

Qualys Cloud Platform

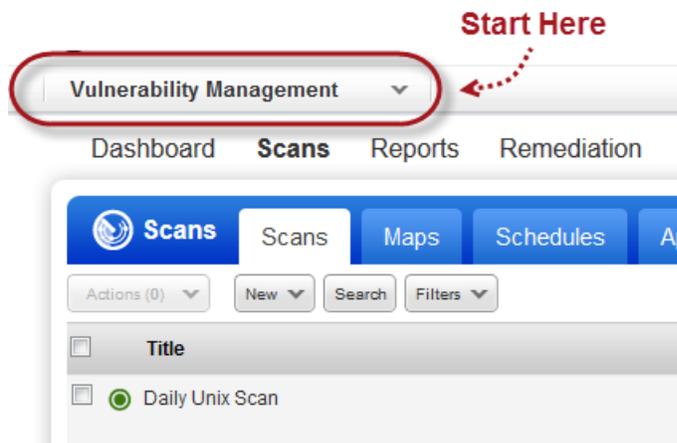
Quick Tour

The Qualys Cloud Platform is a platform of integrated solutions that provides businesses with asset discovery, network security, web application security, threat protection and compliance monitoring. It's all in the cloud - simply log into your account from any web browser to get everything you need to secure all of your IT assets.

Let's take a look at the Qualys user interface and how to get around.

Choose One of our Solutions

Our integrated suite of solutions is presented to you in a single view. Simply choose the solution you're interested in from the module picker and get started right away!



Vulnerability Management ▾

Active Modules (12)

- AV**

AssetView

Discover assets and use dynamic tags to keep your assets automatically organized.
- CA**

Cloud Agent

Stay updated with network security by deploying agents on your hosts.
- VM**

Vulnerability Management

Map and scan your network, prioritize your critical vulnerabilities and fix them.
- CM**

Continuous Monitoring

Set up monitoring and alerting of new security risks
- TP**

ThreatPROTECT TRIAL

Correlate live threat intelligence with your assets
- PC**

Policy Compliance

Define and monitor IT security standards aligned with regulations.
- SAQ**

Security Assessment Questionnaire TRIAL

Automate risk and compliance through questionnaire campaigns.
- PCI**

PCI Compliance

Achieve compliance with the PCI Data Security Standard (DSS).
- WAS**

Web Application Scanning

Identify and manage web application security risks.
- WAF**

Web Application Firewall

Detect attacks and protect your web applications.
- MD**

Malware Detection

Identify and manage web site malware risks.
- Q**

SECURE Seal

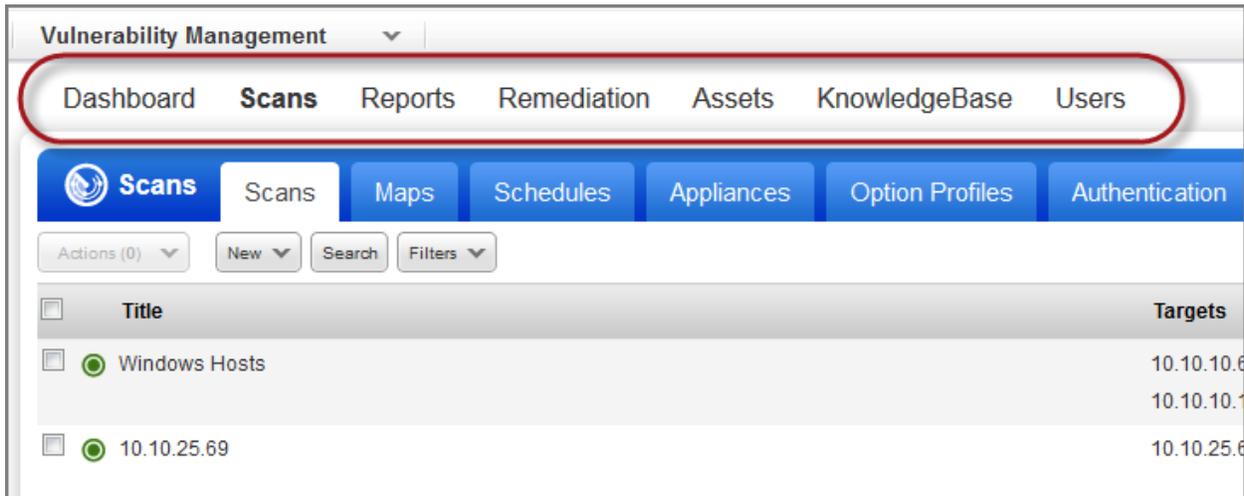
Identify and manage web site malware risks.

Utilities:

- Administration

Go to a Section

You'll see a set of menu options across the top of the screen representing the main areas of functionality. Each section provides workflows specific to the module you're in. For example, go to the Scans section to launch and manage scans; go to the Reports section to run and manage reports.

