Qualys Cloud Platform Service Description

Qualys Cloud Services Overview.

Qualys provides a multi-tenant shared platform ("Platform" or "Shared Platform") and integrated suite of security services ("Qualys Cloud Platform" or "Cloud Services") delivered via the "cloud" that enable organizations to simplify the process and reduce the cost of securing their IT assets and achieving compliance with internal policies and external regulations. Qualys solutions further help organizations to identify IP assets and web applications, collect and analyze large amounts of IT security data, discover and prioritize vulnerabilities, recommend remediation actions and verify the implementation of such actions.

Platform Features:

- The Web User Interface provides access to the Qualys Cloud Platform anytime, anywhere. From a standard web browser users can launch scans, examine vulnerability trends, access fix information, and track vulnerability tickets.
- Centralized Management. The Qualys Cloud Platform provides central management with a Web-based application that allows administrators to create accounts and manage all the aspects of accounts. Larger organizations may have accounts that fall along organizational lines, geographic lines, etc. Each account can share scan results, email alert notification with others, and report based on IP groups, which also may be divided along organizational or geographic lines. Qualys also supports multiple users and Role Based Access Control (RBAC) within accounts. Administrators can limit or grant capabilities per user to conduct scans, create maps, scan IP addresses or groups of addresses, view reports, create reports, create template reports, etc.
- Asset Tagging and Management is a patent pending technology that enables customers to easily identify, categorize, and manage large numbers of assets and automate the process of inventory management and hierarchical organization of IT assets.
- Reporting Dashboards is a configurable reporting engine that provides customers with reports and dashboards based on their roles and privileges.
- Questionnaires and Collaboration is a configurable workflow engine that enables customers to easily build questionnaires and capture existing business processes and workflows to evaluate controls and gather evidence to validate and document compliance. With it, customers can centralize and automate the gathering of risk data, compliance information, and evidence files from employees, partners, vendors, and other subject matter experts.
- Remediation and Workflow is an integrated workflow engine that allows customers to automatically generate help desk tickets (for internal compliance) for remediation and to manage compliance exceptions based on customer-defined policies, enabling subsequent review, commentary, tracking and escalation. This engine automatically distributes remediation tasks to IT administrators upon scan completion, tracks remediation progress and closes open tickets once patches are applied and remediation is verified by subsequent scans.
- Big Data Correlation and Analytics Engine provides capabilities for indexing, searching and correlating large amounts of security compliance data with other security incidents and third-party security intelligence data. Embedded workflows enable customers to quickly assess risk and access information for remediation, incident analysis and forensic investigations.

- Alerts and Notification creates email notifications to alert customers to new vulnerabilities, malware infections, scan completion, open trouble tickets and system updates.
    - **Filter by Category** – Select a category (Certificate, Host, Vulnerability, etc.) and see all alerts that are configured and applicable within your environment.
    - **Filter by Date** – Enter a date range by selecting start and end dates to see all alerts generated within those dates. Filtering the alerts using a date or range allows you to set a baseline and monitor your security trend/posture daily.
- Qualys KnowlegeBase is a proprietary repository and database of known vulnerabilities and compliance controls for a wide range of devices, technologies, and applications that power our security and compliance scanning technology. Qualys updates the Knowledgebase daily with signatures for new vulnerabilities, control checks, and validated fixes and improvements. The Qualys Knowledgebase is CVE (Common Vulnerabilities and Exposures) compliant.
- Inference Based Scanning. Qualys' core scanning technology is Inference Based Scanning, which differs considerably from conventional scanning technologies. Conventional scanning works by picking a tree of related vulnerabilities, usually grouped by host OS, and trying each of the exploits within that tree. The Inference-Based Scanning engine, by contrast, takes an un-trusted approach. It begins by creating an inventory of the operating system, protocols, ports and services of the machine being tested. Then it uses this inventory to seed a Qualys-developed vulnerability expert system, which chooses the appropriate set of vulnerabilities to test and interprets the results based on the configuration detected by the inventory. Due to the nature of scanning and vulnerabilities it uncovers in systems and applications, Qualys recommends that Customers first perform backups of all data contained in or available through the assets or devices prior to performing scans.
- Managed Intranet Scanners can be provided as physical hardware or downloaded as virtualized scanner images on customer's internal networks to securely conduct internal scans. Scanners are provided on an annual subscription basis and managed by Qualys and are designed to self-update daily in a transparent manner using Qualys' automated and proprietary scan management technology.
- Application Program Interfaces, or ("APIs"), provides customers and third parties the ability to embed Qualys technology into their applications to better enable those applications to integrate with the Platform. The API programmatically exposes core Services capabilities, including scan, map, scheduler, and preferences. The API allows users to access and query the Platform and receive Scan Data, permitting the user to customize vulnerability assessment audits and integrate them more tightly with other security processes.

