White Paper

Qualys Cloud Platform:

YOUR END-TO-END SECURITY SOLUTION FOR A PERIMETER-LESS WORLD

QUALYS®

INTRODUCTION

The widespread adoption of cloud computing services and mobile devices by organizations has drastically changed enterprise information security.

Organizations are no longer well served by the conventional approach of protecting the traditional corporate perimeter, whose boundaries consisted primarily of desktop PCs sitting inside offices and servers humming in on-premises data centers.

Today, organizations live in a perimeter-less world. Those clearly defined physical boundaries in which their IT infrastructure was housed have been pushed out, blurred, transformed and in some cases even erased.

Many workloads have been moved to the cloud, a trend that's still accelerating. Meanwhile, desktop PCs have increasingly been replaced as the preferred personal computing device within organizations by a variety of mobile endpoints -- laptops, tablets, smartphones and wearables -- which often spend more time outside of the office than inside.

As a result, CISOs face a new reality in which employees now routinely do things like log into their companies' SaaS-based CRM systems from laptops and smartphones at airport cafés over public Wi-Fi networks.

When CISOs look at the enterprise security marketplace for solutions, they find legacy vendors scrambling to belatedly retrofit their products, rarely with optimal results. CISOs also come across eager startups in precarious financial standing peddling narrowly scoped products aimed at niche use cases.

A CISO who evaluates what these vendors offer will quickly realize that these retooled legacy systems and new point solutions are complex, costly, limited and, worst of all, ineffective.

Qualys saw this shift coming many years ago. Guided by its pioneering vision, Qualys has been deliberately and thoughtfully crafting its integrated cloud platform to meet the challenges that organizations face today in this age of cloud computing and mobility.

Today, the Qualys Cloud Platform is uniquely positioned to provide continuous security for organizations that find themselves having to monitor and protect on-premises, cloud-hosted and mobile IT assets. It's the most advanced security platform available today for the global enterprise with a hybrid infrastructure in a perimeter-less world.

The Qualys Cloud Platform constantly collects, assesses and correlates asset and vulnerability information across customers' cloud instances, on-premises systems and mobile endpoints, giving them a real-time, holistic view of their threat landscape and helping them prioritize their security and compliance remediation.

In this paper, we explain in detail how Qualys accomplishes this via its centrally managed cloud architecture, anchored by a robust back-end threat analysis engine and powered by an integrated suite of security and compliance apps.

"The quality of Qualys WAS is maintained across many different types of applications. It proves to be very thorough and accurate as well as easy to configure and use."

– Ahmad Mahdi
Infrastructure Security Team Manager

Microsoft

The New Perimeter – or Lack Thereof

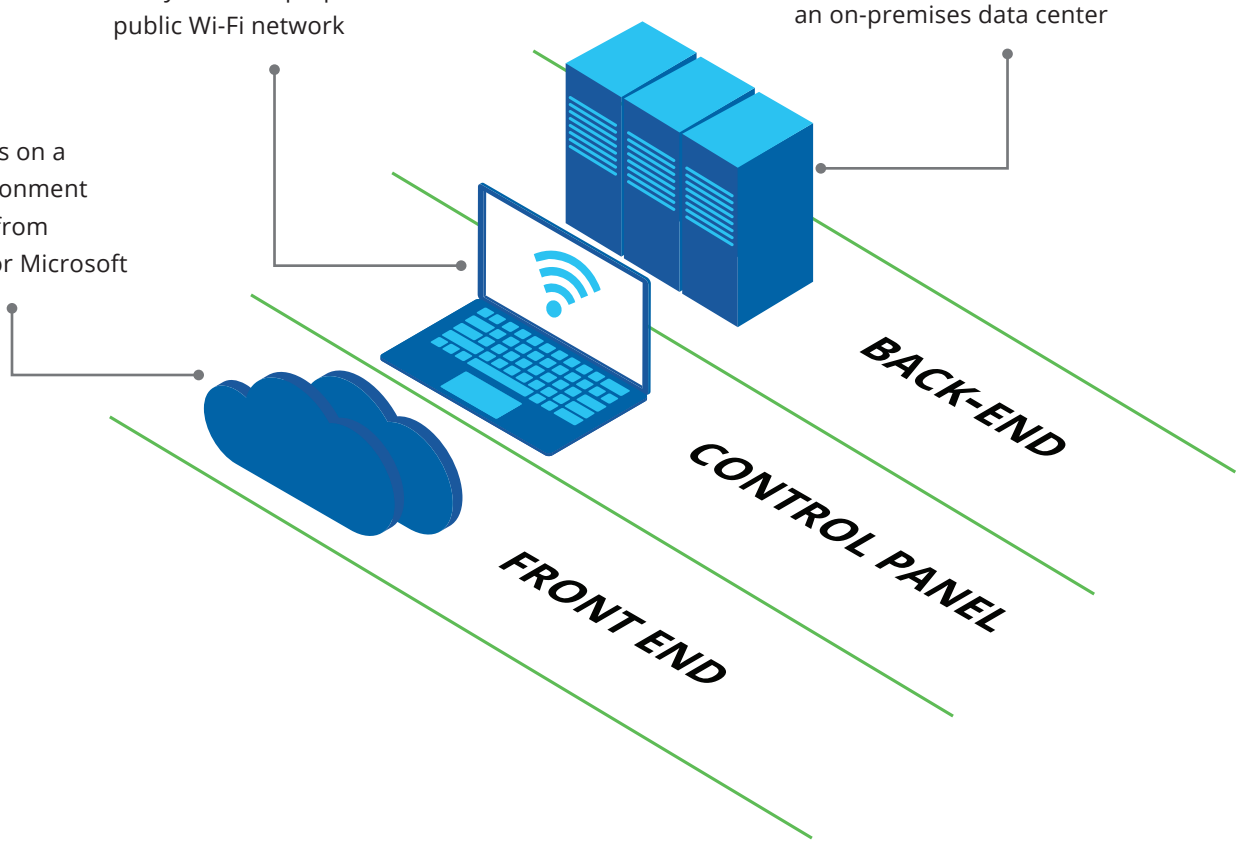
INTRODUCTION

The new information security challenges that cloud computing and mobility have created for IT departments are well exemplified by this hypothetical but very common scenario of a retailer's payments app:

The app's control panel can be accessed by an admin sitting a hotel lobby from a laptop connected to a public Wi-Fi network

The app's back-end process runs in an on-premises data center

The front end runs on a public cloud environment such as the ones from Google, Amazon or Microsoft



The risk to this one application rests in these three different places, so security products that protect only the endpoint, or only the cloud instance, or only the on-premises server don't measure up. Attempting to cobble together a more comprehensive solution by tying heterogeneous products brings integration complexity, higher costs and, very likely, poor performance.

THE NEW BOUNDARIES OF YOUR IT LANDSCAPE

Most perimeters were formerly contained to corporate premises, but now they extend to public, private and hybrid clouds, mobile devices, IoT sensors and even to non-computing appliances.