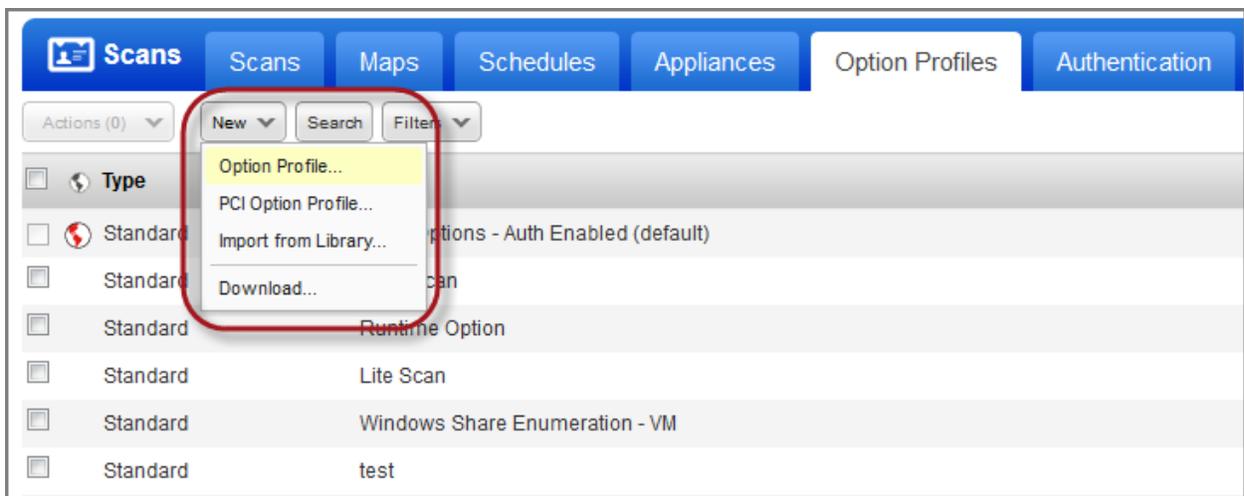


Each section includes at-a-glance all of the tools and setup options you need for success. In the Scans section you have access to your scan schedules, scanner appliances, option profiles, authentication records and scan setup options. This means you don't have to leave the Scans section to set up your scan configurations or set global options related to scans.

Take Action

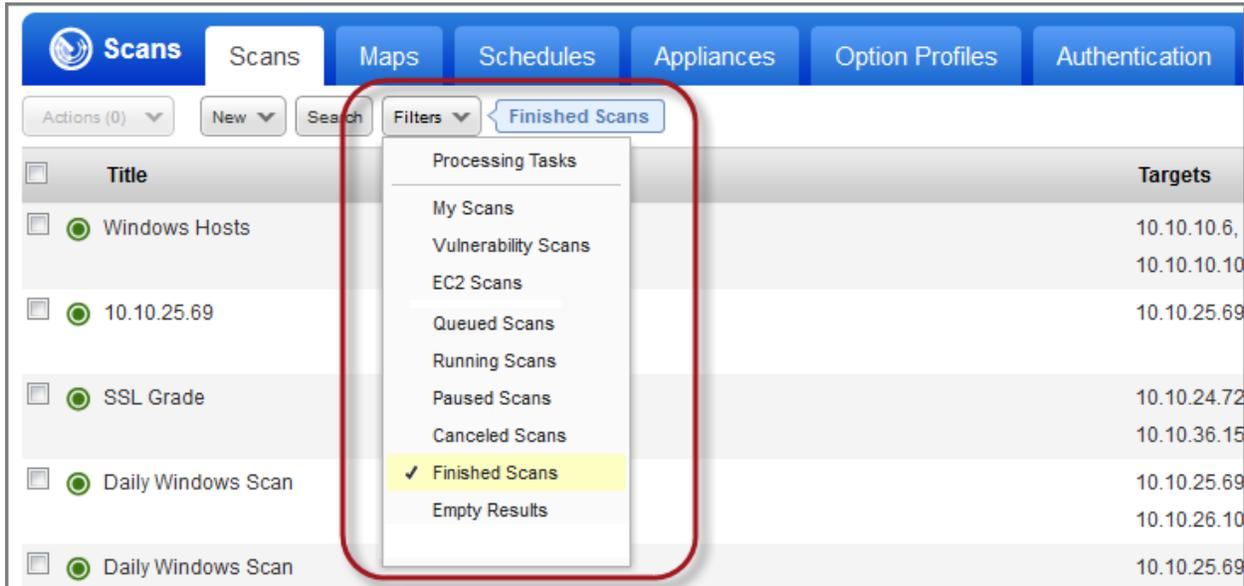
Start New Workflows

The New menu above each list is your starting point for new workflows and configurations. Use the New menu to start scans, run reports, create new option profiles, and so on.



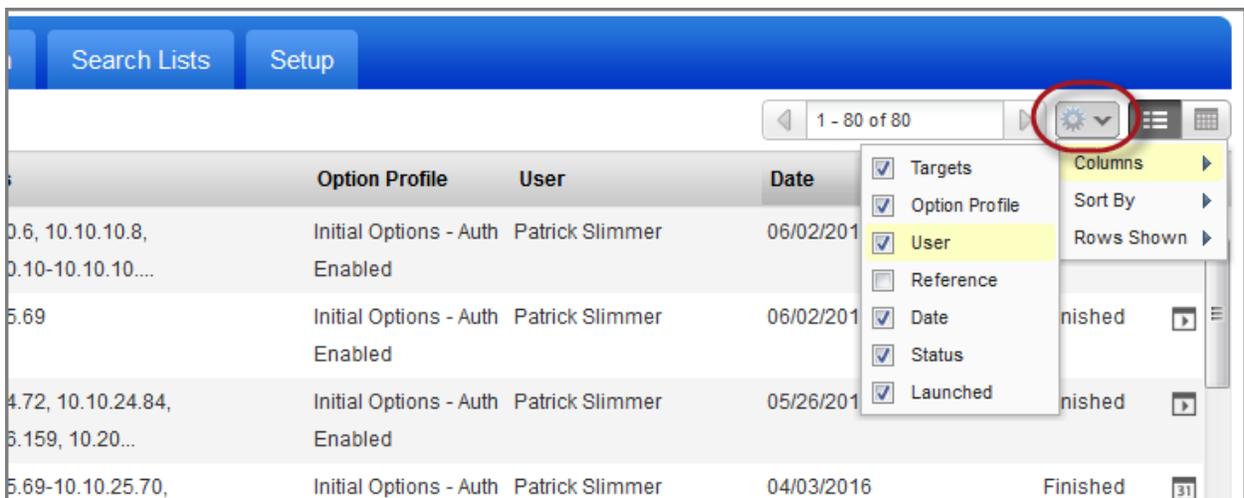
Use Filters

Use filters to change your list view. For example, if you're on the scans list and you're only interested in finished scans, then you would select Finished Scans from the Filters menu. The list is instantly updated and a message appears next to the Filters menu as a visual reminder that filters are turned on. Clear the filter to return to the full list.



