Qualys Web Application Scanning (WAS)

De-risk Your Web Apps & APIs for Reduced Attack Surface

In today's digital landscape, web applications and APIs are critical components of business operations, yet they represent significant attack vectors for cyber threats. Qualys WAS addresses these challenges by offering comprehensive application discovery, continuous vulnerability detection, and automated remediation workflows.

Qualys Web Application Scanning (WAS) empowers organizations to proactively secure their web applications and APIs, reducing web security risks and enhancing compliance through comprehensive discovery and continuous monitoring across the entire web attack surface. By integrating seamlessly with the software development lifecycle, Qualys WAS enables rapid risk remediation, ensuring robust security coverage.

Measure Risk with Comprehensive Discovery

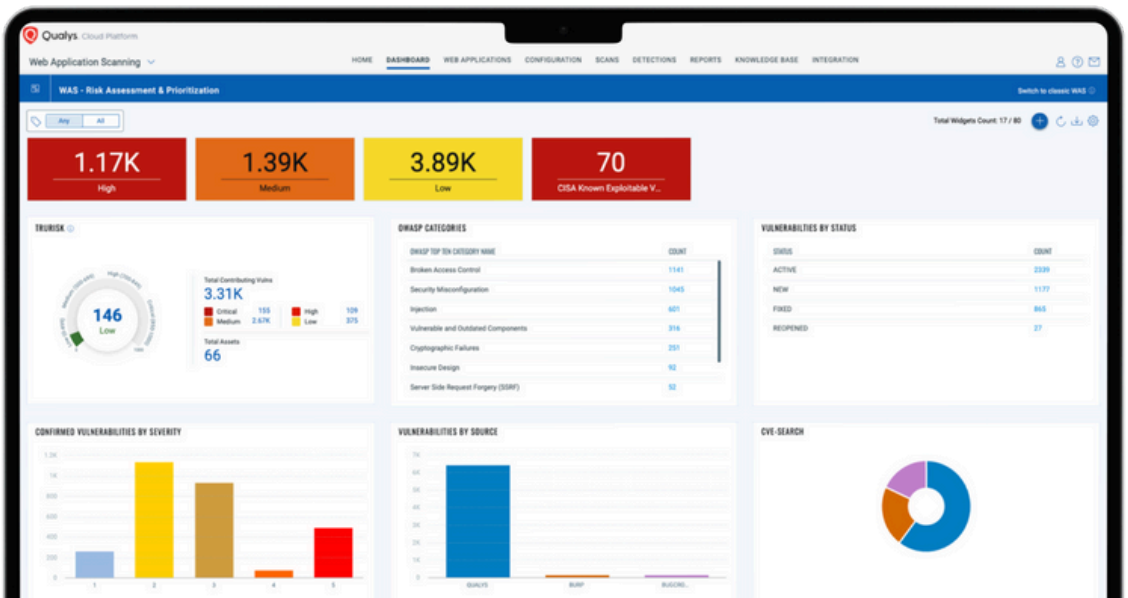
Qualys WAS uncovers all web applications and APIs, including previously unknown or forgotten assets, providing real-time insights into the security posture. This proactive discovery helps organizations quickly integrate these assets into their security programs, ensuring continuous coverage and threat mitigation.

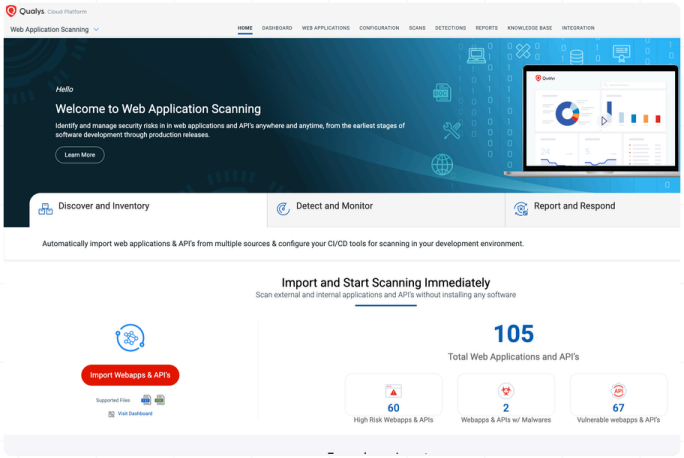
Communicate Risk with Continuous Monitoring

