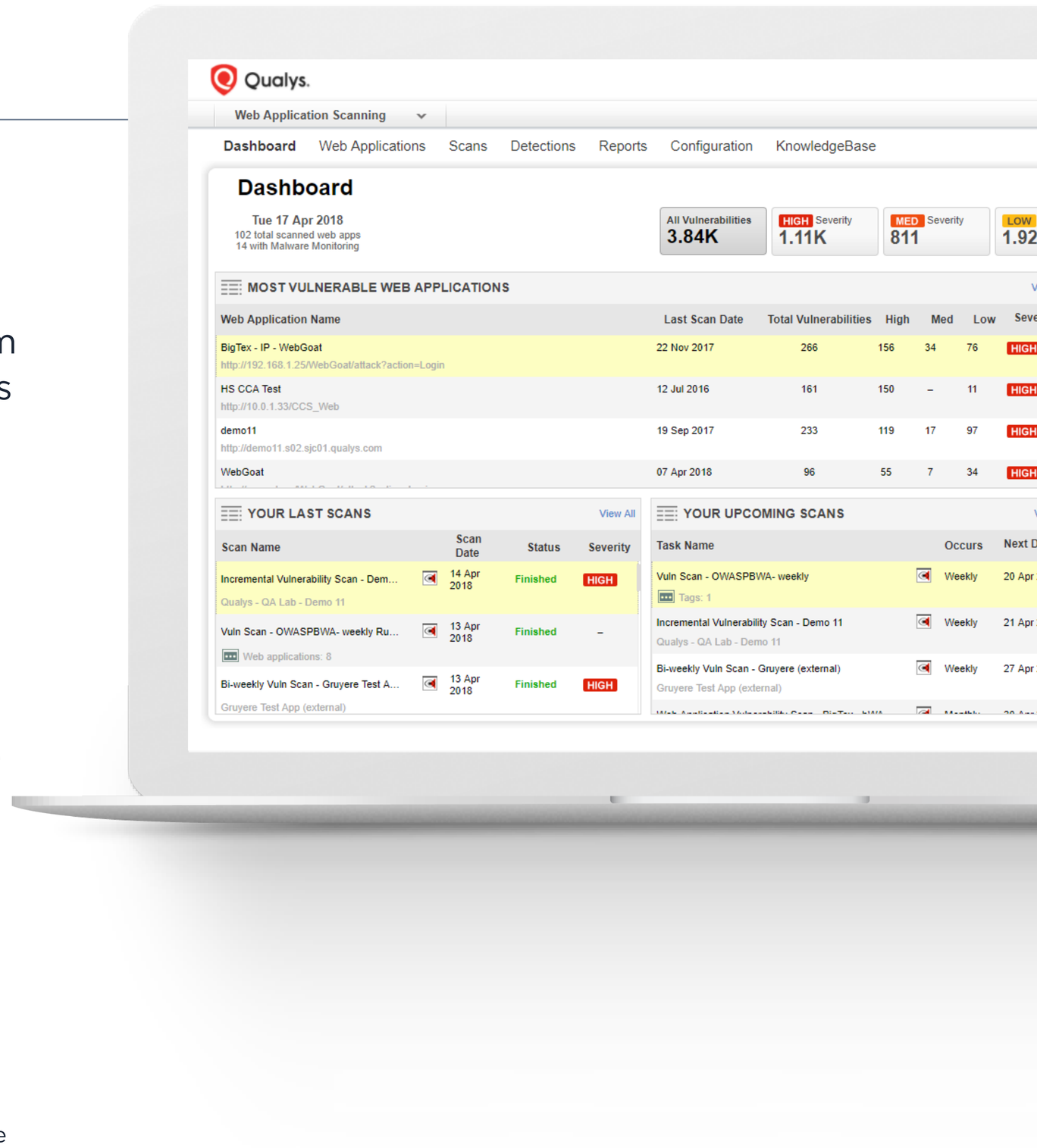
Web Application Scanning

Find, fix security holes in web apps, APIs.