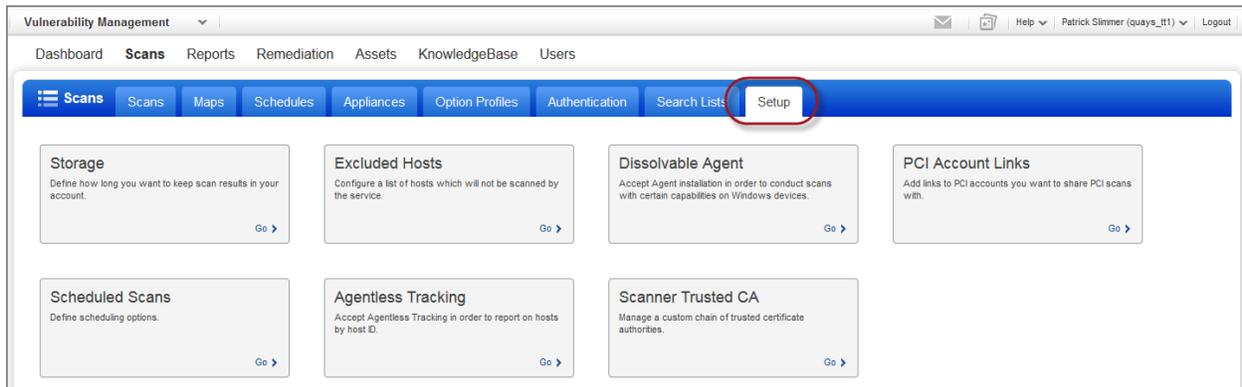
Customize Your View

You can hide columns, change the sorting criteria and specify the number of rows to appear in each list. To do so, use the Tools menu above the list, on the right side.



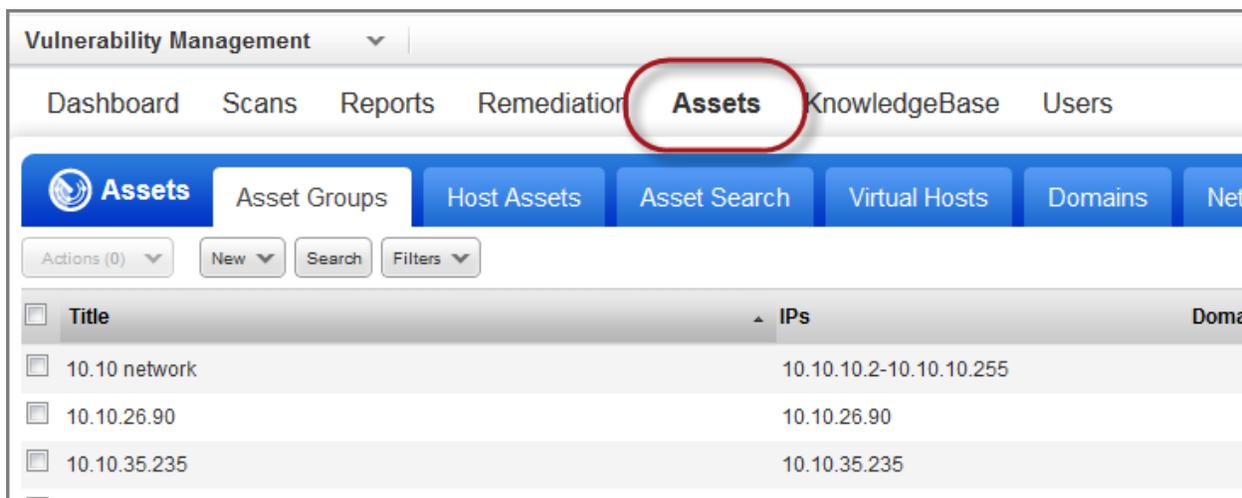
Review Setup Options

Review setup options in the context of your current view. When you're in the Scans section go to the Setup tab to see global options related to scans and scan results. When you're in the Users section go to the Setup tab to see options related to users, and so on. The setup options available to you depend on your service level and subscription settings. The ability to edit setup options is determined by your role and permissions.



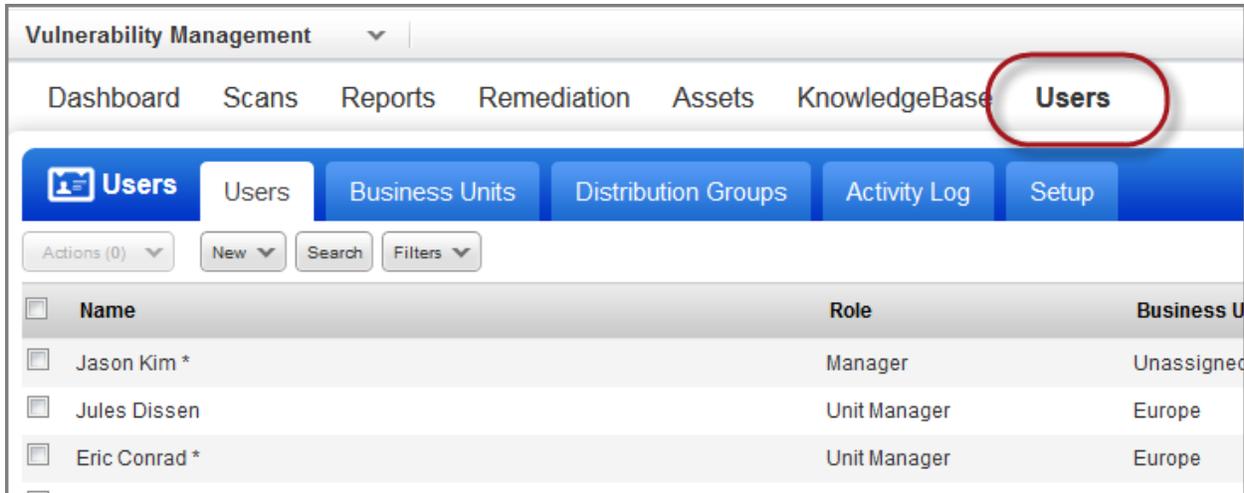
Manage Assets

Your account will include all of the assets that you're scanning or monitoring for security. For example, in Vulnerability Management (VM), go to the Assets section (shown below) to see host assets (IP addresses), domains and virtual hosts in your account. In Web Application Scanning (WAS), you go to the Web Applications section to see the web applications you can scan for vulnerabilities and malware.