Through automated, continuous monitoring, Qualys WAS detects vulnerabilities, misconfigurations, PII exposures. It prioritizes critical risks from OWASP Top 10, zero-day threats, complies with industry standards and regulations. Qualys WAS saves time and resources, preventing loss of brand reputation and value.

Eliminate Risk with Remediation Workflows

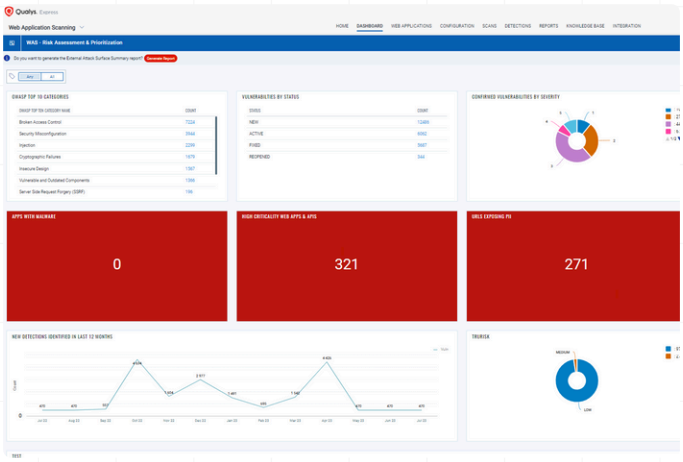
Integrating with CI/CD environments and leveraging ITSM ticketing automation, Qualys WAS supports DevSecOps practices. It promotes collaboration between development, security, and operations teams, reducing Mean Time to Remediation (MTTR) and ensuring robust application security from development to deployment.





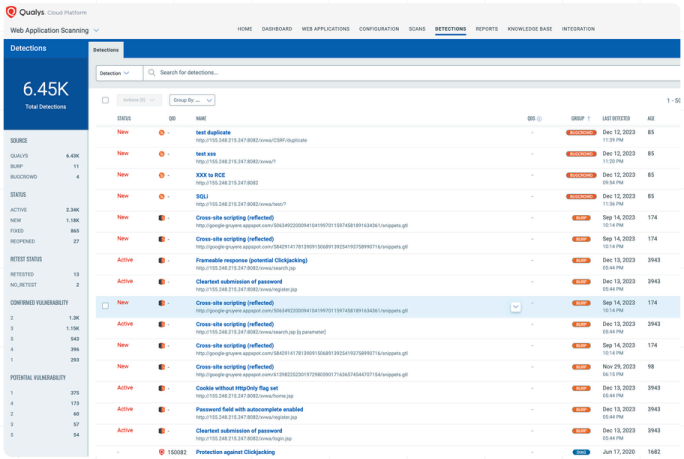
Discover All Web Apps & APIs

Uncover and secure vulnerabilities across all web assets inventory – internal, external, cloud-hosted, forgotten or unknown.



