QSC23

Reducing Risks in Web Applications and APIs with the Qualys Platform

John Delaroderie
Director, Product Management
Web Application Security

Websites and APIs Are Growing Astronomically

How Can Security Teams Keep Up?

Attack Surface is Expanding

- Websites
- Open Source Dependencies
- APIs
- Mobile Applications
- CMS
- Embedded Devices

Source: Forbes

Qualys.

1.13B Websites on Internet Today

20 New websites created every minute

71% Businesses with websites today

28% Business conducted online through websites

80+% API traffic makes up the majority of all internet traffic today

AppSec Program Challenges

How Can Security Teams Keep Up?

50%

Cybersecurity professionals report security is an afterthought in the application delivery chain

92%

Developers report pressure to release code to market faster

Source: AppDyanmics, Security Journey

Most AppSec Programs are Reactionary

- Scans are check-box driven
- Are we scanning everything in our inventory?
- AppSec exists outside of SDLC or CICD pipelines
- Overwhelmed by findings

Qualys.

If You Don’t Know It Exists, You Can’t Secure It

How 4 Days Led to $1.5 Million Ransom

Optus Hack
(2022)

Over 1/3 of Australia’s population were impacted when a 19 year old actor gained access through a forgotten and misconfigured API and copied a large percentage of the company’s consumer database.

Timeline

Sep 20th 2022
Suspicious network activity detected and breach was identified.

Sep 22th 2022
Optus went public with the breach and advised customers of potential for fraudulent activity.

Sep 24th 2022
Credible $1.5M ransom for data posted online.

Qualys.

Why AppSec Matters

Application Security IS Enterprise Security

01 Prioritize Organizational Security

02 Protect Sensitive Data

03 Compliance and Regulatory Requirements

04 Prevent Business Disruption

Source: Security Journey

Qualys.

95% Data breaches in 2022 were though web applications

56% Biggest incidents in past 5 years were related to web application security issues

$76B Cost of web application attacks

42% Business financial loss is due to web application attacks

Reality Today

Qualys.

Malicious Actors Will Find Your Vulnerabilities

Applications are not secure-by-default

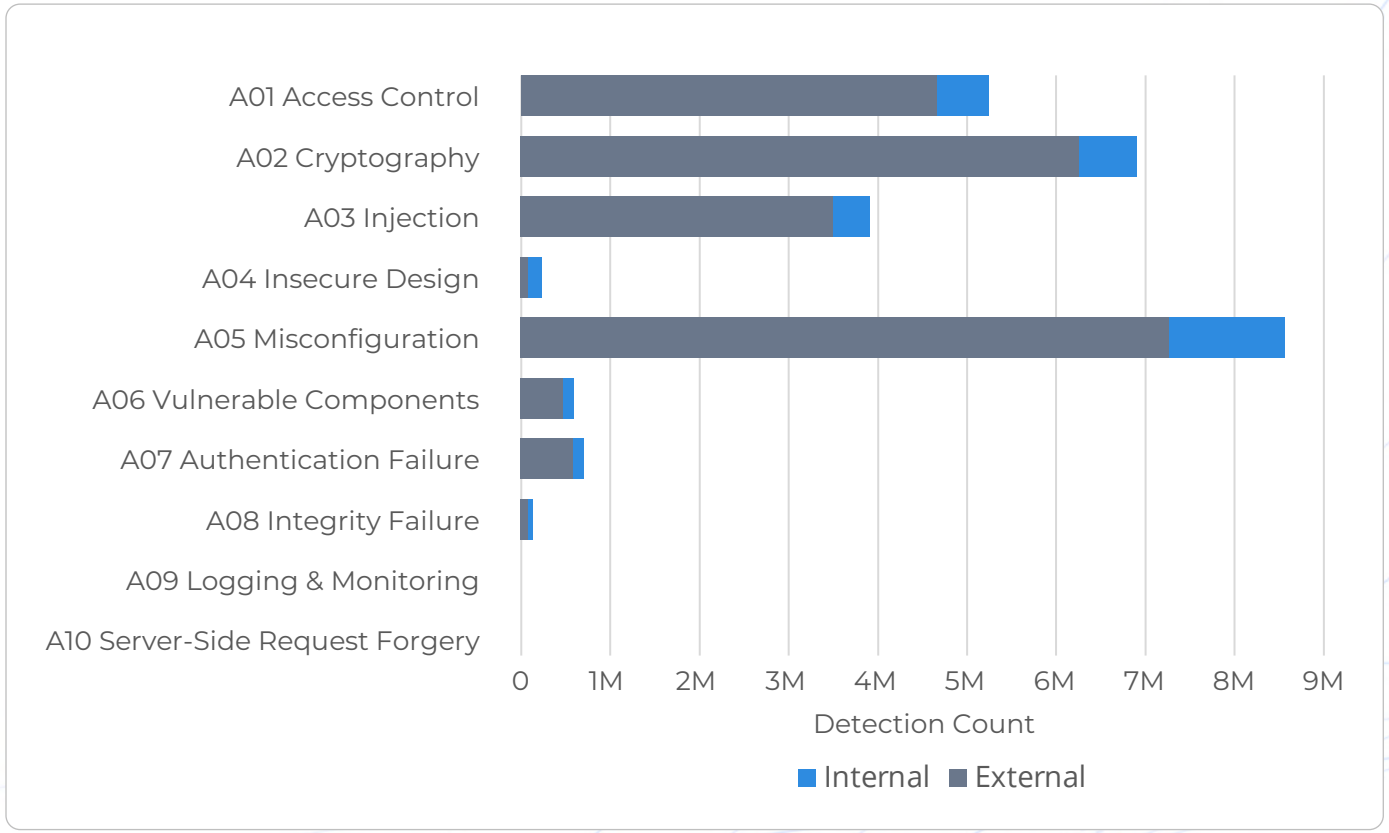
2022 Customer Data Analysis

370,000
Web Applications Scanned

25M
Vulnerabilities Found

33%
Category A05: Misconfiguration

Source: Qualys TruRisk Research Report



Qualys.

The Solution

Qualys.

