Qualys Cloud Platform

One stack to consolidate traditional enterprise security and compliance solutions and secure the digital transformation

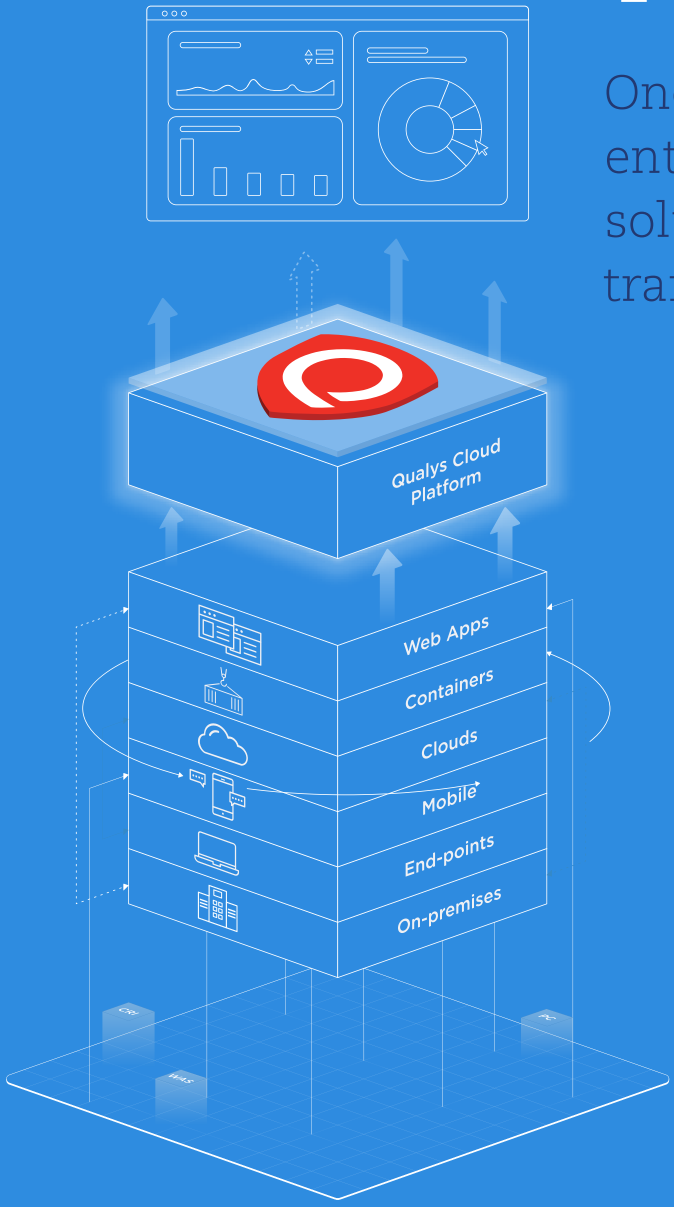


Table of Contents

Introduction

As organizations digitally transform business processes to boost agility and efficiency, IT environments become distributed, elastic and hybrid — a challenge for security teams. CISOs are no longer well served by conventional security products designed to protect traditional, well-defined corporate perimeters where most assets are on premises.

With the adoption of cloud, mobility, virtualization, and other innovations, IT infrastructure frontiers have been pushed out, blurred, and even erased. To regain visibility and control over these new amorphous IT environments, CISOs often resort to accumulating heterogeneous point tools, an ineffective and counterproductive approach.

Because it's difficult to integrate, manage and scale a plethora of disparate security products, this strategy results in operational silos, increased costs and data fragmentation. Worse, it leaves organizations exposed to opportunistic hackers who take advantage of attack vectors created by the speed, openness and interconnectedness of modern IT.

Instead, security must be orchestrated transparently into digital transformation projects. This requires a unified security and compliance platform for prevention, detection and response.

Qualys saw this shift coming many years ago. Guided by its pioneering vision, Qualys has been crafting its integrated cloud platform to meet the challenges of the digital era's increased attack surface.

With Qualys, organizations can build security natively and organically into hybrid IT infrastructures, instead of abruptly bolting it on, as has been done traditionally.

This includes meshing and automating security into DevOps pipelines, which power digital transformation projects by continuously and quickly developing and delivering code. If security remains isolated and is jammed in at the end before software is deployed, it will slow down DevOps' continuous development and delivery, and erase digital transformation benefits.

ORACLE

> "Qualys helps us to make sure that our network is secure and that our systems, and those of our customers, are hardened as well."
>
> Senior Manager,
> GIT Security Engineering Team

In short, the Qualys Cloud Platform continuously assesses organizations' security and compliance posture, with instant visibility across all IT assets — on premises, in clouds, and at remote endpoints — for continuous monitoring and response.

As Robert Ayoub, IDC's Research Director of Security Products, recently stated: "The Qualys Cloud Platform simplifies the complexity associated with managing multiple security solutions, while at the same time increasing the automation, effectiveness and proactive nature of security."

Read on to learn how our platform consolidates and automates security and compliance tasks, and protects hybrid IT environments, via its versatile sensors, back-end analysis engine and integrated suite of apps.

Part I

The Modern IT Environment: Borderless, Distributed, Elastic

Hybrid IT: A Security Challenge Snapshot

The new information security challenges that cloud computing, mobility and other IT innovations 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 in 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 Google Cloud, Amazon AWS or Microsoft Azure.

Back-end
Control Panel
Front-end

The risk to this one application rests in these three different places. Security products that protect only the endpoint, or only the cloud instance, or only the on-premises server fall short. Attempting to assemble a more comprehensive solution by tying together heterogeneous products creates integration complexity, higher costs and, very likely, poor performance.

The new boundaries of your IT landscape

Perimeters were formerly contained to corporate premises, but now they extend to clouds, mobile devices, web apps, IoT sensors and even to non-computing products.

Mobile devices, non-computing appliances and IoT systems

Your perimeter reaches out to every device employees connect to public and home Wi-Fi networks: Laptops, smartphones, tablets and smartwatches. These digital travel companions contain critical confidential data and applications, and are often lost, stolen, and compromised.

Another weak link: Organizations' geographically dispersed locations, such as remote offices and retail stores. These facilities, which house PCs, point-of-sale systems and other endpoints, often have weaker physical and cyber security than larger corporate buildings.

Meanwhile, non-computing devices are connecting to your network, including copiers, printers, thermostats and even Wi-Fi enabled coffee makers in office kitchens.

Businesses are also aggressively adopting IoT and embedding sensors in myriad "things" that were formerly offline: Vehicles, HVAC systems, healthcare instruments, industrial equipment and store shelves. These diverse and dispersed endpoints now collect troves of sensitive data and transmit it back to their organizations' IT systems.

Thus, it's essential for organizations to have tools that let them monitor and strengthen the security and compliance of mobile and non-traditional endpoints, particularly because many tend to be more vulnerable to cyber attacks than standard computing devices.

Cloud computing services

Adoption of cloud computing platform and infrastructure services — PaaS and IaaS — continues growing among organizations globally. Infosec teams must protect these workloads moving from on-premises systems to public clouds. Cloud platform providers operate on a "shared responsibility" model: They protect their cloud platform, while customers are responsible for securing their data and software. Thus, customers must do security and compliance checks on public cloud deployments, as they do for their on-premises systems, including vulnerability management, web app scanning, and policy compliance. To do so, they need security tools that give them visibility into their public cloud workloads and instances.

