Qualys Management Service Descriptions

Version: 3.0, 2021-01-24

Confidentiality: PUBLIC

Qualys
Continuous Security

FORESIGHT®
CYBER

TABLE OF CONTENTS

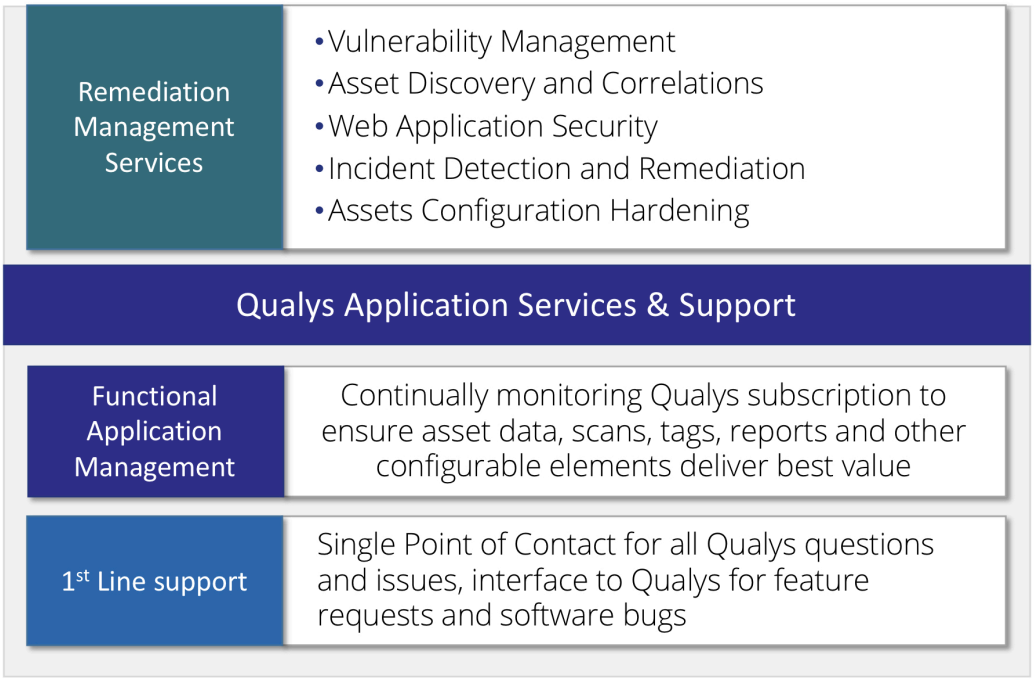
1 INTRODUCTION

Our experts have been using Qualys security platform since 2001 as our preferred scanning and threat intelligence tool.

As part of the service, we setup and manage a new or an existing Qualys installation. This includes identifying all assets of various types within your environment, followed by detailed analysis of detected vulnerabilities, misconfigurations, the production of high-level management reports, and follow-up advice on the optimum course of action to remediate identified risks.

Service and their packages

We recognise that some organisations will want to benefit from our full Qualys services portfolio while some will use their in-house Security Operations capability in relevant domains where Qualys operates.



That is why we have split our Qualys service portfolio divided into the Application management and the Remediation management services respectively.

Table 1 - Overview of Foresight Cyber Qualys services

Service activities	Application management	Remediation management
Services applicable to all Qualys modules		
1st Line support & Troubleshooting	✓	
Monitoring of Qualys activity events and licenses	✓	
Management of Scans, Qualys agents and Qualys appliances	✓	
Asset discovery (hosts and websites), and asset deduplications	✓	
Asset correlation and updates with AD, Azure AD and ServiceNow!	✓	
Asset correlation analysis with other asset sources	On-request	
Asset tags taxonomy management and Cloud tag sync	✓	
Users, roles, and access management	✓	
Management of Qualys Reports & Dashboards	✓	
Foresight Cyber Reports & Dashboards		✓
Remediation management and escalations (all modules)		✓
Educational sessions with stakeholders (IT, developers, etc)	Oon-request and charged per our rates	
Vulnerability Management (VM)		
Vulnerability scanning management	✓	
Remediation policy management (Qualys built in)	✓	
Vulnerability management service		✓
Patch management service		✓
Policy Compliance and Security Configuration Compliance (PC & SCA)		
Policy management	✓	
Compliance scanning management	✓	
Compliance risk assessments		✓
Policy compliance remediation service		✓
Cloud View and Cloud Security Assessment (CSA)		
Management of Cloud connectors	✓	
Remediation management of Cloud security risks		✓
Web Application Security (WAS & MDS)		
Management of customer Web Applications	✓	
Remediation management of web security vulnerabilities		✓
Advanced discovery of web sites and applications		✓
File Integrity Monitoring & Endpoint Detection and Response (FIM & EDR)		
Management of File Integrity Monitoring Profiles	✓	
Investigation of Alerts generated by FIM		✓
Management of Extended Detection and Response Profiles	✓	
Investigation of Alerts generated by XDR		✓