Industry Leading Web App and API Scanning

Securing 3000+ Customer's Web Apps and APIs world-wide since 2009

Qualys Web Application Scanning (WAS)

Is an industry-leading cloud-based AppSec product providing **DAST – Dynamic Application Security Testing** offering through automated end-to-end crawling and testing of modern Web apps and APIs to identify **runtime vulnerabilities, configuration** and **compliance** issues including the **OWASP top 10**.

Secure Web Apps and APIs across any cloud-native or on-prem architecture

Qualys.

De-Risk Your Applications with Qualys WAS

Measure, Communicate, and Eliminate Risk in WebApps and APIs

Measure

- Web Apps, APIs, Malware
- Comprehensive Discovery
- OWASP Top 10
- CVSS 3.1
- CWEs
- KEVs

Communicate

- Dashboards
- Integrations to CICD and Ticketing Systems
- Custom Reports
- Custom Solutions (emails, Slack notifications, etc)

Eliminate

- TruRisk Prioritization
- Code Remediation
- Secure Open Source Libraries
- Commercial Software Patches/Updates
- Firewall Rules
- Security Configuration

Qualys.

“If you cannot measure it, you cannot improve it.”

Lord Kelvin

Qualys.

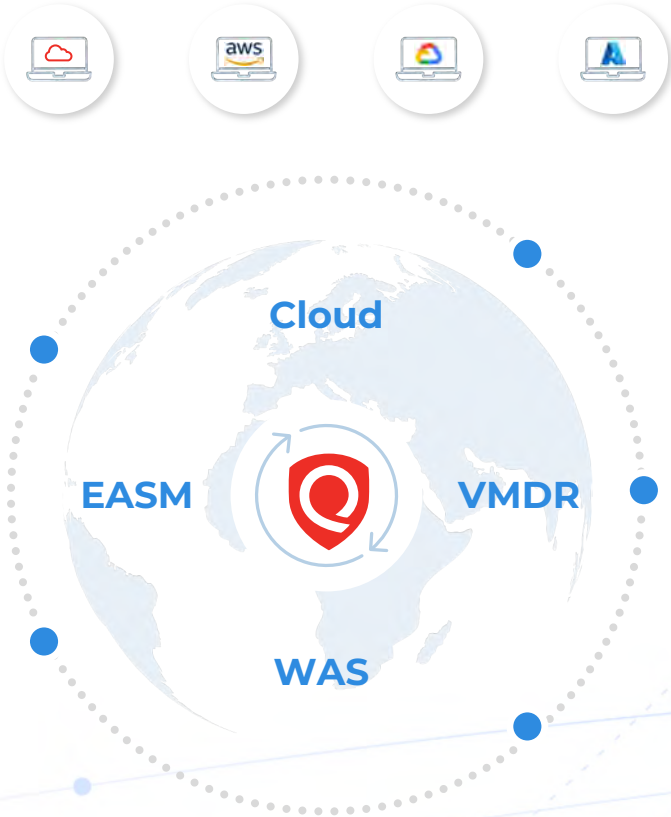
Comprehensive Web App Discovery and Inventory

External Application

Unknown and Orphaned Forgotten Web Apps

Linked External Web Apps

Cloud-Hosted Applications



Internal Application

External Web Servers (Open HTTP Ports)

Internal Web Servers

Linked Internal Web Apps

Qualys.

Actionable Findings to Measure TruRisk

01 CWE

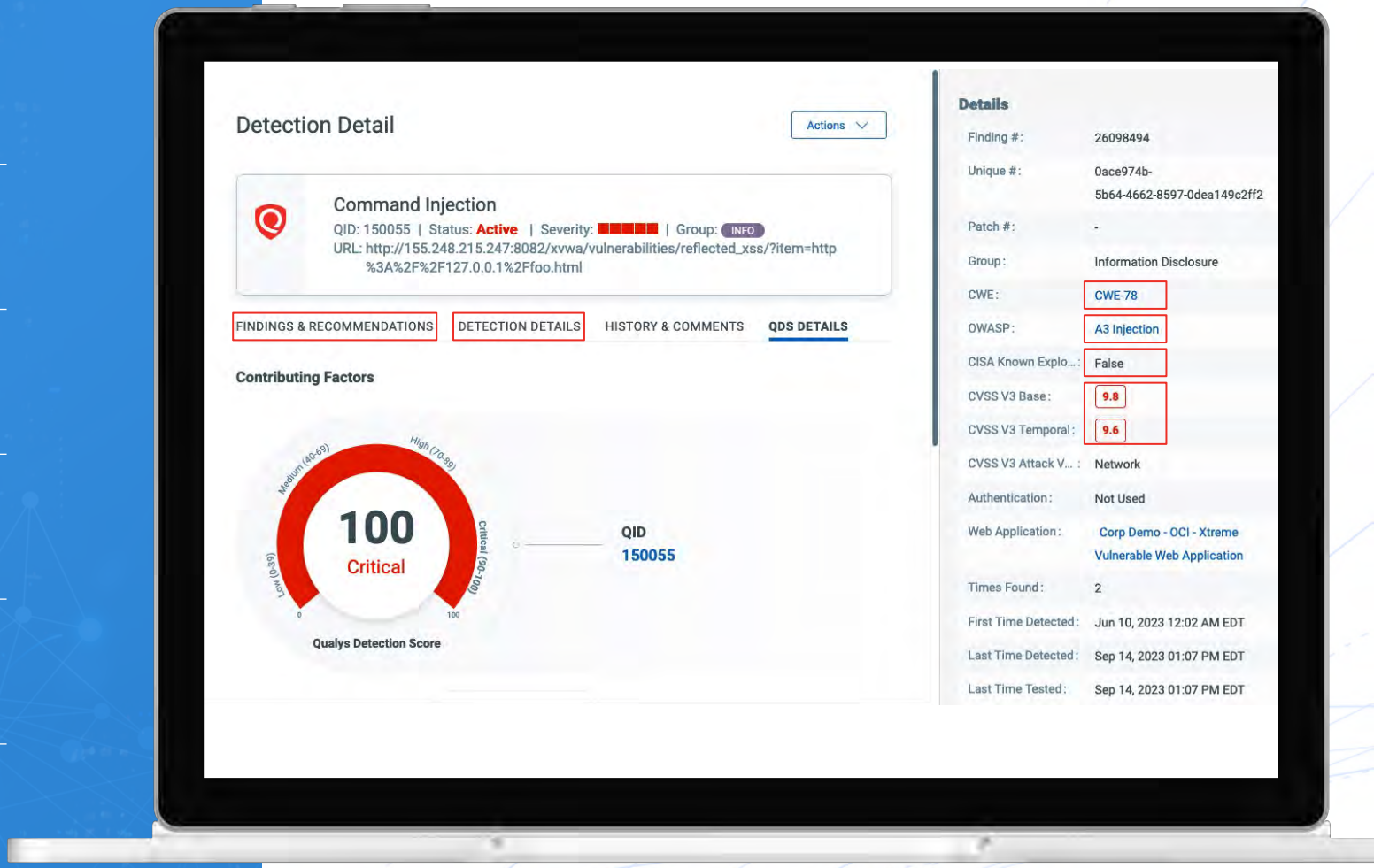
02 OWASP Top 10

03 KEV

04 CVSS

05 Recommendations

06 Req/Resp



Qualys.