Web apps and Dev(Sec)Ops pipelines

As organizations digitally transform operations, these innovations are primarily delivered via web apps: Internet-facing, internal and cloud-hosted web apps, as well as REST API-based web services. With these web apps, organizations simplify and automate key functions and processes for employees, customers and partners. Unfortunately, many web applications are unsafe due to latent vulnerabilities and weak configurations. Unsurprisingly, they've become a favorite vector for data breaches.

A key element for hardening web apps is the integration of security checks throughout the DevOps pipelines where software code is quickly and continuously built and deployed. When security is meshed in, this process becomes a DevSecOps pipeline, in which vulnerabilities and mis-configurations are automatically detected and fixed at every step — from the 'build' to the 'production' stages. That way, security isn't brought in at the end, delaying the CI/CD (continuous delivery / integration) of code that powers digital transformation efforts.

How can you monitor and protect this far-reaching environment?

To defend modern IT environments, you need an integrated, centralized cloud-based platform that gives you a single view of all your IT assets and their vulnerabilities and mis-configurations. You must be able to 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 gives you this holistic and comprehensive view of your threat landscape by cobbling together point products. But it will be complicated, costly and ineffective. Fortunately, such a solution 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."
>
> Senior Manager,
> Information Security

Part II

Qualys Cloud Platform

How can we do what others can’t? It’s all in our cloud-based platform. It continuously collects, assesses and correlates security, IT and compliance data of all assets everywhere — in clouds, on premises, and at mobile/remote endpoints. Qualys Cloud Platform is the complete, end-to-end security solution that gives customers a real-time, holistic view of their threat landscape for comprehensive attack prevention and immediate incident response.

Introduction

Overview of the Qualys Cloud Platform

The Qualys Cloud Platform has been architected with the goal of simplifying security by eliminating friction and making it as intuitive and automated as possible.

It's what Qualys calls "Transparent Orchestration (™)", a principle that represents the future of security, and serves as a key guiding principle and goal for Qualys.

Transparent Orchestration is reflected by the Qualys Cloud Platform's design, in particular its three main pillars: its versatile sensors; massively scalable backend; and integrated suite of cloud apps.

With its always-on sensors, the Qualys Cloud Platform gives organizations continuous, real-time visibility of all their IT assets – on-premises, at endpoints or in clouds – for comprehensive prevention, detection and response. Centrally managed and self-updating, the Qualys sensors come as physical or virtual appliances, or lightweight agents.

Meanwhile, Qualys Cloud Apps provide the tools and capabilities for all your security teams, including those in charge of:

- On-premises infrastructure
- Cloud workloads
- Endpoint devices
- DevSecOps environments
- Web apps
- IT audit and compliance

By consolidating your security stack on the centrally managed and self-updating Qualys Cloud Apps, you can keep your teams in sync. You also eliminate the plethora of siloed, heterogeneous point products that don't interoperate well, and are difficult to integrate and expensive to manage.

Qualys Cloud Platform's state-of-the-art, massively scalable back-end has robust, centralized capabilities for reporting, storage, data analysis, search indexing and asset tagging, among other functionality. A centralized, web-based, single-pane-of-glass UI gives you a complete and continuously updated view of your IT environment and its security and compliance posture.

Qualys also offers a private platform that delivers all the benefits of the Qualys Cloud Platform within the walls of your data center. The Qualys Private Cloud Platform allows organizations to store scan data locally under their control for compliance with internal policies or external regulations.

With this cloud architecture, the Qualys Cloud Platform is uniquely designed for protecting today's hybrid IT environments, including the DevOps pipelines where digital transformation projects are built and deployed.

1+ trillion
security events

3+ billion
IP scans/audits a year

28+ billion
data points indexed on elastic search clusters

99.999%
six sigma scanning accuracy

The Ideal Architecture for Securing Digital Transformation Initiatives

Qualys, a pioneer of cloud-based security and compliance since its founding in 1999, is uniquely positioned to help organizations protect their fast-paced digital transformation deployments without slowing them down.

To build security into digital transformation efforts, organizations must embed infosec processes and tools into the DevOps software development and delivery pipeline. The reason: The mobile and web apps, and web services generated by DevOps teams are the vehicles for new digital transformation initiatives.

Qualys can help your organization facilitate the availability and use of automated security tools for developers and operations staff, so that code can be scanned for vulnerabilities, misconfigurations and other security issues early and often in the software lifecycle.

Embedding security into DevOps – making it DevSecOps – will make code cleaner, and the resulting systems more secure. This approach will foster confidence in security among IT and developer teams, and will help organizations securely accelerate their digital transformation journeys.

In a recent report, 451 Research Senior Analyst Scott Crawford noted that “Qualys’ farsighted cloud strategy has given it a leg up in serving the hybrid enterprise. The company has long provided coverage for what may today be considered ‘legacy’ IT – but its cloud roots inform its strategy for tackling the IT of tomorrow.”

As businesses seek to become more agile, innovative and effective through digital transformation, legacy security approaches could become a drag on the automation, integration and speed that these new techniques depend on, according to Crawford.

“Capabilities native to these new approaches must therefore become a hallmark of an emerging generation of security technologies. Qualys’ SaaS platform is not the only asset it brings to the opportunity; its own experience in developing for the cloud informs it as to what organizations need from their forward-looking security tools.”

Since digital transformation is so closely tied to enterprises’ use of public cloud services, it’s important to highlight how Qualys helps organizations protect their IaaS and PaaS deployments.

As organizations increase their use of public cloud platforms, they encounter security and compliance threats, and cloud-specific challenges, such as:

- Lack of visibility into their cloud assets, usage and resources
- A misunderstanding of cloud providers’ shared security responsibility model

This means that organizations must maintain a continuously updated inventory of cloud workloads, and perform essential security and compliance checks on them.

Qualys provides native integrations and comprehensive security and compliance solutions for public cloud platforms, including AWS, Azure and Google Cloud, to help you:

- Identify, classify, and monitor all cloud workloads and resources for vulnerabilities
- Comply with internal and external policies
- Prioritize vulnerability remediation

- Automatically find and eradicate malware infections on your websites
- Integrate and automate security and compliance throughout your DevOps pipelines

The Qualys Cloud Platform gives organizations the five key pillars of digital transformation security:

- Visibility

It compiles a complete, continuously updated IT asset inventory, and detects changes instantly — on premises, in clouds and at remote endpoints.

- Accuracy

It centrally collects, stores and analyzes all security and compliance data, eliminating the incomplete information from siloed, fragmented point solutions.

- Scale

Its massively scalable cloud architecture protects the largest global, hybrid IT environments.

- Immediacy

Its robust back-end engines deliver instant prevention capabilities and incident response.