2 QUALYS APPLICATION MANAGEMENT

2.1.1 Services applicable to any module

The following services are included for any of licensed modules and are part of the Application management.

a) 1st Line support – clients' teams can use our Qualys service to ask questions how to get the best value out of Qualys investment.

   Troubleshooting - we will always strive to provide the best support possible: however, on occasion, we may need to revert to the vendor (Qualys) for 3rd line specialist support for troubleshooting and error reporting. In those cases, we will fully manage the support cases and strive for quick resolution.

   SLA: Request ticket created on receipt. Normal response time: 2 business days.

b) Monitoring of Qualys activity events – downloading Qualys events into our SIEM and monitoring for security events

   Licence monitoring – monitoring of free and used licenses in all applicable modules and warning of licence count reaching agreed threshold

   SLA: Daily download of events and licences. Automated review by Foresight Cyber Platform on download and alerting per triggered events and alert if licence goes above 80%.

c) Management of Qualys Appliances – installation and monitoring of new appliances, troubleshooting of failed connections and removal of decommissioned appliances from the Qualys subscription. This area applies to virtual and physical units alike, both in active and passive scanner modes.

   SLA: Automated review by Foresight Cyber Platform on download and alerting per triggered events. To install or remove appliance request ticket created on receipt. Normal response time: 2 business days.

d) Management of Cloud Agents – design, creation and management of Cloud Agent license keys; instructing the IT teams on Cloud Agent installation (including remote desktop sharing with our engineers); ensuring acceptable performance levels, and removal of outdated licence keys.

   SLA: Automated review by Foresight Cyber Platform on download. To install or remove Cloud Agent license key request ticket created on receipt. Normal response time: 2 business days.

e) Management of Option Profiles – design and management of Option Profiles for Mapping and Scanning– these are settings that affect performance and breadth of

maps and scans and does incorporate management of authentication credentials (where applicable).

SLA: Request ticket created on receipt. Normal response time: 2 business days.

f) Management of schedules – at service start and subsequently on request, as per the service plan, we manage schedules of maps and scans to ensure optimum utilisation of resources.

SLA: Request ticket created on receipt. Normal response time: 2 business days.

g) Initiating of ad-hoc scans and maps – initiating on-demand ad-hoc scans/maps outside of the agreed schedule.

SLA: Request ticket created on receipt. Normal response time: 2 business days.

h) Asset discovery, inventory, and deduplications

Discovering assets via agents, passive and active scanners, various connectors (e.g. Active Directory, AzureAD), consolidating into Global IT Inventory in Qualys, deduplication of assets.

SLA: Automated review by Foresight Cyber Platform on download and manual monthly report delivered by email upon agreement.

i) Asset taxonomy management & Cloud tags– we replicate required asset metadata in the Qualys subscription using Tag Taxonomy described on page 6 (*Tag Taxonomy categories*). We will ensure that selected or all tags from AWS Cloud are created in Qualys.

SLA: Request ticket created on receipt. Normal response time: 2 business days.

j) Asset correlation analysis – we correlate between Qualys and AD, Azure and ServiceNow! CMDB, delivering precise information (in a form of lists and reports and dashboards) showing any gaps. On request, we will prepare a proposal to add additional systems to this correlation.

SLA: Automated review by Foresight Cyber Platform and manual review monthly

k) Users, Roles and Access management – managing user accounts, roles, and permissions.

SLA: Request ticket created on receipt. Normal response time: 2 business days.

l) Qualys reporting & dashboards management – Management of best practice reports & dashboards related to licensed modules, setup for on-line viewing or sent by emails.

SLA: Request ticket created on receipt. Normal response time: 2 business days.

2.1.2 Tag Taxonomy categories

Qualys Asset Tagging system is a very flexible solution to static and dynamic asset management but with flexibility comes the need for responsible design to ensure tag taxonomy efficiency. As part of our services we work with clients to create taxonomy categories into which tags are defined.

