



ThreatPROTECT

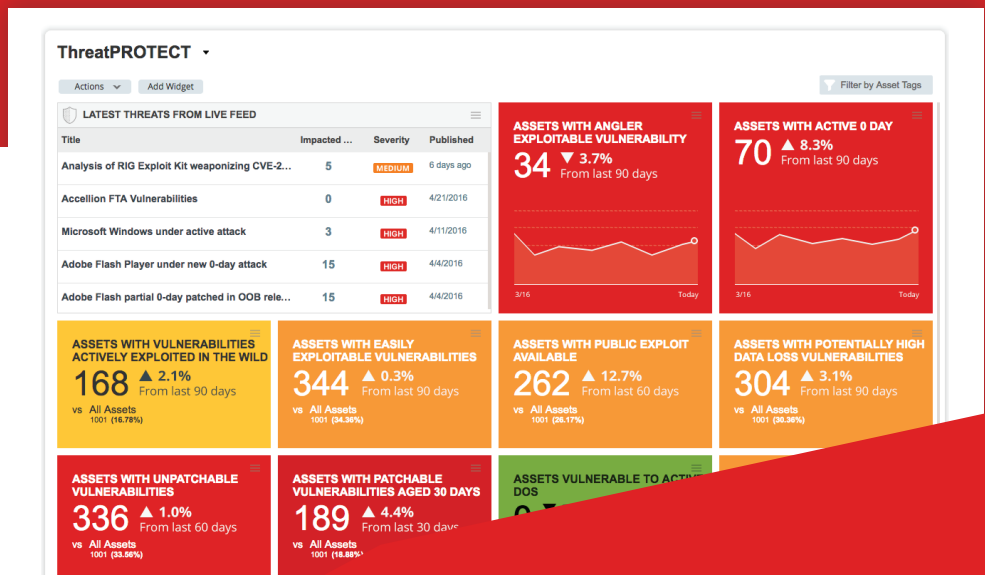
Continuously correlate external threat data against your internal vulnerabilities and flag the IT assets that require immediate remediation

Everything you need for continuous security & compliance

Buy Qualys TP as a standalone application or as part of the Qualys Cloud Platform. It is a security and compliance hub where you can discover, secure and protect all of your global IT assets wherever they reside.

The Qualys Security and Compliance Suite includes these valuable tools:

- AV** – AssetView
- VM** – Vulnerability Management
- CM** – Continuous Monitoring
- TP** – ThreatPROTECT
- PC** – Policy Compliance
- SAQ** – Security Assessment Questionnaire
- PCI** – PCI Compliance
- WAS** – Web App Scanning
- WAF** – Web App Firewall
- MD** – Malware Detection
- SEAL** – Qualys Secure Seal



Qualys ThreatPROTECT (TP) is a cloud-based service that correlates external threat data against an organization's internal vulnerabilities & lets IT pros automatically prioritize remediation work, such as patch deployment & risk mitigation.

Trying to keep up with vulnerability disclosures – to the tune of thousands per year -- is a herculean task. Even the best infosec teams can get overwhelmed attempting to figure out which among those external threats pose the greatest danger to their IT environment at any given moment.

ThreatPROTECT pinpoints the IT assets at greatest risk, taking the guesswork out of what to patch first. With its intuitive dashboard, live threat intelligence feed and powerful search engine, ThreatPROTECT gives you a holistic and contextual "at a glance" view of your constantly changing vulnerability landscape.

Never again leave dangerous gaps inadvertently open for weeks, months or even years. Prioritize vulnerability remediation in an intelligent, deliberate and tactical manner with ThreatPROTECT.

Benefits:

Tame vulnerability data overload and regain control over remediation prioritization.

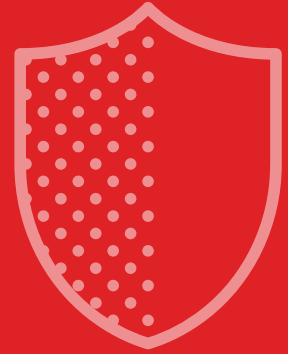
Base remediation actions on continuous and precise correlated threat analysis, not on guesswork nor arbitrary patching schedules.

Save time and make the best use of your patching resources.

Get alerted about old, low-risk vulnerabilities that suddenly become dangerous.

See your entire IT asset inventory and vulnerabilities "at a glance" and drill down into device and software details.

Leverage Qualys' cloud benefits, like not having to install nor maintain ThreatPROTECT.



Key Features:

Live Threat Intelligence Feed

Wake up every morning and see a list of vulnerabilities that pose an immediate risk to your business.

- Keeps organizations up to date on the latest vulnerability disclosures and announcements.
- With its powerful correlation capabilities, displays how many of your IT assets are impacted by each disclosure.
- Lets you drill down and get details of particular vulnerabilities and of affected IT assets.
- Allows fine-tuning of feed list by filtering and sorting items according to a variety of criteria.

Dynamic dashboard

Visualize critical threats to your environment.

- Displays entire threat posture at a glance.
- Provides dynamic, customizable views with specific stats, such as assets with active zero-day vulnerabilities.
- Lets you click through and access more information about the assets flagged as vulnerable.

