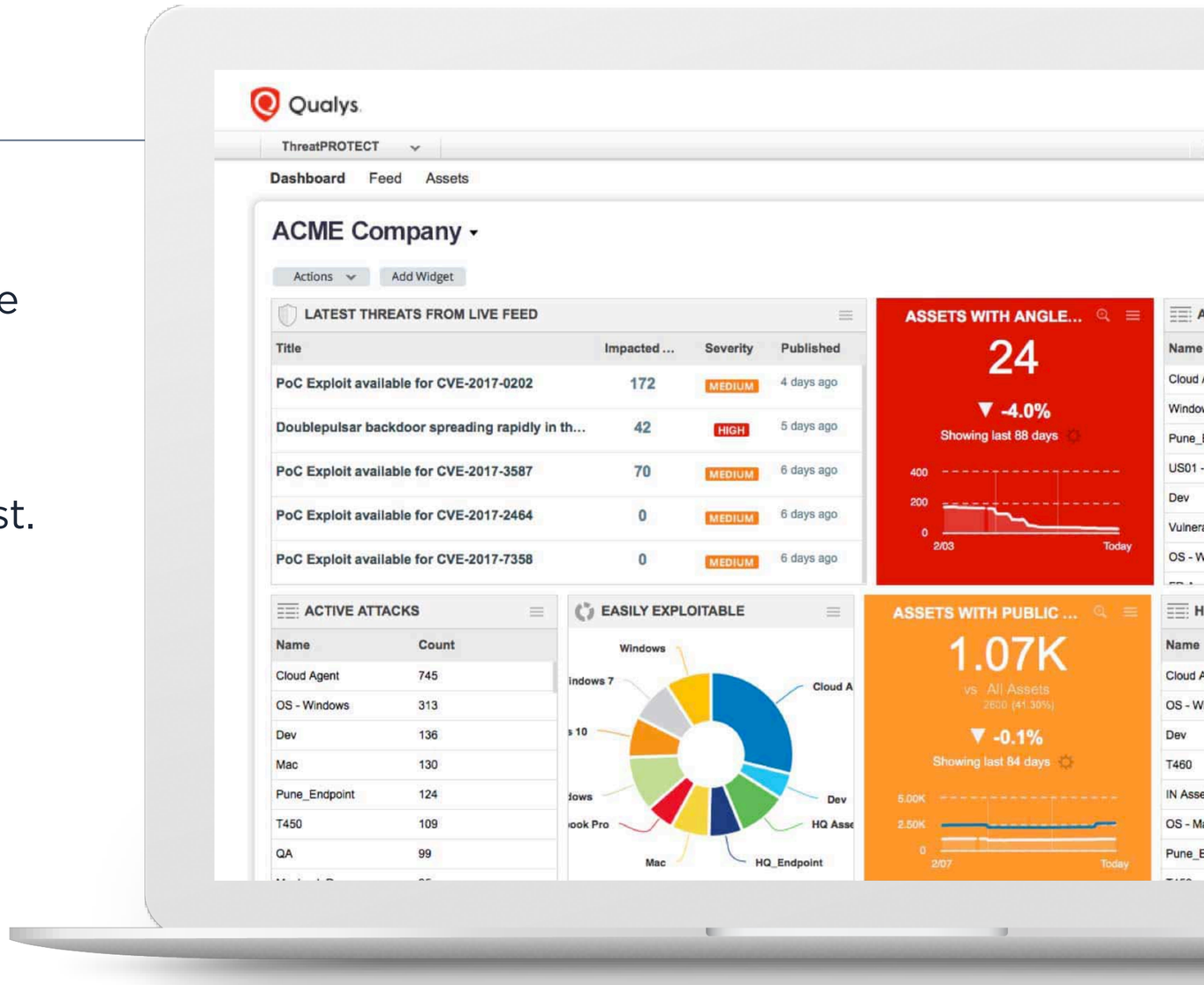
Threat Protection

Pinpoint your most critical threats and prioritize patching.