Platform Components

Security and Data Centers

Qualys' Security Operations Centers (SOCs) offer secure storage and processing of vulnerability data on an n-tiered architecture of load-balanced application servers. High availability, continuously monitored data centers host databases with physical and logical security measures and encrypted data storage.

The Qualys Cloud Platform Security Operations Center and Web service infrastructure are designed with multiple layers of data security to protect customers' vulnerability information. Qualys has implemented many security controls to protect the data from the physical layer through the

application layer.

- The Qualys Cloud Platform service is hosted in colocation datacenters with extensive physical security and environmental controls. Each colocation datacenter has successfully completed an SSAE-16 audit or holds an ISO 27001 certification for the physical security and environmental controls. Qualys reviews the results of these audits as part of Qualys' third party risk management program.
- Within the colocation datacenter, the Qualys Cloud Platform is housed in a cage that is dedicated to Qualys. Strong access controls protect physical access to the cage.
- Qualys Services are protected by IPS/IDS appliances, network-based firewall appliances, web security appliances and file integrity monitoring.
- The Qualys Intranet Scanner appliance runs a hardened Linux operating system with no listening services, and communicates back to datacenter using SSL.
- User interaction with Qualys Cloud Platform requires strong-crypto HTTPS (TLSv1.2 with 256-bit ciphers at least) connections from the user's Web Browser to the Qualys Cloud Platform.

Qualys currently operates Qualys Cloud Platform Security Operations Centers in six locations: Santa Clara, California, USA, Seattle, Washington, USA, Ashburn, Virginia USA, Pune, India, Amsterdam, Netherlands and Geneva Switzerland.

Data Confidentiality

As described above the Qualys Services are provided from a shared multi-tenant platform. Qualys uses a variety of controls to maintain confidentiality of subscription data between customers on the multi-tenant platform.

The Qualys Service Platform prevents disclosure of data from one subscription to another through the following controls:

- Qualys uses access control to ensure that users from one subscription cannot access data from another subscription. Authorization checks are performed to ensure that a user request for specific subscription data is valid.
- Application-specific controls:
  - *Vulnerability Management (VM) & Continuous Monitoring (CM)* - Qualys uses encryption as the primary technical control to mitigate the risk of inter-tenant access to scan result data. Qualys VM uses a unique symmetric encryption key per subscription with the AES-128 encryption algorithm. Scan data is encrypted using AES-128 before it is pushed into the Oracle database. Users can choose to allow Qualys to share encryption keys (to use for data recovery process) or maintain their own symmetric key that is used to decrypt the VM scan result data.
  - *Policy Compliance (PC) & Web Application Scanning (WAS)* - Qualys uses the Oracle advanced security feature Virtual Private Database (VPD) as the primary technical control to mitigate the risk of inter-tenant access to scan result data. VPD is a well-documented feature of Oracle, and additional information is available upon request.

Backup and Data Retention

Qualys retains periodic archive copies of the Qualys Cloud Platform database for operational reasons, to be able to restore databases for disaster recovery and troubleshooting purposes. The backups are

performed to online backup system and to an identical standby server. In addition to the online backup system on the standby server, Qualys also uses encrypted backup tape media to help ensure disaster recovery capabilities. Tape backup schedules include a weekly full backup and daily incremental backups onto encrypted tape media with secure offsite storage.

Securing "Scan Data" obtained via the Services and account related information is stored within the Platform database located in Qualys' secure datacenters. By default, Scan Data is deleted after six (6) months, but scan data retention periods can be configured by subscription managers and the Scan Data can be retained indefinitely so long as the Agreement, the Service and subscription remain active within Supplier' systems. When Scan Data is scheduled for deletion by either the default period referenced previously, or deleted manually by Customer, the Scan Data will remain active in a standby and backup database for up to (1) one week. A copy of the backup database is recorded onto encrypted tape and stored securely offsite for disaster recovery purposes for up to thirteen (13) months. Customer's archived Scan Data is aggregated with all of the data of all of Qualys' customers on the multi-tenant Cloud Platform and cannot be selectively purged or restored from encrypted backup tapes for an individual subscription.

Upon termination of the Agreement, Qualys will automatically delete all Customer Scan Data within 13 months of termination. Customers can request that Qualys delete all online subscription data within one month. Subscription data will remain on encrypted backup tapes for up to one year.