Such a taxonomy allows granular asset grouping used for reporting and dashboards, access control and other functions throughout the Qualys Cloud Platform.

For example, the following taxonomy categories are recommended:

- Location – example: Location:London, Location:Amsterdam, Location:EMEA:Dubai
- Criticality – example: Criticality:Low, Criticality:Medium
- Amazon tags – example: AWS:tags:AppName:SAP
- Exposure – example: Exp:Internet, Exp:Partners:Foresight
- Business domain – example: Domain:Manufacturing
- Application – example: App:SAP, App:Office365, App:ActiveDirectory
- Managed by – example: Managed:ForesightCyber, Managed:ITSecurity

The below services are related to licensed Qualys modules and as such some may not be delivered to a customer.

2.1.3 Vulnerability Management

When a client has the VM licence (including VMDR), we deliver the following services.

a) Vulnerability acquisition management - Timely gathering of vulnerabilities on client's systems either via external, internal scanning or using installed Cloud Agents (compatible systems only)

   SLA: Automated review by Foresight Cyber Platform on download and alerting per triggered events.

b) Remediation policy management (Qualys built in) – We create a set of Remediation policies in Qualys, based on client's vulnerability and patch policies. These Remediation policies generate internal Qualys tickets that are useful for more detailed and granular reporting.

   SLA: Request ticket created on receipt. Normal response time: 2 business days.

2.1.4 Security Configuration Assessment / Policy Compliance module

When a client has the SCA module (including VMDR) or the PC module license, we deliver the following services.

a) Policy management - Management of configuration hardening baselines as per company requirements. Assignment of predefined security configuration policies to individual end point computers (servers and end user devices).

   SLA: Request ticket created on receipt. Normal response time: 2 business days

b) Compliance scanning – Timely gathering of policy compliance status on client's systems either via internal scanning or using installed Cloud Agents (compatible systems only)

   SLA: Request ticket created on receipt. Normal response time: 2 business days.

Policy management limits: Due to complexities of policies, we use standard Qualys policies imported from policy library, and adjust values based on client requirements. Where clients need customised policies, we deliver these on consultancy basis.

2.1.5 Cloud View & Cloud Security Assessment (CSA)

When a client has the Cloud View (including VMDR) or Cloud Security Assessments module license, we deliver the following services.

a) Management of Cloud connectors - establishing connection to clients' Cloud platforms to obtain relevant information

   SLA: Request ticket created on receipt. Normal response time: 2 business days.

2.1.6 Web Application Security & Malware Detection Scanning (WAS & MDS)

When a client has the Web Application Scanning module license, we deliver the following services. *Please note: Malware scanning is included in Web Application Scanning licence.*

a) Management of customer Web Applications in Qualys – setup of web applications, option profiles and authentication; removal of old / stale applications

   SLA: Request ticket created on receipt. Normal response time: 2 business days.

2.1.7 File Integrity monitoring (FIM)

When a client has the File Integrity Modules module license, we deliver the following services:

a) Management of File Integrity profiles– setup of profiles to monitor files and directories and assign these to required assets.

SLA: Request ticket created on receipt. Normal response time: 1 business days.

2.1.8 Endpoint Detection and Response (EDR)

When a client has the Endpoint Detection and Response module license, we deliver the following services.

b) Enrolment of EDR agent versions in Qualys – ensuring the Qualys agents are latest versions supported by EDR.

SLA: Request ticket created on receipt. Normal response time: 1 business days.

3 REMEDIATION MANAGEMENT

3.1.1 Services applicable to any module

The following remediation services are included for any of licensed modules and are part of the Remediation management.

a) Foresight Cyber Reports & Dashboards – management of a series of reports and dashboards in Foresight Cyber platform showing data that are not normally covered by dashboards in Qualys module.

SLA: Request ticket created on receipt. Normal response time: 2 business days

b) Raising service tickets – to remediate discovered vulnerabilities, hardening issues, web weaknesses and cloud mis-configurations – the coverage depends on licenced modules

SLA: Automated tickets by Foresight Cyber Platform according to the agreed and configured vulnerability & patch policy

c) Remediations Escalations – based on the client's security policies, we escalate to appropriate and agreed stakeholders when the SLAs for remediations are not met

SLA: Automated analysis by Foresight Cyber Platform and manual follow up weekly.

