# No jargon, no drama*

norm.
*Reassuringly dull cyber security

## Vulnerability Patch Management Service

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

The Vulnerability Patch Management service is available only in combination with Norm's Vulnerability Management service for Endpoints.

The Vulnerability Patch Management service provides the ability to remotely correlate identified vulnerabilities with patches and remotely deploy them across your endpoints regardless of where and how they are connected to the Internet.

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

- Remote endpoint patching regardless of where the device is located or how it connects to the Internet / Corporate network
- Automated correlation of vulnerability scan and patch data for your endpoints
- Patching support for OS and third-party applications with a single solution
- Delivers total visibility of the technical vulnerabilities and patching status within your IT environment.

The Vulnerability Patch Management service provides the ability to correlate identified vulnerabilities from the Vulnerability Management service and remotely deploy the remediating patch to your endpoints.

### Service Features

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

- Quickly correlate identified vulnerabilities with the corresponding patches
- Schedule and automate endpoint patching regardless where the device is located or how it connects to the Internet / Corporate network
- Prioritise your remediation by assigning a business impact to each asset.
- Discover open vulnerabilities and missing patches quickly
- Track your Endpoint patch status across your entire estate
- Deploy patches on demand at any given point, such as in emergency situations where a vulnerability is suddenly being actively exploited in the wild
- Deliver messages to end-users prompting them, for example, to install a patch or reboot their machine, or informing them about an in-progress deployment
- Continuously monitor endpoint environment for vulnerabilities and their patch status.
- Single patching platform solution that is able to patch operating systems and applications from different vendors, including Windows and over 300 applications (MacOS and Linux coming soon).
- Real-time reporting is available and accessible via Norm's Visualiser portal.

## How the Vulnerability Patch Management service works

The Vulnerability Patch Management service provides the ability to correlate identified vulnerabilities from the Vulnerability Management service and remotely deploy the remediating patch to your endpoints.

Patching on the endpoint is enabled through hosting a local agent on the endpoint device including Laptops, Desktops and Servers. The agent monitors and detects known weaknesses/ vulnerabilities and can install patches given to it from the central norm platform.

Once a vulnerability has been detected from the vulnerability management service, the vulnerability is evaluated, prioritised and correlated to the corresponding OS or 3rd party patch, ready for remote deployment. The patching deployment can then managed & scheduled for automated deployment to your Endpoints regardless of how they are connected to the Internet or your corporate network(s).

The vulnerability patching deployment and Endpoint patching status reports will be presented via our Visualiser portal.

## 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 endpoint agent(s) and integration through co-ordinated installation with your IT/Network team(s) or provider(s)
- Enrolling your agent(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 Endpoint agent, the service requires a local agent installed on the Endpoints (Laptop, Desktop or Server). The agent will regularly perform vulnerability scans and deploy patches to remediate identified weaknesses as instructed from the Norm's Visualiser platform.

| | Endpoint Scanner |
|---|---|
| Name | Qualys Cloud Agent |
| Hypervisor | N/A |
| Host Resources | 512MB RAM, 200MB Storage |
| Access Requirements | Local host |
| Outbound Access on Port 443 | qualysguard.qg2.apps.qualys.eu, 64.39.106.0/24 & 154.59.121.0/24 |
| Image Size | 12MB |
| OS | N/A |

Endpoint Scanner

The Endpoint agent 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 agent is integrated into Microsoft Azure security centre's partner solutions for vulnerability assessment and patch deployment. 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 and patching deployment/scheduling will be 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 agents 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.

The service is currently only available for Windows-based operating systems (MacOS and Linux coming soon).

### Customer Responsibilities

- The Customer will be responsible for hosting Endpoint agents within their corporate environment.
- The Customer shall provide a network connection to the Qualys platforms and allow onward access to Norm's SOC.
- The Customer will work with the norm Security Operations Centre to define a repeatable patching schedule and process.
- The Customer shall nominate an administrator internally for the Norm Visualiser.
- The Customer shall be responsible for user administration within the Norm Visualiser.