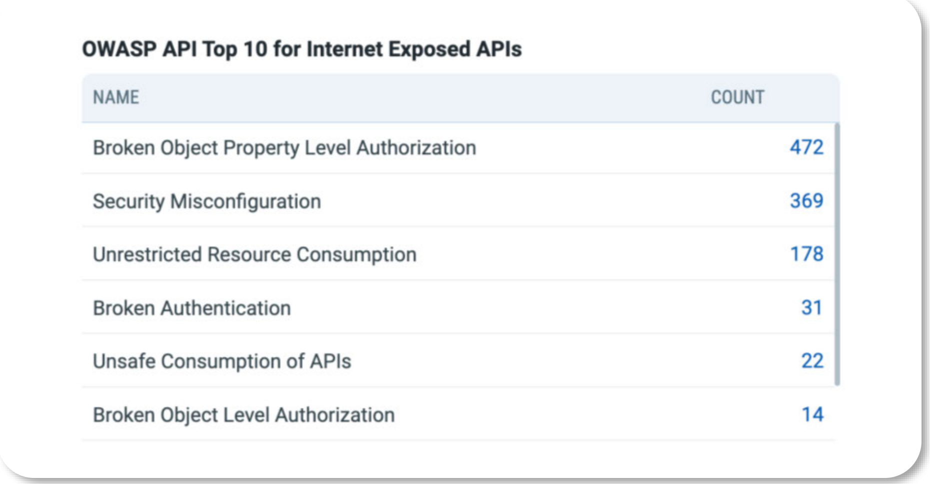
API Risk

Total Contributing Vulns
770

🟥 Critical	0	🟥 High	
🟧 Medium	546	🟨 Low	

Total Webapps
0

Total APIs
11



OWASP API Top 10 for Internet Exposed APIs

NAME	COUNT
Broken Object Property Level Authorization	472
Security Misconfiguration	369
Unrestricted Resource Consumption	178
Broken Authentication	31
Unsafe Consumption of APIs	22
Broken Object Level Authorization	14

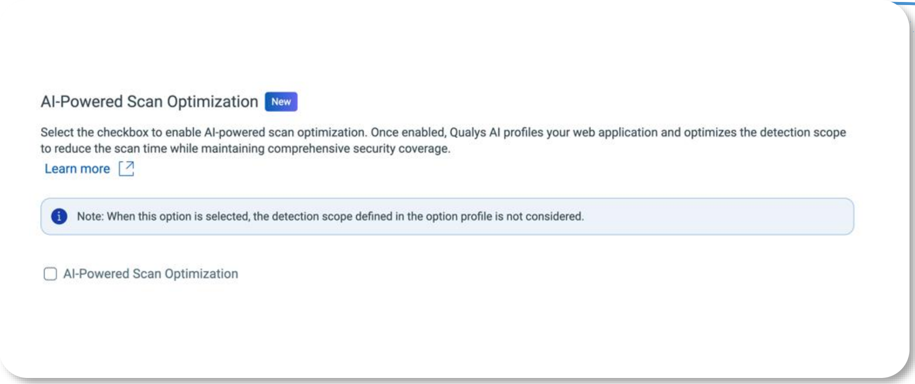
Unified Asset Inventory

Risk Factors Aggregation

Risk Assessment with web app scanning, and malware detection

Plus, the ability to perform AI risk assessments as needed

- **AI-powered scanning cuts scanning time in half**
- Define and **test with custom signatures**
- Detect AI usage and **trigger AI risk assessments for AI components**
- Deep learning powered **scans detect zero-day malware**


AI-Powered Scan Optimization New

Select the checkbox to enable AI-powered scan optimization. Once enabled, Qualys AI profiles your web application and optimizes the detection scope to reduce the scan time while maintaining comprehensive security coverage.

Learn more

Note: When this option is selected, the detection scope defined in the option profile is not considered.