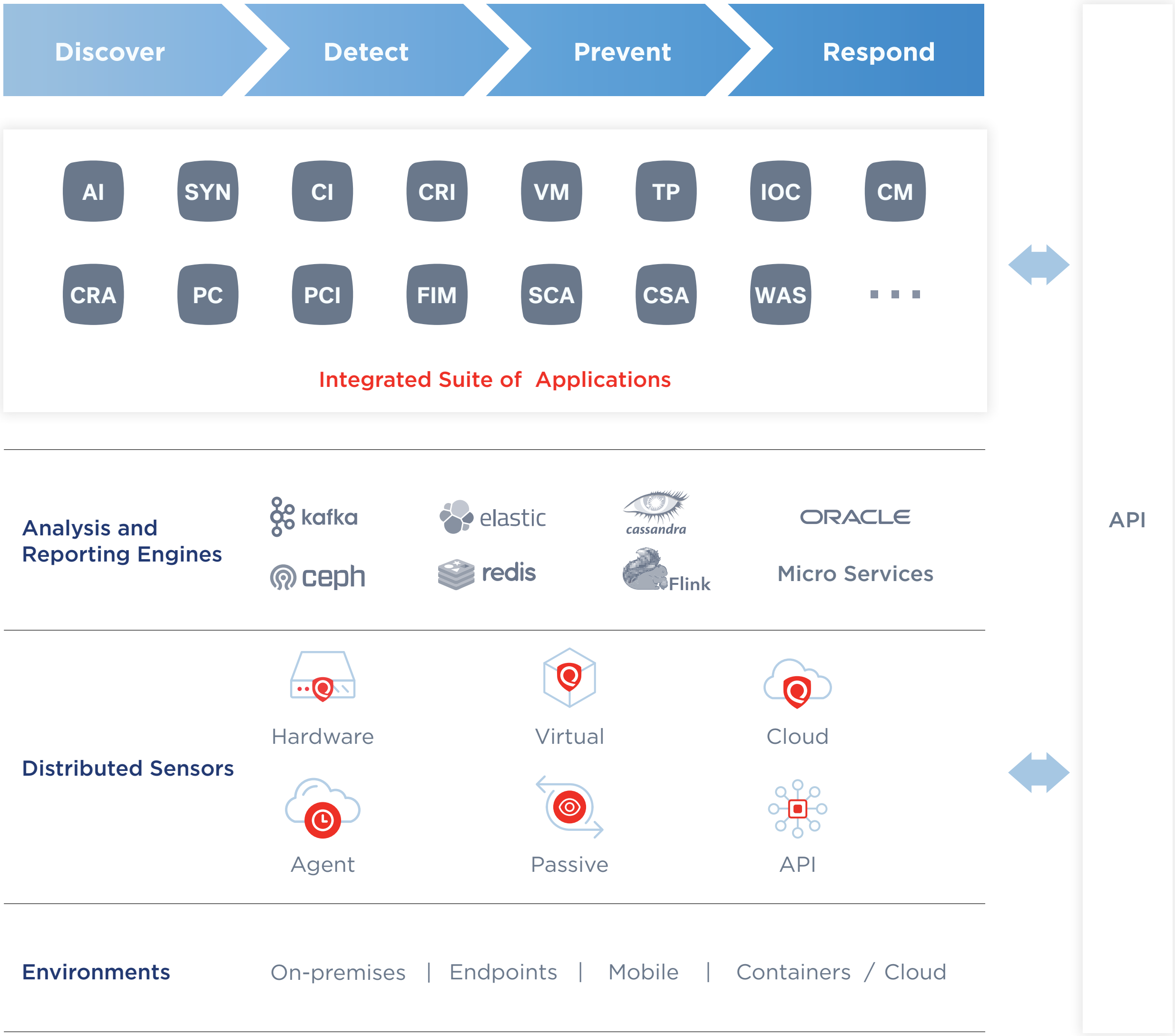
- Transparent Orchestration (™)

It provisions seamless, dynamic and automated security across the IT environment, making it friction-less and intuitive for developers and IT staff.

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.



Versatile Set of Sensors

The Qualys Cloud Platform's sensors – available as physical and virtual appliances, and as lightweight agents – are always on, remotely deployable, centrally managed and self-updating. They enable true distributed scanning and monitoring of all areas of today's hybrid IT environments, including:

- From the Internet
- Within the DMZ
- On the internal network
- On networks hosted by public cloud providers

Qualys sensors collect data from your IT environment and automatically beam it up to the Qualys Cloud Platform, which continuously analyzes and correlates the information to help you quickly and precisely identify and eliminate threats.

Cloud Agents

Works everywhere. The secret to our continuous visibility

Virtual Scanners

Software-only internal scanning, on premises or in the cloud

Scanner Appliances

On-premises hardware scanners for internal networks

Internet Scanners

Fast and efficient external scanning, on premises or in the cloud

Passive Scanners

Real-time network analysis of your data

Out-of-Band Sensors

Secure highly locked-down devices or on air-gapped networks

Cloud Connectors

Collect data from 3rd party cloud platforms and software

APIs

Collect data from 3rd parties such as threat intelligence feeds

Qualys Appliances

Qualys offers various types of scanner appliances:

- Physical appliances that scan IT assets located on your premises
- Virtual appliances that remotely scan your private cloud and virtualized environments
- Internet appliances for fast and efficient external scanning
- Cloud appliances that remotely scan your infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) instances in commercial public cloud platforms

Appliances are configured through an easy to use interface, and activated online through the Qualys web interface.

Passive Network Sensor

Passive Network Sensor (PNS) provides continuous and unobtrusive detection of all network-connected systems and their activity in real time.

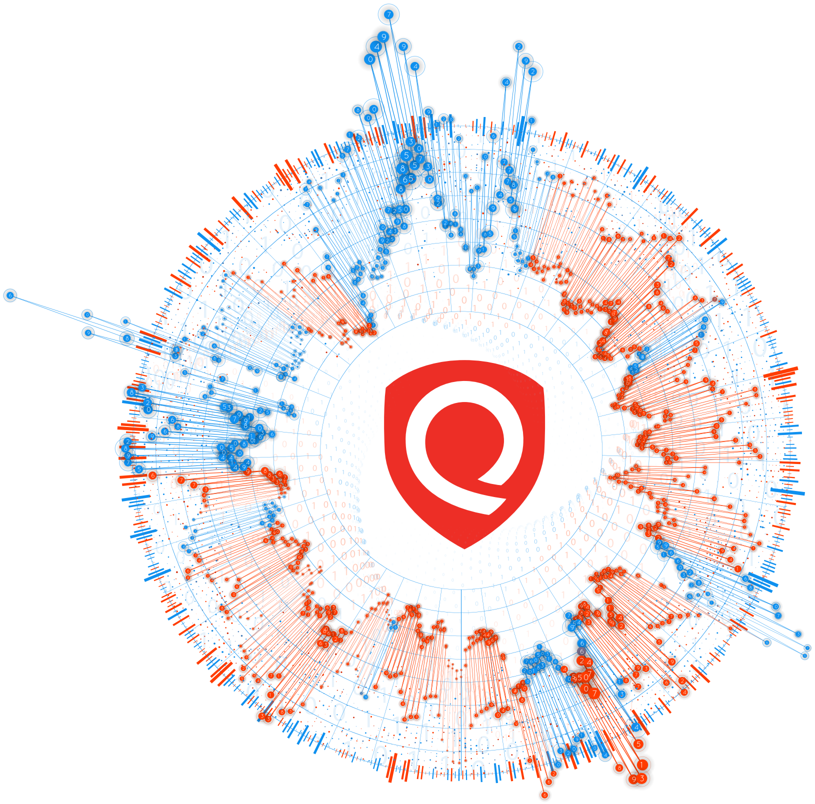
With PNS, customers can:

Eliminate blind spots: The Qualys Cloud Platform aggregates asset telemetry from PNS, Qualys scanners and Qualys Cloud Agents to provide a comprehensive, detailed and multidimensional inventory of all IT assets across hybrid infrastructures. This includes unmanaged devices such as employee-owned smartphones and rogue devices. PNS also discovers and profiles assets that can't be actively scanned nor monitored with cloud agents, such as industrial equipment, IoT systems and medical devices.

Identify suspicious traffic: PNS provides deep packet inspection to continuously analyze and detect suspicious traffic. The Qualys Cloud Platform then correlates these network anomalies to other indications of compromise.

Secure and control network access: PNS lets you respond to threats automatically by controlling access to critical resources. Network access control, informed by PNS real-time detection, autonomously protects the network by quarantining noncompliant devices based on established policies and security posture.

(Qualys PNS is scheduled for general availability in 2019.)