Qualys Threat Protection is a cloud service that correlates external threat indicators against your internal vulnerabilities and IT asset data — letting you control evolving threats and identify what to remediate first.

Between 30% and 40% of disclosed vulnerabilities, amounting to thousands per year, are rated “High” or “Critical.” Unable to fix them all, security teams must pinpoint which pose the highest risk to their organizations. This must be done quickly and precisely because hackers constantly try to exploit these known bugs.

That’s where Qualys TP comes in. Qualys TP layers real time threat information on top of vulnerability detections, so that organizations can prioritize remediation across all of their assets and eliminate the most serious threats in their IT environment. This automated remediation prioritization is based on real time indicators such as vulnerabilities with public exploits and with active attacks. With Qualys TP’s automated and streamlined analysis, you’ll get a clear and continuously current picture of your threat landscape for effective and precise remediation.

Features

Robust data analysis

Threat Protection continuously correlates external threat information against your vulnerabilities and IT asset inventory, leveraging Qualys Cloud Platform’s robust back-end engine to automate this large-scale and intensive data analysis process. With thousands of vulnerabilities disclosed annually, you’ll always know which ones pose the greatest risk to your organization at any given time.

The Live Feed

As Qualys engineers continuously validate and rate new threats from internal and external sources, Threat Protections’s Live Threat Intelligence Feed displays the latest vulnerability disclosures and maps them to your impacted IT assets. You can see the number of assets affected by each threat, and drill down into asset details.

Centralized control and visualization panel

A single, dynamic dashboard includes customizable views, graphs and charts giving you a clear and comprehensive view of your threat landscape at a glance in real time. You can create multiple dashboard views, and break down vulnerabilities by real-time threat indicator (RTI) types, such as zero-day exploits.

Powerful search function

Threat Protection's search engine lets you look for specific assets and vulnerabilities by crafting ad hoc queries with multiple variables and criteria. You can sort, filter, drill down and fine-tune results. Queries can be saved and turned into dashboard widgets, which can display trend graphs for up to 90 days.

Automate and streamline your remediation prioritization process, and patch your most critical bugs before hackers exploit them

Benefits

No more vulnerability data overload

Grants you control over the constant stream of vulnerability disclosures

Instant, comprehensive visibility

Provides a continuously updated view of your IT assets and vulnerabilities

Automated, precise threat risk analysis

Eliminates guesswork and arbitrary remediation schedules

Patching efficiency

Saves you time and helps you make the best use of your remediation resources

sodexo

"Qualys not only highlights and ranks the vulnerabilities, but also makes precise recommendations for how best to remediate them – a critical advantage for teams in smaller business units that may have limited IT security resources."