Ecosystem Integrations for Greater Visibility

Consolidate Vulnerabilities in one pane of glass

01 Burp Integration:

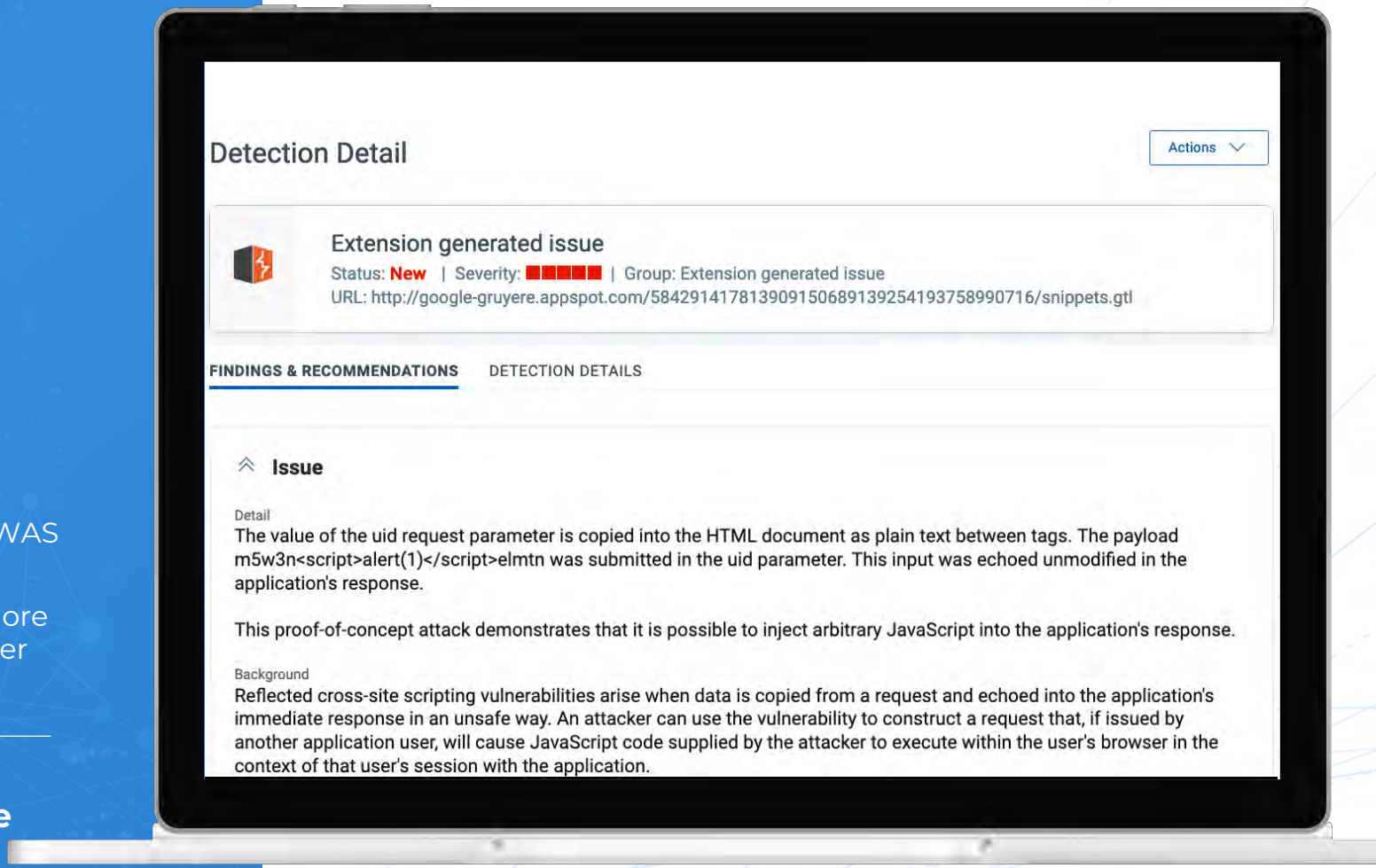
- Import Burp findings directly into WAS
- Push WAS findings into Burp for manual testing

02 BugCrowd Integration:

- Import BugCrowd findings directly into WAS
- BugCrowd bounty hunters get access to WAS scan results so they can focus on more sophisticated business logic attacks better aligned with manual penetration testing

---

Benefits include a comprehensive view of web application and API security and more efficient manual penetration testing.



Qualys.

“The single biggest problem in communication is the illusion that it has taken place.”

George Bernard Shaw

Qualys.