Qualys PNS delivers instant visibility into every asset communicating on your network.

Qualys Cloud Agent

The Qualys Cloud Agent extends security throughout your global enterprise. These lightweight agents (2MB) are remotely deployable, centrally managed, self-updating and consume minimal CPU resources.

Cloud Agents work where it's not possible or practical to do network scanning. They're our preferred method for assets like dynamic IP client machines, remote/roaming users, static and ephemeral cloud instances, and systems sensitive to external scanning.

After their initial deployment, Cloud Agents run a full configuration assessment of their host in the background and upload the collected data to the Qualys Cloud Platform for analysis. Then, as soon as changes occur, Cloud Agents push updates to the platform, ensuring you have the latest IT asset data at your fingertips immediately.

Its many benefits for securing hybrid environments include:

- No scan windows needed. It's always collecting data on assets it's installed on, even when assets are offline.
- Its constant monitoring yields faster vulnerability discovery and patch confirmation.
- No need for complex credential and firewall management. It only communicates outbound to the Qualys platform.
- It works with multiple Qualys apps, which lets security teams remove point-solution agents from assets and consolidate security tools.

Using the Cloud Agent and the multiple Qualys apps that leverage it, organizations can get a multi-dimensional view of a breached asset.

Most versatile, complete set of sensors

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

Qualys Cloud Apps

Qualys has built a comprehensive suite of security and compliance Cloud Apps that stands currently at 18 apps and continues to grow.

The Cloud Apps are self-updating, centrally managed and tightly integrated, and cover a broad swath of functionality in areas such as IT asset management, IT security, web app security and compliance monitoring.

All applications are based on the same platform, share a common UI, feed off of the same scanners and agents, access the same collected data, and leverage the same user permissions. This lowers the complexity of usage while maintaining a high level of access control throughout the organization.

A centralized, web-based, single-pane-of-glass dashboard provides a complete and continuously updated view of your IT environment. This interactive, dynamic dashboard also allows you to aggregate and correlate all of your IT, security and compliance data in one place, drill down into details, and generate reports customized for different audiences.

Often, InfoSec teams use an array of heterogeneous, point tools that don't interoperate well and are difficult and costly to maintain and integrate, making it difficult for CISOs to get a single, unified view of the organization's security and compliance posture.

By consolidating their security stacks with the Qualys Cloud Apps, organizations escape this tool-fragmentation nightmare, tear down organizational silos and keep security teams in sync, including those in charge of protecting:

- On premises infrastructure

Qualys helps secure the organization's networks and data centers with vulnerability management, continuous monitoring, configuration assessment, threat prioritization, file integrity monitoring and indication of compromise.

- Cloud infrastructure

Qualys helps ensure that the organization's VMs, cloud instances and containers are secure and compliant on public cloud platforms. Qualys has agreements and integrations with major cloud providers, so you can do asset inventory, vulnerability management, web app scanning, threat prioritization and policy compliance on workloads.

- IT audit and compliance

Qualys automates compliance and risk management tasks so your company stays on the right side of internal policies and external regulations through asset inventory, vulnerability management, configuration assessments, PCI compliance and vendor risk management.

- Endpoints

Qualys continuously discovers and monitors the growing and increasingly complex universe of networked endpoints via comprehensive asset inventory, vulnerability management, configuration assessments, threat prioritization and indication of compromise.

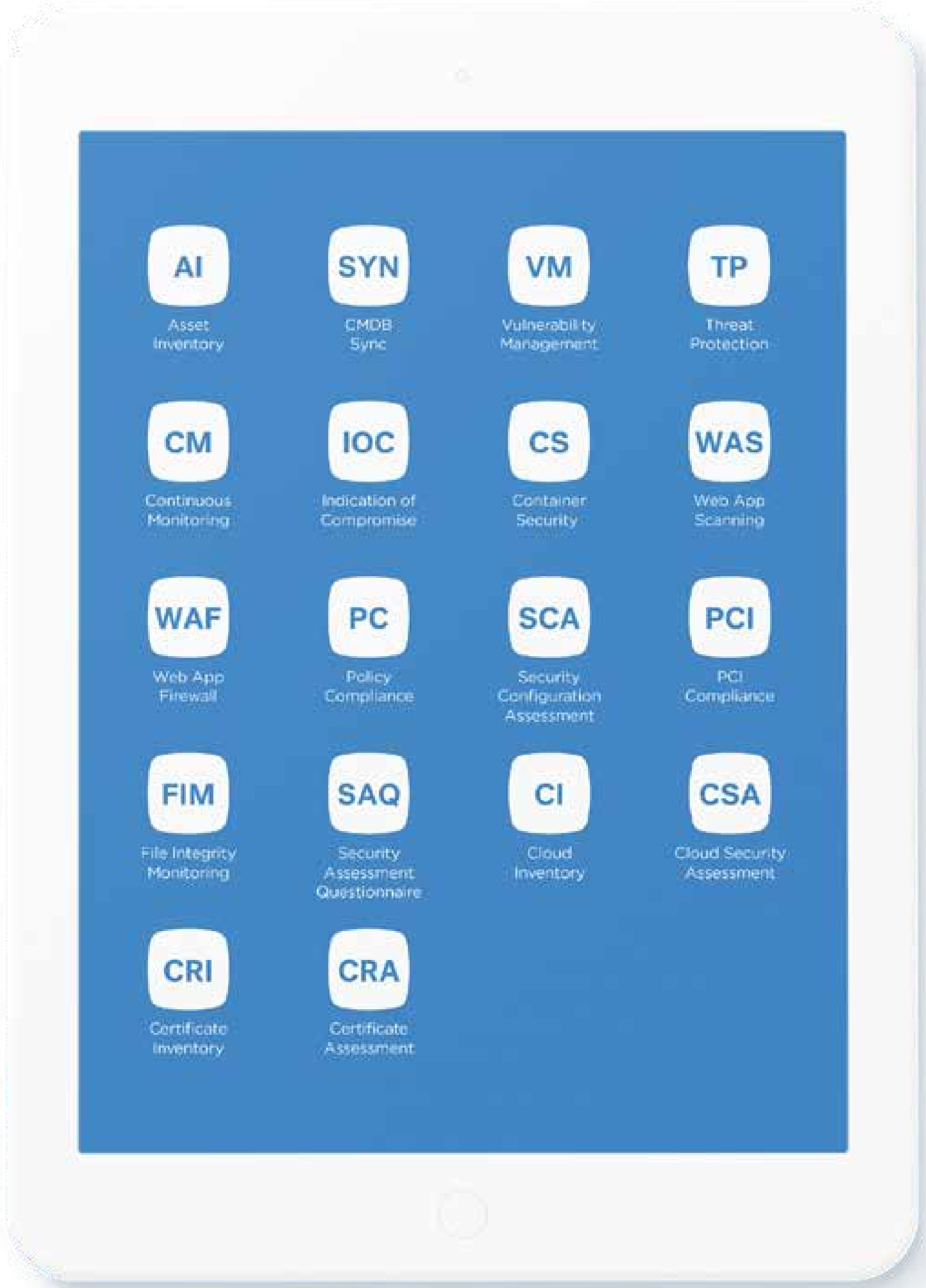
- DevSecOps and web apps

You can use Qualys to automate testing for vulnerabilities and misconfigurations in your code throughout your web app development and deployment pipeline via vulnerability management, configuration assessment, threat prioritization, web app scanning, file integrity monitoring and indication of compromise.

Integrated Cloud Apps

Your organization can use the Cloud Apps it needs, when it needs them, subscribing to one or more of them, and expand your use over time.