Qualys Web Application Scanning (WAS) is a cloud-based service that provides automated crawling and testing of custom web applications to identify vulnerabilities including cross-site scripting (XSS) and SQL injection. The automated service enables regular testing that produces consistent results, reduces false positives, and easily scales to cover thousands of websites. Qualys WAS is bundled with additional scanning technology to proactively monitor websites for malware infections, sending alerts to website owners to help prevent blacklisting and brand reputation damage.

Built on the world's leading cloud-based security and compliance platform, Qualys WAS frees you from the substantial cost, resource and deployment issues associated with traditional software products. Known for its fast deployment, ease of use, and unparalleled scalability -- scanning thousands of web applications per week -- Qualys WAS gives organizations the ease of use, centralized management and integration capabilities they need to keep attackers at bay and their web applications secure.

Key Features

Comprehensive discovery

WAS finds and catalogs all web apps in your network, including new and unknown ones, and scales from a handful of apps to thousands. With Qualys WAS, you can tag your applications with your own labels and then use those labels to control reporting and limit access to scan data.

Deep scanning

WAS' dynamic deep scanning covers all apps and APIs on your perimeter, internal networks, and public cloud instances, and gives you instant visibility of vulnerabilities like SQLi and XSS. Authenticated, complex and progressive scans are supported. With programmatic scanning of SOAP and REST API services, WAS tests IoT services and mobile app backends.

DevSecOps tool

WAS can insert security into application development and deployment in DevSecOps environments. With WAS, you detect code security issues early and often, test for quality assurance and generate comprehensive reports. With a robust API and a native plugin for Jenkins, Qualys WAS provides everything you need to automate scanning in your CI/CD environment.

Malware detection

WAS scans an organization's websites, and identifies and alerts you to infections, including zero-day threats via behavioral analysis. Detailed malware infection reports accompany infected code for remediation. A central dashboard displays scan activity, infected pages and malware infection trends, and lets users initiate actions directly from its interface.

Qualys WAS provides complete, accurate, and scalable web security and enables organizations to assess, track, and remediate web application vulnerabilities. Its capabilities are powered by the Qualys Cloud Platform.

Benefits

Comprehensive protection

Qualys WAS' native integration with Qualys Web App Firewall (WAF) provides for one-click virtual patching of identified vulnerabilities.

Clarity and control

A single interface lets you identify, manage and fix all web app vulnerabilities and misconfigurations.

App dev hygiene

Integrates with the software development lifecycle allowing scans at any time by developers, QA and security teams, as well as automating scans in DevOps and CI/CD pipelines.

Broad threat coverage

Detect, identify, assess, track and remediate OWASP Top 10 risks, WASC threats, CWE weaknesses, and web-based CVEs.

Microsoft

"We found Qualys ideal for our need to assess thousands of websites with limited resources."

Infrastructure Security Team
Manager at Microsoft

Find and catalog all your web apps

Web apps, often plagued by vulnerabilities and misconfigurations due to poor coding and faulty testing, can be put on your network by almost anyone. Large organizations have hundreds, even thousands of them. Qualys WAS gives you visibility and control by finding official and “unofficial” apps throughout your environment, and letting you categorize them.

- Find approved and unapproved web apps in your network with continuous, comprehensive application discovery and cataloging
- Organize your data and reports using your own labels with customizable web app asset tagging

Visualize and document your web app security status with actionable data

Qualys offers unparallelled web app security with the seamless integration of Qualys WAS and Qualys Web Application Firewall (WAF) 2.0, which gives you one-click patching of web apps, including mobile apps and IoT services.