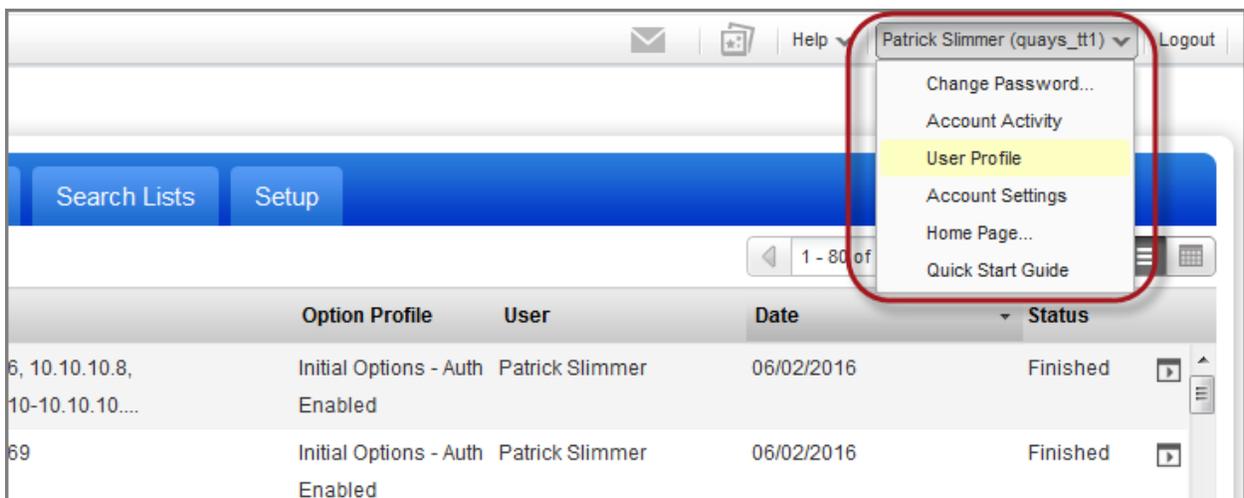
Manage Users

The Users section is where you manage users, business units and distribution groups. Any user with management authority can add users with unique roles and privileges.



Make Changes to Your Account

To change your password, home page, contact information, or email notifications, select from the options that appear below your user name in the top, right corner.

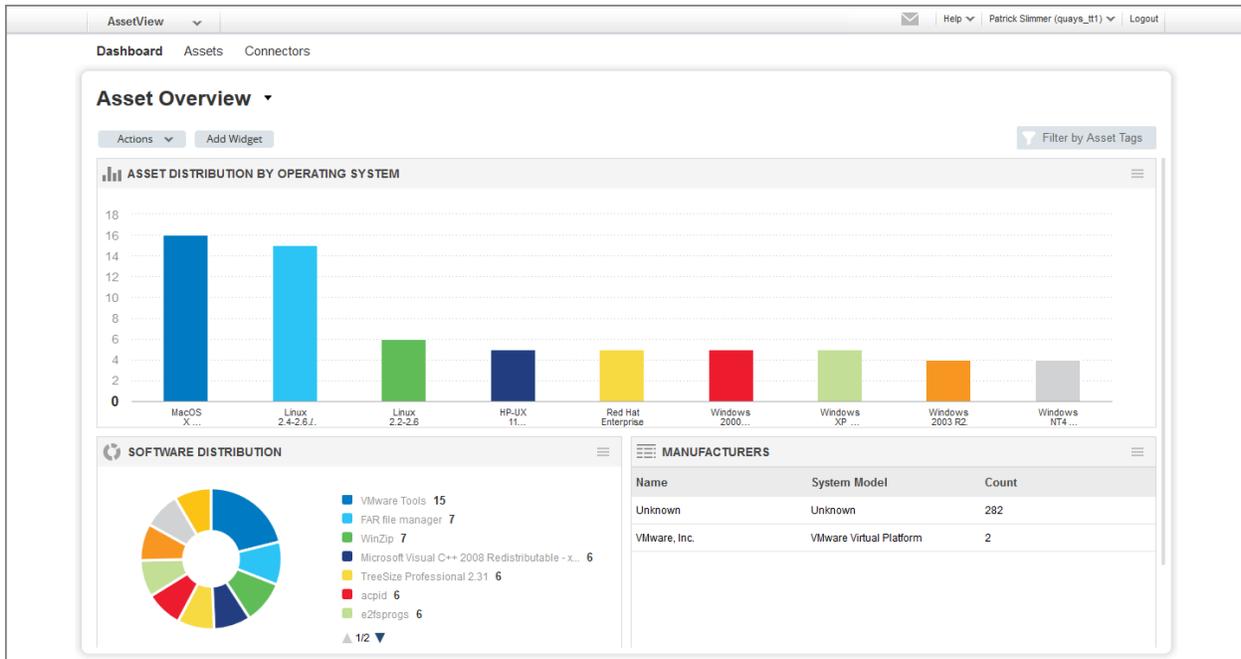


Get Up to Date Views on your IT Assets

Each solution includes an interactive dashboard with a high-level summary of your security and compliance posture based on the latest data available in your account.