Effective and Automated Ticketing Integrations

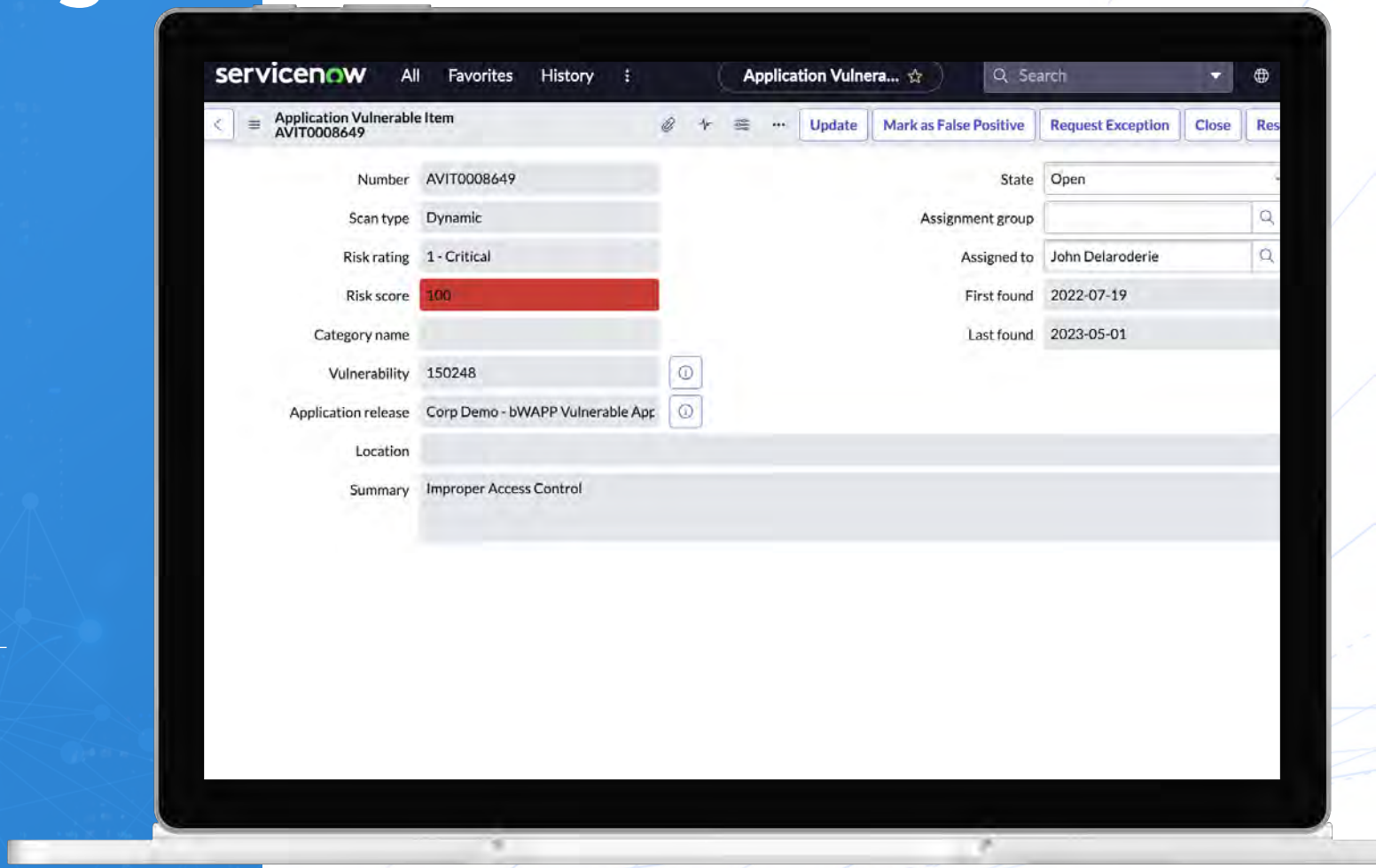
Reduce MTTR with WAS Integrations

01 **Process scan results into ticketing systems to start remediation as soon as vulnerabilities are detected:**

- Service Now Application Vulnerability Response
- Jira

---

02 Create filters, assignment rules, or manually assign tickets to developers or teams for remediation



Qualys.

Building Security Into the CICD Frameworks

Shift Left with WAS Connectors

01 **Launch scans in CICD Pipelines with connectors to:**

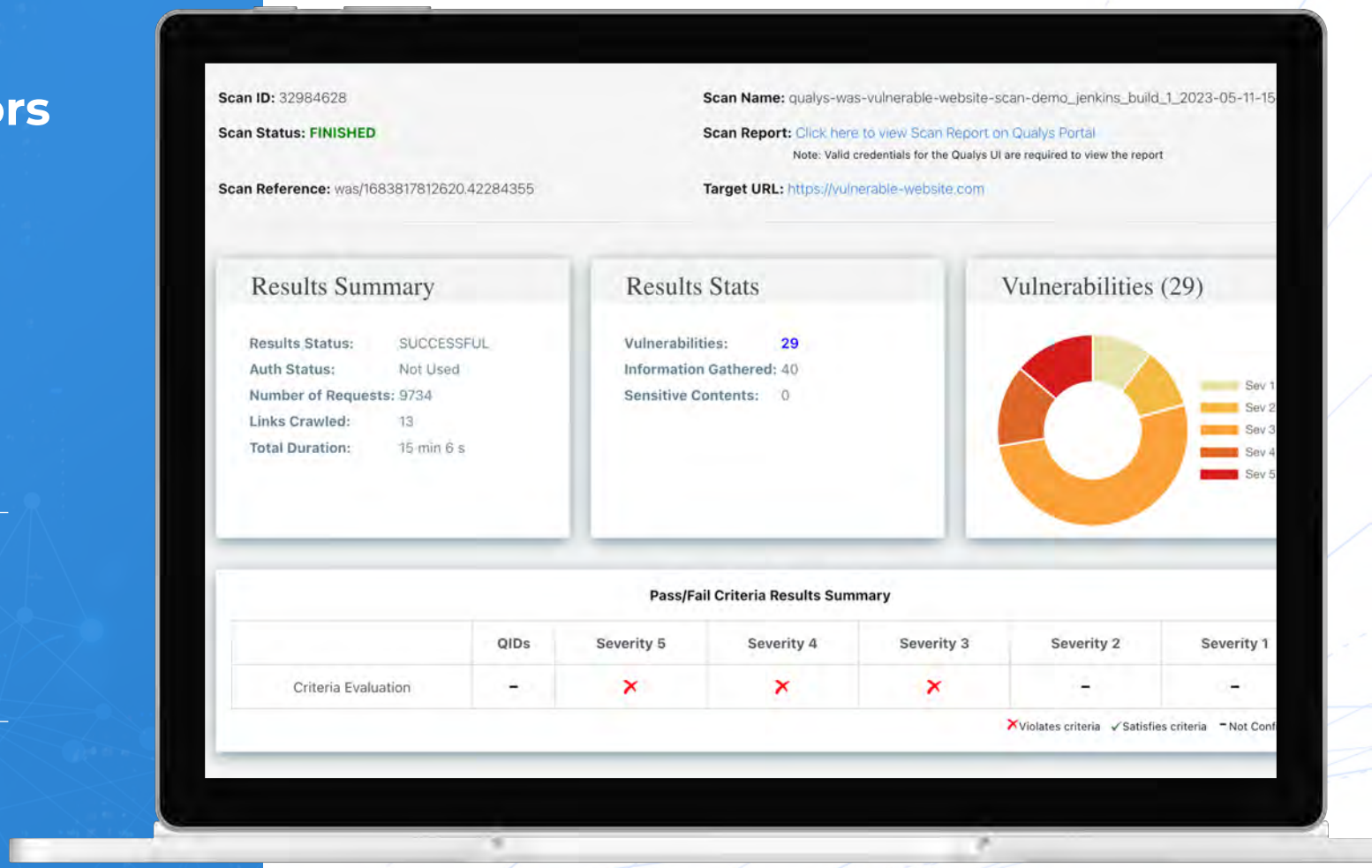
- Azure DevOps
- Jenkins
- Team City
- Bamboo