- Take your results from data to insights to action in minutes by performing powerful analyses of your scans across many applications at once
- Tailor how the results are presented to different audiences with customized report templates
- Get a comprehensive view of scans, reports and vulnerabilities on a single screen with Qualys WAS’ central dashboard
- Boost agile, continuous app development and deployment in DevSecOps environments by catching code and configuration errors early and often, while iteratively building, testing and launching software

Rapidly harden web apps with integrated WAF

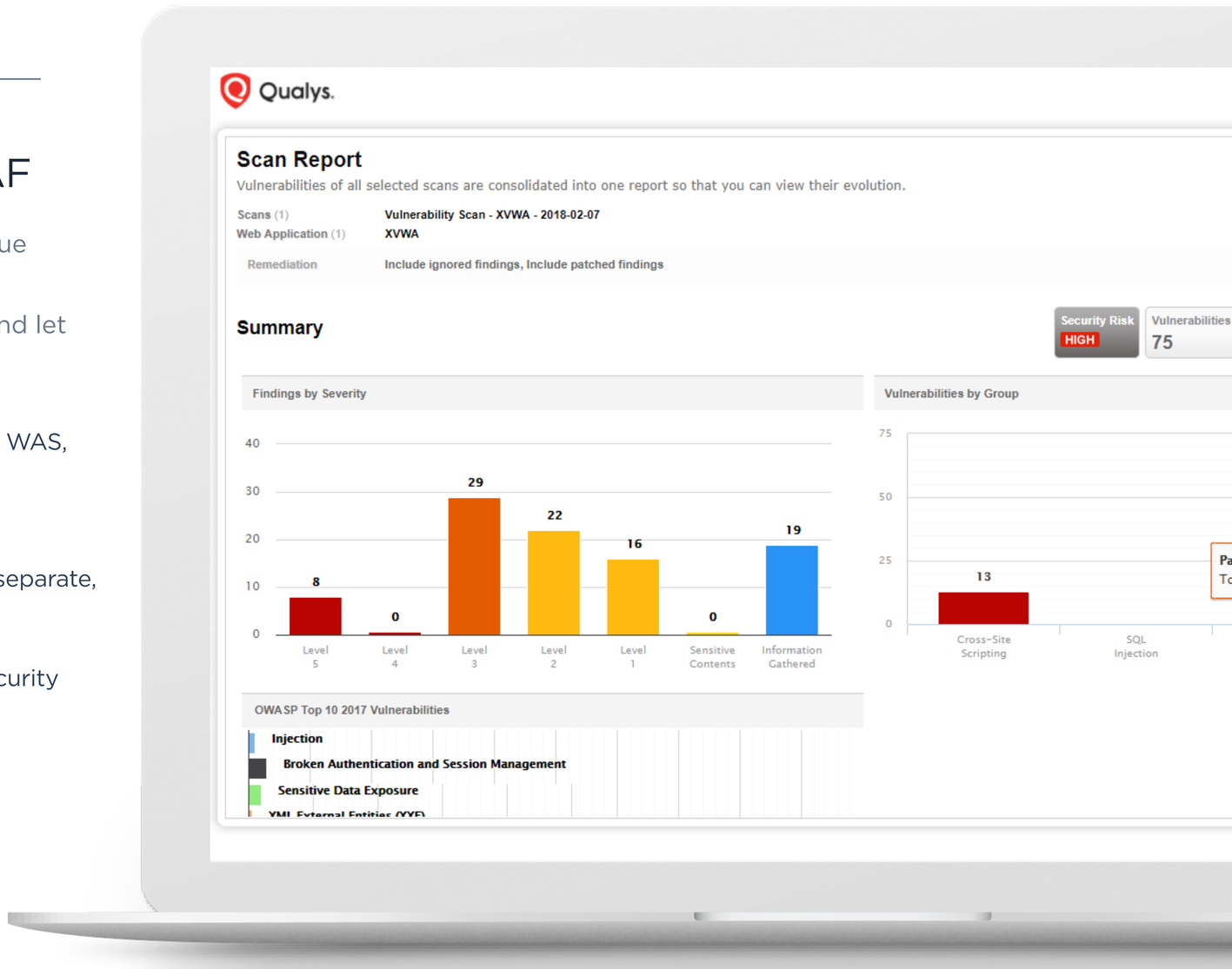
As organizations retool and expand the reach of their web apps to pursue digital transformation innovations, Qualys WAS’ interactive reporting capabilities give you the big picture of your web app security posture and let you drill down into details.