3.1.2 Vulnerability management module

When a client has the VM licence, we deliver the following remediation services.

a) Vulnerability management service – full triage of discovered vulnerabilities according to asset criticality, threat indications, vulnerability severity and company's policy. We then raise remediation tickets (as per 3.1.1 b))

b) Patch management – (for assets in scope of the Qualys Patch Management license) our service will use Qualys PM module to install security patches to assets using an agreed process.

3.1.3 Cloud Security Assessment

When a client has the Cloud Security Assessment licence, we deliver the following remediation services:

a) Remediation management of Cloud Security Risks – full triage of discovered cloud misconfigurations posing security risks, according to criticality, threat indications, and company's policy. We then raise remediation tickets (as per 3.1.1 b))

3.1.4 Web Application Security

When a client has the Web Application Security licence, we deliver the following remediation services:

a) Remediation management of Web Application Risks – full triage of discovered website / web applications vulnerabilities and misconfigurations posing security risks, according to criticality, threat indications, and company's policy. We then raise remediation tickets (as per 3.1.1 b))

b) Advanced discovery of web sites and applications – This special service (if ordered) uses our platform powered by Hardenize service to discover domains and hosts and perform security and configuration hygiene assessments. We then raise remediation tickets (as per 3.1.1 b))

3.1.5 File Integrity monitoring (FIM)

When a client has the File Integrity Modules module license, we deliver the following services:

a) Investigations of FIM Alerts – monitoring and investigating FIM alerts.

SLA: Request ticket created on receipt. Normal response time: 1 business days.

3.1.6 Endpoint Detection and Response (EDR)

When a client has the Endpoint Detection and Response module license, we deliver the following services.

a) Investigations of EDR Alerts – monitoring and investigating EDR alerts.

   SLA: Request ticket created on receipt. Normal response time: 1 business days.

4 REQUIREMENTS FOR THE SERVICE DELIVERY

To deliver the best service possible, we require the following:

- Access to Qualys subscription, licensed by the client covering required modules
- Access to client CMDB(s) or regular supply of asset lists
- Contact details of IT teams
- Where applicable, access to ticketing system over web and API interface
- Qualys API licence purchased (included in VMDR licenses) but needs to be added to Express and Enterprise licenses

Where a Qualys license is not already procured, Foresight Cyber Ltd, as an authorised Qualys reseller, will be pleased to offer a favourable quotation

4.1 Client access to the Qualys platform

Clients have full access to Qualys subscription provided by Foresight Cyber, however, to provide quality services we ask clients not to make changes to Qualys without consulting with our team.

4.2 Contacting our support team

Our service is designed to be semi-automated: therefore, it is extremely important that communications between the Foresight Cyber support team and the client team is always maintained as closely as possible.

Our team is accessible via email and Microsoft Teams – individual engineers have named accounts, and these are shared with clients at the start of the service. Each client is given a dedicated mailbox to send requests.

Document changes

24th January 2021 – Version 3.0 (major version)

- Added FIM and EDR services

1st July 2020 – Version 2.5 (major version)

- Changing Silver, Gold and Platinum tiers to packages
- Restructuring services
- SLA changes - Expanded SLAs per service and automatic alerting definition

17th March 2019 – Version 2.1

- Updated introduction section
- Tiers renamed to Silver, Gold and Platinum.
- Added Gold tier service to Web Application Scanning module section
- SLA changes - Expanded SLAs per service

25th September 2018 – Version 2.0 (major change)

- Change of tiers – Standard and Advanced
- Change of SLAs

15th January 2018 – version 1.5 (major version)

- Changes in tiers and SLAs

30th May 2017 – initial version 1.0

Foresight Cyber Ltd

Registered & Business address UK
71-75 Shelton Street,
Covent Garden, London, WC2H 9JQ,
United Kingdom

Business address CZ:
Fryštátská 64/9, 733 01 Karvina,
Czech Republic

Contacts:
UK Office: +44 20 8159 8942
General enquiries: info@foresightcyber.com
Finance team: finance@foresightcyber.com
Data protection Office: dpo@foresightcyber.com
Directors: directors@foresightcyber.com

https://foresightcyber.com
@foresightcyber.com

VAT: GB144735213
Company number: 06871193
D-U-N-S number: 211601017

OUR CERTIFICATIONS

aws CERTIFIED Solutions Architect Associate

CISSP® ISSAP®

CCSP℠

CISSP® ISSMP®

CISSP®

CISCO CERTIFIED CCNA

CCSK™ Certificate of Cloud Security Knowledge

CYBER ESSENTIALS PLUS

Qualys®

SKYBOX™ SECURITY