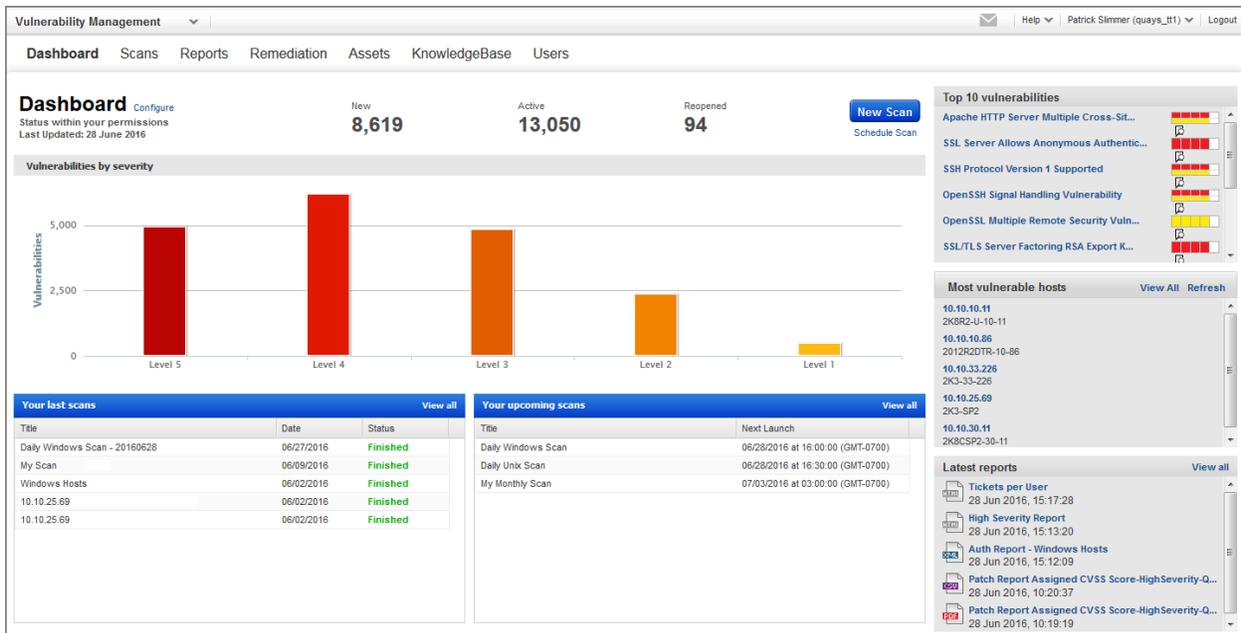
AssetView (AV)

AV gives you a centralized location where you can view and query all of your asset data instantly. It brings security and compliance information together in one place, and lets you visualize your asset data in many ways.



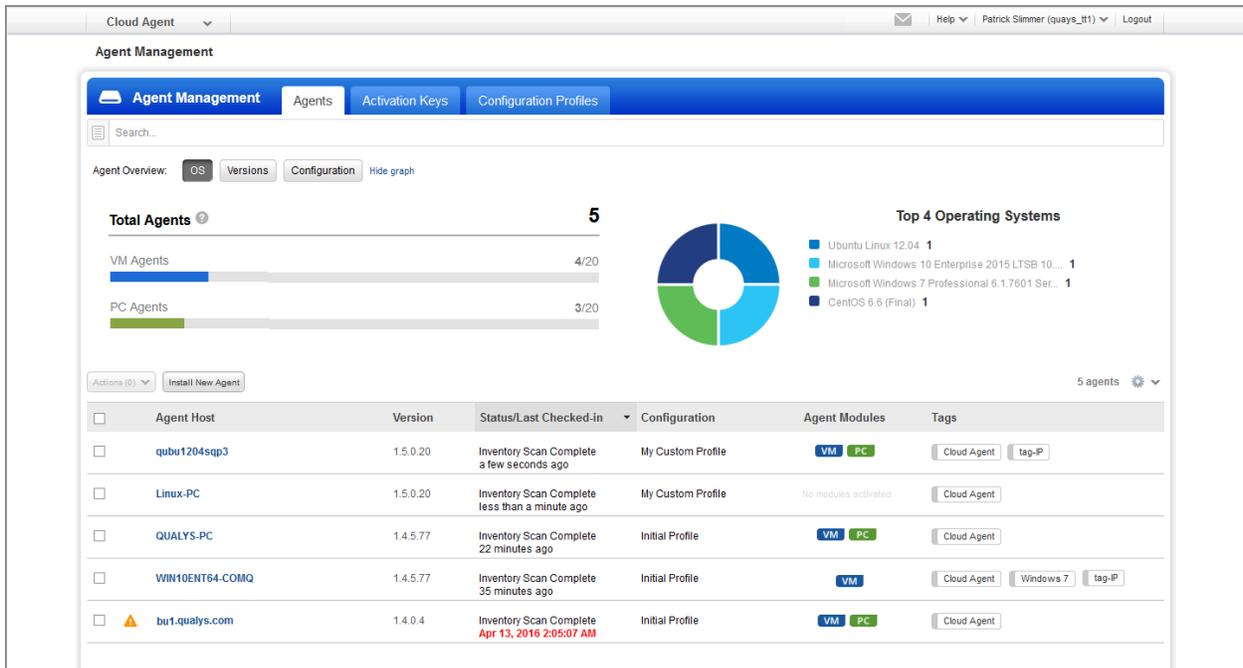
Vulnerability Management (VM)

Find out where your IT systems are vulnerable to the latest threats & how to protect them.