☐ AI-Powered Scan Optimization

4600+

customers

Trust Qualys web application and API risk assessment capabilities

~3300

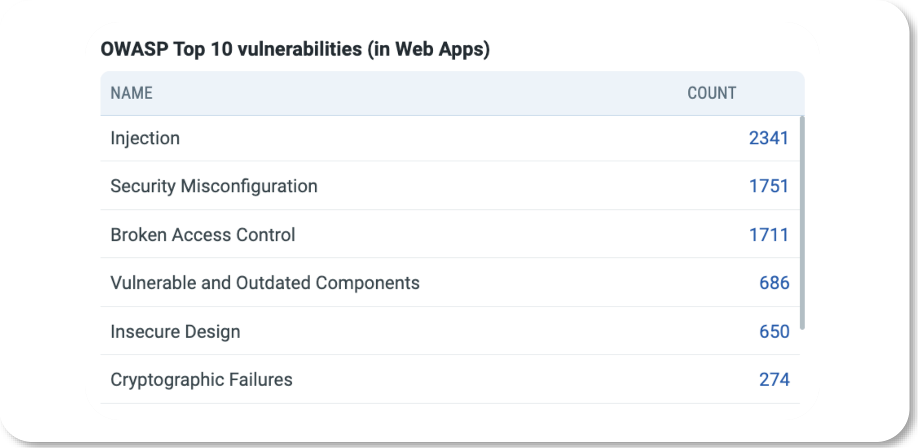
QIDs for web apps

Including OWASP Top 10 and Sensitive Data leakage checks

~99%

Accuracy

Deep learning powered Web Malware Detection and Monitoring

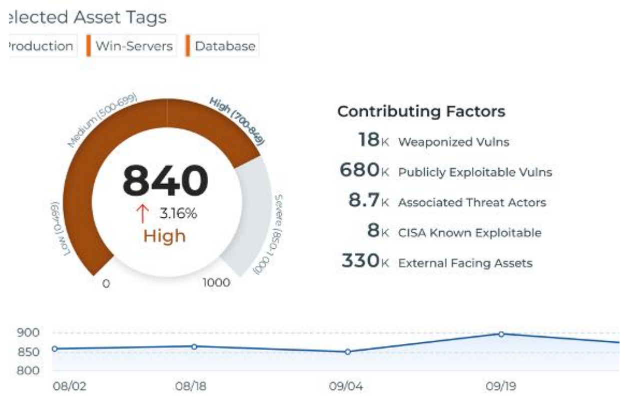

OWASP Top 10 vulnerabilities (in Web Apps)

NAME	COUNT
Injection	2341
Security Misconfiguration	1751
Broken Access Control	1711
Vulnerable and Outdated Components	686
Insecure Design	650
Cryptographic Failures	274

Unified Asset Inventory

Risk Factors Aggregation

Risk Response Orchestration with Integrated Workflows



elected Asset Tags

rroduction | 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

servicenow

Jira

GitHub

Bamboo

TeamCity

Prioritize Automatically

Prioritize based on

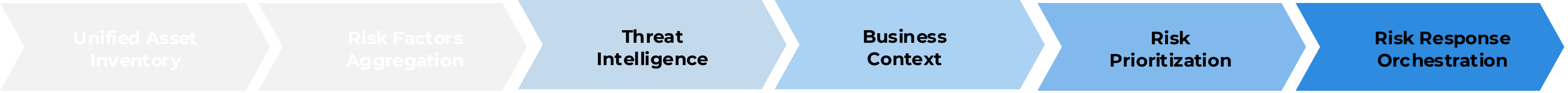
- Business Asset context
- Threat Context correlated with Vulnerabilities detection

Triage Automatically

Automated Ticket Creation - Automatically generate tickets in ITSM systems, assign them to the appropriate teams for remediation

Retest Automatically

Automated security testing before deployment with pass/fail criteria based on scan results.



Unified Asset Inventory

Risk Factors Aggregation

Threat Intelligence

Business Context

Risk Prioritization

Risk Response Orchestration

ASPM – Application Security

Comprehensive Discovery & Inventory

- Qualys Connectors – VMDR, CSAM/EASM, TotalCloud, etc.
- Multi-Cloud (e.g., AWS, GCP, Azure, Direct Cloud APIs)
- Containers (e.g., Docker, Kubernetes, Service Mesh Arch, Istio, Kuma)
- API Gateways (e.g., Apigee, Mulesoft, AWS API Gateway)
- External-Facing/Internet-Exposed Assets & Certificates
- Third-Party Integrations (e.g., Postman, Burp Suite, Swagger)
- **SAST and SCA** Integration with Checkmarx, Synk, Veracode

Measure and Prioritize Risk

Enterprise TruRisk™ Platform

Web Apps | **APIs** | **Web Malware**

DAST, API Testing, AI-Powered Scanning,
Deep Learning-based Web Malware Detection

Prioritize with TruRisk™

Risk Orchestration & Remediation

- Automated Patching of underlying infrastructure
- Isolation of servers, API endpoints or hosts
- Mitigation techniques for web apps & APIs
- Remediation Workflows with DevOps & ITSM integration

Customer Outcomes

360° Visibility → App Security Posture Management → Risk Prioritization → Risk Remediation

Scale Your AppSec with Agentic AI

Cyber Risk Assistant

- For conversational, AI interface

Manages AppSec program with Natural Language Query Interface

- Show me all my web apps
- Show me a summary of all web application findings
- Show me my top toxic combinations