Many customers are using multiple Cloud Apps to develop a more complete understanding of their environment's security and compliance posture. The Qualys Cloud Platform currently provides the following Cloud Apps:



Asset Management

AI

Qualys Asset Inventory (AI)

Qualys AI gives you a complete, continuously updated inventory of all your IT assets everywhere: on premises, in clouds or at mobile endpoints. It lists assets' installed software, existing vulnerabilities and hardware details. A powerful search engine lets you do ad hoc queries and refine them using different criteria.

SYN

CMDB Sync (SYN)

This certified application synchronizes Qualys AI data with ServiceNow's Configuration Management system. Device changes are immediately transmitted to the Qualys Cloud Platform and then synchronized with ServiceNow, ending unidentified and misclassified assets, and data update delays.

CI

Cloud Inventory (CI)

Qualys CI gives you a comprehensive inventory of your public cloud workloads and infrastructure. It continuously discovers resources in your public cloud deployments and gives you a "single-pane-of-glass" view across all of them from a central control panel.

CRI

Certificate Inventory (CRI)

Qualys CRI assembles and continuously updates an inventory of your TLS/SSL digital certificates on a global scale by continuously detecting and cataloging every certificate from any Certificate Authority. It also stops expired and expiring certificates from interrupting critical business functions, and offers direct visibility of expired and expiring certificates right from the dashboard.

IT Security

VM

Vulnerability Management (VM)

Qualys VM is an industry leading and award-winning solution that automates network auditing and vulnerability management across an organization, including network discovery and mapping, asset management, vulnerability reporting and remediation tracking. Driven by our comprehensive KnowledgeBase of known vulnerabilities, Qualys VM enables cost-effective protection against vulnerabilities without substantial resource deployment.

TP

Qualys Threat Protection (TP)

With Qualys TP, you can pinpoint your most critical threats and identify what you need to remediate first. Qualys TP continuously correlates external threat information against your vulnerabilities and IT asset inventory, so you'll always know which threats pose the greatest risk to your organization at any given time.

CM

Qualys Continuous Monitoring (CM)

Built on top of Qualys VM, Qualys CM watches your network for threats and unexpected changes, before they turn into breaches. Whenever it spots an anomaly in your network, it immediately sends targeted alerts to exactly the right people for each situation and each machine. With it, you can track what happens throughout your public perimeter, internal network, and cloud environments.

IOC

Indication of Compromise (IOC)

Qualys IOC delivers threat hunting, detects suspicious activity, and confirms the presence of known and unknown malware for devices both on and off the network. From its single console, you can monitor current and historical system activity for all on-premises servers, user endpoints, and cloud instances.

CS

Container Security (CS)
Qualys CS continuously discovers, tracks and protects containers in DevOps pipelines and deployments across cloud and on-premises environments. It gives you complete visibility of container hosts by gathering comprehensive topographic information about your container projects — images, image registries, and containers spun from the images. Qualys also CS lets you scan, protect and secure running containers.

CRA

Certificate Assessment (CRA)
Qualys CRA lets you assess your digital certificates and TLS configurations by providing continuous monitoring, dynamic dashboarding and custom reporting of certificate issues and vulnerabilities. Qualys Certificate Assessment generates certificate instance grades using a straightforward methodology that allows administrators to assess often overlooked server SSL/TLS configurations without having to become SSL experts. It also identifies out-of-policy certificates with weak signatures or key length.

CSA

Cloud Security Assessment (CSA)
Qualys CSA automates continuous monitoring of your public cloud infrastructure, detects misconfigurations, malicious behavior and non-standard deployments, and provides remediation steps. Qualys CSA supports REST APIs for seamless integration with the CI/CD tool chain, providing DevSecOps teams with an up-to-date assessment of potential risks and exposure.

Compliance Monitoring

PC

Policy Compliance (PC)
Qualys PC performs automated security configuration assessments on IT systems throughout your network, helping you reduce risk and continuously comply with internal policies and external regulations. With PC, you can leverage out-of-the-box library content to fast-track your compliance assessments using industry-recommended best practices.

PCI

PCI Compliance (PCI)
Qualys PCI streamlines and automates compliance with PCI DSS requirements for protecting the collection, storage, processing and transmission of cardholder data. Qualys PCI scans all Internet-facing networks and systems with Six Sigma (99.9996%) accuracy, generates reports and provides detailed patching instructions. An auto-submission feature completes the compliance process.

FIM

File Integrity Monitoring (FIM)
Qualys FIM logs and centrally tracks file change events on common enterprise operating systems. Qualys FIM collects the critical details needed to quickly identify changes and root out activity that violates policy or is potentially malicious. Qualys FIM helps you comply with change control policy enforcement and change monitoring requirements.

SCA

Security Configuration Assessment (SCA)
A Qualys VM add-on, Qualys SCA expands your VM program with automatic assessment of IT assets' configurations using the latest Center for Internet Security (CIS) Benchmarks for operating systems, databases, applications and network devices. SCA users can automatically create downloadable reports and view dashboards.

SAQ

Security Assessment Questionnaire (SAQ)
Qualys SAQ automates and streamlines third-party and internal risk assessment processes, so you don't have to do them manually. With SAQ, you easily design surveys to assess respondents' procedural controls of IT security policies and

practices. SAQ automates the launch and monitoring of assessment campaigns, and provides tools for displaying and analyzing the data.