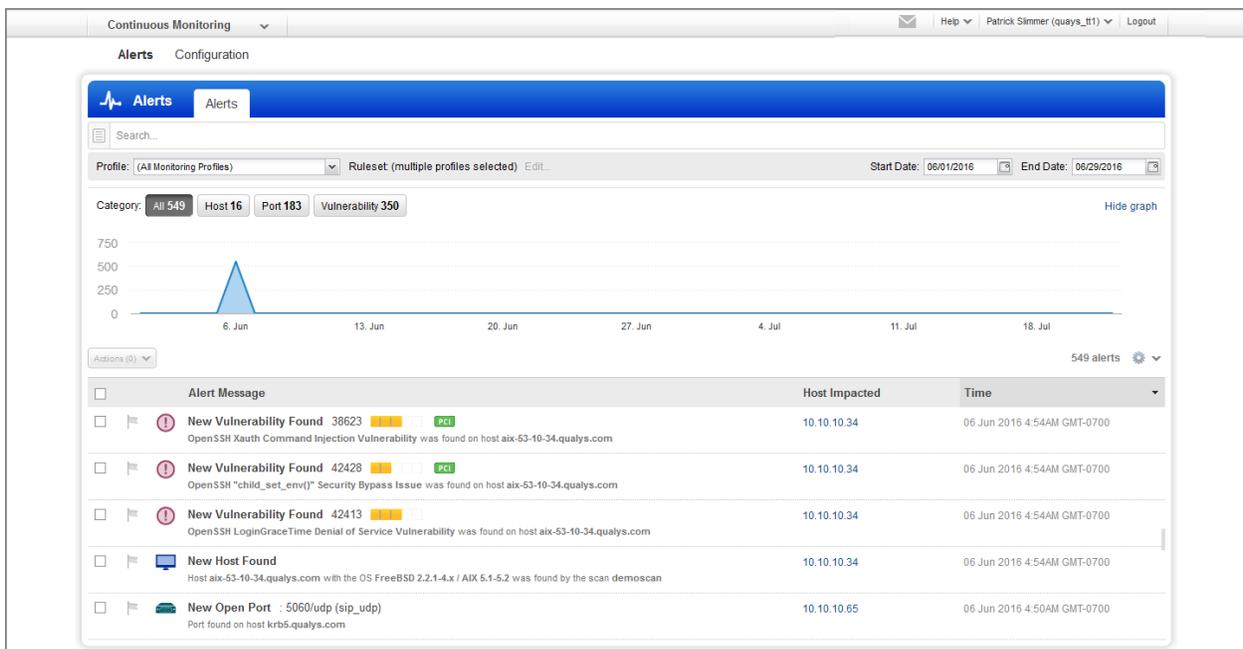
Cloud Agent (CA)

Get continuous security updates through the cloud by installing agents on your hosts.



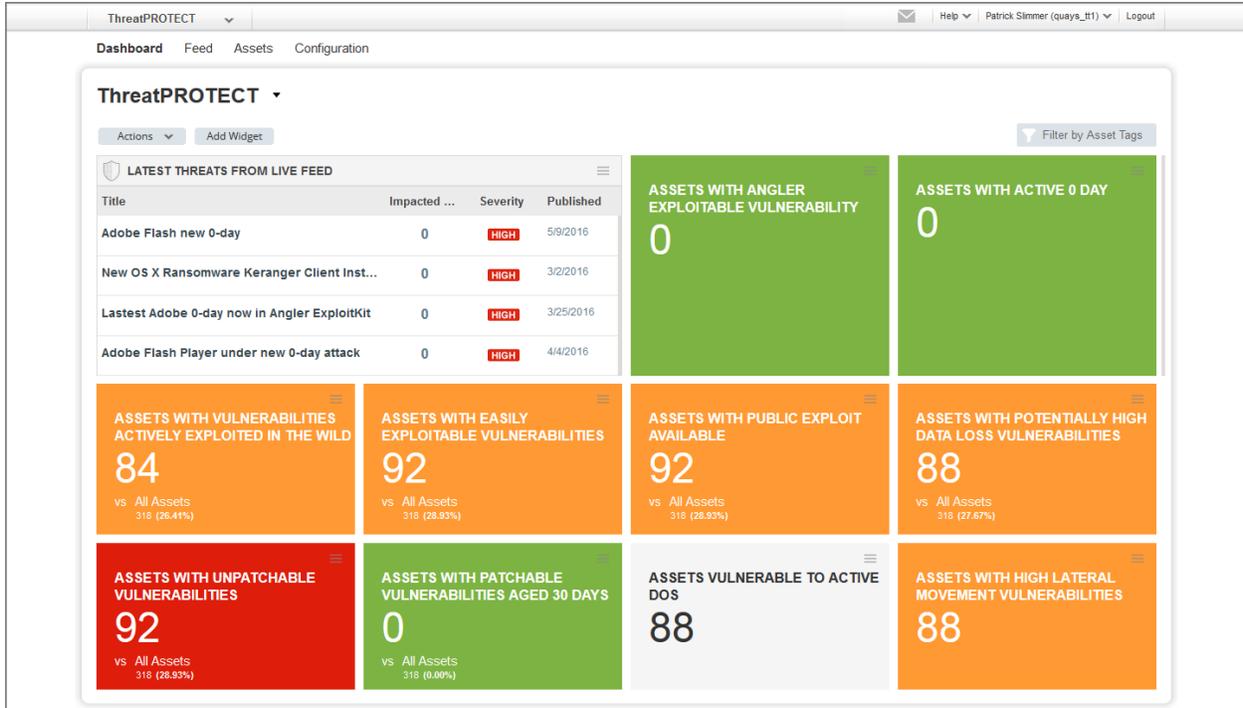
Continuous Monitoring (CM)

Immediately receive alerts when new security risks are detected by your vulnerability scans. Changes to hosts will be monitored and alerts will be generated every time a change occurs.



