No jargon, no drama*

*Reassuringly dull cyber security

Vulnerability Management Service

Norm's Vulnerability Management Service is a module from Norm's Cyber Security as a Service (CSaaS) offering.

Norm's Vulnerability Management Service is comprised of four key security modules:

- Internal Network Infrastructure Scanner
- External Network Infrastructure Scanner
- Endpoint Scanner
- Web Application Scanner

The Vulnerability Management service monitors your whole corporate environment through scanning and monitoring all the devices connected to your internal and external networks including your internet-facing applications/services. Each device/application's scanned information is scrutinised and analysed for vulnerabilities. Those identified are then scored based upon their criticality.

This service module focuses on the **Technology** element of Norm's holistic trinity of cybersecurity - **People**, **Process and Technology**. Its purpose is simple:

- **Continuous security monitoring of your corporate environment; Network, Endpoints and Web Applications**
- **Automatically alerts and grades identified vulnerabilities associated with your devices or web applications**
- **Delivers total visibility of all technical vulnerabilities within your IT environment that require attention.**

The Vulnerability Management service constantly monitors your corporate network/web applications providing visibility of the weak points in your environment and recommended actions to remediate.

Service Features

You will gain access to Norm's managed service offering the following features:

- Powered by Qualys' Vulnerability Management platform, each vulnerability is evaluated and scored using an industry-leading, continuously updated global knowledge base to highlight the criticality of each discovered vulnerability to assist in prioritising remediation. The platform allows the customer to;
    - Prioritise your remediation by assigning a business impact to each asset.
    - Identify which Operating System, ports, services and certificates are on each device on your network.
    - Continuously monitor your perimeter and internal environment for unexpected changes or unexpected devices.
    - Dynamically tag assets to automatically categorise hosts by attributes, including network address, open ports, OS, software installed, and vulnerabilities found.
- In-depth and broad visibility and detection of weaknesses and vulnerabilities throughout your organisation's corporate environment through four key scanners:
    - **Internal Network Infrastructure Scanner** provides a virtual network appliance hosted within your corporate environment that continuously monitors your corporate network-connected devices for known weaknesses and vulnerabilities. This will not only scan and scrutinise all connected devices from Laptops, Desktops, Servers but other infrastructure

& IoT devices such as routers, firewalls, switches, CCTV, printers, phones including rogue/unknown devices.

- External Network Infrastructure Scanner provides a cloud-hosted appliance that continuously monitors your corporate network traffic for known weaknesses and vulnerabilities. This will scan and scrutinise all externally facing devices from servers, routers, firewalls, VPN gateways, etc.
- Endpoint Scanner is provided by utilising agent-based software that is hosted on Endpoint devices including Laptops, Desktops and Servers, which monitors and detects known weaknesses and vulnerabilities. The agent eliminates the need for establishing scanning windows or integrating with credential vaults for gaining access to systems – or to know where a particular asset resides. The agent also avoids the need for complex Firewall configuration or credential management typically required for remote scanning. With agent-based vulnerability assessment, you will be able to provide 100 per cent coverage of your installed infrastructure
- Web Application Scanner focuses on all the corporate business applications in your network including new and unknown ones. It provides dynamic deep scanning, covers all apps on your perimeter, in your internal environment and under active development, and even APIs that support your mobile devices. The scanner will detect OWASP's top 10 risks such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and unvalidated redirection. Authenticated, complex and progressive scans are supported. With programmatic scanning of SOAP and REST API services, this scanner tests IoT services and APIs used by mobile apps and modern mobile architectures.

- We schedule network scans once a week by default for the Internal, External and Web Application scanners and every 4 hours for Endpoint scanners. Changes to this schedule can be made as required at an additional cost.
- The service continuously scans and identifies vulnerabilities with Six Sigma (99.99966%) accuracy, protecting your IT assets whether residing on premise, in the cloud or on mobile endpoints. The executive dashboard displays an overview of your security posture and access to remediation details.
- Real-time reporting is available and accessible via Norm's Visualiser portal.

How the Vulnerability Management service works

The Vulnerability Management service monitors your whole corporate environment through scanning and monitoring all the devices connected to your internal and external networks as well as your internet facing applications/services. Scans are scheduled once a week by default for Internal, External network and Web Applications scans and every 4 hours for Endpoint scans. Changes to this schedule can be altered as required.

Once a vulnerability has been detected, the vulnerability is evaluated and scored using an industry-leading, constantly updated, global knowledge base to highlight the criticality of each discovered vulnerability and help prioritise remediation.