Cyber Risk Agent

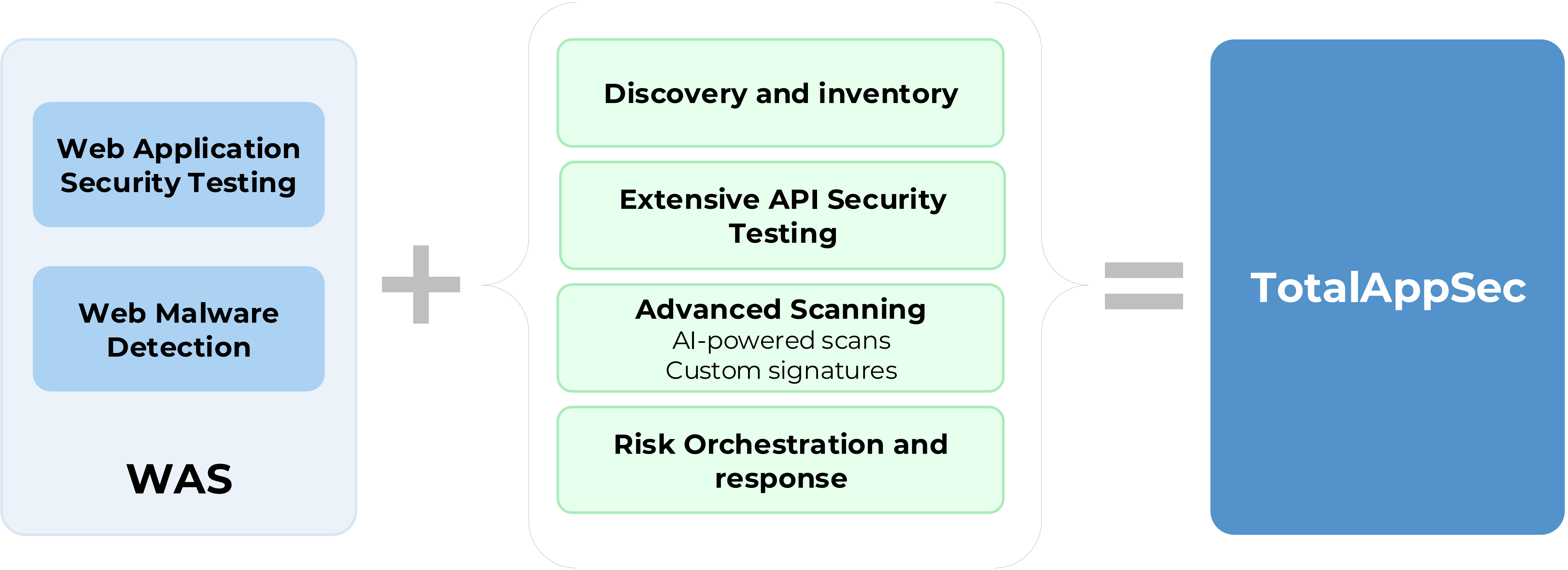
- Digital collaborator for repetitive workflow

Agentic AI-powered health checks

- The Cyber Risk Agent monitors web applications and APIs onboarded in TotalAppSec
- And recommends configuration changes for optimal and comprehensive testing

Upgrade to TotalAppSec

Benefit from New Capabilities



Web Application Security Testing

Web Malware Detection

WAS

Discovery and inventory

Extensive API Security Testing

Advanced Scanning
AI-powered scans
Custom signatures

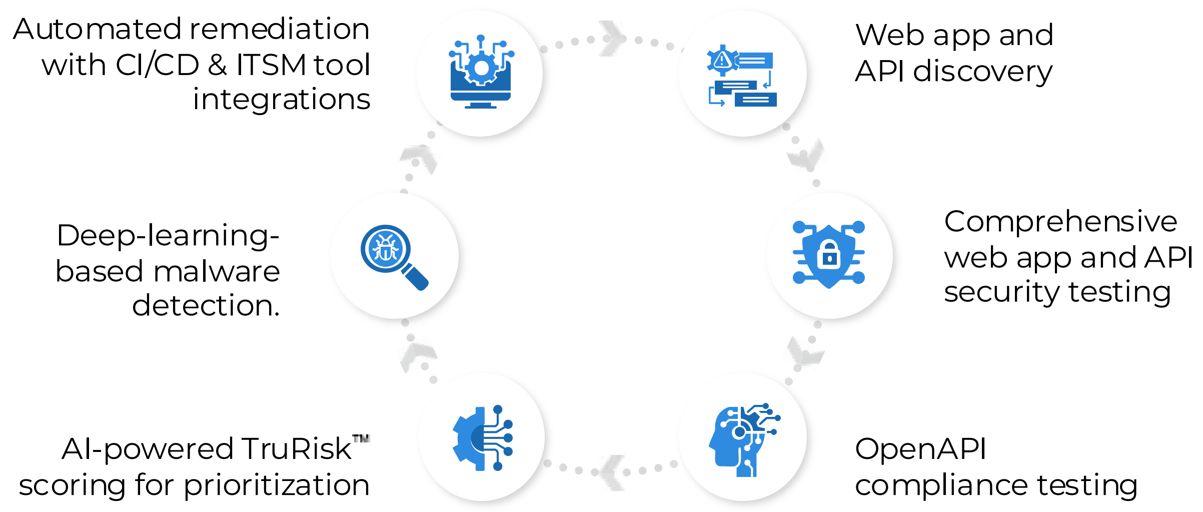
Risk Orchestration and response

TotalAppSec

TotalAppSec Packaging & Licensing

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

Base Package Features*


Automated remediation with CI/CD & ITSM tool integrations
Web app and API discovery
Comprehensive web app and API security testing
OpenAPI compliance testing
AI-powered TruRisk™ scoring for prioritization
Deep-learning-based malware detection.

