Vulnerability Patch Management Service

What is it?

The **norm.** Vulnerability Patch Management service remotely correlates identified vulnerabilities with available patches, which are then remotely deployed across an organisation's endpoints, regardless of where and how they are connected to the Internet.

The service provides in-depth, broad visibility and detection of vulnerabilities and quickly identifies the relevant patch, which is then deployed from a centralised platform. Endpoint patching is enabled by installing a lightweight agent on endpoint devices.

The purpose of the service is simple:

- To provide remote endpoint patching, regardless of device location or how it connects to the Internet or corporate network
- To automatically correlate vulnerability scan results and patch data, save time in identifying and prioritising vulnerabilities, and ascertain which patch is required before deployment
- To provide visibility of software vulnerabilities and patching status within the IT environment
- To deliver clear results via the online portal

Why now?

The majority of breaches are enabled as a result of missing patches[*], something which is easy to resolve in principle, but can be very time consuming to identify, track and manage.

Technology is consistently evolving, and cyber criminals are continuously refining attack techniques. New vulnerabilities are constantly being discovered for a wide range of technologies including laptops, desktops, servers, IoT devices and web applications.

[*] Examples of breaches and ransomware attacks arising from unpatched vulnerabilities include Equifax and Marriott, at an approximate cost of £1.1bn and £100m respectively.

Ensuring that corporate devices, servers and applications are protected first requires complete visibility of vulnerabilities and their respective criticality in order to prioritise what to patch first. Patched systems also need to be monitored on a continuous basis to ensure that the vulnerability isn't re-exposed due to system roll backs or other events.

Can you afford to leave your business infrastructure unpatched and unsecured?

What's included?

- Access to the Vulnerability Patch Management platform, powered by Qualys vulnerability management software. Vulnerabilities are identified via endpoint sensors and are evaluated, prioritised and correlated with the corresponding operating system or third-party patch, ready for remote deployment
- In-depth, broad visibility and detection of vulnerabilities with the relevant patch instantly identified and ready to deploy from a centralised platform. Patching on the endpoint is enabled through hosting a local agent on the endpoint device
- An endpoint agent is software that is installed on endpoint devices including laptops, desktops and servers. The agent monitors and detects known weaknesses/vulnerabilities and is able to deploy patches issued by the central **norm.** platform
- Access to a single patching platform solution that is able to patch operating systems and applications from different vendors, including Microsoft (for Windows operating systems and applications), and over 300 third-party applications
- Management of the vulnerability remediation process from a central dashboard, allowing organisations to target critical Common Vulnerabilities and Exposures (CVEs) without researching knowledge base articles, manually deploying patches and verifying their remediation
- Real-time reporting via the **norm.** Visualiser portal

Want more detail?

For the full Service Description of our Vulnerabilty Patch 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**

In a nutshell…

The **norm.** Vulnerability Patch Management service is a comprehensive vulnerability management solution that takes away the strain and hassle of identifying vulnerabilities, and finding and deploying the appropriate patches.

Unpatched servers and devices are an open invitation to hackers and cybercriminals, and staying one step ahead of them requires a continuous patch management regime. **norm.** provides this reassurance via its transparent and simple to deploy service.

How does it work?

The **norm.** Vulnerability Patch Management service identifies missing patches and correlates them with vulnerabilities identified by the Vulnerability Management service, with the option to remotely deploy the relevant patch onto endpoints.

Patching on the endpoint is enabled through installation of a local agent on devices including laptops, desktops and servers. The agent monitors and detects known missing patches and vulnerabilities, installing patches on-demand from the central **norm.** platform.

Once a vulnerability has been detected by the Vulnerability Management service it is evaluated, prioritised and correlated with the corresponding OS or third-party patch, ready for remote deployment. Patch deployment can then be managed and scheduled for automated deployment to the endpoints regardless of whether they are connected to a corporate network(s) or the Internet.

Vulnerability patching deployment and endpoint patching status reports are presented via the **norm.** Visualiser portal.

FAQs…

I patch regularly using an automated tool, isn't this the same?

Many patching solutions are focused on a limited set of operating systems and third-party applications, which can mean that you need to use multiple patching deployment solutions depending on the vendor. Furthermore, these patching solutions often don't correlate vulnerabilities with the corresponding patch. Internal IT teams then need to identify and obtain the correct patch for each vulnerability, and deploy it themselves. The Vulnerability Patch Management service from **norm.** provides automated correlation of vulnerabilities to patches and enables the scheduling of remote patch deployment to endpoints irrespective of how they connect to the Internet or a corporate network. This service saves hours of IT resource by automatically patching vulnerabilities as they are discovered.

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 companies access to our highly trained team of experts. They do all of the complex work and will advise on a remediation plan which prioritises the most critical and or common vulnerabilities. Results are available clearly and simply via the **norm.** Visualiser portal which gives the information you need, at your fingertips, in a format that everyone can understand

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

BYOD is increasingly common now and our Endpoint Agent 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 Endpoint Agents are installed you will start to see information immediately. **norm.** can suggest multiple installation options, tailored to your specific infrastructure and requirements, to enable you to quickly and easily deploy the agents to your technology estate.

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

The **norm.** Vulnerability Patch 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.