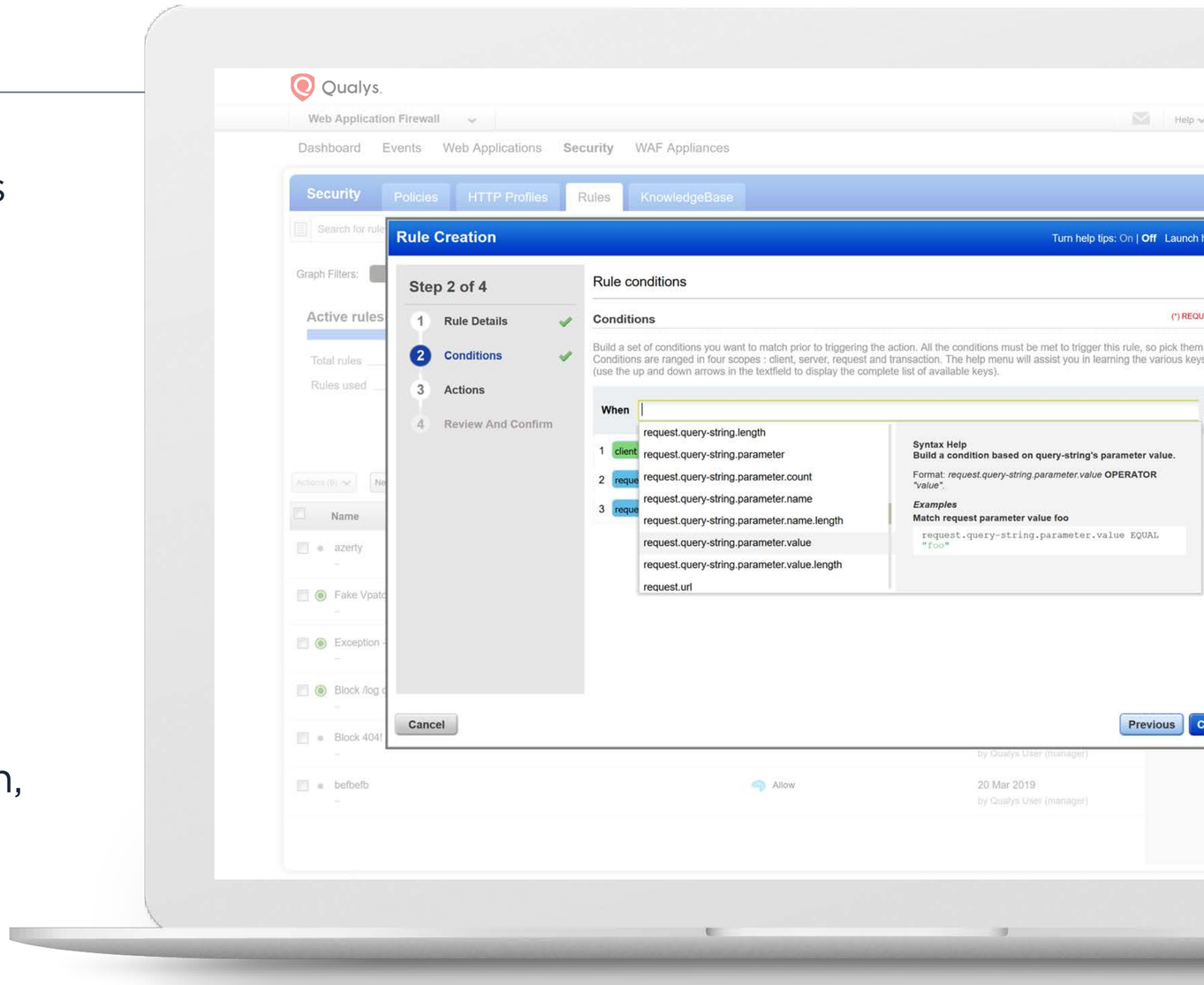
Web Application Firewall

Block attacks and virtually patch web application vulnerabilities.



