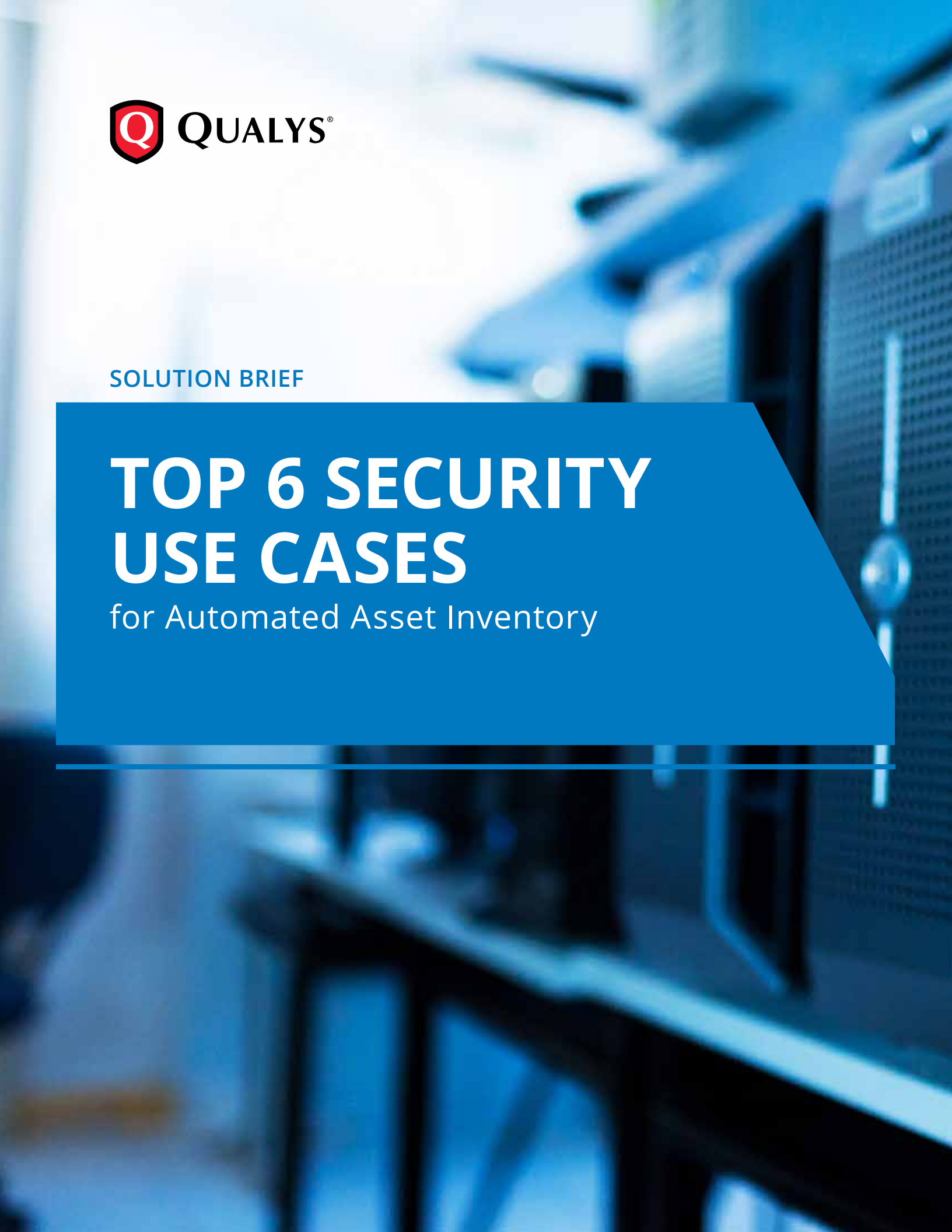


QUALYS®

SOLUTION BRIEF

TOP 6 SECURITY USE CASES

for Automated Asset Inventory

Overview

Automated asset inventory might not be the first thing that comes to mind when considering cutting-edge security technologies. In the context of today's distributed enterprise, however, it's essential. Since the apps, systems, and services your users access to conduct business are already in the cloud, it makes sense to consider looking to cloud-based technologies to keep track of them all.