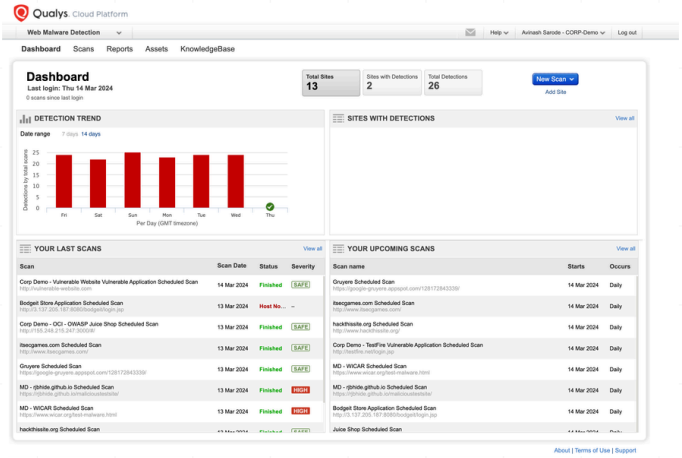
Detect PII Exposures

Guard against hefty fines from exposed personal data (PII) & compliance issues with standards like GDPR, PCI DSS, HIPAA, etc



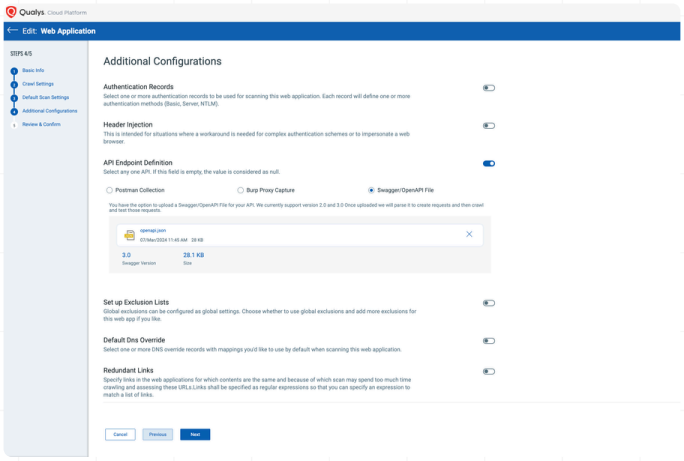
Merge Third-Part Data

Consolidate third-party and manual penetration test data with automated WAS findings for a unified, complete security overview



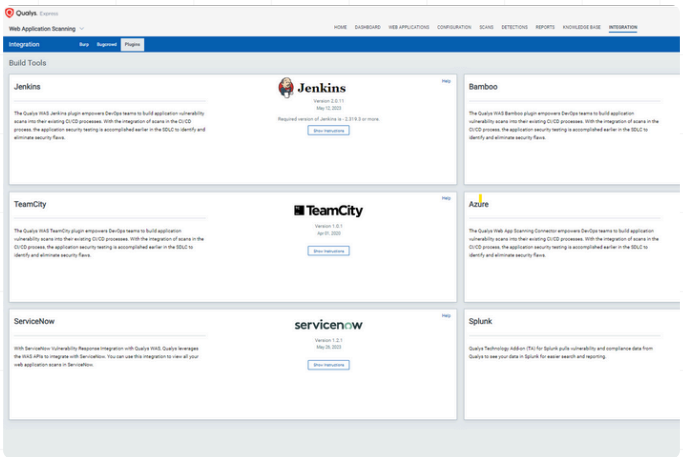
Prevent Malware Data Theft

Detect and eliminate malware threats, using behavioral analysis for zero-day threats, to safeguard your business reputation.



Discover & Identify API Security

Proactively scan REST/SOAP APIs, API connectors and microservices to secure your web traffic and prevent exploitations.



Quickly Shift Left or Right

Reduce MTTR by embedding WAS in CI/CD environments or ITSM ticketing systems to align security, development and operations.

Features of Qualys Web Application Scanning (WAS)

Measure Web App & API Risks

Comprehensive Discovery

Finds and catalogs all web apps in the network, scales from a few apps to thousands, and allows tagging for organized reporting and access control. Automates the discovery of both known and unknown web apps, which aids in comprehensive security coverage. Tagging helps in organizing and managing web apps effectively, enhancing the focus on security efforts.

Broad Threat Coverage

Detects, identifies, assesses, and helps remediate OWASP Top 10 risks, WASC threats, CWE weaknesses, and web-based CVEs. Provides a broad range of threat detection capabilities, ensuring that web applications are protected against a wide array of vulnerabilities and compliance issues, thereby enhancing overall web security posture.