*Qualys Integrations - Natively Integrated with Qualys VMDR, CSAM/EASM
*Included Connectors - ADO, Jenkins, Bamboo, Team City, Splunk, ServiceNow, BurpSuite, Jira

✓ **Single SKU Licensing** can be used for – **Web App or API endpoint.**

- Includes access to future roadmap features like GCP/OCI app discovery and integrated ASPM capabilities.
- No module fee

✓ **Base Package**

- Minimum 5 units.
- **Flexible allocation** between web apps and APIs based on customer needs.

✓ **Enterprise Licensing**

- Custom pricing for enterprises with broad, complex environments.

✓ **SMB/SME Licensing**

- Discounted pricing bundle for SMB/SME to drive velocity

Qualys ROCon 25
The Risk Operations Conference
AMERICAS

Demo

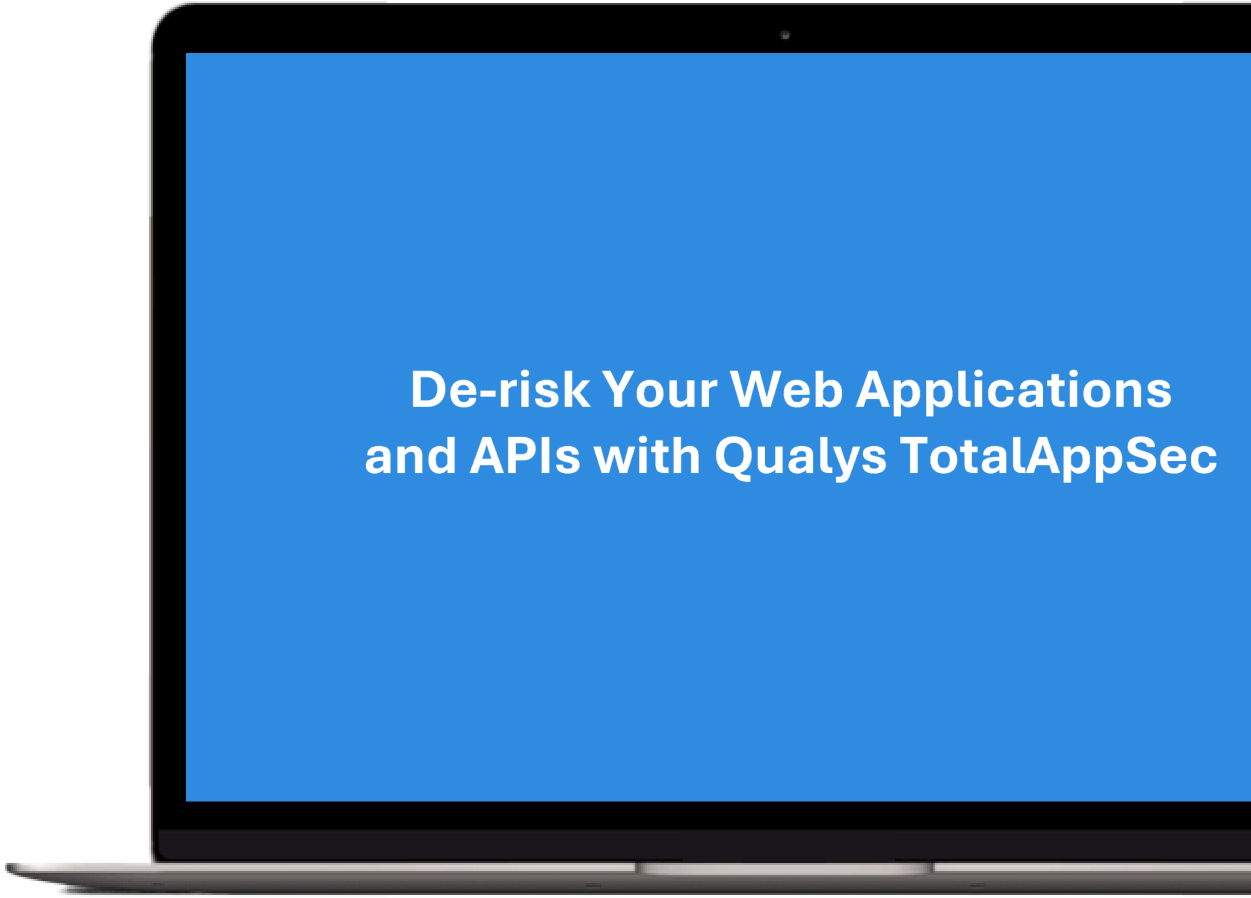
Get Your Free Web Application and API Security Report

- Know your application's TruRisk
- Detect OWASP Top 10 vulnerabilities
- Detect Sensitive Data Exposure
- Detect and Monitor for Malware
- Prioritize and Remediate

No Subscription Required!

