Symantec Patch Management Solution 8.1

Visibility. Security. Productivity.

Data Sheet

Overview

An effective and comprehensive patch management strategy is an essential part of securing and protecting your organization. The vast majority of vulnerabilities being exploited are ones for which a fix has already been available from the software vendor such as the WannaCry ransomware attack that took place two months after the patch had been released by Microsoft.

Symantec Patch Management Solution can assist organizations in meeting their security needs by automating the detection and facilitating the remediation of security vulnerabilities for multiple operating systems (Windows®, Mac®, Red Hat, CentOS and SUSE) and for Microsoft applications and over 50 third-party Windows applications (Adobe®, Java Runtime, common browsers and plug-ins, etc.). Patch Management Solution provides visibility into newly released software updates and the means to identify computers susceptible to the vulnerabilities addressed by such updates. It also automates the download of software update packages from vendor sites and the distribution of those packages to computers which require those patches.

Minimizing risk—saving invaluable time and resources

Today's IT world consists of widespread worms, malware, and ransomware targeting and exploiting known vulnerabilities on unpatched and/or under-patched systems, resulting in costly, unproductive downtime and in some cases enormous damage to a company's reputation. In addition, most organizations have remote workers who may seldom connect to the corporate network making it easy for these systems to get behind in software updates and patches. It only takes one unpatched system to wreak havoc in an environment.

Further fueling the need for effective, timely management of patch updates, fixes, and remediation is an increasing concern around governance and regulatory compliance (HIPPA, PCI, and many others) has forced enterprises to implement better control and oversight of their software and devices.

Real-world patch management

Symantec Patch Management Solution is specifically designed to minimize the time investment needed to allocate to patch updates, fixes and remediation activities, and possible unintended consequences to the users. Patch Management does this by:

- Offering broad coverage across Windows, Mac, Red Hat, CentOS, and SUSE platforms and third-party Windows applications to effectively respond to today's threats. Our approach is based on extensive work with our customers to effectively model the patch management process with detailed analytics to help determine overall risk and provide visibility into key performance parameters to gauge effectiveness.

- Helping to ensure the appropriate priority of any given update is not set higher than is absolutely necessary. Higher priority updates are subject to more stringent service level agreements (SLAs) which are costly and time consuming for the IT staff to support and more likely to cause disruption to end users due to compressed schedules and increased numbers of updates with needlessly high priorities.

- Automating and optimizing the patch process which often involves multiple different hardware and application owners who must study and weigh-in on the impact of applying an update to the resources for which they are responsible.

- Reducing service interruptions and unintended consequences. Patch Management Solution can help in this area by targeting computers or groups of computers directly to the patch policy to perform testing to determine the likelihood of system or application problems before rolling out the patch system wide.

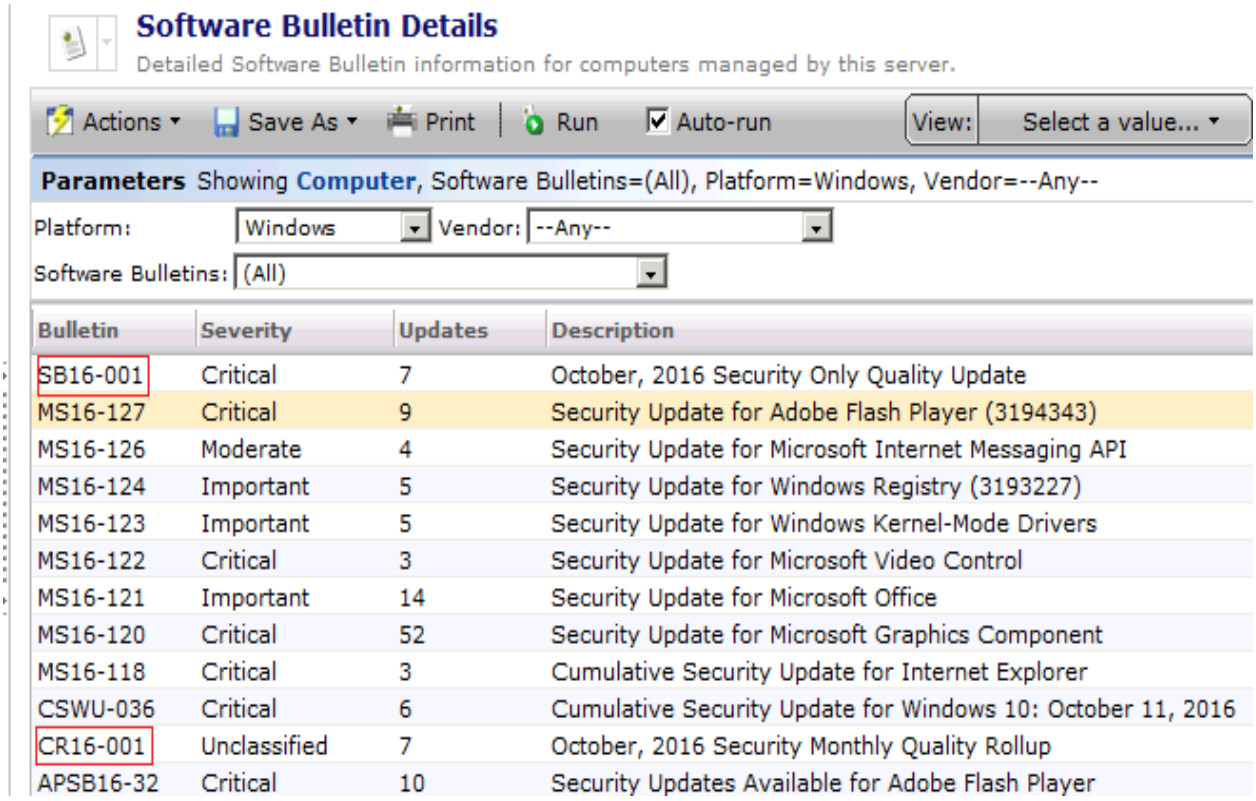
- Reducing the time required to perform patch-related updates with the software. This includes reducing the number of clicks required to create policies and exclusions, improving the overall effectiveness of reports, especially those used for highlighting and troubleshooting exceptions, and enabling the whole process to proceed as quickly as the participants can push it.