The vulnerability reports and recommendations will be presented via our Visualiser portal for real-time reporting.

On-Boarding Process

Once your order is received, a member of our customer experience team will take ownership of your order and contact you to introduce themselves as your project lead. They will arrange a Welcome call with you to guide you through the process, outlining who will be responsible for each element of the installation, and introduce you to your Norm technical lead. The onboarding process will include:

- Providing you with our service handbook detailing our service operational processes, SLA and contacts
- Providing you with your scanner(s) and integration through co-ordinated installation with your IT/Network team(s) or provider(s)
- Enrolling your scanner(s) into Norm's security platform(s)
- Providing access to Norm's Visualiser platform

Once the service is fully deployed our customer experience team will provide you with access to the Norm visualiser. This visualiser will provide you with an overview of all the vulnerabilities detected on your environment, including detailing their criticality and recommended remediation steps. A list of all endpoints will also be available to give you full visibility of your protected environment.

The SOC will also be on hand to provide technical advice and assistance on cyber-security queries or issues should this be required.

Technical Requirements

For the Internal Network and Endpoint scanning, the service requires a local appliance or agent installed either in the internal network or on the Endpoints (Laptop, Desktop or Server). These scanners will regularly perform scans with all scan logs and results sent securely to Norm's Visualiser platform.

	Internal Network Infrastructure Scanner	Endpoint Scanner
Name	Qualys Vulnerability Scanner	Qualys Cloud Agent
Hypervisor	ESXi, Hyper-V, AWS, Azure, GCP	N/A
Host Resources	1vCPU, 4GB RAM, 60GB HDD	512MB RAM, 200MB Storage
Access Requirements	All subnets to be scanned	Local host
Outbound Access on Port 443	qualysguard.qg2.apps.qualys.eu, 64.39.106.0/24 & 154.59.121.0/24	qualysguard.qg2.apps.qualys.eu, 64.39.106.0/24 & 154.59.121.0/24
Image Size	1GB	12MB
OS	Hardened RHEL	N/A

Internal Network Scanner

The Internal Network Scanner can be deployed onsite in a virtualised stack or an enterprise cloud environment providing it can access all subnets that require scanning. The scanner will perform scans on the Internal network for non-Windows/Linux/macOS and Windows devices and is able to connect for authenticated scans.

The scanner will be a Hardened RHEL image with very limited access and configuration options, managed through the Qualys Cloud Portal. The scanner will require outbound Internet access on port 443 and the ability to call back to Qualys on qualysguard.qg2.apps.qualys.eu on 64.39.106.0/24 & 154.59.121.0/24.

Endpoint Scanner

The Endpoint Scanner is a lightweight software agent that resides on any applicable hosts, i.e. Windows/Linux/macOS. The agent, provided by Norm, is centrally managed in the Qualys Cloud Portal and self-updating.

Additionally, the Endpoint Scanner is integrated into Microsoft Azure security centre's partner solutions for vulnerability assessment. The security centre detects the virtual machines without the agent and automatically deploys them. The initial establishment of the service within this environment is via a unique licence key that is issued as part of the service onboarding process.

Consumes a maximum of 5% CPU resources for host scanning. After their initial deployment, the agents run a full configuration assessment of their host in the background and upload the collected data to the Qualys Cloud Platform for analysis.

To install the Windows Agent, you must have local administrator privileges on your hosts. To install the Linux Agent, BSD Agent, Unix Agent or Mac Agent you must have root privileges, non-root with Sudo root delegation, or non-root with sufficient privileges (VM scan only).

Service Availability

Upon subscription, to the service, the customer will be provided with access to Norm's Visualiser where all of the data from the various scans will be made available. The Norm Visualiser is available 24x7.

The service is managed within norm's UK based Security Operations Centre (SOC), 24hrs a day, every day of the year. The Customer Experience teams are available during UK business hours, Monday to Friday 9:00 to 17:30hrs, excluding public holidays.

Software updates and patching for Internal and Endpoint Scanners will be automatically managed by the Norm platform.

The Customer Experience and SOC teams will be on hand to provide technical advice and assistance for any queries or issues should this be required.

Customer Responsibilities

- The Customer will be responsible for hosting the Internal and Endpoint Scanners within their corporate environment.
- The Customer shall provide a network connection for the Internal Scanner, ideally with static IP or DHCP reservation.
- The Customer shall provide a network connection to the Qualys platforms and allow onward access to Norm's SOC.
- The Customer shall nominate an administrator internally for the Norm Visualiser.
- The Customer shall be responsible for user administration within the Norm Visualiser.