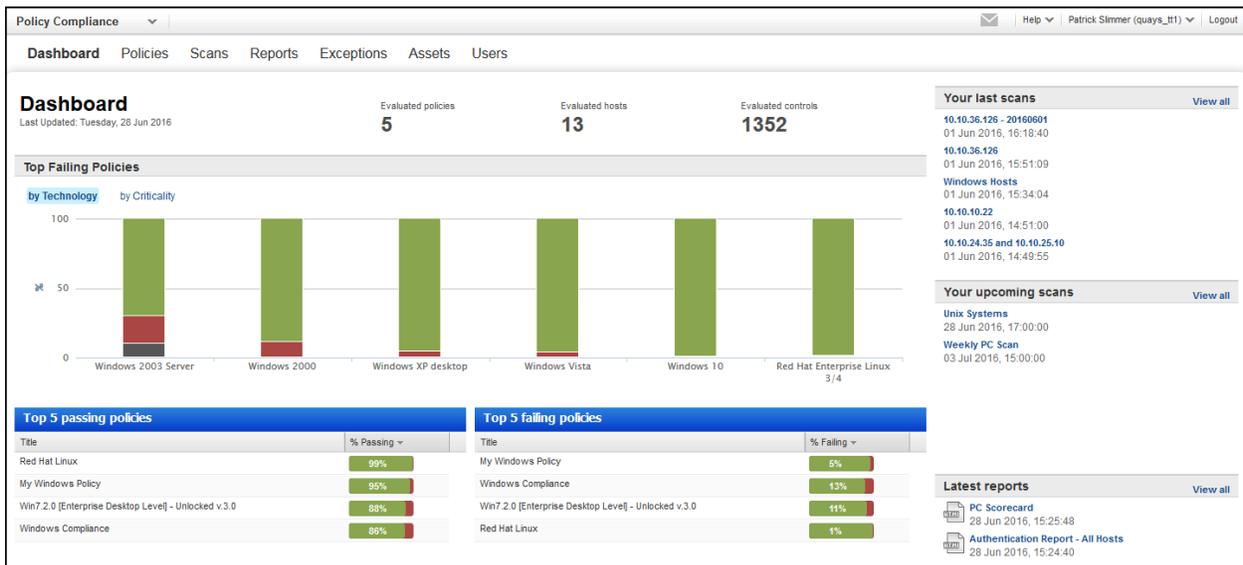
ThreatPROTECT (TP)

Automatically prioritize the vulnerabilities that post the greatest risk to your organization. ThreatPROTECT correlates active threats against your vulnerabilities.



Policy Compliance (PC)

Get automated security configuration assessments on IT systems throughout your network. Reduce risk & continuously comply with internal policies and external regulations.



Security Assessment Questionnaire (SAQ)

Collect and analyze the risk and compliance data you need, from your employees and third party vendors, through automated campaigns.

Security Assessment Questionnaire

Help | Patrick Slimmer (quays_it1) | Logout

Dashboard Campaigns Reports Templates Users

Dashboard
Last login: Tue 28 Jun 2016

Active Campaigns: 9 | Active Questionnaires: 29 | Idle Questionnaires: 29 | Completed Questionnaires: 2

[Create New Campaign](#)

MY ACTIVE CAMPAIGNS

Title	Progress	Due Date	Last Update
Promnetwork campaign Due Date: Jun 28, 2016	3 questionnaires 0%	28 Jun 2016 16 hours ago	20 Jun 2016 June 20, 2016
My Gartner campaign Due Date: Jul 12, 2016	3 questionnaires 0%	12 Jul 2016 a few seconds ago	15 Jun 2016 June 15, 2016
my camp Due Date: Jun 21, 2016	2 questionnaires 0%	21 Jun 2016 June 21, 2016	14 Jun 2016 June 14, 2016
Prev_demo Due Date: Jun 22, 2016	3 questionnaires 0%	22 Jun 2016 6 days ago	13 Jun 2016 June 13, 2016

CAMPAIGNS STATUS

Active: 9 | Complete: 2 | Inactive: 1

LATEST USER ACTIVITY

User	Questionnaire Title	Progress
Harim singh quays_xc15	Promnetwork campaign - tim... Due Date: 28 Jun 2016	0 / 132 answered 0%
Harim singh quays_xc15	Promnetwork campaign - jenn... Due Date: 28 Jun 2016	0 / 132 answered 0%
Harim singh quays_xc15	Promnetwork campaign - davi... Due Date: 28 Jun 2016	0 / 132 answered 0%
Jenny Mann jenny.mann@a...	My Gartner campaign - jenny... Due Date: 12 Jul 2016	4 / 17 answered 23%

CAMPAIGN DISTRIBUTION

Bar chart showing distribution of campaigns by duration: Overdue (6), 0-7 days (2), 7-14 days (0), 14-30 days (2), 1-2 months (0), 2-6 months (0), monthly or plus (0).

TEMPLATES IN DRAFT (ACTIVITY)

Title	Last Update
Promnetwork demo Author: Harim singh	20 Jun 2016 June 20, 2016
My template Author: Harim singh	15 Jun 2016 June 15, 2016
my temp Author: Harim singh	14 Jun 2016 June 14, 2016
demo Author: Harim singh	13 Jun 2016 June 13, 2016

Web Application Scanning (WAS)

Identify vulnerabilities and security risks on your web applications, including cross-site scripting (XSS) and SQL injection.

Web Application Scanning

Help | Patrick Slimmer (quays_it1) | Logout

Dashboard Web Applications Scans Burp Reports Configuration KnowledgeBase

Dashboard
Tue 28 Jun 2016
313 total scanned web apps
94 with Malware Monitoring

All Vulnerabilities: 20.0K | HIGH Severity: 2.60K | MED Severity: 2.23K | LOW Severity: 15.2K | Malware: 88 detections

[New Scan](#) | [Add Web Application](#)

MOST VULNERABLE WEB APPLICATIONS

Web Application Name	Last Scan Date	Total Vulnerabilities	High	Med	Low	Severity
Demo Web Application http://testurl.com:8080/secure/management/secure/login.php	20 Apr 2016	107	35	2	70	HIGH
My Web Application http://testurl.com:8080/secure/management/secure/Andex.php	29 Mar 2016	108	31	1	76	HIGH
site10 http://10.20.20.20	29 Mar 2016	166	29	23	114	HIGH
Catalog Web Application http://10.20.20.20	29 Mar 2016	200	27	22	151	HIGH
Carla Web Application	29 Mar 2016	156	26	13	117	HIGH