---

02 Create build pass/fail criteria based on vulnerability severities

---

03 View all scan artifacts directly in CICD tools



Qualys.

Customize Visibility For Data-Driven Action

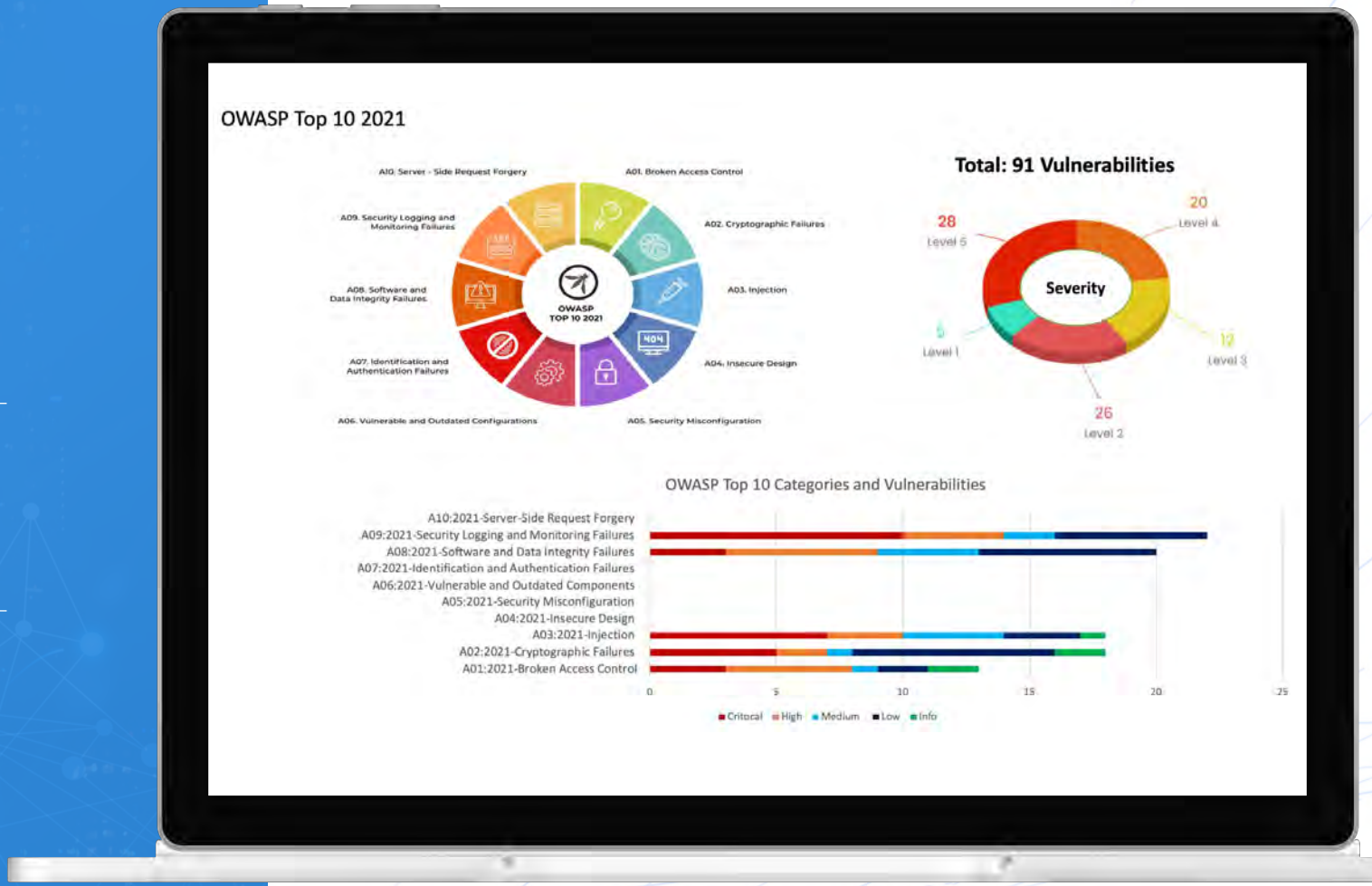
Get the information you need the way you need it

01 Dashboards with customizable widgets let you see the data and metrics important to you

02 Customized scheduled reports deliver content to ensure critical information is never out of date

03 Custom solutions through the Qualys API allow you to build your own tools and integrations to reach stakeholders where they need it

- Slack
- Email
- Teams



Qualys.