Username and Passwords

Upon the Service Commencement, described further below, Customer will receive a user name and password for accessing the Platform. Qualys generates Customer's password in encrypted form and only Customer has access to password. Customers are responsible for keeping its user name and password(s) confidential. Customer shall notify Qualys immediately upon learning of any unauthorized use of Customer's user name or password. Until Customer notifies Qualys of any unauthorized use of Customer's user name or password, Customer will be responsible for all activities and charges incurred using Customer's user name and password.

Disaster Recovery (DR)

Qualys currently operates four Qualys Cloud Platform shared sites: two platforms located in a data center in Santa Clara, California, one platform in Seattle Washington, one platform in Ashburn, Virginia and one platform in a Geneva, Switzerland, which is the European data center. Qualys does not replicate, copy, or move subscriptions between the Santa Clara, Seattle, Ashburn or Geneva platforms. The three platforms in Santa Clara, California, Seattle, Washington and Geneva, Switzerland are completely independent of each other. All Qualys Cloud Platform shared sites are designed as active sites.

Qualys performs daily and weekly incremental backups and monthly full backups of all data, and the encrypted backup tapes are stored off site in a secure facility.

In the event of a disaster impacting the availability of the Santa Clara or Seattle facilities, subscriptions from the Qualys Cloud Platforms would be operated utilizing the Ashburn site until the Santa Clara or Seattle facility could be reactivated. The Santa Clara and Seattle sites and Ashburn site are designed for data replication between the US sites, enabling the capability to provide a greatly reduced recovery time objective (RTO), and improved recovery point objective (RPO) in the event of a site disabling disaster.

Service Descriptions

Qualys Cloud Services enable Customers to subscribe to one or more security and compliance solutions based on their initial needs and expand their subscriptions over time to new areas within the organization or to additional Qualys Cloud Services. The Qualys Cloud Services are further described below.

- Asset Inventory (AI) - Asset Inventory constantly gathers information on all assets, listing installed software, existing vulnerabilities and hardware details. Clicking on an asset record lets you see all the details Asset Inventory has collected about it. A powerful search engine lets you do ad hoc queries and refine them using different criteria.
- CMDB Sync (SYN) - Qualys SYN complements ServiceNow CMDB with detailed data on new and changed IT assets. The data comes from Qualys' Asset Inventory application which leverages Qualys' highly distributed and scalable cloud platform, and various data collection tools, including Qualys' groundbreaking Cloud Agents, to compile and continually update a full inventory of your IT assets everywhere: on premises, in elastic clouds and mobile endpoints.
- 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.
- Threat Protection (TP)– New vulnerabilities are disclosed every day, amounting to thousands per year. Qualys recognizes not all vulnerabilities are created equal. Qualys Threat Protection is a cloud-based solution that helps IT professionals like you automatically prioritize the vulnerabilities that pose the greatest risk to your organization. How? By correlating active threats against your vulnerabilities.
- Continuous Monitoring (CM) – Built on top of Qualys Vulnerability Management, Qualys Continuous Monitoring (CM) is a next-generation cloud service that 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, informative 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 – anywhere in the world. You never know when and where an attack is coming, but you can always know you'll be ready.
- Indication of Compromise (IOC) - Qualys IOC (currently in Beta) uses the Cloud Agent's non-intrusive data collection and delta processing techniques to transparently capture endpoint activity information from assets on and off the network in a way that is more performant than other solutions' query-based approaches or distributed data collectors.
- Web Application Scanning (WAS) – Qualys WAS uses the scalability of our cloud platform to allow organizations to discover, catalog and scan all an organization's web applications. Qualys WAS scans and analyzes custom web applications and identifies vulnerabilities that threaten underlying databases or bypass application access controls. It utilizes behavioral and static analysis to detect malware and monitor web sites on an ongoing basis.
    - *Malware Detection (MD)* –Detailed malware infection reports accompany infected code for remediation. A central dashboard displays scan activity, infected pages and malware infection trends, and lets users initiate actions directly from its interface. Malware detection functionality is provided via an optional add-on.