Sign Up for Free Trial:

https://www.qualys.com/forms/web-application-scanning/



De-risk Your Web Applications and APIs with Qualys TotalAppSec

Qualys.

ROCon 25

The Risk Operations Conference

AMERICAS

Risk Assessment with API scanning, web app scanning, and malware detection

Plus the ability to perform AI risk assessments as needed

- **AI-powered scanning cuts down scanning time in half**
- Deep learning powered **scans detect zero-day malware**
- Ability to define and test custom signatures
- Detect AI usage and **trigger AI risk assessments for AI components**

~3300

QIDs for Web apps

Including OWASP Top 10 and Sensitive Data leakage checks

~600

QIDs for APIs

Including checks for OWASP Top 10 for APIs, Sensitive Data leakage and compliance to OAS

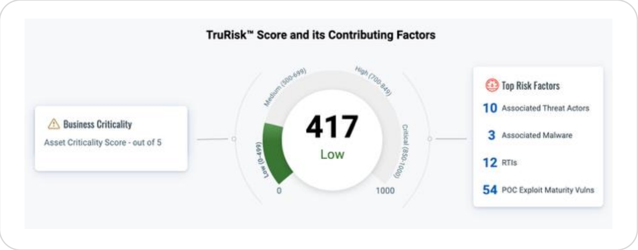
~99%

Accuracy

Deep learning powered Web Malware Detection and Monitoring

Unified Asset Inventory

Risk Factors Aggregation



TruRisk™ Score and its Contributing Factors

Business Criticality

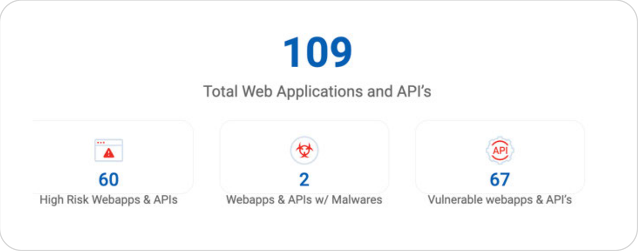
Asset Criticality Score - out of 5

417

Low

Top Risk Factors

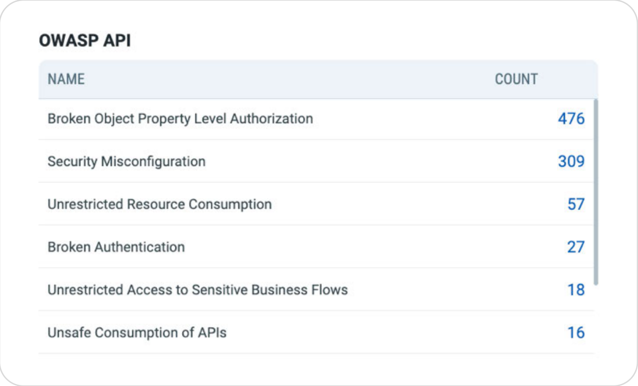
10	Associated Threat Actors
3	Associated Malware
12	RTIs
54	POC Exploit Maturity Vulns



109

Total Web Applications and API's

60	2	67
High Risk Webapps & APIs	Webapps & APIs w/ Malwares	Vulnerable webapps & API's



OWASP API

NAME	COUNT
Broken Object Property Level Authorization	476
Security Misconfiguration	309
Unrestricted Resource Consumption	57
Broken Authentication	27
Unrestricted Access to Sensitive Business Flows	18
Unsafe Consumption of APIs	16

TotalAppSec In Action

Siemens’ Journey with Qualys

Introduction

Joe Moore
Cybersecurity Architect

- Architect and data analytics expert for the advanced cybersecurity group
- 15+ years cybersecurity expertise
- 10+ years in application security
- Digital industries software division of Siemens

Siemens

- Founded 1847; global leader in industrial & building automation, rail, and health tech
- 320,000 employees; HQ: Munich & Berlin
- Siemens DI Software: Engineering software for design, manufacturing and lifecycle management

https://www.sw.siemens.com

Siemens Environment

- Hybrid estate: on-prem apps + cloud-native; serverless APIs; legacy-backed APIs
- Dozens of dev teams, varied maturity levels, many products, many audiences
- Teams choose scan points (per merge, per sprint, pre-release)
- We always test production; cadence varies weekly/monthly
- Goal: protect customer data to earn and keep trust