Streamlined process for updating Windows 10, Windows 7/8.1, and Office 365

The initial release of Windows 10 marked a fundamental shift to a "Windows-as-a-service" paradigm for updating the operating system. A short time later, Microsoft adopted a similar model for keeping Windows 7 and 8.1 up-to-date. The move to a "Windows-as-a-service" model was not unprecedented as Microsoft had been using a similar model for keeping Office 365 up-to-date. Along with the shift to a service-based paradigm, Microsoft introduced significant changes to the manner in which updates are packaged, distributed, and installed.

Patch Management Solution detects Windows 10 and Windows 7/8.1 devices that require Cumulative Updates, Feature Updates, Monthly Quality Rollups, or Monthly Security Updates, installs the updates, and tracks the updates' rollout using compliance reports.

For sites where large file sizes are an issue because of the lack of an onsite package server, Patch Management Solution supports data transfer efficiencies using multicasting or peer-to-peer package download capabilities. Both solutions let devices download packages from other devices at their site rather than requiring each device to download packages directly from the Notification Server or a package server across a Wide Area Network (WAN), which can significantly impact bandwidth. This solution can result in package payload distribution reductions as much as 90% lower than when compared to not using peer-to-peer.



Software Bulletin Details

Detailed Software Bulletin information for computers managed by this server.

Actions | Save As | Print | Run | Auto-run | View: Select a value...

Parameters Showing **Computer**, Software Bulletins=(All), Platform=Windows, Vendor=--Any--

Platform: Windows Vendor: --Any--

Software Bulletins: (All)

Bulletin	Severity	Updates	Description
SB16-001	Critical	7	October, 2016 Security Only Quality Update
MS16-127	Critical	9	Security Update for Adobe Flash Player (3194343)
MS16-126	Moderate	4	Security Update for Microsoft Internet Messaging API
MS16-124	Important	5	Security Update for Windows Registry (3193227)
MS16-123	Important	5	Security Update for Windows Kernel-Mode Drivers
MS16-122	Critical	3	Security Update for Microsoft Video Control
MS16-121	Important	14	Security Update for Microsoft Office
MS16-120	Critical	52	Security Update for Microsoft Graphics Component
MS16-118	Critical	3	Cumulative Security Update for Internet Explorer
CSWU-036	Critical	6	Cumulative Security Update for Windows 10: October 11, 2016
CR16-001	Unclassified	7	October, 2016 Security Monthly Quality Rollup
APSB16-32	Critical	10	Security Updates Available for Adobe Flash Player

Figure 1: Patch Management Solution supports the new “rollup” model for Windows 7, 8.1, and Windows 10.

Patch Management Solution will also identify Office 365 installations that need updating and then download and install only the content required by the local “click-to run” installation on each device. The solution will first download the Office 365 update to a central repository and then distribute it using its package server infrastructure, if present, to get the updated content closer to the devices that need it.

The Symantec Management Agent dynamically determines the nearest package server on each device when an update to Office 365 is required, modifying the path to the update package location in a configuration file used by Office 365’s native update capabilities. The Symantec Management Agent then invokes Office 365’s native update capabilities, resulting in only the content needed by each device being downloaded from the package server. This approach utilizes the Symantec package server infrastructure without requiring additional hardware or services, thus leveraging the incremental differencing functionality built into Office 365’ native update capabilities to minimize the load on network bandwidth.

For a more detailed explanation on how Patch Management Solution simplifies the process for updating Windows 10, 7/8.1 and Office 365, refer to this Solution Brief.