- Web Application Firewall (WAF) – Qualys WAF delivers enterprise-grade web application security without the costs, footprint, and complexity associated with appliance-based web application firewall solutions. It protects web applications from attack vectors by enhancing default web application configurations and virtual patching. Qualys WAF also improves web site performance by reducing page load times and optimizing bandwidth, leveraging our global network of web caches.
- Policy Compliance (PC) – Qualys PC enables organizations to analyze and collect configuration and access control information from their networked devices and web applications and automatically maps this information to internal policies and external regulations in order to document compliance. Qualys PC is fully automated and helps reduce the cost of compliance without requiring the use of software agents.
  - SCAP Compliance Audit. – Safely and accurately scan your computers for potential security risks and experience what the award-winning Qualys security and compliance suite can do for you. The SCAP Compliance Audit is powered by Qualys FreeScan, a free security tool that may be used to perform up to ten (10) unique security scans of business networks, computers and applications.
- PCI Compliance (PCI) – Qualys PCI can provide organizations storing cardholder data a cost-effective and highly automated solution to verify and document compliance with PCI DSS. Qualys PCI allows merchants to complete the annual PCI Self-Assessment Questionnaire, as well as performing vulnerability scanning for quarterly PCI audits and web application security.
- File Integrity Monitoring (FIM) –Deciding what to monitor is a challenge for most security teams, so FIM comes with out-of-the-box profiles based on industry best practices and vendor-recommended guidelines for common compliance and audit requirements, including PCI mandates.
- Security Configuration Assessment (SCA) - Qualys SCA is an add-on for Qualys Vulnerability Management that lets you assess, report, monitor and remediate security-related configuration issues based on the Center for Internet Security (CIS) benchmark. It supports the latest out-of-the-box CIS benchmark releases of operating systems, databases, applications and network devices.
- Security Assessment Questionnaire (SAQ) – Qualys Security Assessment Questionnaire is a cloud-based service that enables you to collect and analyze information about your business easily, quickly, and without reinventing the wheel. With this service, you can expand the scope of risk and compliance data beyond technical vulnerabilities to verify that third-party vendors are compliant with emerging regulatory requirements. By automating a traditionally manual process, Qualys Security Assessment Questionnaire frees you from unreliable and labor-intensive approaches such as email and spreadsheets and optimizes the accuracy of your audit results.
- Qualys Cloud Agent. – 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. Cloud Agents collect data from across your entire infrastructure, and consolidate it in the Qualys Cloud Platform for you to view.
  - *Cloud Agent for Vulnerability Management (VM)*. Cloud Agent for VM eliminates the need for establishing scanning windows or integrating with credential vaults for gaining access to systems – or to know where an asset resides. With agent based vulnerability assessment, you will be able to provide 100 percent coverage of your installed infrastructure. With accurate,

instantly updated information from the Cloud Agent, you will always know what vulnerabilities and configuration issues exist on difficult-to-assess targets.

- *Cloud Agent for Policy Compliance (PC)*. Cloud Agent for Policy Compliance turns Qualys' PC offering into a real-time compliance assessment solution. Now you can continuously evaluate configurations of all relevant assets (including mobile and virtual) against standards and benchmarks such as PCI-DSS, CIS, ISO, HIPAA and many others.
- *Cloud Agent for Elastic Virtual Cloud Environments*. Cloud Agent greatly simplifies asset discovery, tracking, security and compliance monitoring in dynamic cloud environments like Amazon EC2 and Microsoft Azure. Visibility is enabled by embedding the agent into master images of your cloud servers.

- Qualys API. – The Qualys API allows third parties to integrate their own applications with Qualys cloud security and compliance solutions using an extensible XML interface. The API functions described in this guide are available to customers with Qualys Vulnerability Management (VM) and Policy Compliance (PC).
- Zero-Day Risk Analyzer. – This new service is delivered as part of the QualysGuard® Cloud Platform and it includes Verisign's iDefense zero-day vulnerabilities and global threats. This service from Qualys allows customers to analyze zero-day threats and estimate their impact on their assets and critical systems based on information collected from previous scan results. It provides the following capabilities to customers:
  - Latest Information and signatures for iDefense exclusive zero-day threats
  - Customizable alerting and email notifications on new zero-days and critical threats that could impact corporate assets
  - Actionable data with estimates about what systems are at risk using existing asset information from previous scans
  - Risk modeling to help determine the benefit of mitigating actions on exposed systems

Service Commencement

Customers must first enroll online via the web and complete an online registration. Upon completion of the registration, Customer will receive an email activation email from Qualys Support establishing the date the subscription starts ("Subscription Start Date") and login credentials to begin utilizing the Qualys Cloud Platform subscription.

Modification of Services by Qualys.

Qualys may modify this Service Description upon sixty (60) days prior notice. If such modification materially decreases the functionality of the Cloud Services, Customer may terminate the Cloud Services (without penalty or termination fees) by written notice within thirty (30) days following receipt of Qualys' notice.

Technical Support and Training

Qualys offers Customers online and in person training free of charge to all Customers as part of our Cloud Services offerings. These resources can be found at Qualys Training & Support website: http://www.qualys.com/training. Qualys also offers 24x7 technical support via phone and email. Details can be found at http://www.qualys.com/support.