Qualys Web Application Firewall (WAF) is a virtual appliance-based service that reduces the operational cost and complexity of application security. Leveraging a unified platform, it continuously detects attacks using in-house inspection logics and rulesets, and virtually patches web application vulnerabilities if needed. Its simple, scalable and adaptive approach lets you quickly block web application attacks, prevent disclosure of sensitive information, and control when and where your applications are accessed.

Qualys WAF can be used alone, or paired with Qualys Web Application Scanning (WAS). Together, they make identifying and mitigating web application risks seamless – whether you have a dozen apps or thousands. You scan your web applications using Qualys WAS, deploy one-click virtual patches for detected vulnerabilities in WAF and manage it all from a centralized cloud-based portal. Qualys WAF can be deployed in minutes, supports SSL/TLS, doesn't require special hardware and frees you from the substantial cost and resources required to use traditional products.

Features

True, integrated web app security

Qualys gives you a single, interactive console for web application vulnerability detection (Qualys WAS) and protection (Qualys WAF) for seamless identification and mitigation of risks — for a dozen apps or thousands. Scan your web apps using WAS, and deploy virtual patches for confirmed vulnerabilities to WAF. You can manage it all from a centralized portal. Security teams can now secure their web apps without having to involve network security teams — lowering operational complexity and costs.

Cloud agility

With no special hardware to buy nor maintain, Qualys WAF virtual appliance can be deployed and scaled up quickly on premises using VMware, Hyper-V or Docker; and in public cloud platforms, such as AWS, Azure or Google Cloud Platform, including using Kubernetes for PaaS use-cases. Application traffic stays in your environment to minimize latency and maintain control. WAF continuously communicates with the Qualys Cloud Platform, tracking configuration changes and sending it the latest security events.

Full visibility into firewall operation

WAF gives you complete visibility into its data for continuous monitoring, risk assessments and remediation plans. A dashboard summarizes website traffic information and security event trends. Detailed threat information lets you assess severity and adjust security settings. Search for suspicious activity and drill down into threat data to gain actionable insights. WAF continuously indexes security events into your local Elasticsearch or Splunk clusters, making your data instantly discoverable.

Strong rules, flexible control

WAF protects your web apps using security policies backed by Qualys' security intelligence, and one-click responses to security events. You can address your own security needs with simple, customizable and reusable policies and rules. Qualys' out-of-the-box specific policies are designed for popular platforms such as WordPress, Joomla, Drupal, Magento, Microsoft OWA and Sharepoint, Apache Tomcat, and Red Hat JBoss. It also includes generic templates for unknown applications and frameworks.

Qualys WAF provides immediate remediation to protect your web applications against attacks and to give your development team time to fix important security issues. Its capabilities are powered by the Qualys Cloud Platform.

jive

"We are excited that Qualys WAF will allow us to act quickly and respond to threats by using the one-click virtual patching feature to remediate active vulnerabilities."

David Cook
Chief Security Officer at Jive Software

Benefits

Immediate, comprehensive protection
Provides virtual patching and authenticated scanning (ScanTrust) via the WAS-WAF deep integration

Seamless scalability
Scales with ease to handle hundreds or thousands of web applications

Breach prevention
Prevents breaches by hardening web applications against current and emerging threats thanks to Qualys' out-of-the-box policies

Low TCO
Cuts costs by reducing time, effort and complexity for web application security