Automated Crawling and Testing

Automated service that regularly tests web applications for vulnerabilities such as XSS and SQL injection, with capabilities to scale up to thousands of websites. Consistent, regular testing reduces false positives and scales easily, ensuring thorough and reliable vulnerability identification across numerous web applications. This helps maintain security standards consistently with minimal manual intervention.

Deep Learning-Based Web Malware Detection

Unlike traditional hash-based detection methods, Qualys's deep learning-based web malware detection provides an advanced, AI-powered solution to protect against modern malware threats, including sophisticated zero-day attacks, with a 99% detection accuracy to secure IT environments and protect business reputation. It proactively monitors for both known and novel malware threats, preventing potential blacklisting, identifying negative reputations like Google Safe Search and malicious third-party content providers or external links.

PII Collection & Exposure Detection

Through comprehensive scanning and monitoring, Qualys WAS ensures that sensitive data is protected, reducing the risk of regulatory non-compliance and safeguarding user privacy. It detects Personally Identifiable Information (PII) collection and exposure within web applications and helps comply with data protection regulations such as GDPR, HIPAA, and PCI DSS by identifying and managing PII vulnerabilities.

API Scanning

By utilizing OAS, Swagger files, Postman collections, WSDL files, Qualys WAS can parse endpoints and operational procedures to conduct thorough API testing. It performs testing of IoT services, mobile apps, and API-based connectors to identify runtime vulnerabilities in both REST and SOAP APIs, enhancing the protection of critical API endpoints against threats and vulnerabilities in interconnected systems & applications

AI-Powered Scanning

AI-powered Scan significantly increases the efficiency of vulnerability assessments by focusing resources on areas most likely to contain vulnerabilities, reducing the time required to identify critical issues in large applications. Leveraging deep learning algorithms to scan large applications, AI-Powered Scanning uses clustered checks, where the scanning process is directed and intensified based on initial detections, allowing for a more targeted and faster assessment.

Deep Scanning

Comprehensive scanning covering all apps and APIs, including authenticated, complex, and progressive scans. Supports programmatic scanning of SOAP and REST API services. Offers deep visibility into vulnerabilities like SQL injection and XSS across all web applications and APIs, ensuring a robust defense against common and complex attack vectors. Authenticated scans mimic real-user interactions for more accurate testing.

Progressive Scanning

Allows for scans to be conducted in phases to minimize the impact on application performance. Progressive Scanning offers a more flexible approach to scanning, reducing the potential for disruptions on live web applications while still ensuring comprehensive vulnerability assessment.

Authenticated Scanning

Enhances security assessments through authenticated scanning, simulating real user interactions and utilizing advanced scans with Selenium to provide deep insights into authenticated areas of web applications. Authentication mechanisms for scanning supports complex authentication scenarios and improves scan accuracy for authenticated sessions that require complex login mechanisms for a deeper and more effective assessment.

Features of Qualys Web Application Scanning (WAS)

Measure Web App & API Risks

Third-Party Vulnerability Consolidation

Consolidates vulnerabilities identified through both automated scans in Qualys WAS and third-party tools for manual penetration testing and bug bounty programs like Portswigger, Burp, ZAP, Bugcrowd, and HackerOne. It allows these tools to import their own findings while also ingesting & correlating WAS vulnerabilities for bi-directional analysis.

Integration with Bugcrowd

Manages and correlates findings from multiple sources like Bugcrowd with bidirectional import and export of scan results, improving the visibility of web application vulnerabilities.

Burp Log File Upload

Facilitates seamless integration of external scan data into WAS, enhancing the robustness of vulnerability management.

Integration with Qualys VMDR

Streamlines web server scans by identifying and mitigating vulnerabilities as a powerful combination with Qualys WAS for comprehensive visibility, continuous monitoring, and efficient remediation of web server vulnerabilities.