Mobile devices, non-computing appliances and IoT systems

Your perimeter reaches out to every one of your laptops that is being used right now by an employee sitting in an airport terminal and connected to a Wi-Fi network. Of course, it's not just laptops: There are smartphones, tablets, smartwatches, fitness trackers and other such devices that are your employees' digital travel companions. Often lost, stolen and misplaced, they contain valuable and confidential corporate data and applications.

Let's not forget all the potential entryways that exist for hackers in organizations' geographically dispersed locations, such as small remote offices and retail stores. These facilities, which house PCs, point-of-sale systems and other vulnerable endpoints, often don't have the same level of physical and cyber security as their organizations' larger corporate buildings.

Meanwhile, there are a whole bunch of non-computing devices getting attached to your network that weren't in the past. These include copiers, printers, smart thermostats and even Wi-Fi enabled coffee makers and refrigerators in the office kitchen.

Businesses are also aggressively adopting IoT and embedding sensors in all sorts of "things" that were formerly offline, including company vehicles, HVAC systems, healthcare devices, industrial equipment, parking lots, store shelves, heavy machinery and jet engines.

These widely diverse and dispersed endpoints will be collecting sensitive data about their organizations' operations and transmitting it back to their data repositories for analysis. Thus, it's essential for organizations to monitor the security and compliance of these newly connected devices because they tend to be more vulnerable to cyber attacks than typical computing devices: If they're not properly protected, it's easier to sniff passwords off of those devices, sensors and appliances, and it's simpler to compromise and break into them.

Cloud computing services

Adoption of cloud computing software, platform and infrastructure services -- SaaS, PaaS and IaaS -- continues on the upswing among organizations of all sizes globally. As workloads shift from on-premises systems to public, private and hybrid clouds, requirements for asset discovery, security and compliance change significantly, both from security and compliance perspectives. For example, you may find that your cloud service providers make it difficult or outright impossible for your organization to perform vulnerability scanning on your cloud instances.

HOW CAN YOU MONITOR AND CONTROL THIS FAR-REACHING ENVIRONMENT?

To protect your organization in this brave new world, you must have a single view across your entire IT infrastructure via a central dashboard, where you can slice and dice the data, visualize it with graphs and reports, and analyze and share it with multiple stakeholders.

You could attempt to build a system that can give you this holistic and comprehensive view of your IT asset and vulnerability landscape by cobbling together a variety of products. But it will be a highly complex and costly endeavor that may never yield the desired results.

Fortunately, you don't need to buy third-party point products and hire a systems integrator to configure and install such a system for you. It already exists: the Qualys Cloud Platform.

"We use Qualys as a way to paint a picture of security and feed it to our executives. The reports give senior executives a concise, real-time view into eBay's security risks and measure change in those risks as we implement security measures."

– Chris Lalonde
Senior Manager
Information Security

Qualys Cloud Platform:

How can we do what others can't? It's all in our cloud-based architecture, which is the opposite of the on-premises, multi-tier architecture upon which legacy enterprise security solutions are based.

THE BENEFITS OF SaaS

A Single, Comprehensive View

Central analysis of data from many different sensor types is only possible in the cloud. Our easy-to-deploy appliances and lightweight agents automatically beam up to the Qualys Cloud Platform the security and compliance data they're constantly gathering from customers' IT environments.

Best-of-Breed Applications

Our cloud architecture allows us to provide a complete set of integrated, best-of-breed applications, correlate disparate data from on-premises systems, endpoints and cloud instances, and easily add new services.

No Hardware or Software To Maintain

Legacy architectures are rigid, complex and ultimately limited. They typically consist of multiple on-premises servers, each one operating different functions, and requiring in house backups, updates and maintenance.

The Qualys Cloud Platform is self-updating and always on, so it has an immediate positive impact on productivity because the IT department doesn't have to manage and maintain it: You don't need to procure hardware and install and update the software. You don't need to migrate its databases. You don't need to back up the data. You don't need to refresh the signatures file or the analysis engines.

Hit the Ground Running

The Qualys Cloud Platform is integrated, easy to set up and inexpensive to maintain. You can get results right away after logging into our browser-based console for the first time. Its solutions can be deployed and operated without the need for professional services help.

Pay as You Go

Qualys also gives you more control over licensing costs via its flexible, subscription-based model, which saves you from having to plunk down a lot of money upfront for perpetual licenses and suffering buyer's remorse when you find you overpaid.

Flexibility

Qualys offers subscription packages tailored for small, mid-size and large organizations.

Customers also get the flexibility to purchase Qualys Cloud Platform app subscriptions a la carte.

UNPARALLELED ACCURACY IMMUNIZES YOUR ORGANIZATION AGAINST BREACHES

Qualys vulnerability scans, the most difficult type of scan, consistently exceed Six Sigma 99.99966% accuracy, the industry standard for high quality.

Designed to protect organizations against external breaches and internal compliance violations, the Qualys Cloud Platform is built around four key pillars that amount to a sort of systemic vaccination for your IT environment against active vulnerabilities, slashing your risk of getting breached:

DISCOVER

Discovering and categorizing assets and identifying vulnerabilities at scale

DETECT

Offering configurable and powerful reporting and searching capabilities

PRIORITIZE

Automating and improving the prioritizing of threat remediation

RESPOND

Managing the actual process of planning remediation, generating service tickets and applying patches to at-risk IT assets

If your most critical vulnerabilities are patched, you greatly increase your protection against attacks that get through your firewall, such as viruses that arrive via email . With Qualys, you immunize your IT assets against critical threats.

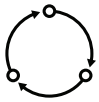
COMPLETE CONTROL AND VIEW OF IT ASSETS PAIRED WITH CONTINUOUS SECURITY

The Qualys Cloud Platform gives you comprehensive asset discovery, continuous processing of the data and a full visibility of your vulnerabilities, all updated in real time around the clock.

Unlike legacy products in which scanning needs to be scheduled or manually triggered, the Qualys Cloud Platform is on autopilot, collecting information all the time, correlating external threat data with your internal IT asset inventory and compliance requirements, to pinpoint what needs to be patched or mitigated right away.

Our highly scalable cloud platform annually performs 3+ billion scans, logs 100+ billion detections and collects, processes and analyzes 1+ trillion security data points, as it combines continuous discovery of assets and vulnerabilities, real-time distributed data collection, indexing and storage, and a robust analytics correlation back-end engine.