Pre-Qualys Challenges

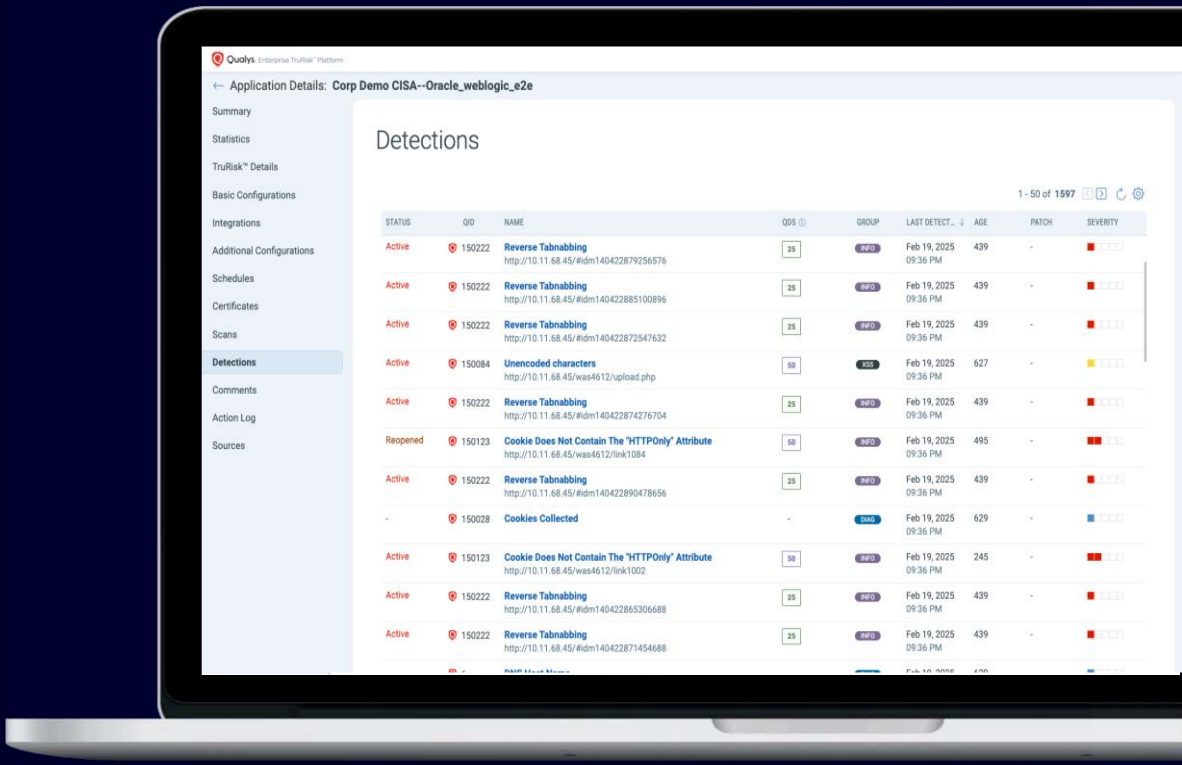
- Pre-Qualys: the Internet as a noisy, unreliable vulnerability finder
- Ad-hoc reports (good actors *and* attackers)
- Inconsistent visibility across apps/APIs/ environments
- Limited formal reporting; central team reviewed production scans for follow up
- Needed a common baseline and repeatable disciplines

AppSec Testing Requirement: Protect Customer Data

- Non-intrusive production scanning with predictable cadence
- Standard baseline across teams; policy-driven expectations
- DAST for web apps + API coverage (now & expanding)
- Actionable alerts; critical SLA target
- Roadmap: shift left; automate API test generation; integrate ticketing (ServiceNow)

How We Use Qualys: Overview

- Teams self-initiate scans at merge/sprint/milestone; central production scans weekly/monthly
- Direct access to production results; email notifications for anomalies
- Fixes targeted within the next sprint; criticalities ~3-day SLA
- API scanning underway; broader automation planned