Search Engine

- Gives you a powerful tool to proactively look for specific assets and vulnerabilities.
- Lets you craft ad-hoc queries with multiple variables and criteria, such as: **asset class, vulnerability type and operating system**
- Allows for search results to be further sorted, filtered and refined.
- Lets you save queries and turn them into permanent dashboard views.

Datasheet: Qualys ThreatPROTECT

The screenshot displays the 'Live Feed' interface, which is updated 5 minutes ago. It features a search bar and a 'Saved Searches' dropdown. The main content area shows a list of security alerts, each with a title, severity level, date, and number of impacted assets. The alerts include:

- Analysis of RIG Exploit Kit weaponizing CVE-2016-0034** (MEDIUM) - April 26, 5 Impacted Assets. Details: Exploit kit authors often update the capabilities of their exploit kits by adding support for new vulnerabilities so that they can compromise and install malware or ransomware on even more machines. As part of the ThreatPROTECT research team, I analyze exploit kits to keep track of the latest vulnerabilities being incorporated into them. Back in...
- Accellion FTA Vulnerabilities** (HIGH) - April 21, 0 Impacted Assets. Details: Security researcher Orange recently managed to gain access to a file transfer server at Facebook. He used a set of vulnerabilities that he found in the product that provides the service: the Accellion File Transfer Server (FTA). He notified Facebook under their bug bounty program and was awarded US\$ 10,000. Accellion addressed...
- Microsoft Windows under active attack** (HIGH) - April 11, 3 Impacted Assets. Details: Microsoft published MS16-039 for all versions of Windows on April 12, 2016. MS16-039 addresses four vulnerabilities, one rated "critical" allowing for Remote Code Execution, three rated "important" allowing for escalation of privilege. Two of the "important" vulnerabilities (CVE-2016-0165 and CVE-2016-0167) are under activ...
- Adobe Flash Player under new 0-day attack** (HIGH) - April 04, 15 Impacted Assets. Details: Adobe announced that a new version of their Flash Player product is expected to be released this week. The new version will address CVE-2016-1019, a critical vulnerability that is currently being exploited in the wild. However, if you are current with your Flash player patches you are protected. If you have the newest Flash player installed...
- Adobe Flash partial 0-day patched in OOB release** (HIGH) - April 04, 15 Impacted Assets. Details: Adobe addressed a partial 0-day vulnerability in its Flash player with a software release on April 7, 2016. The new version of Flash fixes 24 vulnerabilities, with CVE-2016-1019 under active attack through the Magnitude Exploit Kit. The vulnerability is a partial 0-day because in the newest version of Flash a mitigation strategy introduced by Adob...

Key Features continued:

Visualization and alert capabilities

Measure your progress and remediation efforts with real-time trend analysis, and get alerted when new active threats surface in your environment.

- Generates reports, graphs and charts.
- Lets you display them on dashboard and share them with colleagues.
- Sends notifications alerting when pre-set parameters and thresholds are reached and when pre-determined events occur.

The screenshot shows a Qualys alert interface. At the top left is the Qualys logo and a 'Sign on' link. The main alert banner is blue and contains the text: 'NEW ACTIVE THREAT ALERT', '04:21 PST | April 11, 2016', 'Microsoft Word Under Active Attack' with a 'HIGH' severity indicator, and a red box stating '3 impacted assets'. Below the banner, there is a link to view details within ThreatPROTECT. The main body of the alert contains text about Microsoft's MS16-039 patch for Windows, detailing four vulnerabilities (one critical, three important) and two under active attack. It describes a typical attack scenario involving Adobe Flash, CVE-2016-0165/7, and Remote Access Tools (RATs). At the bottom, it states 'Our Real-time Threat Indicator (RTI) for QID: 91204 is set to: **ActivelyAttacked**' and shows a video player with a thumbnail of a man speaking, titled 'Microsoft Word under active Attack'.

About Qualys

Qualys, Inc. is a pioneer and leading provider of cloud-based security and compliance solutions with over 8,800 customers in more than 100 countries. Qualys solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.



Comprehensive vulnerability information from internal and external sources

Qualys security engineers continuously validate and rate new threats.

- Leverages threat data from Qualys research labs and external partners and sources, including Core Security, Exploit Database, Immunity, TrendMicro, VeriSign iDefense.
- Classifies these RTI (real-time threat indicator) data points, such as attacks and exploits, into these more precise categories, helping you prioritize remediation more precisely:

- Zero Day
- Public Exploit
- Actively Attacked
- High Lateral Movement
- Easy Exploit
- High Data Loss
- Denial of Service
- No Patch
- Malware
- Exploit Pack

Order
ThreatPROTECTION
now, visit
networking4all.com

*There's nothing to install
or maintain*

About Networking4all

Networking4all is a professional and service-oriented supplier of online security products for websites, servers and applications since the foundation in 2000. Networking4all is greatly appreciated by their clients for our personal service, expertise and fast issuance, and they strive to find the best solution for every client's particular online security needs. That's why their motto is 'together, we make the internet safe'.