John Bruylant
Group CTO at Sodexo

Mesh your IT inventory data with threat information

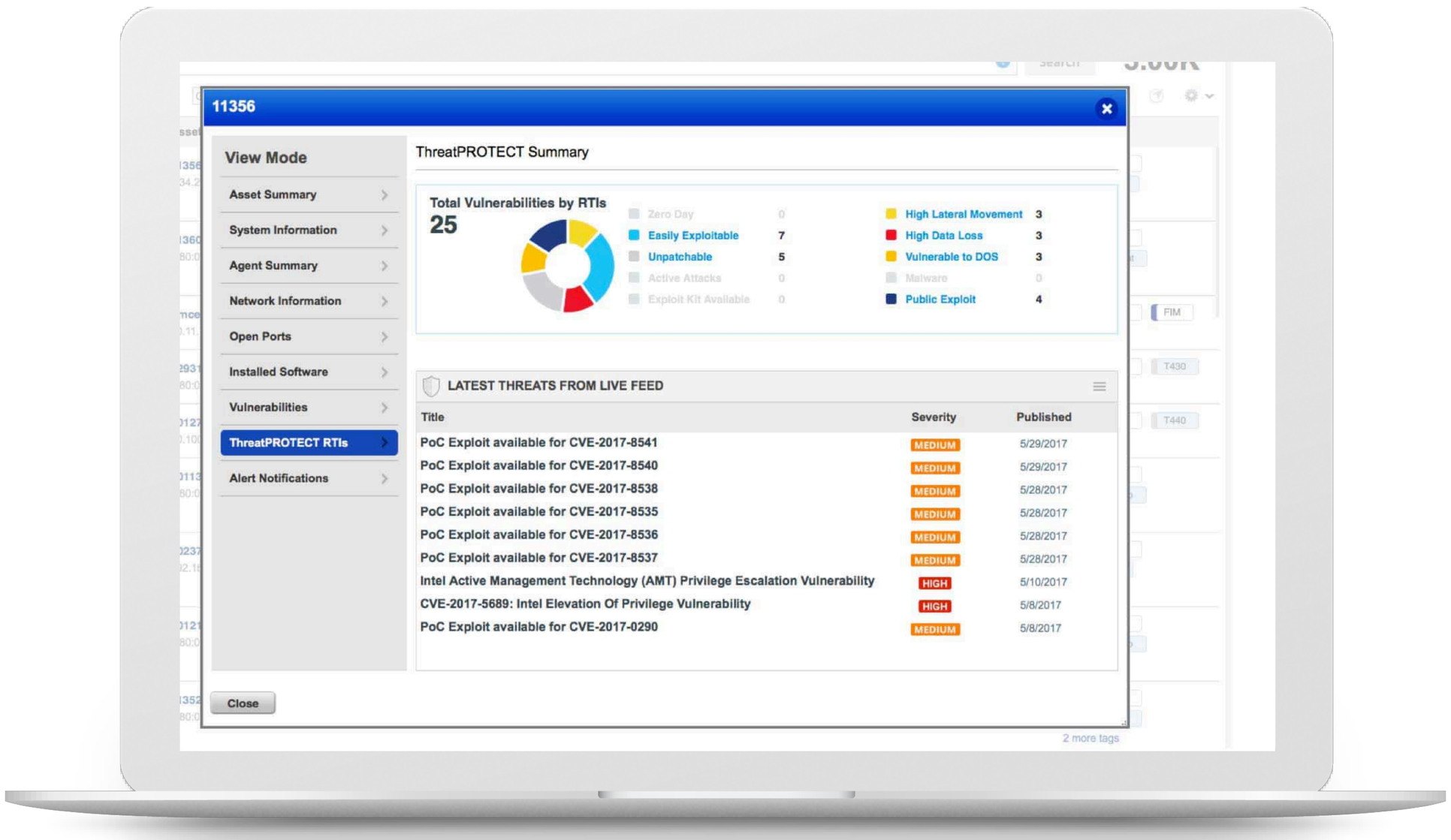
Threat Protection continuously correlates external threat data with vulnerability gaps in your IT environment, so your remediation prioritization decisions are rooted in concrete, up-to-date, applicable data, not in guesswork or arbitrary schedules. That way, you'll stay a step ahead of hackers, patching bugs before bad guys exploit them.

- Leverages the comprehensive IT asset cataloging of Qualys Asset Inventory and the Six Sigma vulnerability detection accuracy of Qualys Vulnerability Management
- Lets you prioritize remediation with precision and nimbleness in a continual, contextual and automated manner, so the constant stream of bug disclosures don't overwhelm you
- Connects the dots and flags at-risk IT assets wherever they reside – on premises, in cloud environments or at mobile endpoints
- Helps improve the efficiency of DevOps teams by bringing threat prioritization clarity into the application development and deployment lifecycle
- Gives you a dynamic snapshot of all the vulnerabilities that exist in your IT environment at any given moment
- Using actionable intelligence, allows you to assess how critical certain threat scenarios are in your organization's specific context, since every IT environment is different