3+ Billion
Scans



100+ Billion
Detections, Collects, Processes and Analyzes

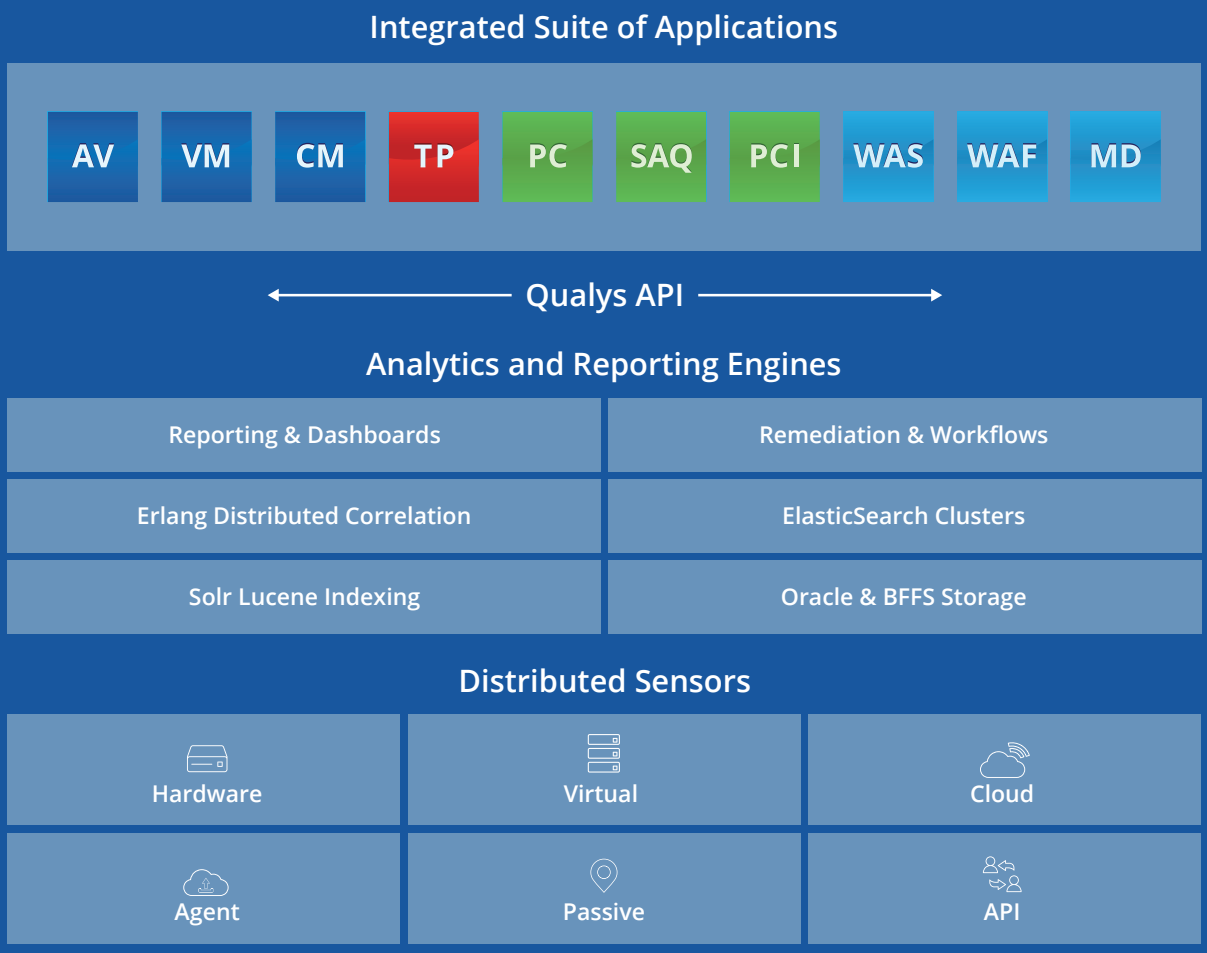
1+ Trillion
Security Events

Qualys Cloud Platform:

HOW IT OPERATES

The Qualys Cloud Platform is built upon a robust, modular, scalable and flexible infrastructure that leverages virtualization and cloud technologies, and lets us allocate capacity on demand.

Let's zoom in and see the Qualys Cloud Platform in action.



Data Collection

The Qualys Cloud Platform collects security data across every type of IT infrastructure using a variety of methods and sensors, including:

Physical Applicances

These self-updating scanners are placed on customer premises, where they provide continuous security and compliance monitoring of IT assets.

Virtual Appliances

They work like the physical appliances but in private cloud and virtualized environments without the need to install a hardware box in a customer's office or data center.

Cloud Appliances

Designed for customers who want to scan their IaaS and PaaS instances in commercial cloud computing platforms, they're pre-certified to work in AWS and Azure and they're fully automated with API orchestration.

Cloud Agents

These lightweight software agents go into a variety of assets to continuously monitor and asses their security and compliance. They work in real-time without the need to schedule scan windows nor to manage credentials and firewalls.

Passive Appliance

They sniff network devices and traffic, doing real-time discovery and identification, including of unauthorized devices, APT traffic and malware files. It profiles unknown devices types based on traffic and activity patterns.

APIs

Using the Qualys API, third parties can integrate their own applications with Qualys cloud security and compliance solutions using an extensible XML interface. Today, we enable almost all of the major functions of the Qualys Cloud Platform with APIs.

Physical Appliances

These are self-updating hardware boxes designed to be placed on customer premises, such as data centers or office locations. These scanners provide continuous security and compliance monitoring of IT assets and transmit the data to the Qualys Cloud Platform's back end engine. They update themselves in the background with the latest vulnerability signatures and with kernel refreshes. Customers don't have to touch them once they've been deployed.

Virtual Appliances

Available on multiple hypervisors, these work like the physical appliances, with the difference that it's not necessary to deploy an actual hardware box on the customers' premises.

Cloud Appliances

These run within commercial cloud computing platforms such as Amazon's AWS and Microsoft's Azure, allowing Qualys customers to scan their workloads in those environments and transmit the information back to our central platform. Qualys has formal partnerships with Amazon and Microsoft.

Cloud Agents

These are lightweight software agents that can go into a variety of assets, such as on-premises servers, virtual machines, cloud apps and endpoint devices, where they continuously monitor for changes and assess their security and compliance status. They transmit back to the Qualys back end what they detect for analysis and classification. The agents work in real-time without the need to schedule scan windows nor to manage credentials and firewalls, which makes them particularly beneficial for monitoring occasionally connected mobile devices.

Qualys Cloud Agents are centrally managed, can be deployed and uninstalled remotely, and use up a minimal amount of computing resources on their host devices and networks. They employ a Delta-based approach and collect raw data points, such as registry keys, running processes, network connections and files, which are evaluated continuously in the Qualys Cloud Platform back end.

A central console lets you manage the agents from a single place. They're fully integrated with the Qualys Cloud Platform and can be linked via an API with third-party SIEM (security information and event management), CMDB and help desk ticketing products. The Cloud Agent Platform puts Qualys in a unique position to protect IoT (Internet of Things) systems through agents that reside on IoT endpoints.