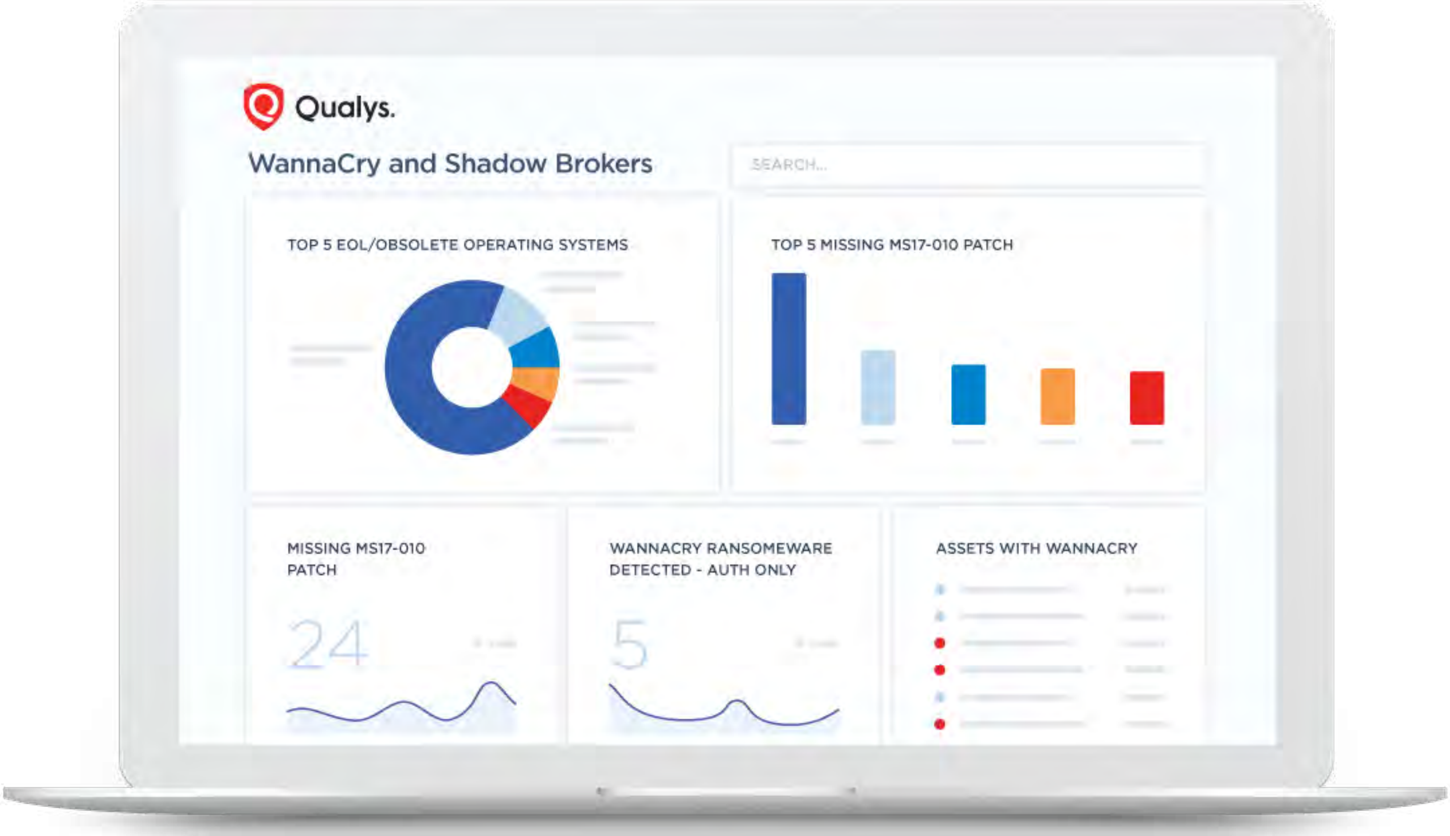
Web Application Security

Web Application Scanning (WAS)

Qualys WAS continuously discovers and catalogs web apps in your network and detects vulnerabilities and misconfigurations. Its integration with Qualys WAF provides one-click patching of web apps. With WAS, you can also insert security into DevOps environments. Qualys WAS also identifies and removes malware from websites using behavioral and static analysis.

Web Application Firewall (WAF)

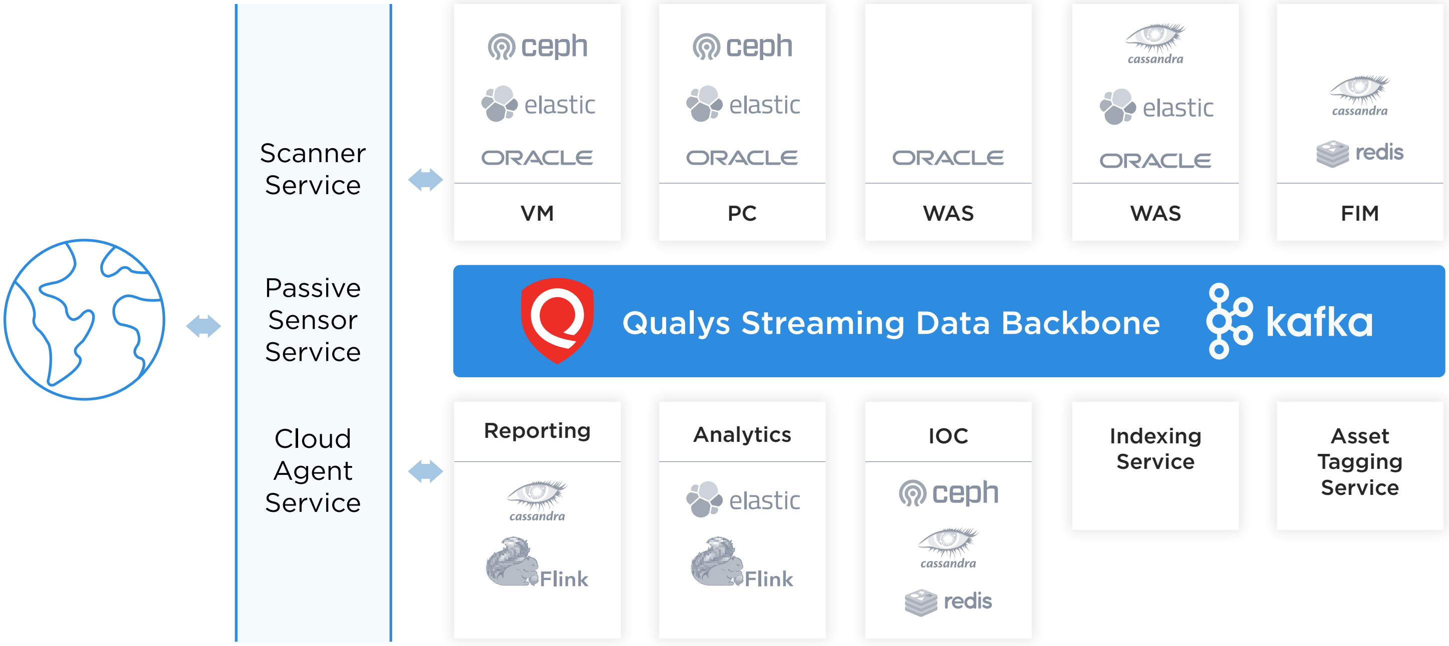
Simple, scalable and adaptive, Qualys WAF blocks attacks, and lets you control when and where your applications are accessed. Qualys WAF and Qualys WAS work together seamlessly. You scan web apps with Qualys WAS, deploy one-click virtual patches for detected vulnerabilities in WAF, and manage it all from a centralized cloud-based portal. It can be deployed in minutes.


Qualys.
WannaCry and Shadow Brokers
SEARCH...
TOP 5 EOL/OBSOLETE OPERATING SYSTEMS
TOP 5 MISSING MS17-010 PATCH
MISSING MS17-010 PATCH
24
WANNACRY RANSOMEWARE DETECTED - AUTH ONLY
5
ASSETS WITH WANNACRY

Customizable, user-defined dynamic dashboard for real-time tracking progress of WannaCry remediation alerts

BACK-END 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.

Advantages of our cloud-based architecture

- 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.

- Easy and intuitive

There's nothing to install or manage, and all services are accessible on the cloud via web interface. Qualys operates and maintains everything. The platform is always on and self-updating.

- Lower operating costs

With everything in the cloud, there are no capital expenditures, no extra human resources needed, and no infrastructure or software to buy and maintain. Qualys also gives you more control over licensing costs via its flexible, subscription-based model.

- Easy global scanning

Easily perform scans on geographically distributed and segmented networks both at the perimeter, behind the firewall, on dynamic cloud environments and endpoints.

- Seamless, flexible scaling

Qualys Cloud Platform is a scalable, end-to-end solution for all aspects of IT security. Once deployed, add new coverage, users and services as you need them. Subscription packages are tailored for organizations of all sizes. Customers can also purchase app subscriptions a la carte.

- Up-to-date resources

Qualys has the largest knowledge base of vulnerability signatures in the industry, and performs over 3 billion IP scans per year. All security updates are made in real time.

- Securely stored data

Vulnerability data is securely stored and processed on an n-tiered architecture of load-balanced servers. Our encrypted databases are physically and logically secure.

Our apps and services are delivered either via our public cloud platform, or private cloud platform

Public Cloud Platform Option

Our public cloud platform, which is multi-tenant, multi-layer, and highly-scalable, is offered from data centers in Santa Clara, California; Ashburn, Virginia; Geneva, Switzerland; Pune, India; and Amsterdam, the Netherlands.

Qualys' public cloud platform can be accessed around the clock from anywhere through a Web browser, and consistently maintains 99% availability. It's updated transparently, without interruption to users, and is only briefly taken offline once a quarter for maintenance.