For the security and compliance professional, it's critical to have access to a reliable and accurate asset inventory, especially when investigating security incidents and verifying and demonstrating compliance.

TOP 6 SECURITY USE CASES FOR CLOUD BASED AUTOMATED ASSET INVENTORY:

1 Pinpoint & prioritize vulnerabilities

2 Find unauthorized software

3 Discover and alert on policy violations

4 Support forensic investigations

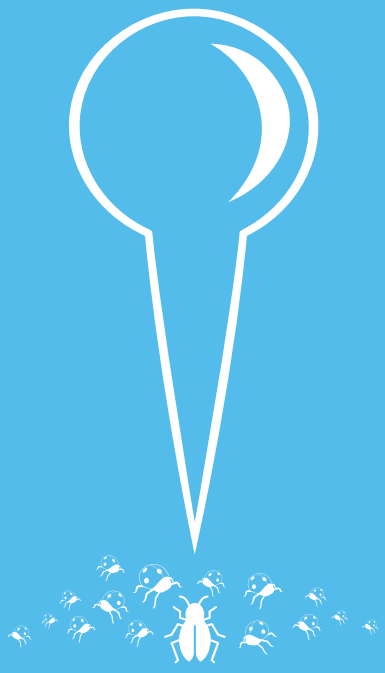
5 Reconcile software asset licensing costs

6 Support M&A integrations

#1 Use Case

Pinpoint and prioritize vulnerabilities that are actively being exploited

Most global organizations are dealing with thousands of vulnerabilities across thousands of systems and applications. Trying to mitigate them all at once is a lost cause. With an automated asset inventory that's correlated to vulnerability information, it's easy to run a query that finds assets that have specific vulnerabilities that are being actively exploited in the wild. After all, these are the most critical exposures to fix first.



Time is of the essence. In a recent study of data breaches, 99.9% of exploited vulnerabilities were compromised more than a year after the CVE was published.

– Verizon Data Breach Investigations Report 2015[1]

1 http://www.verizonenterprise.com/DBIR/2015/

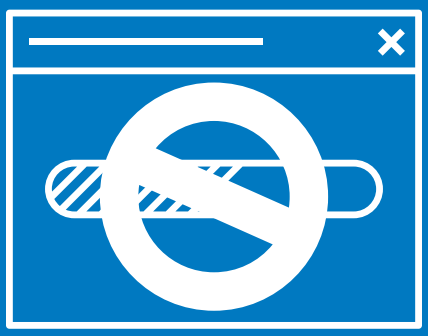
#2 Use Case
Find unauthorized software

As the corporate user has gained more control over the computers they use to do work, IT security teams have had to tolerate the risks associated with having less control over these endpoints. These risks include malware infection, system compromise, data leakage, and more – all easily exploited via a simple download of unauthorized software to a user's laptop.

Based on these risks, it's essential for IT security teams to have the ability to query their assets to discover unauthorized software that is installed and is actively running. In addition, by setting up alerts to be triggered when unauthorized software is installed IT gains granular control over policy enforcement and response – across remote, roaming and distributed endpoints.

Unauthorized software poses risks that can extend beyond cybersecurity vulnerabilities, threats and exploits. It could also pose legal and financial risks to your organization if the installed software isn't authorized or licensed for use.

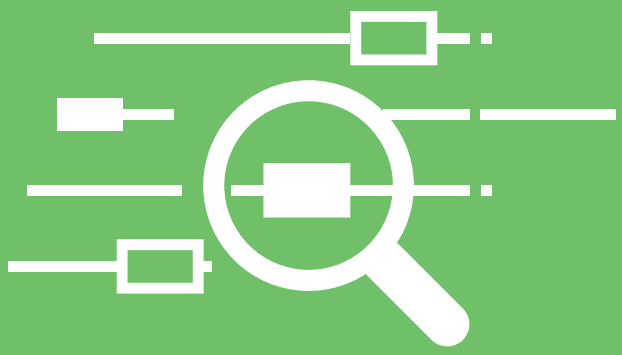
This enables a new level of real-time risk reporting for your executive stakeholders, and positions IT security teams as the leaders in transformational risk management.



