WHITE PAPER

# How SolarWinds Patch Manager Can Help the NHS Avoid Ransomware Attacks

solarwinds government

# How Solarwinds Patch Manager Can Help the NHS Avoid Ransomware Attacks

In May of 2017, the WannaCry virus took a dramatic toll on the U.K.'s National Health Service (NHS)—the largest single-payer healthcare system in the world.

According to a report released by the National Audit Office (NAO)*, the attack is believed to have infected machines at 81 health trusts—which accounts for nearly one-third of NHS trusts in the U.K. In addition, according to the report, 19,500 medical appointments were cancelled, computers at 600 general practices were locked, and five hospitals had to divert ambulances to other medical facilities.

WannaCry works by infecting an organisation's infrastructure and encrypting its data, then requiring a ransom payment to unencrypt the data and have it be accessible once again.

"The WannaCry cyberattack … was a relatively unsophisticated attack and could have been prevented by the NHS following basic IT security best practice," stated Amyas Morse, head of the National Audit Office, in conjunction with issuing the report. "There are more sophisticated cyberthreats out there than WannaCry, so the NHS needs to get their act together to ensure they are better protected against future attacks."

According to the report, the vulnerability was able to penetrate the system because of a lack of patching. Patches are provided by vendors to resolve known vulnerabilities.

## THE VALUE OF PATCH MANAGEMENT

Patch management is a basic IT security function. The value in performing regular patch management is undeniable, particularly as IT vendors make it easier and easier to implement. That said, many organisations do not perform patch management frequently or effectively for a variety of reasons—the most common of which include the complexity of patching, lack of time, and a lack of visibility into patching across the organisation.

Enter SolarWinds® Patch Manager. In addition to helping eliminate the possibility of an infection by a WannaCry-type virus, SolarWinds Patch Manager was designed to alleviate many of the pain points government IT pros feel today.

- Security. There are a wide range of applications in use across every NHS trust. And the larger the trust, the more complex and varied the number and types of applications. Inconsistent third-party patching is a common challenge and can lead to security vulnerabilities.
- Compliance. This is a non-negotiable item when it comes to security in particular. An NHS trust that does not remain compliant—that is, not up-to-date on all patches—is a highly vulnerable organisation (as evidenced by the successful WannaCry attack).

» Visibility. It can be nearly impossible to know the status of a trust's software—what patches were most recently applied, if any were applied at all—without broad visibility across the trust. A lack of visibility to updated patch statuses makes it difficult to understand where the organisation stands in terms of security, compliance, and other critical components of a solid infrastructure.

» Automation. Manual patch approvals, packaging, and publishing processes are challenging to manage, and do not scale. And, they're quite time consuming—all of which leads NHS trusts to patch far less frequently than they should, which almost always ensures the introduction of inconsistencies and vulnerabilities.

Patch Manager solves all of these challenges by organising and managing available patches and automatically updating the appropriate endpoints at the appropriate times—workstations and servers alike. With this capability, Patch Manager enhances security, improves compliance, introduces cross-organisation visibility, and provides automation and reporting. Not only does this help keep the trust's servers and workstations up-to-date with the latest software patches, it helps eliminate vulnerabilities as soon as they are discovered and resolutions are available.

## KEY FEATURES OF PATCH MANAGER

Patch Manager is intuitive patch management software that provides automated patching of Microsoft® servers, workstations, and third-party applications.

Most importantly, Patch Manager ***integrates with Microsoft WSUS and SCCM capabilities*** *already in place*. Patch Manager scales to the current environment, regardless of whether it's sitting on top of a single instance at a single site or across your enterprise. And, because it works with WSUS and SCCM, it includes an extensive catalogue of third-party updates (including Java®, Adobe®, Firefox®, Chrome®, and more), as well as custom software packages. That catalogue is something that SCCM in particular does not offer; using SCCM and Patch Manager together provides dramatic advantages over using SCCM on its own.

Additionally, Patch Manager leverages an update management wizard to ***automate the patching processes***. Group policies stay the same; Patch Manager simply creates a pre- and post-installation environment to help ensure successful, automated patching.

Finally, Patch Manager ***provides a range of reports and dashboard views***—out-of-the-box reports as well as the ability to create custom reports. These views provide critical compliance information, and go so far as to send notifications via email or provide a console message when there is a patching anomaly. Compliance reports in particular are something SCCM users do not get out of the box, providing another advantage of using SCCM and Patch Manager together.

SolarWinds Patch Manager does not stop there. Patch Manager also provides the following:

» Intuitive web interface. Patch Manager's web user interface provides a view of important patch management data alongside other SolarWinds products in an integrated web console. An NHS trust can view the latest available patches, top 10 missing patches within the environment, and general health overview of the environment based on which patches have been applied.

» Extended power of Microsoft WSUS. Patch Manager works with and extends Microsoft WSUS to provide more control and power over the patch management process with dynamic patch management, immediate updates, scheduled reboots, easy reporting, full asset inventory, and more.

» Advanced before-and-after package deployment actions. SolarWinds Patch Manager's PackageBoot™ provides the ability to create advanced before and after package deployment scenarios to help ensure that even the most complicated patches (such as Oracle® Java) get deployed successfully—without complicated scripting.

» Patch physical servers and virtual machines. SolarWinds Patch Manager makes it easier to manage patches on virtual desktops and servers with the ability to patch offline machines, organise virtual machines into groups, and inventory virtual machines trust-wide.

## PATCHING MADE SIMPLE

The primary reason to implement SolarWinds Patch Manager can be summed up in a nutshell: SolarWinds Patch Manager simplifies many of the steps in the patch management process—from research to scheduling, deployment, reporting, and more—saving hours of time and making it easier to keep hundreds or hundreds of thousands of servers and workstations patched.

While the reason to implement may be simple, the value goes well into the depths of the NHS trust, by decreasing security risks, enhancing compliance, and enhancing overall performance—in addition, of course, to preventing further infections by WannaCry and other viruses.

## ABOUT SOLARWINDS®

SolarWinds provides powerful and affordable IT management software to customers worldwide, from Fortune 500® enterprises to small businesses, managed service providers (MSPs), government agencies, and educational institutions. We are committed to focusing exclusively on IT, MSP, and DevOps professionals, and strive to eliminate the complexity that our customers have been forced to accept from traditional enterprise software vendors. Regardless of where the IT asset or user sits, SolarWinds delivers products that are easy to find, buy, use, maintain, and scale while providing the power to address key areas of the infrastructure from on-premises to the cloud. This focus and commitment to excellence in end-to-end hybrid IT performance management has established SolarWinds as the worldwide leader in both network management software and MSP solutions, and is driving similar growth across the full spectrum of IT management software. Our solutions are rooted in our deep connection to our user base, which interacts in our THWACK® online community to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at www.solarwinds.com.

## LEARN MORE

NATIONAL GOVERNMENT
Phone: +353 21 2330440
Email: nationalgovtsales@solarwinds.com
www.solarwinds.com/nationalgovernment

FEDERAL
Phone: 877.946.3751
Email: federalsales@solarwinds.com
http://www.solarwinds.com/federal

** Investigation: WannaCry cyber attack and the NHS | Report by the Comptroller and Auditor General | 27 October 2017 | https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/ | File: Investigation-WannaCry-cyber-attack-and-the-NHS.pdf*