“Even a correct decision is wrong when it was taken too late”

Lee Iacocca

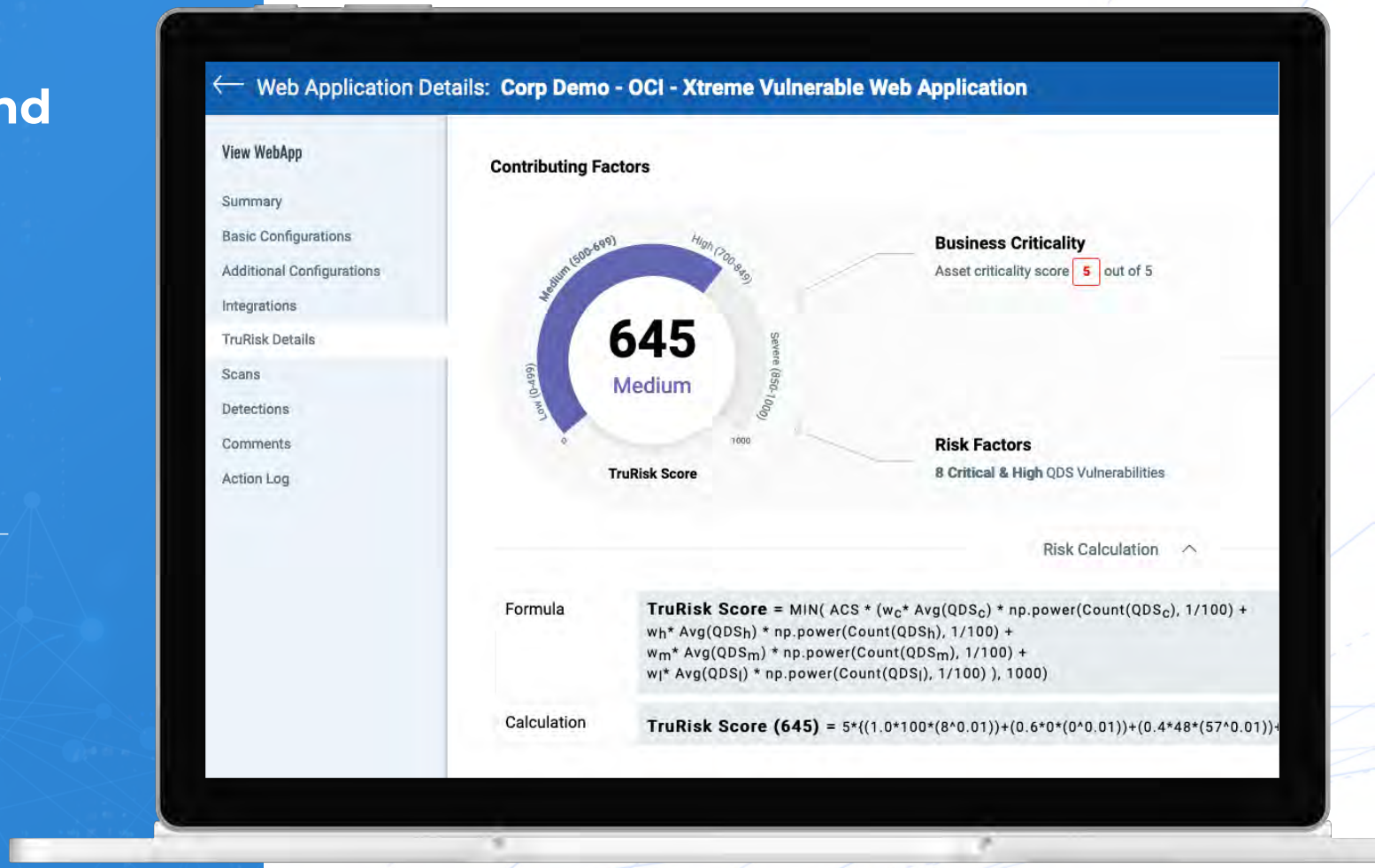
Qualys.

Qualys TruRisk to Prioritize Risk Elimination

Prioritize Web Applications and Plan Remediation Based on Intelligent Risk Algorithms

01 Configure business criticality for applications and APIs to provide greater context to threats, risk, and potential impact

02 Weighted QDS scoring of vulnerabilities provides greater insight than severity or CVSS scoring alone



Qualys.

Drive Secure Coding With Qualys WAS

Eliminate Software Vulnerabilities in Custom Code with Specific Solution Options

01

Code Remediation

For each detection, get detailed solutions to resolve even the most complex vulnerabilities

02

Secure Vulnerable Libraries

Quickly identify vulnerable JavaScript libraries to protect against attacks and known exploits

03

Commercial Software Patches and Updates

Vulnerable software from commercial vendors are flagged so that you can apply the updates and patches needed to keep your web applications secure

04

Security Misconfigurations

Security Misconfigurations are the most common vulnerabilities in web applications today. Qualys WAS will identify these misconfigurations and help you configure them to maximize their effectiveness

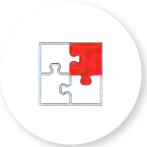
Qualys.

Measure, Communicate, and Eliminate Risk

Reduce Risks in Web Apps and APIs with the Qualys Platform

Comprehensive Discovery
Discover internal, external & previously unknown web assets and forgotten web applications exposed to the internet.

PII Collection and Exposure Detection
Prevent financial loss due to PII data theft and fines.



Ecosystem Consolidation
Import vulnerabilities from 3rd party manual penetration tests alongside WAS detections for a comprehensive view of web application security.

API Scanning
Runtime vulnerabilities in REST and SOAP APIs can identified before attackers can exploit them.

Malware Detection
Protect business name and reputation while preventing financial loss due to malware data theft.

CICD Integrations
With customized pass/fail criteria for builds, developer teams can be sure their applications deploy without software vulnerabilities.

Ticketing Integrations
Leveraging ticketing automation allows remediation to start as soon as the scan completes, reducing MTTR.

Qualys TruRisk
Intelligent risk-based prioritizations of web applications and APIs.

Qualys.

Start Your Free Trial Today

Already a Qualys Customer?

Contact your TAM to start your free trial

New to Qualys?

Sign up for a free trial at:
https://www.qualys.com/apps/web-app-scanning/

Qualys.

Vertiv Scanning Embedded Devices with Qualys WAS

Jeremy Block
Director of Product Security

Jeremy Block

- Director of Product Security
- 5 years with Vertiv
- 18+ years in Engineering
- B.S. Electrical and Computer Engineering from Ohio State University
- Extensive experience with embedded system development
- Security and Engineering cannot be truly successful without each other

Qualys.

VERTIV™

Future-Ready Technology From Edge to Cloud

- Liquid Cooling Options for Data Centers
- Micro Data Center & Edge White Space
- Complete Power Management
- Thermal Management
- Prefabricated Modular Solutions
- Continuity Services

Qualys.