Passive Appliance

This appliance, due to ship in the second half of 2016, is a centrally managed, self-updating sensor that sniffs network devices and traffic, doing real-time discovery and identification, including unauthorized devices, APT traffic and malware files. It plugs into a switch mirroring port, does OS fingerprinting, identifies ports and protocols used and discovers apps and services on devices. It profiles unknown devices types based on traffic and activity patterns, so you may deduct something is a printer based on the port it's using and how much data it's receiving. It will let you detect, say, a personal laptop that an employee is using for the first time to access corporate data or applications, even if they're connecting from their home network or a public Wi-Fi hotspot. All of the information it gathers is sent back to the Qualys back end for analysis.

APIs

The Qualys Cloud Platform has APIs (application programming interfaces) that allow it to be integrated with threat intelligence feeds, configuration management databases (CMDBs) and log connectors.

Having all these options -- agentless, agent-based and passive -- means that organizations can use any combination of methods, tools and technologies that make the most sense for their particular infrastructure and needs.

DATA CATEGORIZATION, VISUALIZATION AND ANALYSIS

The platform's asset tagging and management capabilities let customers identify, categorize and manage large numbers of IT assets and automates the process of inventorying and organizing them hierarchically.

Meanwhile, a highly configurable reporting engine powers the creation of reports, graphs and dashboards so that customers can generate visual representations of the data.

Our analytics engine indexes petabytes of security and compliance data gathered from our customers' IT environments, makes this information searchable and correlates it against external threat data contained in the Qualys KnowledgeBase.

The data analysis is done from a variety of angles and perspectives. For example, if the Qualys Cloud Platform detects that a registry key was changed or added in a Windows laptop, the data is beamed up to the back-end engine, where it's analyzed in a multi-dimensional way. In this case, the Qualys Cloud Platform will explore possible reasons for the registry alteration, investigating whether a policy compliance violation is behind it or whether it points to a malware infection. In short, Qualys Cloud Platform takes this one data point and analyzes it multiple times, a task that otherwise the organization could only perform by purchasing several point solutions from other vendors.

Our integrated workflow service lets customers quickly make risk assessments and access information for remediation, incident analysis and forensic investigations. Customers can generate help desk tickets, manage policy and compliance exceptions, and track and escalate patching and risk mitigation efforts.

The Qualys Cloud Platform can also trigger notifications to proactively alert customers about a variety of actions and incidents, such as the detection of new vulnerabilities and malware infections, completion of scans, opening of trouble tickets and system updates.

The result is continuous security and compliance of IT assets wherever they reside, which you need because hackers don't operate in accordance with scheduled scans: They're all over the world, attacking organizations around the clock.

"Qualys helps us to make sure that our network is secure and that our systems, and those of our customers, are hardened as well."

– Leonid Stavnitser
Senior Manager
GIT Security Engineering Team

ORACLE®

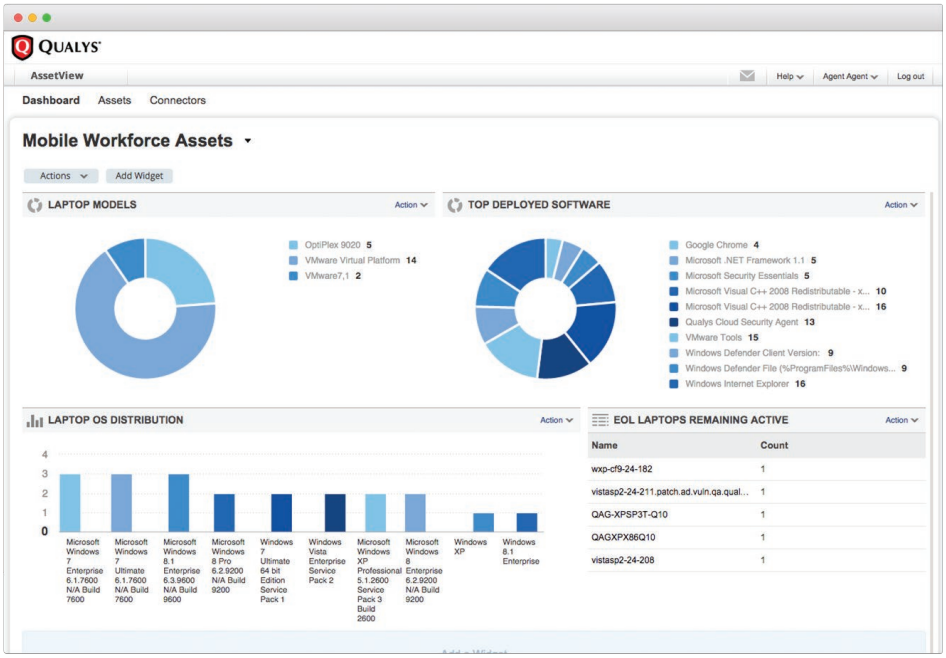
Integrated Suite of Security and Compliance Applications

Here's how the Qualys Cloud Platform applications automate and enhance the lifecycle of your asset discovery, network security, threat protection, compliance monitoring and web application security.

VULNERABILITY ASSESSEMENT

AssetView

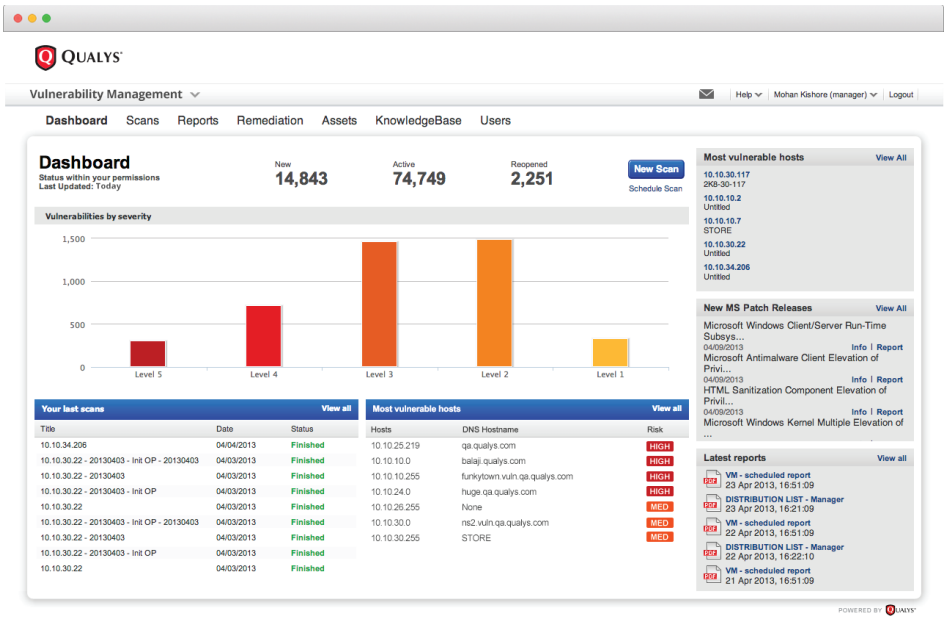
Effective endpoint security and compliance requires having comprehensive asset visibility and control, something which has become harder to accomplish as new types of devices proliferate on enterprise networks. AssetView generates and continuously updates an inventory of an organization's assets, and consolidates all the asset details in one place, so you get a unified view of each one. With AssetView, the IT department can know which assets exist on their environment, where they're located, who manages them and what security risks they carry. AssetView scales to millions of assets and provides powerful search and reporting capabilities. It also integrates with third-party products such as the ServiceNow Configuration Management System and Splunk Enterprise.