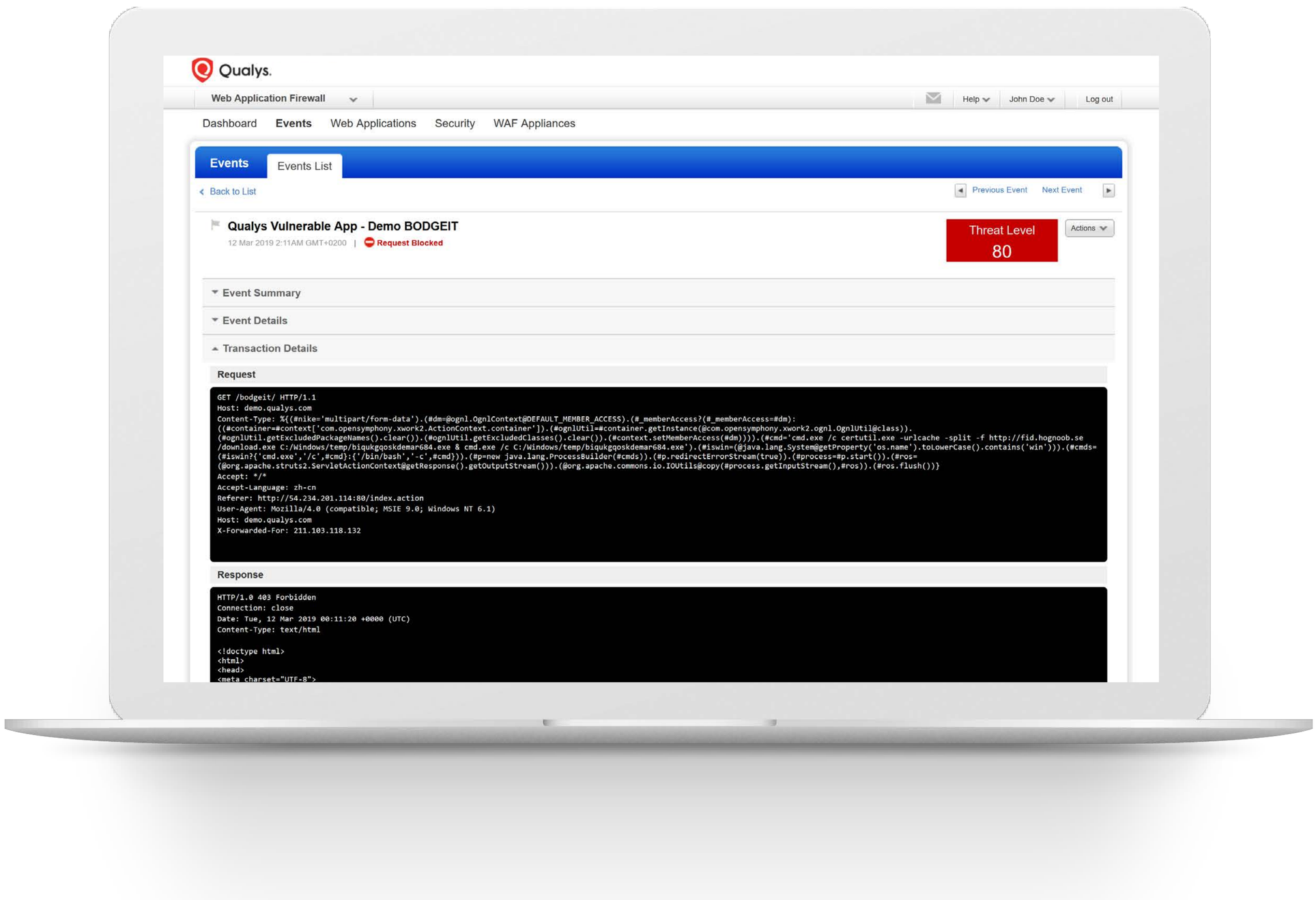
Compliance simplification
Streamlines and facilitates compliance by addressing web application firewall requirements in industry mandates and government regulations

Always up to date
Provides the best ruleset for blocking the latest attacks and zero-day vulnerabilities thanks to continuous maintenance from Qualys' security researchers

Prevent breaches by blocking attacks on web server vulnerabilities

You can't protect – nor defend yourself from – what you don't know is in your network, like unapproved devices and unauthorized software. Qualys gives you full horizontal visibility of all hardware and software, scaling up to millions of assets – on premises, in cloud instances and mobile endpoints.