Stored data is kept encrypted. Qualys encrypts each user's data uniquely, so that only the user who created the data can access it. Qualys has no insight into customer data. Qualys does not have access to the encryption key, so Qualys can't decrypt stored data.

The Qualys Cloud Platform resides behind network-based, redundant, highly-available firewalls and intrusion monitoring solutions. In addition, each host runs a localized firewall on top of the customized, hardened Linux distribution, which is unique to Qualys.

The platform is hosted in data centers subject to at least an annual SSAE 16 or industry standard alternative audit by an internationally-recognized accounting firm. All Qualys devices are located in physically secure, dedicated, locked cabinets protected by multiple-factor authentication, including biometrics.

Core services include:

- Asset Tagging and Management
- Reporting and Dashboards
- Questionnaires and Collaboration
- Remediation and Workflow
- Big Data Correlation and Analytics Engine
- Alerts and Notifications

Private Cloud Platform Option

For organizations that need to keep their security and compliance data under their control, we offer the Qualys Private Cloud Platform, which has all the features of our multi-tenant public cloud platform. The Qualys Private Cloud Platform is ideal for businesses located in countries with strict data sovereignty rules, government agencies with data possession requirements, and MSSPs that want to provide more exclusive offerings.

Available as a full server or virtual rack for large organizations, and as a standalone appliance for smaller businesses, the all-in-one devices are pre-loaded with the Qualys software and pre-configured for quick and easy deployments. All physical rack and cabling work is completed before the appliance arrives. They're remotely updated and maintained by Qualys, which even handles any necessary hardware expansion.

Qualys Subscriptions

SMB, mid-size, enterprise, consultant and MSPs, government

Qualys caters to organizations of all types and sizes with various subscription options. Offerings can be tailored and expanded to fit customer needs, with pricing based on selected Qualys Cloud Platform features, apps, scanners and agents, and on the range of monitored IT assets.

We offer subscriptions for enterprises, mid-size organizations, small businesses and government agencies. We also have a subscription for consultants and MSPs that use Qualys to provide security and compliance services to their clients.

All subscriptions include free training and support. Customers can also scan their devices and web apps an unlimited number of times, and use an unlimited number of Cloud Agents.

Let's look at each offering individually.

Qualys for Small Businesses

IT security is often a weak link at small businesses, because they lack in-house resources and knowledge in this area. With the Qualys Express Lite cloud suite of security and compliance solutions, small businesses can monitor security and compliance right from a browser. Its capabilities include continuous network monitoring, vulnerability management, threat prioritization, PCI compliance, vendor risk management, and web application scanning.

- 256 IPs for scans
- 25 web apps for scans
- 2 scanners
- 3 users

Qualys for Mid-Size Organizations

For mid-size businesses, Qualys can help simplify their IT security and lower their cost of compliance. The Qualys Express cloud suite includes capabilities for IT asset inventorying, vulnerability management, continuous network monitoring, web application scanning and firewall, threat prioritization, policy compliance including PCI, and vendor risk management.

- 5,120 IPs for scans
- 200 web apps for scans
- 5 scanners
- Unlimited users
- Remediation ticketing & tracking
- Integration with public clouds

Qualys for Enterprises

Qualys offers large organizations a complete security and compliance solution, so they slash their TCO by eliminating traditional, standalone products that have limited functionality and operate in silos.

- Unlimited IPs for scans
- Unlimited web apps for scans
- Unlimited scanners
- Unlimited users
- Remediation ticketing & tracking
- Integration with public clouds

Qualys for Consultants and MSPs

The challenges, demands and pressures faced by security consultants are intensifying, as their customers' IT infrastructures become more complex and hackers get more bold and effective.

To succeed, consultants can't just rely on their know-how and experience: They must also arm themselves with the best software tools available to do their jobs.

With its cloud-based, centrally managed Consulting Edition offering, Qualys stands apart in this market full of manual tools with limited functionality.

Consulting Edition helps consultants and MSPs offer their customers a wide range of first-class security and compliance assessment services.

- Multi-tenancy: Easily organize and manage data from your multiple clients from a central dashboard. As you conduct scans, results are directly associated with the appropriate client records. You can segment clients' unique network environments.
- Flexibility and Comprehensiveness: Offer a broad range of services, including vulnerability management, policy compliance, and web app scanning -- on premises, in clouds and at endpoints. This is made possible by Qualys' versatile sensors, including local, virtual and cloud scanners; Cloud Agents; and passive network sniffer. All processes can be automated using Qualys' APIs.
- Actionable Reporting: Create client-focused reports that show vulnerability trending and that can be exported in a variety of formats (HTML, DocX, MHT, XML, PDF, CSV). You can add your logo and personalize reports with your organization's branding.

Qualys for Government

As the government embraces digital transformation, cloud adoption is at the forefront. Securing digital efforts by identifying, detecting, and responding to cyber threats while meeting regulatory and compliance requirements is critical to this transformation. To be successful, local, state and federal agencies and the DoD require an integrated security and compliance platform, ensuring complete and continuous control of their evolving IT environments.

The FedRAMP-authorized Qualys Gov Platform provides a unified solution that agencies can deploy with ease and at scale, offering visibility of their IT assets' security and compliance status. The Qualys Gov Platform overcomes limitations of legacy enterprise security products designed for homogeneous, encapsulated environments. Instead, the Qualys Gov platform offers the scale, agility and versatility desired by advanced cyber defense practitioners that must protect today's hybrid, borderless and fast-changing IT environments.

Qualys Gov Platform highlights:

- **FedRAMP Authorized and CDM Approved**: Qualys Gov Platform obtained FedRAMP Authorization to Operate (ATO) in 2016, and is on the Approved Products List of the General Services Administration's CDM program.
- **Deployment Flexibility**: For agencies with strict data storage requirements, Qualys' Private Cloud Platform (PCP) option provides all Qualys Gov Platform benefits within your datacenter, letting you store data under your control.
- **Custom Templates for Federal Agencies**: Qualys Cloud Apps offer multiple out-of-the-box templates, capabilities and pre-built content designed to streamline compliance with federally mandated regulations and policies.
- **End-to-End Security Platform**: Fully mapped to the NIST Cybersecurity Framework, Qualys Gov Platform helps your organization from identification and detection, to protection and response.

Qualys Community Edition

To help small organizations tackle today's security and compliance challenges, Qualys offers the Qualys Community Edition, a free version of its platform. With Qualys Community Edition, small businesses can leverage the accuracy and reliability of Qualys Cloud Platform to discover IT assets and vulnerabilities, identify compliance gaps and get detailed reports.

Using Qualys agents and scanners, this community edition provides asset discovery, vulnerability assessment, configuration assessment, web app scanning, and inventory of public cloud workloads.

Via the platform's interactive, customizable and dynamic dashboard, Qualys Community Edition gives small organizations a unified, streamlined view of the assets and web apps being monitored.

