Vulnerability Management Service

What is it?

The **norm.** Vulnerability Management Service provides regular scans of your corporate network infrastructure, endpoint devices and web applications in order to identify any potential weak points in your IT environment.

As part of the service, every device and application is analysed and scored according to the criticality of any vulnerabilities which have been found.

Features of the service include:

- **Identification of vulnerabilities** within the corporate IT environment through continuous monitoring of networks, endpoints, and applications
- **Automatic alerts** and scoring system to enable your technology team to take remedial action against identified vulnerabilities
- **Near real-time visibility** of the results and recommended actions via the **norm.** Visualiser portal

Why now?

One of the main causes of cyber-attacks is the exploitation of known software vulnerabilities and configuration issues.

All modern software and applications contain vulnerabilities, and new vulnerabilities are constantly being reported. Cyber criminals, hackers and nation states are therefore constantly working to find innovative ways of taking advantage of these vulnerabilities in order to gain access to corporate networks and sensitive data.

Protection against such attacks requires constant assessment, prioritisation and resolution of vulnerabilities. It is also important to ensure that once patched or fixed, the vulnerability will not be exposed due to system roll backs or resets.

What's included?

Access to the **norm.** Vulnerability Management Service - powered by Qualys's Vulnerability Management platform - with each identified vulnerability evaluated against an industry-leading, constantly updated, knowledge base. The service will highlight the criticality of each discovered vulnerability and support the prioritisation of remedial measures.

Comprehensive visibility of all corporate environments through four key scanner types:

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

The service continuously scans and identifies vulnerabilities with Six Sigma (99.99966%) accuracy, protecting your IT assets on premise, in the cloud and on mobile endpoints It's executive dashboard displays an overview of your security posture and access to remediation steps, including near real-time reporting available via the Visualiser portal.

Want more detail?

For the full Service Description of our Vulnerability Management Service <<ClickHere>>.
To register your interest and get one of the team to call you <<ClickHere>>
or just give us a call on **+44 (0)20 385 55242.**

***Reassuringly dull cyber security**

norm.

In a nutshell…

The **norm.** Vulnerability Management Service provides regular scans of your corporate network infrastructure, endpoint devices and web applications in order to identify any potential weak points in your IT environment.

How does it work?

The Vulnerability Management Service monitors your whole corporate environment. It scans and monitors all devices connected to your internal and external networks, in addition to web-facing applications and services. Scans are scheduled on a weekly basis for internal and external networks, as well as web applications. Endpoint scans are performed every four hours. Changes to this schedule can be made as required.

Once a vulnerability has been detected, it is evaluated and scored against an industry-leading knowledge-base. Each discovered vulnerability is then prioritised according to its criticality and required remediation measures.

How do the four key scanners work?

- **Internal Network Scanner** - monitors internal corporate networks for network connected devices and analyses known weaknesses and vulnerabilities. It not only scans connected devices such as laptops, desktops and servers, but also includes infrastructure and IoT devices including routers, firewalls, switches, CCTV, printers and phones including rogue devices.
- **External Network Scanner** - monitors external corporate network facing devices and analyses the results against known weaknesses and vulnerabilities. It scans all externally facing devices including servers, routers, firewalls and VPN gateways.
- **Endpoint Scanner** – monitors endpoint devices such as laptops, desktops and servers and analyses the results against known weaknesses and vulnerabilities. The agent eliminates the need for complex firewall polices, scanning windows and integration with credential vaults in order to gain access to systems – or to know where a particular asset resides.
- **Web Application Scanner** – monitors corporate business applications including new and unknown applications. It provides dynamic deep scanning, and covers all perimeter applications in your internal environment and under active development, including APIs that support 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.

FAQs…

I do Windows patching regularly, isn't this the same?

Ensuring your Windows machines are patched is an essential part of your security regime. However, this doesn't cover all of the other devices on the network or your web applications. Our service eliminates the headache of patching for all network connected devices.

Will I need cyber security trained staff to understand the reports from this service?

We know how hard it is to recruit and retain good cyber security staff, that's why we give you access to our highly trained team of experts. They do all the complex work for you, and we provide visibility into the results via our clear and simple Visualiser portal with the information you need, at your fingertips, in a format that everyone can understand.

Most of my applications are web-based now, don't AWS and Azure deal with this?

AWS and Azure may provide the resources for cloud computers, but the security of servers and web applications is still your responsibility. Our web application scanner means you are always notified when vulnerabilities are detected, even in the cloud.

Some of my staff are using BYOD, can this work for them?

BYOD is really common now and our endpoint scanner means you can relax, knowing that even the BYOD devices connecting to your network are patched and monitored.

How long does the service take to set up?

Once the scanners are setup and connected to the portal, you will start to see information immediately.

Is there any benefit to the business beyond the direct security improvements?

The **norm.** Vulnerability Management Service not only demonstrates that your business takes cyber security seriously, it also reduces your operational risk, helps to safeguard your reputation with customers, suppliers and regulatory bodies (such as the ICO), and ultimately improves the value of your business.

norm.