CATALOG

Total: 189
155 New, 27 Rogue, 1 Approved, 0 Ignored, 6 In Subscription

YOUR LAST SCANS

Scan Name	Scan Date	Status	Severity
Demo Web App - VM Demo Web Application	29 Jun 2016	Running	-
Web Application Vulnerability Scan - ... waf-site4	06 May 2016	Finished	LOW
Web Application Vulnerability Scan - ... waf-site4	06 May 2016	Finished	MED
Sched - DNS	06 May 2016	Finished	LOW

YOUR UPCOMING SCANS

Task Name	Occurs	Next Date
Demo Web App - VM Demo Web Application	Daily	30 Jun 2016
Monthly Discovery Scan phpBB HTTP Basic	Monthly	01 Jul 2016
Weekly WAS Vulnerability Scan Demo Web Application	Weekly	04 Jul 2016

LATEST REPORTS

- WebApp - Custom template with tags (html) 28 Jun 2016
- Catalog - Custom template with tags (html) 28 Jun 2016
- Scorecard - Custom template with tags (html) 28 Jun 2016
- May 20 (Email - HTML ZIP) 28 Jun 2016
- Test Schedule by Tag 28 Jun 2016
- Scorecard XML Error 28 Jun 2016

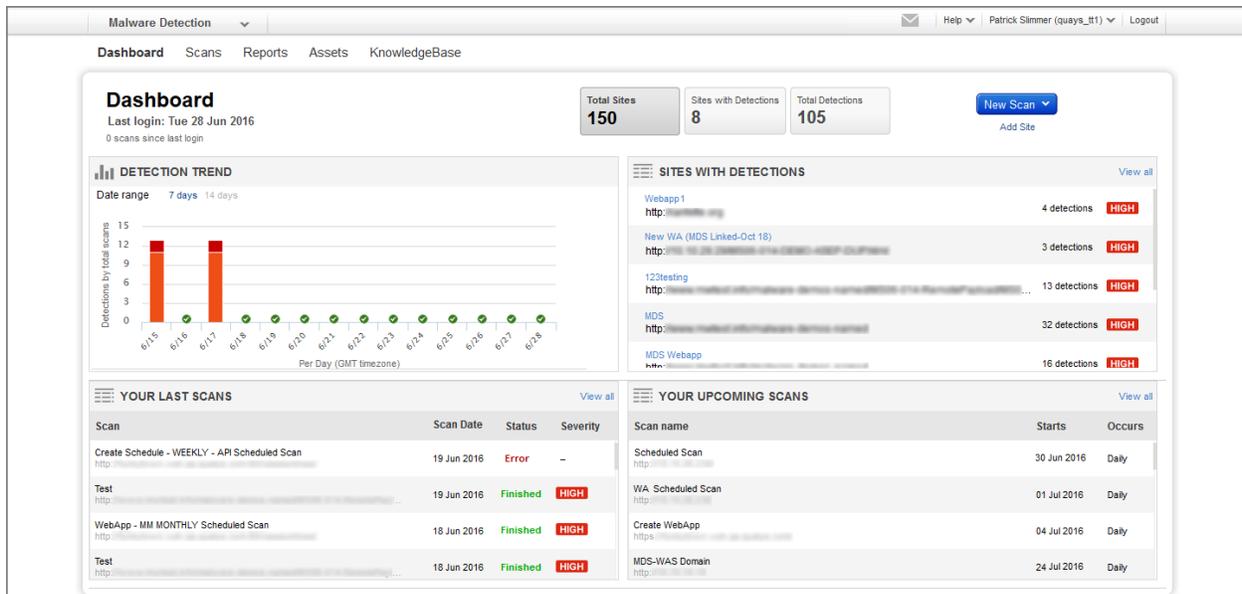
Web Application Firewall (WAF)

WAF is our next-generation cloud service that brings an unparalleled combination of scalability and simplicity to web app security.



Malware Detection (MD)

MD lets you quickly identify and eradicate malware that could infect your website visitors and lead to loss of data and revenue.



PCI Compliance (PCI)

Achieve and validate compliance with the PCI Data Security Standard (PCI DSS). Use our solution for PCI compliance testing, reporting and submission. Qualys is an Approved Scanning Vendor (ASV).



The screenshot shows the Qualys PCI Compliance dashboard. At the top, it says 'Payment Card Industry Compliance' and 'Jason Kim [Sports Shop, Inc.] | Help | Log Out'. On the left is a navigation menu with 'Home', 'Network', 'Compliance', 'Submitted Reports', 'Web Applications', 'Questionnaires', 'Account', and 'Contact Support'. The main area is titled 'Compliance Status' and contains a table with the following data:

Overall Status	Hosts	Vulnerabilities	Potential Vulnerabilities	Actions
	In Account: 2 Not Live: 0 Compliant: 2 Not Compliant: 0 Not Current: [N/A] 0	 HIGH 0  MED 0  LOW 0	 HIGH 0  MED 0  LOW 0	 Generate

SECURE Seal (Seal)



The image shows the Qualys SECURE Seal banner and the Malware Detection section. The banner is blue and contains the Qualys SECURE logo and the text: 'This site has been scanned for Network, Web Application Vulnerabilities and Malware.' Below the banner is the URL <http://www.qualys.com>. The Malware Detection section features a red biohazard icon with a green checkmark and the text: 'Malware Detection Scanned Thu, Feb 16, 2012 at 3:27 AM, Coordinated Universal Time The Qualys Malware Detection service evaluates the site for the presence of malicious software the web site could unintentionally be infecting visitors with.'

Demonstrate to your customers that you maintain a rigorous and proactive security program by displaying the Qualys SECURE seal on your website.