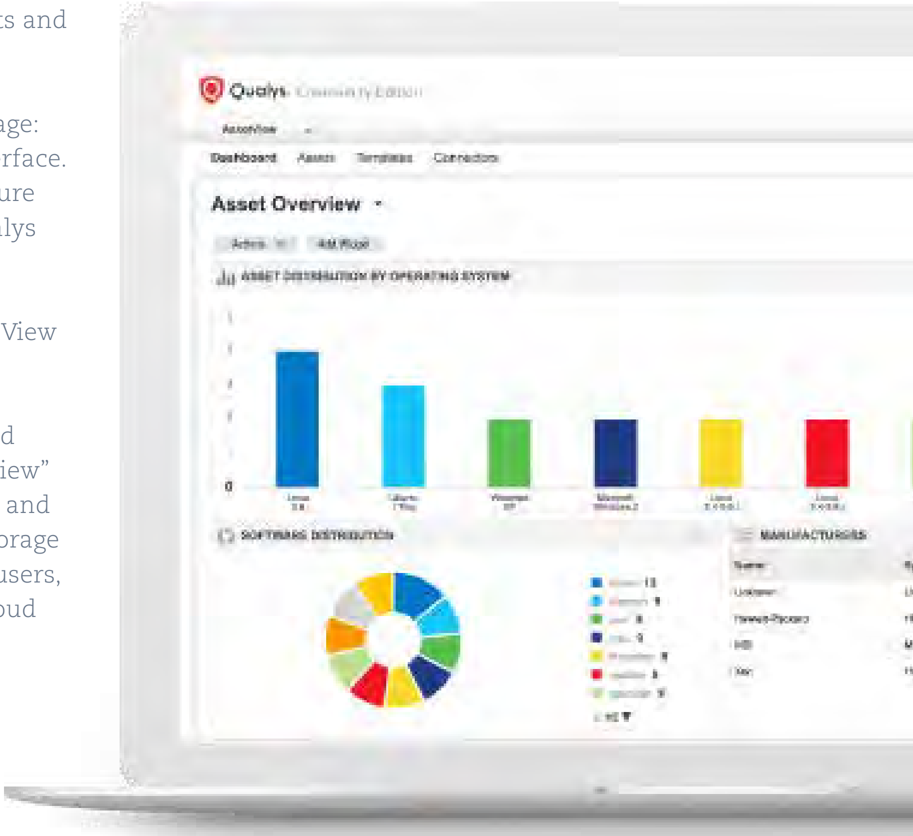
There's nothing for them to install, maintain or manage: All services are in the cloud, accessible via a web interface. Qualys Community Edition scans their IT infrastructure as well as web applications against the complete Qualys Knowledgebase of vulnerabilities.

Qualys Community Edition comes with Qualys CloudView and Qualys CertView.

CloudView lets organizations see all their public cloud assets and resources from a central, "single pane of view" interface. It continuously discovers and tracks assets and resources such as instances and virtual machines, storage buckets, databases, security groups, ACLs, ELBs, and users, across all regions, multiple accounts and multiple cloud platforms.

CertView lets organizations take back control of their Internet-facing certificates by inventorying and assessing them. It gives you visibility into all of your Internet-facing certificates and SSL/TLS configurations, and lets you centrally control and visualize prioritization of certificate and configuration remediation. Customizable dashboards with highly configurable widgets help you see your certificate status, grade information and vulnerability data.

CloudView and CertView are also available as stand-alone free apps outside of the Community Edition offering.



qualys.com/communityedition

COMPREHENSIVE TRAINING AND SUPPORT

Qualys is 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 Foster 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.

Part III

Customers

Customer Base

The best testament to the quality of our products is our customer base. Qualys has more than 10,300 customers from all major vertical industries in over 130 countries. We have a majority of the Forbes Global 100 and Fortune 100 as customers.

9 of the top 10 in **Software**

8 of the top 10 in **Consumer Discretionary**

8 of the top 10 in **Consumer Staples**

8 of the top 10 in **Major Banks**

8 of the top 10 in **Technology**

8 of the top 10 in **Telecommunications**

7 of the top 10 in **Healthcare**

6 of the top 10 in **Industrial & Materials**

5 of the top 10 in **Insurance**

ADP
DAIMLER
Agilent
Authorized Distributor
LOCKHEED MARTIN
GM
AVAYA
THE HOME DEPOT
BASF
We create chemistry
NISSAN
bp
accenture
Deloitte.
DU PONT
Lilly
DOW JONES
WB
VISA
cisco
hp
THOMSON REUTERS
EY
SYBASE
Goldman Sachs
SOCIETE GENERALE
KPMG
pwc
Bank of America
ally
ORACLE
STARZ
intuit.
starwood
Hotels and Resorts
Ogilvy
viacom
Symantec
STAPLES
MORNINGSTAR
amazon
kpn
TOSHIBA
VERISIGN
gsk
CATERPILLAR
Russell Investments
WILLIAMS SONOMA

Qualys also has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, AT&T, HPE, BT, Deutsche Telekom, HCL Technologies, IBM, Infosys, NTT, Verizon and Wipro.

Geisinger Finds Cure in Continuous Security Monitoring

Geisinger

Geisinger Health System uses Qualys Cloud Platform's, Vulnerability Management, PCI, Web Application Scanning and Cloud Agent 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."

Cloud Agent Boosts Vulnerability Detection at Synovus

SYNOVUS®

The Qualys Cloud Agent is 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 prescheduled 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.

Capital One Builds Security Into DevOps

Capital One has embedded automated security checks into its DevOps pipeline with the help of Qualys, dramatically accelerating the assessment of vulnerabilities and mis-configurations in its virtual machine images and containers.

As a result, the code created in the DevOps pipeline is certified as secure and released to production without unnecessary delays. This allows Capital One to consistently boost its business across the board by quickly and continuously improving its web properties, mobile apps, online services and digital offerings.

"This has provided a huge benefit to the entire company," said Emmanuel Enaohwo, Capital One's Senior Manager for Vulnerability/Configuration Management.

Building a secure AMI bakery

Initially, Capital One's process for certifying the security of Amazon Machine Images (AMIs) was manual and slow, taking up to two weeks, as the DevOps and security teams got on a "fix / find / verify" loop.

To shorten this process, the DevOps team was given API access to the security team's Qualys vulnerability management and policy compliance tools.

This allowed developers to run scans themselves, get reports, remediate and re-scan as needed, without involving the security team. This shortened the process to under 24 hours.

Capital One also seeds the Qualys Cloud Agent on every AMI deployed to production, so it's alerted immediately about newly-discovered security and compliance issues on live instances.

With the Cloud Agent on almost every AMI passing through its DevOps "bakery", Capital One achieved 95% assessment coverage of its IP addresses.

The agent has boosted accuracy of detection of vulnerabilities and mis-configurations, slashing false positives, and quickening scan data availability.

"All these KPIs are met because of the integration with DevOps using the Qualys Cloud Agent and APIs," he said.

Securing containers

Capital One uses Docker containers to add speed and flexibility to its application development and delivery.

To protect these environments, Capital One chose Qualys Container Security (CS), which provides continuous discovery and tracking of containers in DevOps pipelines.

Capital One uses Qualys CS's plug-in for the Jenkins CI/CD tool, so DevOps teams can scan and fix container images themselves.

Part IV

The future

A Peek at What's Coming

The Qualys Cloud Platform will continue to grow in scope as we push ahead of competitors. New products that are in the works include cloud apps to manage patches and digital certificates.

Also in the pipeline: a mobile security offering that will include Cloud Agents for iOS, Android & Windows Mobile, EMM (enterprise mobility management) capabilities, as well as asset inventory, vulnerability management, threat detection and policy compliance and enforcement.

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: Building security seamlessly into hybrid IT environments to enable the digital transformation.

Qualys.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 10,300 customers in more than 130 countries, including a majority of each of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and consolidate their security and compliance solutions in a single platform and build security into digital transformation initiatives for greater agility, better business outcomes and substantial cost savings. The Qualys Cloud Platform and its integrated Cloud Apps deliver businesses critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance and protection for IT systems and web applications on premises, on endpoints and elastic clouds. Founded in 1999 as one of the first SaaS security companies, Qualys has established strategic partnerships with leading managed service providers and consulting organizations

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

919 E Hillsdale Blvd, 4th Floor Foster City, CA 94404 USA
T: 1 (800) 745 4355,
info@qualys.com