For example, with AssetView, you can quickly get a list of all of your Lenovo devices. You can narrow down that list by filtering the results according to various criteria, such as device location, operating system, CPU type or, particular vulnerability. And you can click on a specific asset and obtain granular details on it, such as who was its most recent logged-in user, hardware specs, installed software, network location, detected vulnerabilities, and the like, all continually updated.

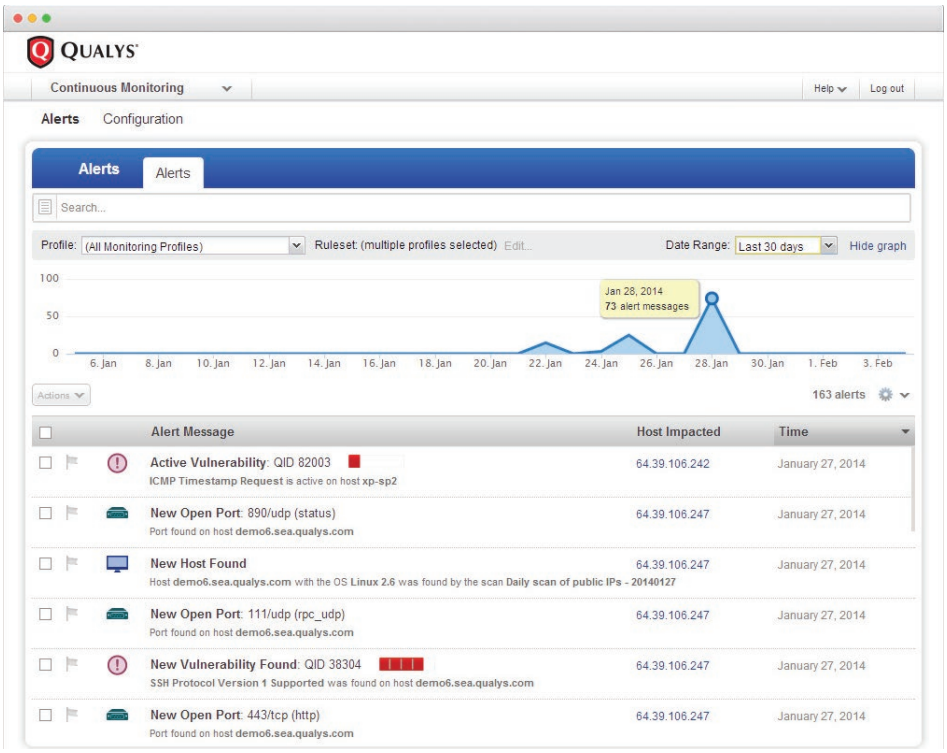
Vulnerability Management (VM)

This cloud service is at the core of the suite and provides comprehensive visibility into the vulnerabilities in your IT systems, letting security teams continuously identify threats and monitor changes in their network. Qualys VM visually maps every device and application on the network, and lets you access configuration details for each. It uncovers new or forgotten devices, scans for vulnerabilities everywhere and automatically assigns remediation tickets, integrating with third-party ticketing systems.



Continuous Monitoring (CM)

Qualys Continuous Monitoring (CM) lets you identify threats and monitor unexpected changes in your network before they turn into breaches. With it, you can track what happens within your internal environment, and Internet-facing devices throughout your DMZs and cloud environments -- anywhere in the world. CM brings a new approach to vulnerability management and network security, enabling you to immediately identify and proactively address potential problems such as: Unexpected Hosts/OSes; Expiring SSL Certificates; Inadvertently Open Ports; Severe Vulnerabilities; and Undesired Software. CM requires no special hardware and can be set up with a few simple clicks. A user simply needs to identify the host or hosts that need to be monitored, who to alert when states change, and what that change might be.