Integration with Qualys CSAM/EASM

Streamlines External Attack Surface Management and ensures continuous monitoring of all your digital assets derived from subsidiaries, mergers, or acquisitions. Qualys CSAM/EASM users can effortlessly enable web application scanning on critical assets with a comprehensive inventory of web servers.

Path Fuzzing Rules

Improves scan accuracy by allowing specific URL path components to be ignored, reducing redundant crawling.

Form Training

Allows customization in form interactions to enhance scan precision to ensure more accurate vulnerability detection by simulating realistic user inputs and behaviors, thereby improving the overall effectiveness of web application security assessments.

MultiScan

Allows precise scheduling of scan start times and durations, ensuring thorough and flexible vulnerability testing.

FQDN and DNS information via Catalog Discovery

Improved discovery capabilities enhance the visibility of web applications within the network.

Partial Scan Insights with OAuth2 Support

View Partial Scan Data for Service Error Detected Scans, Added OAuth2 Support for Swagger/API file authentication. Allows viewing of findings from incomplete scans due to service errors, and supports OAuth2 for authenticating Swagger/OpenAPI files, enhancing flexibility in handling scan results and authentication methods for API scanning.

Severity Mapping for Burp Issues

Severity assignment in WAS for Burp issues now considers both Burp Severity and Burp Confidence. This improvement ensures that the severity of vulnerabilities identified through Burp scans is more accurately represented in WAS, leading to better prioritization and remediation efforts. By considering both the severity and the confidence level of the findings, users can more effectively focus their attention on the most critical issues.

XSS Power Mode Option Profile

Introduces a comprehensive scan for XSS vulnerabilities. The XSS Power Mode provides an enhanced mechanism to detect and mitigate XSS vulnerabilities, offering robust protection against such attacks.

CSV Import Tagging

Allows tagging of web applications during CSV import. Tagging during import helps in better organization and management of web applications.

Features of Qualys Web Application Scanning (WAS)

Measure Web App & API Risks

Swagger-based REST API Scanning

Enables scanning of Swagger-based REST APIs. Swagger-based API scanning extends security coverage to API endpoints.

Qualys Browser Recorder for Selenium Script

Facilitates creating Selenium scripts for defining crawl scope. The Qualys Browser Recorder enhances automation capabilities for web application testing.

Enhanced API Management

API features for managing web applications and scans, including improvements to API security and performance, automation and integration of WAS capabilities into their workflows, allowing for scalable and streamlined vulnerability management processes.

Emerging Vulnerabilities Detection

New detection capabilities for emerging vulnerabilities and refinement of existing detection techniques to improve scan effectiveness. Users can ensure that their web applications are protected against the latest vulnerabilities and that scans are effectively identifying potential security issues.

Scanning options for modern web applications

Advanced crawling technology provide better coverage and accuracy when scanning modern web architectures, ensuring that vulnerabilities in Single Page Applications (SPAs) and other complex web applications are effectively identified.

TruRisk™ Score for an Application

Derived by combining all risk elements—the Qualys Detection Score (QDS) for the application and its criticality score. The holistic approach of this calculation ensures that the resulting score accurately reflects the potential impact and urgency of addressing the risks associated with individual applications and groups of applications for prioritized remediation.

CVSS V3 Scoring System

CVSS V3 Scoring System for vulnerabilities, restrictions on assignment of system and dynamic tags from WAS UI, and various dashboard enhancements. Adoption of the CVSS V3 scoring system provides an advanced assessment of vulnerabilities' severity, helping users prioritize remediation efforts more effectively. Restrictions on tag assignment and dashboard improvements enhance user experience and data visualization.

Communicate Web App & API Risks

Centralized, Intuitive Dashboard

A single, intuitive dashboard for full visibility over scans & reports, simplified vulnerabilities management, centralized control over remediation turning scan results into actionable data, and customization of report templates for different audiences. The dashboard allows detailed drilldowns, monitors scan activity, infected pages, malware trends, and initiates actions directly from the interface.