← Application Details: **Corp Demo CISA--Oracle_weblogic_e2e**

Detections

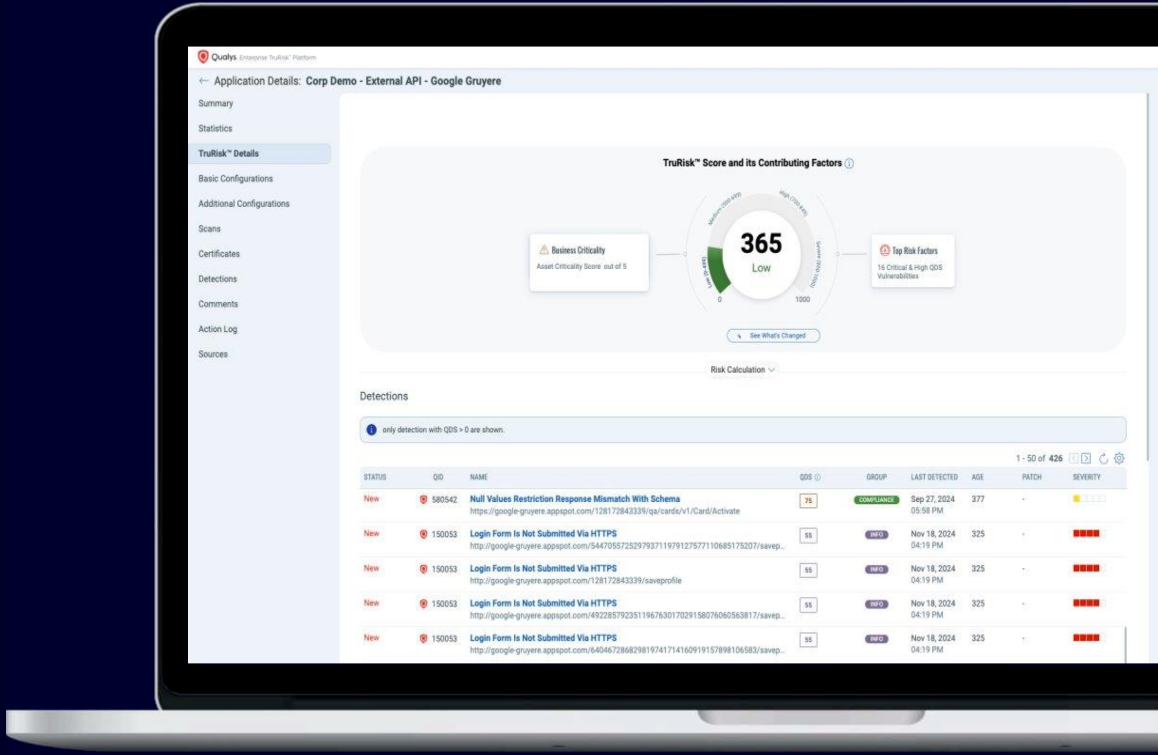
1 - 50 of **1597**

STATUS	QID	NAME	QDS	GROUP	LAST DETECT... ↓	AGE	PATCH	SEVERITY
Active	150222	Reverse Tabnabbing http://10.11.68.45/#idm140422879256576	25	INFO	Feb 19, 2025 09:36 PM	439	-	🟥
Active	150222	Reverse Tabnabbing http://10.11.68.45/#idm140422885100896	25	INFO	Feb 19, 2025 09:36 PM	439	-	🟥
Active	150222	Reverse Tabnabbing http://10.11.68.45/#idm140422872547632	25	INFO	Feb 19, 2025 09:36 PM	439	-	🟥
Active	150084	Unencoded characters http://10.11.68.45/was4612/upload.php	50	XSS	Feb 19, 2025 09:36 PM	627	-	🟨
Active	150222	Reverse Tabnabbing http://10.11.68.45/#idm140422874276704	25	INFO	Feb 19, 2025 09:36 PM	439	-	🟥
Reopened	150123	Cookie Does Not Contain The "HTTPOnly" Attribute http://10.11.68.45/was4612/link1084	50	INFO	Feb 19, 2025 09:36 PM	495	-	🟥🟥
Active	150222	Reverse Tabnabbing http://10.11.68.45/#idm140422890478656	25	INFO	Feb 19, 2025 09:36 PM	439	-	🟥
-	150028	Cookies Collected	-	DIAG	Feb 19, 2025 09:36 PM	629	-	🟦
Active	150123	Cookie Does Not Contain The "HTTPOnly" Attribute http://10.11.68.45/was4612/link1002	50	INFO	Feb 19, 2025 09:36 PM	245	-	🟥🟥
Active	150222	Reverse Tabnabbing http://10.11.68.45/#idm140422865306688	25	INFO	Feb 19, 2025 09:36 PM	439	-	🟥
Active	150222	Reverse Tabnabbing http://10.11.68.45/#idm140422871454688	25	INFO	Feb 19, 2025 09:36 PM	439	-	🟥

SIEMENS

Results

- ✓ Disciplined, repeatable scanning vs. prior ad-hoc model
- ✓ Remediation SLAs for Critical, Highs, Medium/Lows met
- ✓ **TISAX compliant**
- ✓ **Scaled AppSec program by 400% with only a 20% increase in team size**


Qualys Enterprise TruRisk™ Platform
← Application Details: Corp Demo - External API - Google Gruyere
Summary
Statistics
TruRisk™ Details
Basic Configurations
Additional Configurations
Scans
Certificates
Detections
Comments
Action Log
Sources
TruRisk™ Score and its Contributing Factors
Business Criticality
Asset Criticality Score out of 5
365
Low
0
1000
Top Risk Factors
16 Critical & High QDS Vulnerabilities
See What's Changed
Risk Calculation

Detections

only detection with QDS > 0 are shown.