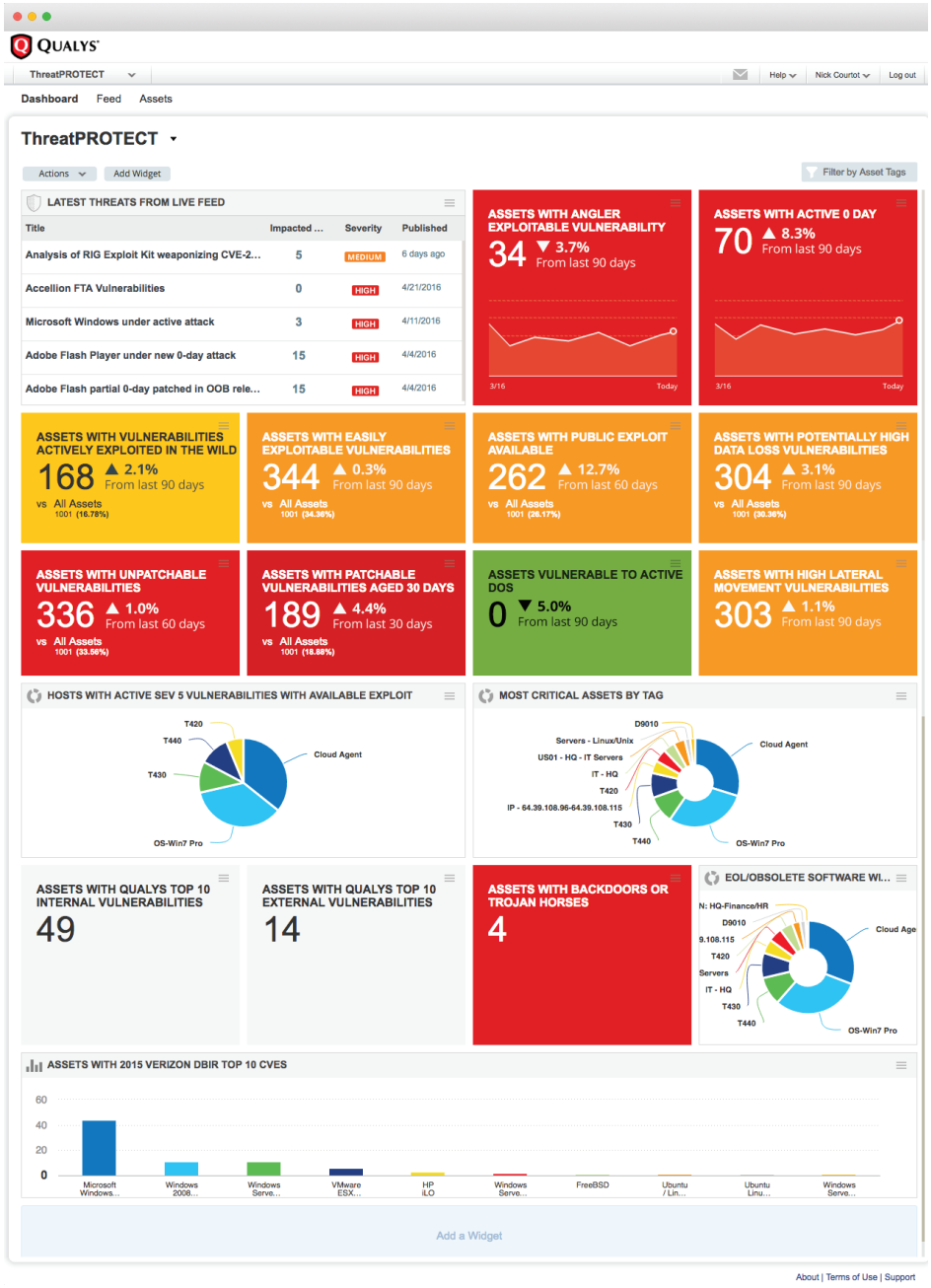


Vulnerability Assessment | Threat Prioritization | Compliance Monitoring | Network and App Security

PRIORITIZATION OF REMEDIATION WORK

ThreatPROTECT (TP)

ThreatPROTECT leverages the data gathered, analyzed and classified by Vulnerability Management, AssetView and other Qualys Cloud Platform components to precisely identify the IT assets that are most at risk within an organization at any given point. ThreatPROTECT does this by correlating external threat data against an organization's internal vulnerabilities. By pinpointing the IT assets that must be patched right now, ThreatPROTECT helps IT departments solve one of their biggest challenges: Prioritizing remediation, at a time when new vulnerabilities are disclosed every day, amounting to thousands per year. ThreatPROTECT has a Live Threat Intelligence Feed, a dynamic and customizable dashboard, graphing and reporting capabilities, and a powerful search engine. With ThreatPROTECT, IT departments get a holistic and contextual view of their organization's ever changing threat landscape.



COMPLIANCE MONITORING

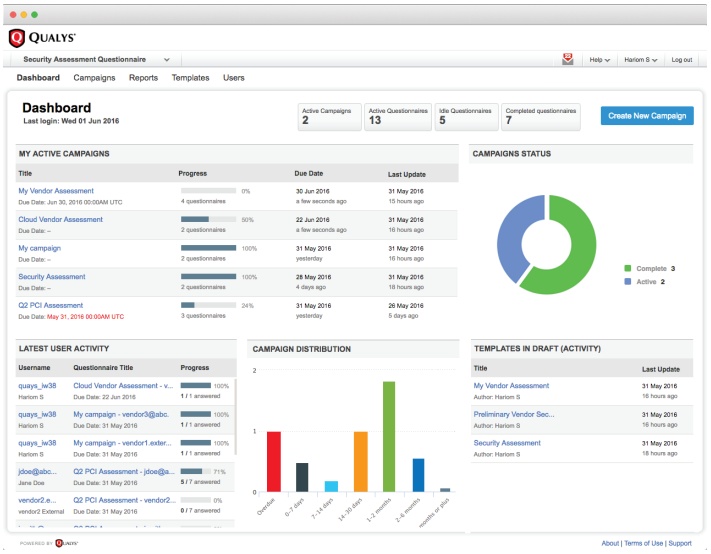
Security Assessment Questionnaire (SAQ)

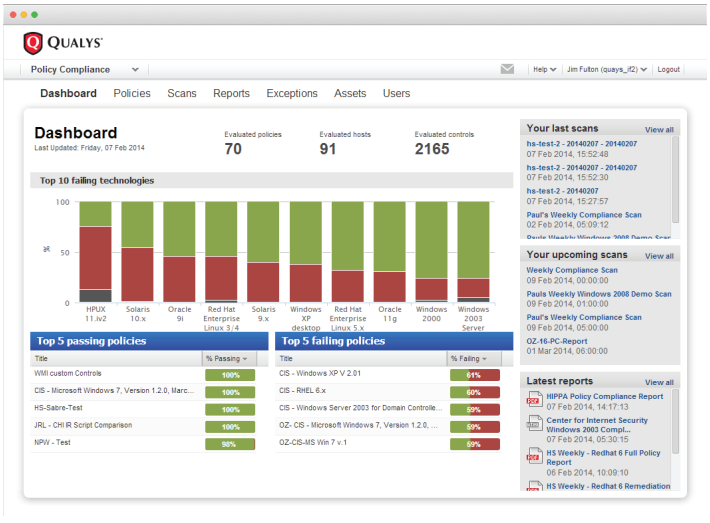
SAQ automates a key aspect of policy compliance: assessing the security risk presented by the businesses processes of the third parties you associate with, such as partners, vendors, suppliers and consultants. SAQ lets organizations generate customizable questionnaires for third-party security assessments and compliance audits. Instead of relying on a slow, laborious and inaccurate manual process using email and spreadsheets, organizations can use the cloud-based SAQ to automate and speed up tasks such as campaign management, template creation, questionnaire distribution and result analysis.

Policy Compliance (PC)

Policy Compliance (PC) performs automated security configuration assessments on IT systems throughout your network. It helps you to reduce risk and continuously comply with internal policies and external regulations. Qualys PC frees you from the substantial cost, resource and deployment issues associated with traditional software products. Known for its fast deployment, ease of use, unparalleled scalability, and rich integration with enterprise GRC systems, Qualys PC is relied upon by leading companies around the world.

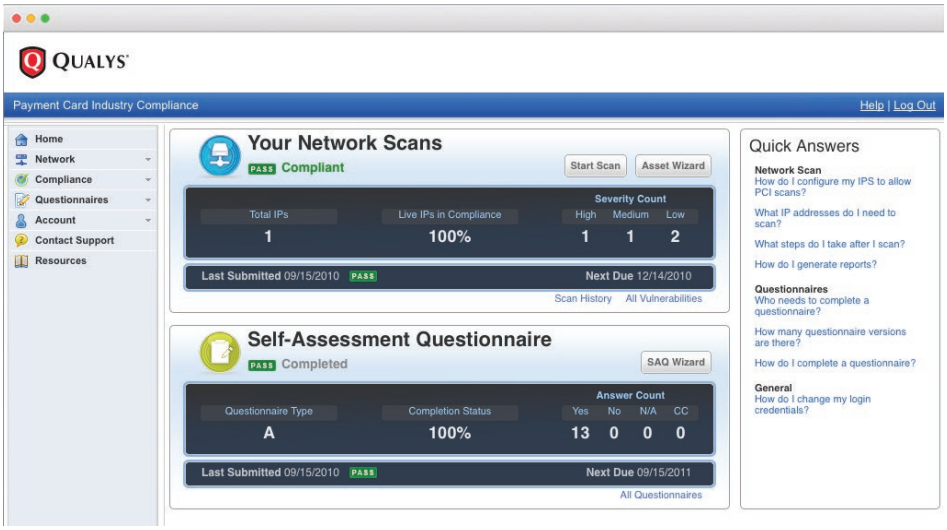
Qualys PC automates the processes of defining policies, specifying controls, assessing compliance, remediating violations and documenting changes. With Qualys PC, IT departments can see their security configuration issues accurately and in one place.