- From a single console, you can detect web application vulnerabilities with WAS, and rapidly protect them from attack with WAF for true, integrated web application security
- Avoid the redundancies and gaps that come with trying to glue together separate, siloed solutions, as the Qualys Cloud Platform keeps everything in sync
- Integrate web app scan data via a rich, extensive set of APIs into other security and compliance systems, such as firewalls, and SIEM and ERM solutions

Perform deep, exhaustive application scans at scale

Unsafe web applications offer hackers an attractive attack surface and convenient entry point into your IT environment. When breached, web apps can expose massive amounts of confidential business data. Qualys WAS protects you with incisive, thorough, precise scans, scaling up to thousands of web apps and with negligible false positives.

- Secure very large web apps with progressive scanning, which lets you scan in incremental stages and bypass restrictions preventing you from scanning an app in one pass
- Detect OWASP Top 10 risks such as SQL injection, cross-site scripting (XSS), XML External Entities (XXE), broken authentication, and misconfigurations
- Test IoT services and mobile apps as well as API-based business-to-business connectors, with Qualys WAS’ SOAP and REST API scanning capabilities
- Test like a real user with authenticated scanning, including advanced scans using Selenium, the open source browser automation system for web app testing
- Set scans’ exact start time and duration with MultiScan
- Complete scans more efficiently -- less idle time and greater coverage -- with automatic load-balancing of multiple application scans across a pool of scanner appliances
- Rid your websites and apps of malware -- including the type that eludes anti-virus software, which Qualys WAS removes using behavioral analysis -- and trigger alerts
- Consolidate automated scan data from WAS with data from manual testing approaches - via integrations with Burp Suite and Bugcrowd - to get a complete view of your web app vulnerabilities
- Prioritize remediation and focus on the most critical flaws



Powered by the Qualys Cloud Platform – the revolutionary architecture that powers Qualys' IT security and compliance cloud apps

Sensors that provide continuous visibility

On-premises, at endpoints or in the cloud, the Qualys Cloud Platform sensors are always on, giving you continuous 2-second visibility of all your IT assets. Remotely deployable, centrally managed and self-updating, the sensors come as physical or virtual appliances, or lightweight agents.

Respond to threats immediately

With Qualys' Cloud Agent technology, there's no need to schedule scan windows or manage credentials for scanning. And Qualys Continuous Monitoring service lets you proactively address potential threats whenever new vulnerabilities appear, with real-time alerts to notify you immediately.

All data analyzed in real time

Qualys Cloud Platform provides an end-to-end solution, allowing you to avoid the cost and complexities that come with managing multiple security vendors. The Qualys Cloud Platform automatically gathers and analyzes security and compliance data in a scalable, state-of-the-art backend, and provisioning additional cloud apps is as easy as checking a box.

See the results in one place, anytime, anywhere

Qualys Cloud Platform is accessible directly in the browser, no plugins necessary. With an intuitive, single-pane-of-glass user interface for all its apps, it lets you customize dashboards, drill down into details, and generate reports for teammates and auditors.

Cloud Platform Apps

Qualys apps are fully integrated and natively share the data they collect for real-time analysis and correlation. Provisioning another app is as easy as checking a box.

ASSET MANAGEMENT

- AI Asset Inventory
- SYN CMDB Sync

IT SECURITY

- VM Vulnerability Management
- TP Threat Protection
- CM Continuous Monitoring
- IOC Indication of Compromise
- CS Container Security

WEB APP SECURITY

- WAS Web App Scanning
- WAF Web App Firewall

COMPLIANCE MONITORING

- PC Policy Compliance
- SCA Security Configuration Assessment
- PCI PCI Compliance
- FIM File Integrity Monitoring
- SAQ Security Assessment Questionnaire

CLOUD SECURITY

- CI Cloud Inventory
- CSA Cloud Security Assessment

CERTIFICATE SECURITY

- CRI Certificate Inventory
- CRA Certificate Assessment

Request a full trial (unlimited-scope) at qualys.com/trial

Qualys is easy to implement, easy to use, fully scalable – and require NO infrastructure or software to maintain.