- Protect cloud apps
  - Quickly and easily protect apps in public or private clouds by deploying Qualys Virtual Firewall Appliances alongside your web apps. No need to buy nor maintain special hardware
  - Add as many applications as necessary as often as you need, as these virtual machines scale seamlessly.
  - Ensure high performance and availability of business-critical web apps thanks to built-in load balancing and application monitoring.
  - Enforce applications' SSL/TLS layer thanks to Qualys WAF's offloading capability
- Adopt a new approach for web app security with Qualys WAF's adaptive policies, which are always up to date and don't require specialized expertise, nor complex rulesets to configure and maintain
  - Describe the security level for each application with a few clicks, and Qualys WAF automatically decides what to do in different situations
  - Simplify Qualys WAF configuration with Qualys generic templates, or with specific policies for popular platforms such as WordPress, Joomla, Drupal, Magento, Microsoft OWA and Sharepoint, Apache Tomcat, and Red Hat JBoss
- Defend yourself from current and future threats with customizable protection
  - Block a wide range of attacks such as Cross-Site Scripting (XSS), SQL injection, Remote Command Execution, XXE and more with native protection. As new threats emerge, Qualys' security experts update WAF's rules, which are then downloaded and spotted by the proprietary detection engine.
  - Tailor how Qualys WAF handles different types of threats, from simply logging the event to actively blocking it.
  - Create custom security rules to address specific security needs of your application and reduce the attack surface.
  - Maintain website uptime by complementing network DDoS defenses with controls over applications' latency.
- Protect your users against clickjacking, Cross-Site Scripting (XSS), and other browser-based attacks with Qualys WAF's security features for modern web browsers
- Integrate WAF API into your DevSecOps environment and protect web servers hosting the apps you're rapidly and iteratively developing and deploying



Benefit from native, deep integration between WAF and WAS

Empower security professionals to rapidly discover and mitigate critical security concerns. With the new ScanTrust feature, Qualys WAF combines with Qualys WAS to provide true visibility for your web applications: Detect with WAS, protect with WAF and get scalable scanning, false-positive reduction and one-click patching to web apps.

- From a single console, use WAS to detect vulnerabilities in web apps, including mobile and IoT apps, and – with one click – mitigate them with WAF virtual patches
- Leverage the creation of these virtual patch rules to fine-tune policies, remove false positives, and customize security rules
- Avoid the redundancies and gaps that come with trying to glue separate, siloed solutions. Reduce operating costs by reducing staff
- Evaluate and create exceptions to web events to better prioritize and mitigate vulnerabilities by combining WAF rules and policies with WAS scan data
- 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

Simplify IT compliance

It's easier than ever for employees to bypass their IT department and adopt web apps, a trend that generates significant security and compliance risks. Simultaneously, the quantity and complexity of government regulations, industry mandates and internal policies that impact InfoSec technologies and processes continues to grow. WAF can help you comply.

- Address mandates such as PCI DSS 6.6 that require app firewalls
- Comply with policies and regulations that prohibit access to certain web applications or information from particular locations by restricting access from specific countries or network address blocks
- Prevent transmission of sensitive data by blocking users' ability to upload or download content or files in unapproved or suspicious formats

Visualize and report

You need an easy, intuitive way of understanding the security of all your web applications at once. WAF gives your security team complete visibility into its data for continuous monitoring, risk assessments and remediation paths. WAF tools for visualization and reporting include a graphics-rich dashboard, interactive insights and detailed information on each threat and ways to address it.

- Spot unusual patterns in the dashboard, which shows summarized website traffic information and trends of WAF security events, including when they occurred and where they originated
- Quickly assess severity and adjust your security settings for aggressive mitigation or to minimize false positives by leveraging detailed information on each threat detected by WAF
- Use extensive filtering and dynamic search capabilities to identify suspicious activity, drill down into threat data and the Qualys KnowledgeBase, and gain actionable insights into the threat landscape

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

Sensors that provide continous 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.

- **AI** — Asset Inventory
- **VM** — Vulnerability Management
- **PM** — Patch Management
- **CI** — Cloud Inventory
- **WAS** — Web Application Scanning
- **SCA** — Security Configuration Assessment
- **SAQ** — Security Assessment Questionnaire
- **SYN** — CMDB Sync
- **TP** — Threat Protection
- **IOC** — Indication of Compromise
- **CSA** — Cloud Security Assessment
- **WAF** — Web Application Firewall
- **PCI** — PCI Compliance
- **OCA** — Out of Band Configuration Assessment
- **CRI** — Certificate Inventory
- **CM** — Continuous Monitoring
- **CRA** — Certificate Assessment
- **CS** — Container Security
- **PC** — Policy Compliance
- **FIM** — File Integrity Monitoring

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

It's an out-of-the-box solution that's centrally managed and self-updating.