#3 Use Case
Discover and alert on policy violations

In addition to installing unauthorized software, there are a number of user behaviors that can increase risk as well as undermine a company's security and compliance posture. Here are a few sample policy violations that you could discover by querying an automated asset inventory:

- **Modified configurations** – Disabling a personal firewall or adjusting the browser's security settings on one system could potentially expose entire organizations to malware infection risks, so it's essential to have the ability to identify this behavior and respond.
- **Privilege escalation** – A user attempting to access a privileged account, or add privileges to an existing account could be a signal of an active attack at worst, and at a best, an error in judgment and a policy violation. In either case, the best practice is to set up automated queries and reports, for further investigation and response.



#4 Use Case
Support forensic investigations

As soon as a system compromise is suspected, it's essential to collect, correlate and search across as much information about that asset as possible: installed software, software vulnerabilities, hardware configuration, running processes, logged in users, and a number of other attributes. In addition to a rich asset inventory, it's particularly important to have a history of all changes on the system to support an incident response workflow, build timelines, and capture forensic evidence.

During the process of investigating an incident, you'll have more questions than answers, especially at the start, and you'll need to pivot from one set of assets and attributes to other sets. Since you don't have the time to structure complicated SQL queries and wait for the results to finish, simple and flexible query capabilities that return answers instantly are a critical success factor.

#5 Use Case
Reconcile software asset licensing costs

According to the BSA Software Alliance, most organizations are 20% under-licensed. For those organizations that are forced to do "true-up" processes and find themselves out of compliance, the fees can be quite costly. In addition to the costs of those extra licenses, organizations may also get hit with back maintenance fees as well as penalties for being out of compliance[2]. Real-time queries for installed software across all your systems can provide the insight needed to stay in compliance with your software vendor licensing agreements. Additionally, you can quickly verify if the software that's been installed is necessary, because you can identify the last time it was used, and by which logged in user.

2 http://blog.shi.com/2013/06/10/the-real-costs-of-being-out-of-compliance-with-your-software-licenses/#.Vi-8AhBJZsY

#6 Use Case
Support M&A integrations

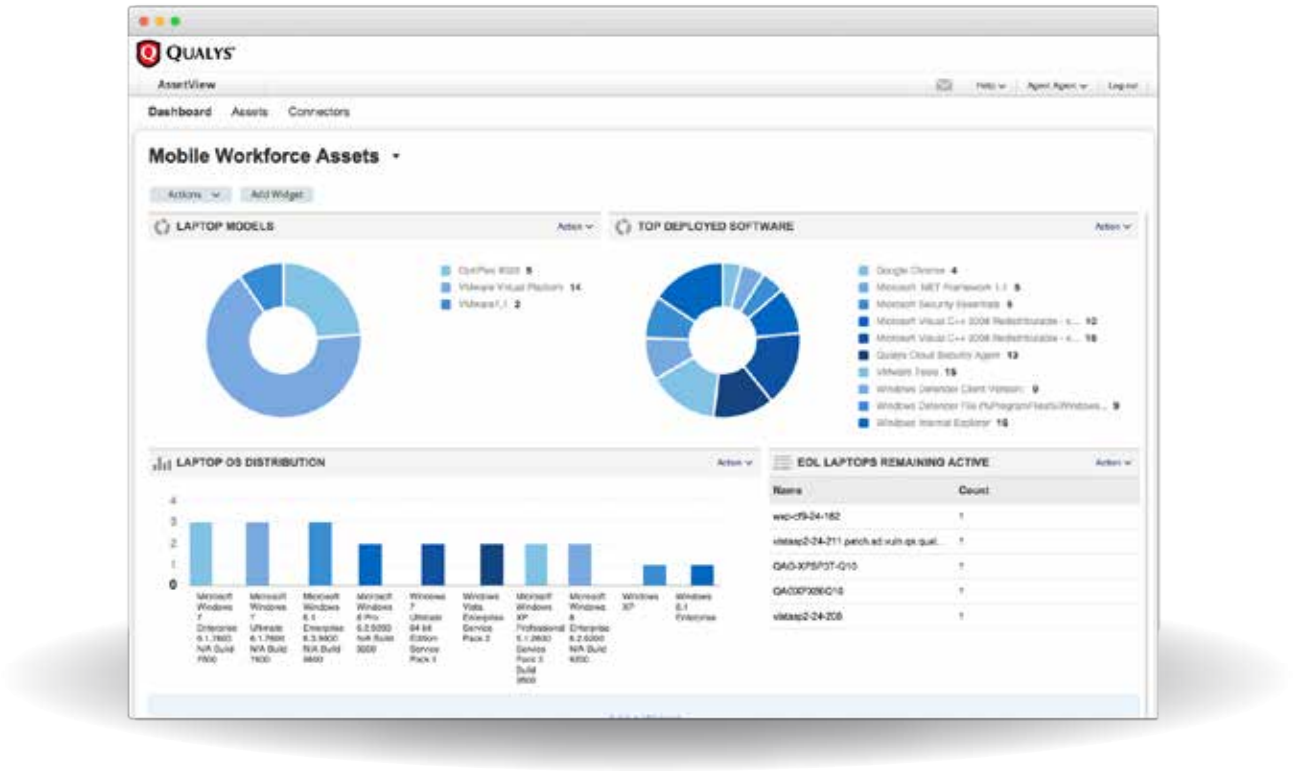
As enterprises consolidate assets and asset repositories across their integrated networks, clouds, and application infrastructures, things begin to get complicated quickly. IT and IT security teams work together to scan these new environments for vulnerabilities, configuration compliance checks, and other key indicators of security and compliance posture while still trying to reduce risk and uncertainty. A key first step for business unit integration involves updating and consolidating asset repositories.