About Vertiv

IT Infrastructure Support Since 1965

750,000+ Customers Today

27,000 Global Employees

24 Manufacturing Centers

19 Customer Experience Centers

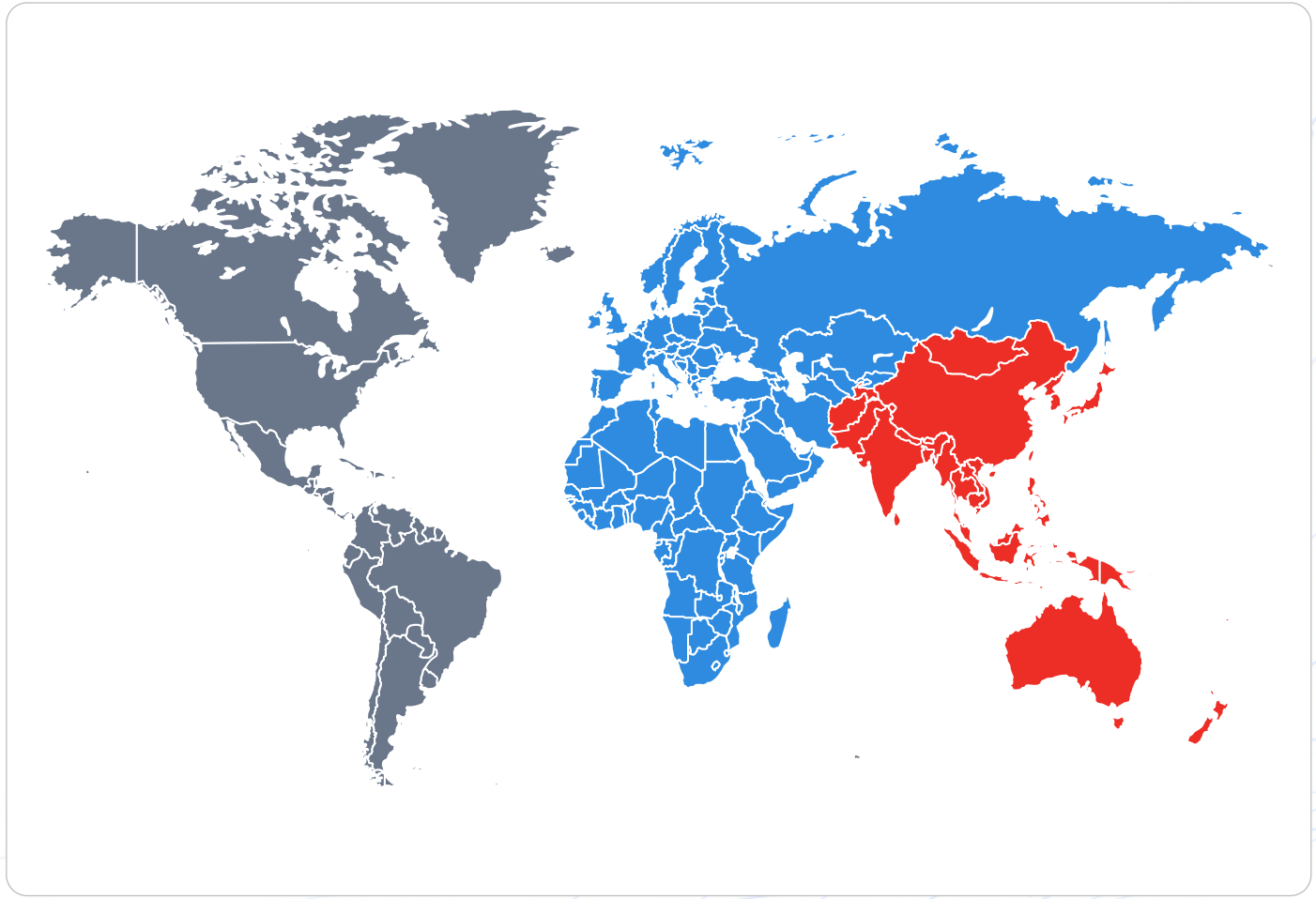
2,740 Global Patents

770+ Pending Patents

220+ Global Service Centers

3,500+ Global Field Service Engineers

87% First-Time Fix Rate in Site Emergency Visits



Qualys.

Challenges with Embedded Devices

- Vertiv currently manufactures a wide array of devices with an equally broad spectrum of unique firmware.
- Many of these devices run a web server and application for user interface and system integration.
- Embedded devices running web applications are susceptible to the same attacks faced by more typical web applications – SQLi, XSS, etc.
- Unlike typical web applications, embedded devices often have more limited options for patching and remediation – (limited connectivity and frequently new firmware must be downloaded and replaced on the device.)
- Consumers expect that the embedded devices will be free from vulnerabilities and may test them directly.

Qualys.

Critical Requirements We Were Looking For

- **Accurate Reporting** of vulnerabilities in custom code and 3rd party opensource software
- Identify risk based on **OWASP Top 10, CWSS, and CVSS** for prioritizing remediation
- **Identify Security Misconfigurations** in embedded devices
- **Automated Reporting** delivery to developers to reduce Time-To-Remediation
- **Clear and Concise** remediation steps to facilitate efficient resolution of vulnerabilities

Qualys.