Visualization and Document Security

Advanced reporting and visualization tools provide a comprehensive view of the security status of web applications, enabling detailed analysis and actionable insights. Helps organizations understand their security posture in depth and make informed decisions based on detailed analyses of vulnerabilities and scans, improving strategic security planning and response efforts.

Security Mapped PDF Reports

PDF report mapped to CWE/OWASP/WASC for various QIDs, and display of scan summaries and web application filters to align findings with security standards like CWE, OWASP, and WASC.

Simple, Easy-to-Use Interface

A simple, intuitive user interface with easy access to critical functions helps easily manage web applications and APIs and perform scans for users to interact with the WAS platform. The Qualys Unified Dashboard and Qualys Query Language (QQL) for searching allows users to manage, search, review and analyze vulnerabilities in web applications and APIs.

Features of Qualys Web Application Scanning (WAS)

Eliminate Web App & API Risks

App Dev Hygiene

Supports a secure development lifecycle by enabling scans at various stages of app development and deployment by developers, QA, and security teams, automating scans in DevOps and CI/CD pipelines, reducing the risk of vulnerabilities making it to production and helping continuous security assessment without disrupting development workflows.

DevSecOps Integration

Facilitates the integration of security into DevSecOps environments and CI/CD pipelines like Azure DevOps, Jenkins, Github, TeamCity, Bamboo, etc., allowing for continuous assessment and remediation of security issues in application development and deployment cycles.

ITSM Integration for Remediation

The integration with operational tools like Splunk, JIRA, ServiceNow streamlines efficient tracking and resolution of security issues by automating vulnerability management workflows for quicker remediation.

Automatic Load-Balancing

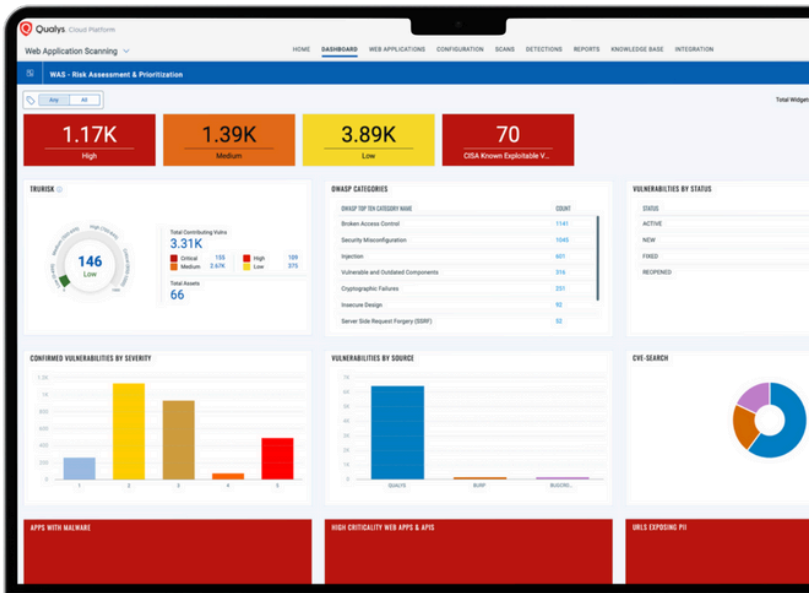
Automatic load-balancing efficiently distributes scans across scanner appliances, ensuring faster, more efficient completion of scans, optimizes resource use and enhances overall scan performance.

Extensive API Support

Ensures seamless security by integrating scan data with other security and compliance systems via rich APIs to prevent redundancies and gaps, keeping solutions in sync. Extensive API support enables the automation and customization of security and QA testing workflows, connecting Qualys WAS with existing software and processes, including firewalls, SIEM, and ERM solutions.

Get Your Free Application Risk Report

Download Now



For more information,
reach out to us at +1 800 745 4355 or visit our website

About Qualys
Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based Security, Compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. Qualys, Qualys VMDR® and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.
For more information, please visit qualys.com