PCI Compliance (PCI)

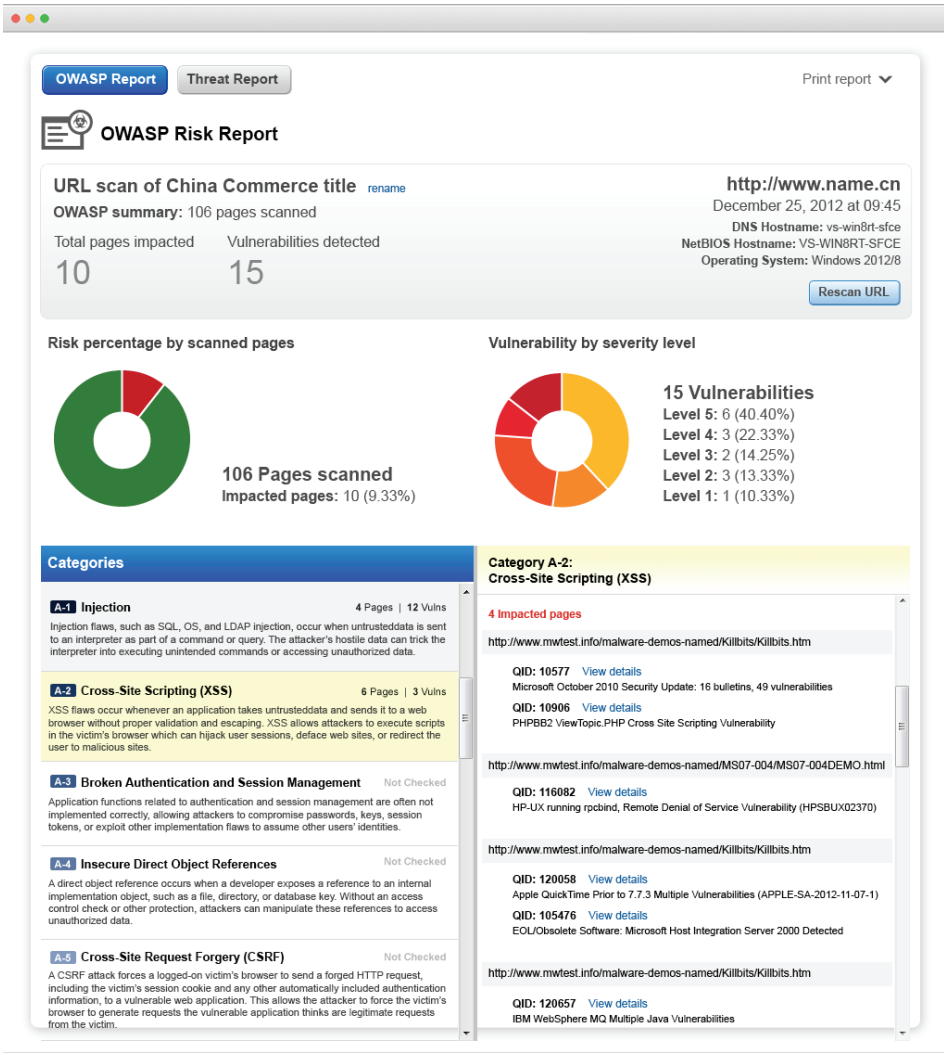
Qualys PCI provides businesses, online merchants and member service providers (MSPs) an easy, affordable and automated way to achieve compliance with the Payment Card Industry Data Security Standard. Known as PCI DSS, the standard provides organizations the guidance they need to ensure that payment cardholder information is kept secure from possible security breaches. PCI automates compliance testing, reporting and submission, letting merchants and MSPs submit the PCI self-assessment questionnaires, and conduct network and web application security scans to identify and eliminate security vulnerabilities. The Qualys PCI "auto submission" feature completes the compliance process, allowing users to submit compliance status to one or multiple acquiring banks.



NETWORK AND APPLICATION SECURITY

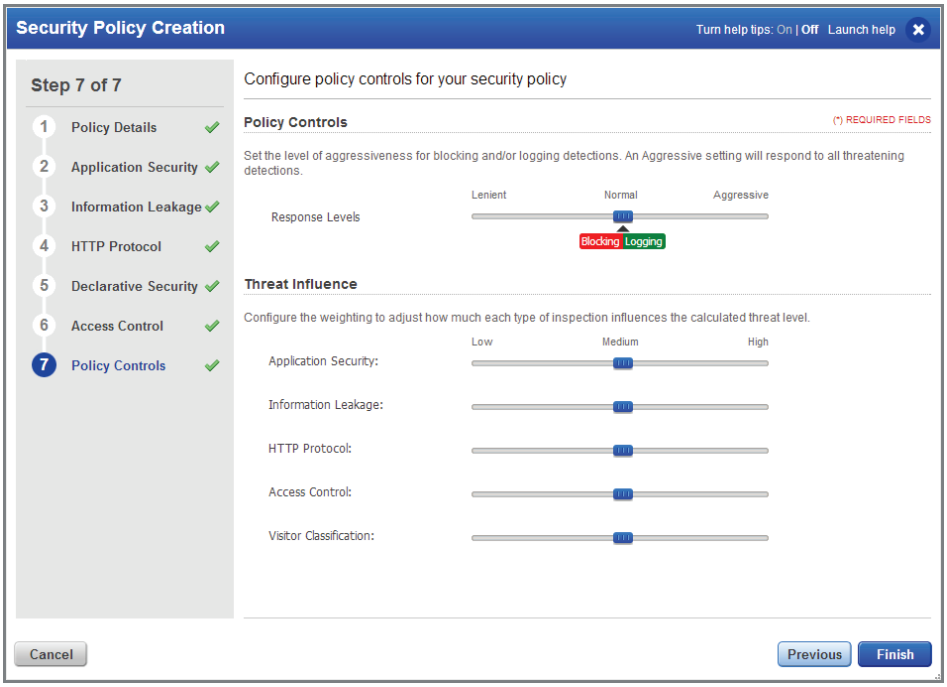
Web Application Scanning (WAS)

Qualys WAS lets you continuously discover, catalog and scan web apps to detect vulnerabilities and website misconfigurations. It provides automated crawling and testing of custom web applications to identify vulnerabilities including cross-site scripting (XSS) and SQL injection. The automated service enables regular testing that produces consistent results, reduces false positives, and easily scales to secure a large number of websites. It proactively scans websites for malware infections, sending alerts to website owners to help prevent black listing and brand reputation damage.