Peer-to-peer content distribution

Patch Management Solution 8.1 adds optimization capabilities for content distribution through peer-to-peer downloads. Endpoints with the peer-to-peer mechanism enabled will periodically (on a predetermined schedule) check for updates among endpoints nearby and automatically download the new content to stay up to date.

This new functionality provides a scalable distribution model that utilizes the endpoint to supplement the Symantec management infrastructure, minimizing the impact on network bandwidth without requiring any changes to network or security configuration. This is a major benefit for distributing Windows 10 and Office 365 updates due to their large file sizes that make downloading from a remote site across a WAN undesirable in many cases.

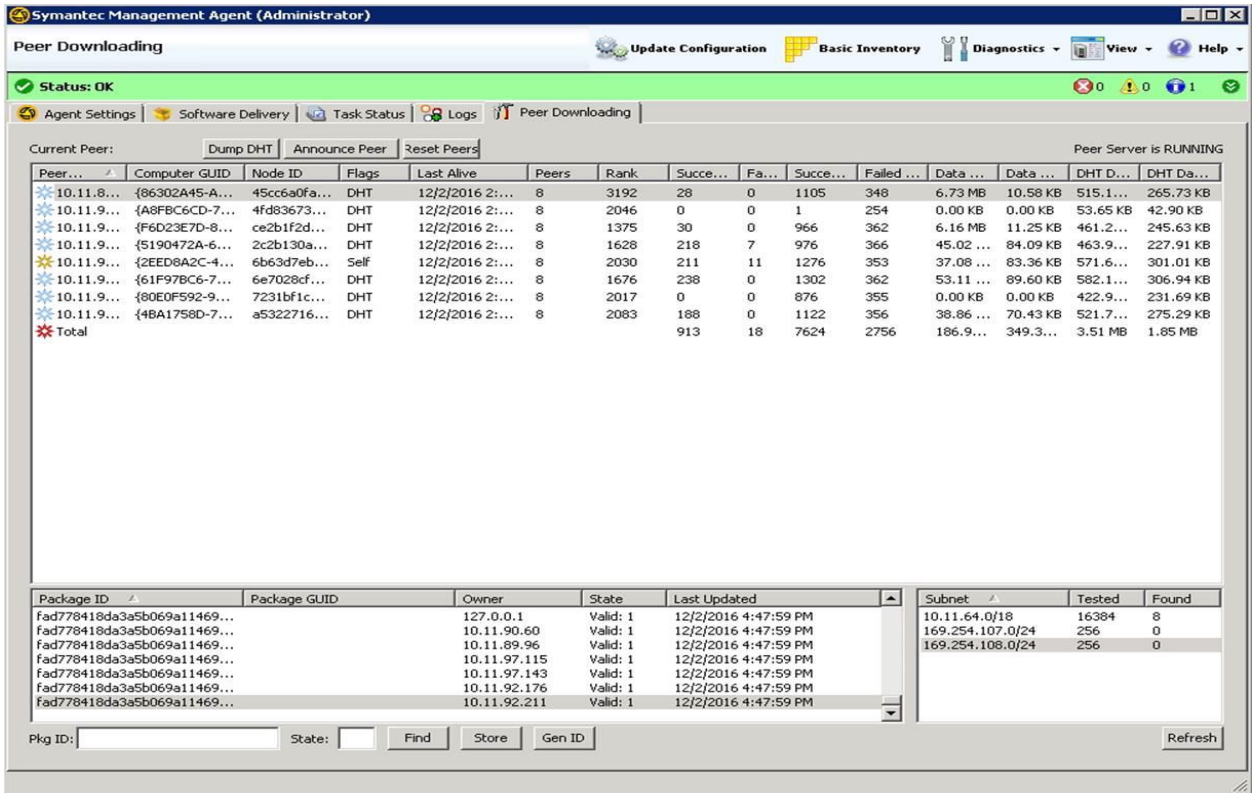


Figure 2: Patch Management Solution 8.1 adds optimization capabilities for content distribution through peer-to-peer downloads

Key features

- Broad, holistic patch management support: Use a single product to ensure that Windows, Mac, Red Hat®, CentOS and SUSE computers are properly patched and updated
- Ability to patch and update systems that are outside the firewall via cloud-enabled management
- Support for the new update models for Windows 7, 8.1, 10, and Office 365
- Support for security and non-security related updates, including service packs: Maintain visibility into newly released security updates and automate the detection and facilitate the remediation of vulnerabilities. Ensure that Microsoft operating systems and applications are kept up-to-date with non-security related updates and service packs.
- Support for over 50 third-party Windows applications: Mitigate the threat posed by the most vulnerable Windows applications by automating the detection and facilitating the remediation of vulnerabilities in the most commonly used applications from non-Microsoft vendors.
- Pre-defined reports and IT analytics: Use real-time compliance and exception reports to make smarter, faster decisions to determine overall risk status. Analyze trends and track progress against key performance indicators.

More Information

Visit our website

http://go.symantec.com/itms

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2017 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

21215280-2 07/17