How We Use WAS

Dynamic Scanning in Embedded Applications

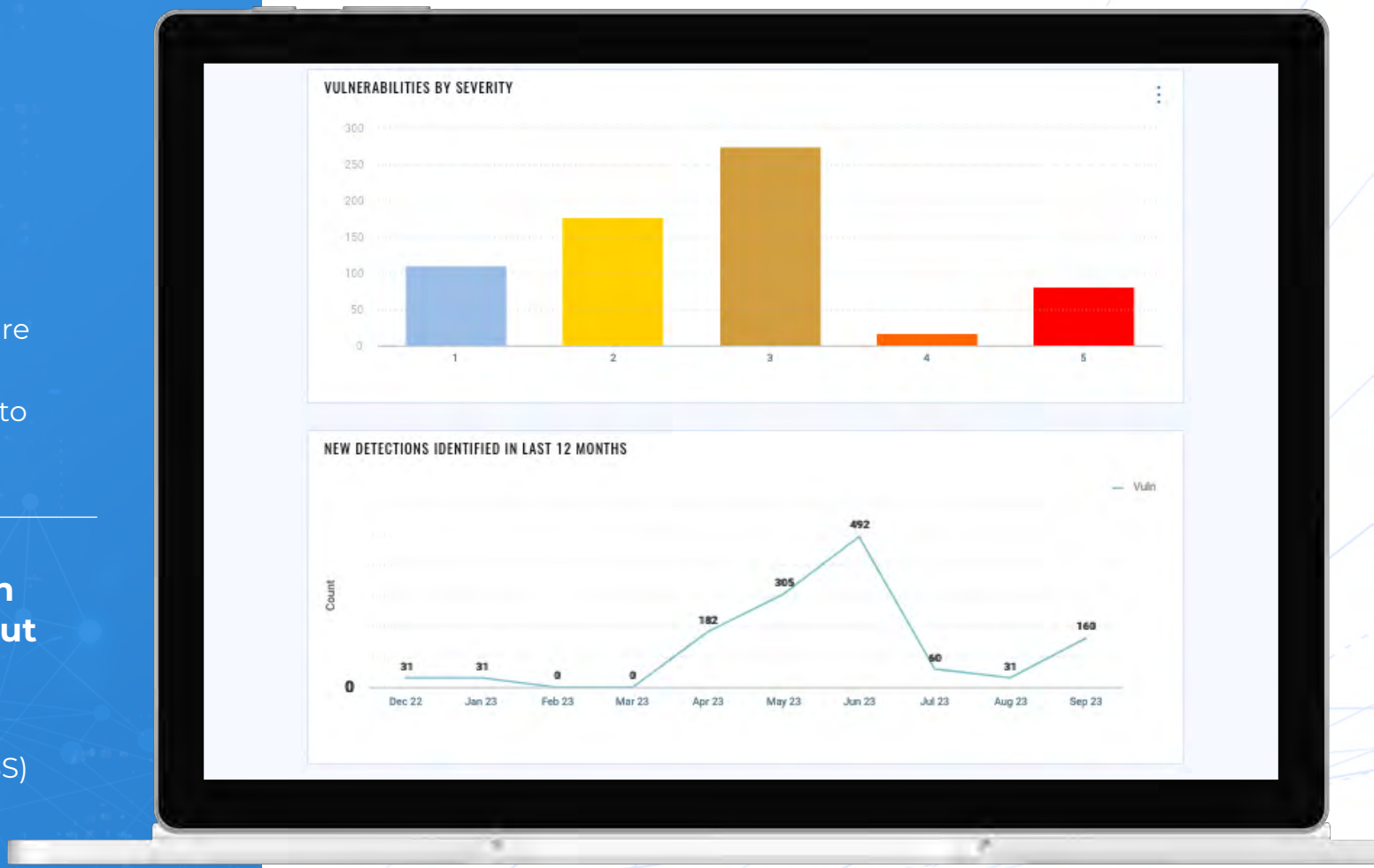
Runtime dynamic testing against Embedded Devices running web applications

- WAS scans are performed during the firmware development process
- Testing results are parsed out and pushed into tickets via API integration

---

Prioritization of risk-based remediation focuses on various factors to include but not limited to:

- OWASP Top 10
- Common Weaknesses Scoring System (CWSS)
- Common Vulnerability Scoring System (CVSS) 3.1

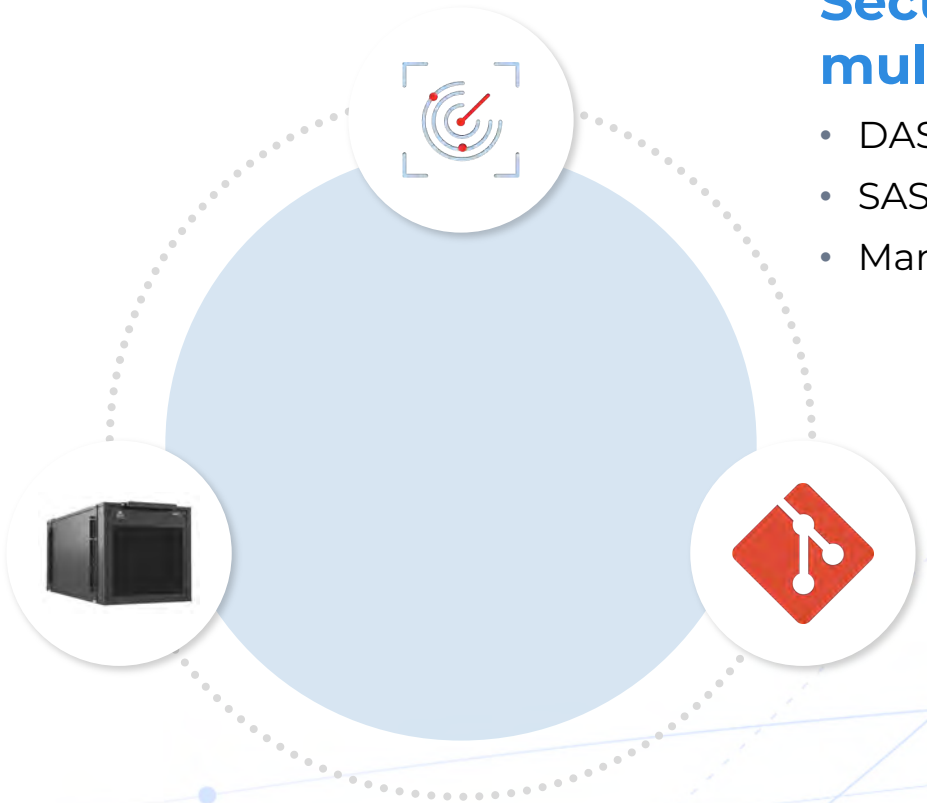


Qualys.

Vertiv Embedded Device Testing Program Data Flow Diagram

Security Testing multiple tools/vendors

- DAST
- SAST
- Manual penetration testing



Testing performed on actual product

Testing integrated into SCM

Qualys.

Vertiv Embedded Device Scanning Program Results

- Efficiently identify and remediate risks
- Prioritized actionable findings with relevant context delivered to the engineering teams for intelligent planning
- **Reduction in ‘low hanging fruit.’** Most findings that customers would otherwise find with their own AppSec programs
  - Greater customer trust
  - Reduction in total cost of security issues

Qualys.

Final Thoughts

Qualys.


SC
23