The challenge is determining the single source of truth.

Using your vulnerability management program to drive an integrated and unified asset inventory provides the due diligence you need before integrating acquired assets into your environment. By automatically assessing assets for vulnerabilities and insecure configurations, you can integrate them more quickly, effectively shrinking these critical windows of vulnerability. Additionally, providing a consolidated view of the security and compliance posture of assets across business units – new and old - reduces risk and promotes productivity during these disruptive transitions.

Qualys AssetView:
Automated, Cloud-based Asset Inventory

Qualys AssetView is a free cloud-based IT asset inventory service that lets your company search for information on any asset where an agent is deployed, scaling to millions of assets for organizations of all sizes. Global IT assets can be searched in seconds and an up-to-date inventory is continuously maintained – no polling is required.



http://www.qualys.com/**AssetView**

AssetView quickly gives your IT and security teams a complete, up-to-date view of IT assets in your environment. This centrally managed service enables more effective management and security of endpoints, all via your favorite web browser. And because it's delivered on Qualys Cloud Platform, you can correlate this rich asset data with vulnerability and compliance data collected from other subscribed services such as Qualys Vulnerability Management and Qualys Policy Compliance.

Key Features:

Comprehensive, scalable view of endpoints

Access a continuously updated inventory of asset details, capable of scaling to millions of assets, making it useful for the largest enterprise environments.

Handles virtualized environments with ease

AssetView takes a unique approach to detecting whether a system is simply moving around the network or if it's been cloned such as in Virtual Environments. The service helps keep track of the constant proliferation of images inside and outside of the environment.

Minimal impact on systems and networks

Since AssetView uses self-updating agents that look only for changes from the host's previous state, networks and systems are not impacted. No polling of agents is required to update the asset inventory, allowing inquiries even for offline or unreachable endpoints.

Extensible

AssetView is integrated with both Qualys Vulnerability Management and Qualys Policy Compliance, and is designed to grow with an expanding network.

Fast, accurate and actionable data

AssetView provides a new layer of intelligence into the current state of endpoints, cataloging details about services, file systems and the registry, as well as a wealth of additional information to manage and secure systems.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 8,000 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of 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. For more information, please visit www.qualys.com. Qualys and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

Qualys, Inc. - Headquarters
1600 Bridge Parkway
Redwood Shores, CA 94065 USA
T: 1 (800) 745 4355, info@qualys.com

Qualys is a global company with offices around the world. To find an office near you, visit **http://www.qualys.com**