Web Application Firewall (WAF)

Qualys WAF brings scalability and simplicity to web application security. Its automated, adaptive approach lets you quickly and more efficiently block attacks on web server vulnerabilities, prevent disclosure of sensitive information, and control where and when your applications are accessed. Qualys WAF complements the global scalability of Qualys Web Application Scanning (WAS). Together, they make identifying and mitigating web application risks seamless – whether you have a dozen apps or thousands. Qualys WAF can be deployed in minutes, supports SSL/TLS, and doesn't require special expertise to use. It delivers a new level of web application security and compliance while freeing you from the substantial cost, resource and deployment issues associated with traditional products.



The suite will continue growing with upcoming apps including Passive Scanner (PS), File Integrity Monitoring (FIM), Indicators of Components (IoC) and Patch Management (PM).

For organizations that, due to internal policies or external regulations, can't use Qualys' multi-tenant, shared public cloud architecture, we offer our Qualys Private Cloud Platform. The PCP is a family of self-contained, pre-configured appliances that offer the security and compliance services of the Qualys Cloud Platform but on premises within a customer's or partner's data center. The high-performance appliances are easy to deploy and are centrally managed and remotely updated by Qualys. The PCP products come as purpose-built hardware boxes and virtualized appliances. They can be configured as fully connected, so Qualys manages the platform remotely around the clock over a secure VPN, requiring no touch from the customers, or as partially connected, in which Qualys manages the platform remotely over a bastion server and the customer controls the VPN schedule.The latest addition to this product family is the PCP Appliance for small and medium-size organizations.

Comprehensive Training and Support

Qualys isn't content with its industry-leading technology, because it's deeply aware of the importance of partnering with and supporting its customers every step of the way.

Qualys provides free product training and 24 x 7 telephone support. Calls are answered within one minute and involve a collaborative approach with support, operations and engineering staff. Support emails are answered in under 24 hours on average. We have customer support centers in our Redwood City, California headquarters; Raleigh, North Carolina; Reading, United Kingdom; and Pune, India.

In addition, the Qualys website has a support community with more than 20,000 members, training videos and a knowledge base. There, Qualys employees and customers meet to share best practices and answer each other's questions.

Customer Base

The best testament to the quality of our products is our customer base. Qualys has more than 8,800 customers from all major vertical industries in over 100 countries, including Oracle, T-Mobile, Comcast, Facebook, Verizon, Microsoft, Toshiba,Home Depot, Nissan, MetLife, BASF, Williams-Sonoma, Daimler, GlaxoSmithKline, Pfizer and GM. We have a majority of the Forbes Global 100 and Fortune 100 as customers.

- 9 out of the top 10 **Technology**
- 9 out of the top 10 **Retail**
- 9 out of the top 10 **Biotechnology**
- 7 out of the top 10 **Chemical**
- 7 out of the top 10 **Banking**
- 6 out of the top 10 **Software**
- 6 out of the top 10 **Telecom**
- 6 out of the top 10 **Media**
- 6 out of the top 10 **Car Manufac.**
- 6 out of the top 10 **Food Retail**

Geisinger

Geisinger Health System uses Qualys Cloud Platform, and specifically the Vulnerability Management, PCI, Web Application Scanning and Cloud Agent components, to help protect its IT environment, which contains a mix of on-premises and cloud systems. The Danville, Pennsylvania healthcare services provider has several data centers, over 20,000 endpoints and thousands of servers.

Geisinger has been a Qualys customer for about 8 years, during which time it has deepened its use of Qualys products.

"We started with traditional vulnerability management, but we've expanded our use as our organization has grown along with the complexity of the devices, applications and infrastructure, especially on equipment that directly impacts patient care," says Nathan Cooper, information security analyst in cyber operations at Geisinger.

Geisinger, which has 30,000 employees, piloted Cloud Agent on the servers of its security team department. "It passed. There were no discrepancies between the agent and the Qualys Cloud Platform VM vulnerability scans," Cooper says. "Now we can have the agent added to our base server image so that any new server that's built from our virtual template instantly has the agent installed. That means, new servers immediately report themselves to the Qualys Cloud Platform."

"Right out of the gate we know that a new system is provisioned and in our vulnerability management life cycle," Cooper says. "That's precisely how the Qualys Cloud Agent, powered by the Qualys Cloud Platform, helps Geisinger improve its vulnerability management efforts and achieve the real-time, continuous security both the security team and Geisinger needed."

The Cloud Agent is also making a difference at Synovus Bank, a financial services company based in Columbus, Georgia with about $28 billion in assets.

Synovus started using Qualys VM to perform frequent vulnerability scans for all internal and external assets; receive faster notification and remediation for zero day and critical threats; and improve its vulnerability analysis and security patching programs by providing data that can be used to prioritize patch distribution.

The company then adopted Cloud Agent to sharpen the collection of vulnerability information from its laptops. Unlike desktop workstations, servers and network appliances, laptops are mobile and thus are intermittently connected to its network, so at Synovus they often missed pre-scheduled vulnerability scan windows.

With Cloud Agent, Synovus was able to discover vulnerabilities in laptops in near real time and with more precision. It soon found out that, contrary to its previous estimates, its average laptop didn't have 30 vulnerabilities but rather about 200 vulnerabilities.

Synovus changed its laptop patching schedule and increased it to a daily frequency. The results: its average laptop now has about 10 vulnerabilities, a dramatic drop.

"Cloud agent had an immediate impact," says Corey Reed, a senior security analyst at Synovus.

Synovus likes that the Cloud Agents require minimal maintenance because they're self-updating, and that they can be easily deployed through group policy and SCCM (System Center Configuration Manager). Synovus also appreciates the negligible impact Cloud Agents have on its network and IT assets because the agents consume very little computing resources.

The Future

The Qualys Cloud Platform will continue to grow in scope as we push ahead of competitors. New services that are in the works include File Integrity Monitoring, Passive Network Analyzer, Indicator of Compromise Detection and Patch Management.

Qualys will also continue to extend its revolutionary Cloud Agent technology to bring our security and compliance monitoring to more and more platforms and types of endpoints.

As we continue to innovate and deliver industry-leading products, customers will keep reaping the unique benefits of our Qualys Cloud Platform, with its cloud oriented, modular, comprehensive and integrated architecture, including:

- **Unified suite of best of breed solutions**
- **Global delivery**
- **Faster, simpler, inexpensive deployment**
- **Higher quality**
- **Continuous improvements**

Qualys: Bringing continuous security to the global enterprise with the most advanced security platform.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 8,800 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**