1 - 50 of 426

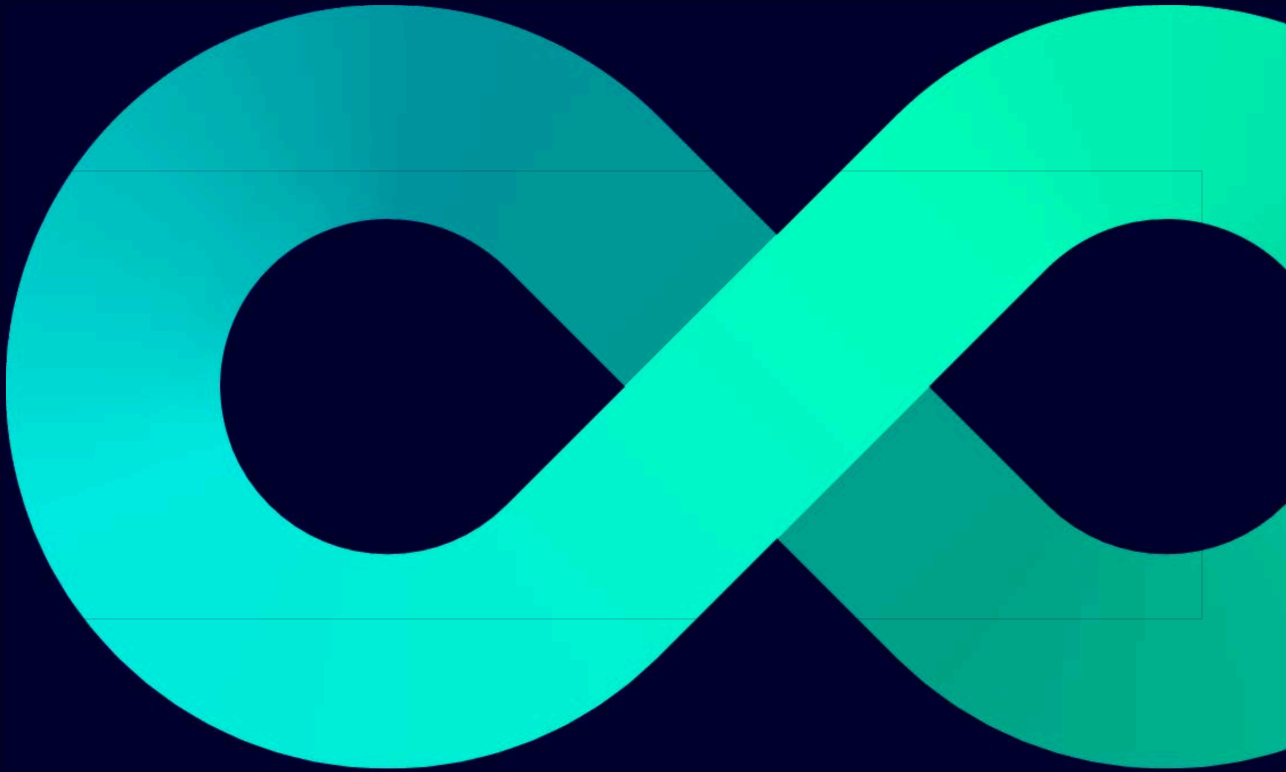
STATUS	QID	NAME	QDS	GROUP	LAST DETECTED	AGE	PATCH	SEVERITY
New	580542	Null Values Restriction Response Mismatch With Schema https://google-gruyere.appspot.com/128172843339/qa/cards/v1/Card/Activate	75	COMPLIANCE	Sep 27, 2024 05:58 PM	377	-	■□□□□
New	150053	Login Form Is Not Submitted Via HTTPS http://google-gruyere.appspot.com/544705572529793711979127577110685175207/savep...	55	INFO	Nov 18, 2024 04:19 PM	325	-	■■■■□
New	150053	Login Form Is Not Submitted Via HTTPS http://google-gruyere.appspot.com/128172843339/saveprofile	55	INFO	Nov 18, 2024 04:19 PM	325	-	■■■■□
New	150053	Login Form Is Not Submitted Via HTTPS http://google-gruyere.appspot.com/49228579235119676301702915807606056381 7/savep...	55	INFO	Nov 18, 2024 04:19 PM	325	-	■■■■□
New	150053	Login Form Is Not Submitted Via HTTPS http://google-gruyere.appspot.com/640467286829819741714160919157898106583/savep...	55	INFO	Nov 18, 2024 04:19 PM	325	-	■■■■□

SIEMENS

Road Ahead

- Inventory + exposure context beats raw vulnerability counts
- Use TruRisk to prioritize, brief leadership, and drive accountability
- Standardize cadence; enforce SLAs; own production scans centrally
- Automate API testing + ticketing to compress MTTR
- Start with structure, Scale with automation

Thank You



Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.

Contact

Published by Siemens 2025

Joe Moore
Cybersecurity Architect
Digital Industries Software
https://www.sw.siemens.com/
Milford, Ohio
USA

Mobile +15132529613

E-mail joe.moore@siemens.com

LinkedIn https://www.linkedin.com/in/joemoore3/