Look for specific assets and vulnerabilities

Threat Protection's search engine gives you a powerful tool to look for specific assets and vulnerabilities. You can quickly and proactively identify systems across your entire environment exposed to specific threats, and take remediation steps right away. The search syntax is intuitive and the product has a query auto-complete feature. Threat Protection's search engine lets you:

- Craft ad hoc queries with multiple variables and criteria – such as asset class, vulnerability type, RTI, tag and operating system – so you can, for example, look for all vulnerabilities that have a severity rating of "5", are easy to exploit and were disclosed within the last five days
- Sort, filter and refine search results
- Save any search, download results and share them
- Turn queries you run regularly into permanent dashboard widgets whose information is dynamically updated in real time



See a live feed of vulnerability disclosures

Threat Protection's Live Threat Intelligence Feed keeps organizations up to date on the latest vulnerabilities and news, so you're informed about new disclosures and about existing bugs whose risk severity has increased.

- Plugs into the fire hose of external vulnerability disclosures, so you're aware of the latest threats out in the wild
- Displays how many of your IT assets are impacted by each disclosure, thanks to the product's powerful data correlation capabilities.
- Segments its content into different columns, including one for "high rated" items Qualys flags and another one for your handpicked "favorites" that you can pin to the feed UI
- Lets you click on feed entries and drill down into details and more granular information of a particular vulnerability and of the affected IT assets
- Allows you to fine-tune and narrow down the feed list by filtering and sorting items according to a variety of criteria, and download that set for remediation teams

Identify and weigh characteristics that intensify a vulnerability's danger

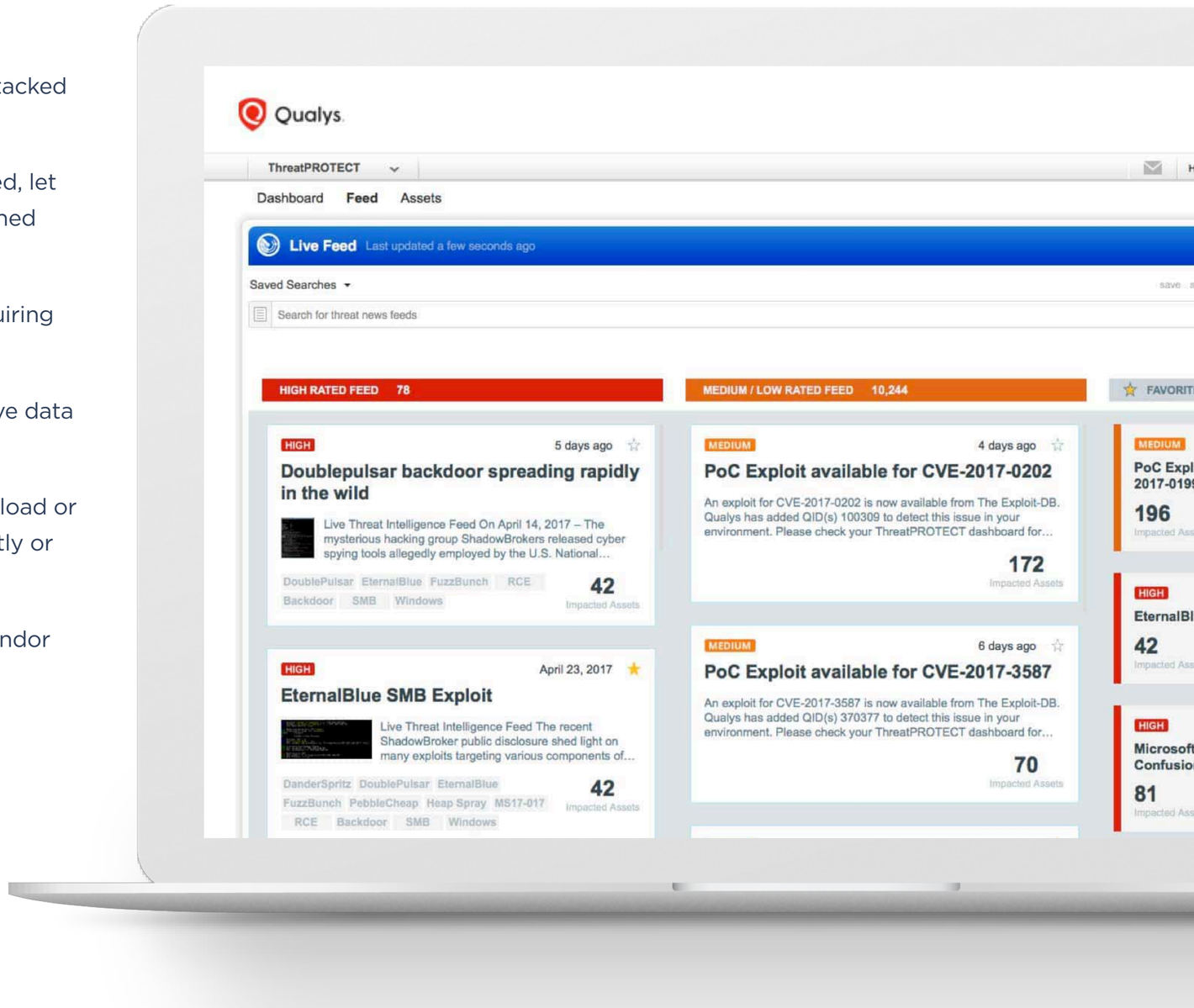
Threat Protection appends real-time threat indicators (RTIs) to vulnerabilities, tapping findings from Qualys and external sources. Combining this threat data with internal criteria, such as an asset's role, helps you prioritize remediation. For example, you can see all RTIs for vulnerabilities on a host, and drill down to specific vulnerabilities behind an RTI. Threat Protection RTIs include:

- **ZERO DAY** – Vulnerabilities for which there is no vendor patch available and for which an active attack has been observed in the wild
- **PUBLIC EXPLOIT** – Vulnerabilities whose exploit knowledge is well known and for which exploit code exists and is publicly available
- **ACTIVELY ATTACKED** – Vulnerabilities that are being actively attacked in the wild
- **HIGH LATERAL MOVEMENT** – Vulnerabilities that, if compromised, let the attacker propagate the attack broadly throughout the breached network
- **EASY EXPLOIT** – Vulnerabilities that can be exploited easily, requiring few skills and little knowledge
- **HIGH DATA LOSS** – Vulnerabilities whose exploit will yield massive data loss
- **DENIAL OF SERVICE** – Vulnerabilities whose payload could overload or crash the compromised systems so that they become permanently or temporarily unavailable
- **NO PATCH** – Vulnerabilities for which there isn't a fix from the vendor
- **MALWARE** – Vulnerabilities associated with malware infection
- **EXPLOIT KIT** – Vulnerabilities for which an exploit kit is available

Centrally control and visualize the threat prioritization process

Customizable dashboards with dynamic widgets help you see your threat landscape in a holistic, consolidated way. You can drill down on the data, mine it for patterns, slice and dice it, aggregate it in custom reports and represent it graphically. This visualization and analysis yields deep insights for patch prioritization.

- Includes a view for the live feed, as well as a variety of widgets based on RTIs, in the default dashboard setup
- Allows you to create customized dashboards tailored for different IT and business roles
- Lets you click through and access more information about the assets flagged as vulnerable
- Allows you to create dashboard widgets manually or from any search query
- Lets you set specific thresholds for widget data, and trigger certain actions in response, such as the widget's background color changing from green to red
- Sends you notifications when used in conjunction with Qualys Continuous Monitoring
- Generates reports that you can quickly and easily share across the IT department with those responsible for patching the affected systems
- Displays trend indicators in widgets, showing data fluctuations over time



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.