

Patch Management: An Essential Process



Detailed reporting on endpoints

View detailed reports about hardware and software inventory, data encryption, firewalls and anti virus packages, and missing patches on laptops and distributed PCs.

Visibility in the "Mobile Blind Spot"

Monitor laptops and mobile devices in the field, beyond the reach of conventional management and reporting tools.

Simplify IT Operations

Work smarter and faster by quickly locating the data necessary to proactively remediate issues before they occur.

Immediate cost savings

Reduce management and support costs with no investment in hardware and modest subscription fees.

Patch Management is an essential process for companies today, but is also becoming much more tedious and costly, requiring a large amount of internal time and resources. Patch management can be one of the most costly and time-consuming activities for IT groups, at a time when budget dollars and staff time are desperately needed for new projects.

The risk of infection via malware, or breach caused by unpatched vulnerabilities, is much greater on endpoints that are not up to date with necessary critical security patches. Infection can lead to data breaches, stolen IP, higher help desk costs and lower end user productivity. The average organizational cost of a data breach increased from \$6.65 million in 2008 to \$6.75 million in 2009.

Evidence shows that patching is more important than ever. Thousands of new vulnerabilities are discovered every year for both Operating Systems and Applications such as Adobe Reader, Apple QuickTime and Sun Java. Hackers are exploiting known vulnerabilities faster, and the cost of data breaches remains high.

MaaS360's Patch Management Service

MaaS360's Patch Management service provides centralized reporting and the ability to deploy and install Microsoft OS security patches to endpoints without any end user interaction. This service can help reduce the risk of endpoint exposure across multiple Windows Operating Systems and decrease operational costs of managing and deploying Microsoft Operating System patches, while keeping IT departments in control. Patch Management also insures that systems are always up to date, on-LAN or off-LAN, with the latest security releases in a quick and convenient deployment method.

MaaS360's Patch Management Service:

- Deploys quickly and cost-effectively, since no infrastructure or large software implementation is needed.
- Extends IT's reach to patch both on- and off-LAN devices, protecting both the device and the data that resides on it.
- Improves visibility and control over device patch status.
- Simplifies daily IT patching workflows—from discovery, packaging and testing through to deployment, tracking and reporting.
- Reduces cost of patch operations.



Figure 1: MaaS360's robust, cloud-based infrastructure delivers patches to both on- and off-LAN devices

Detailed Patch Status Reports

MaaS360's Patch Management Service provides detailed information about missing Microsoft operating system patches on laptops and PCs. Summary graphs show at a glance how many patches have not been applied and how many systems are missing patches, classified by the number of patches missing.

Detailed reports show exactly which patches are missing from each system. These reports give administrators the information they need to address critical vulnerabilities in Microsoft operating system software before they are exploited by hackers and virus writers.



Figure 2: Click on summary reports to see detailed information in "drill-down" reports

Self Service Patch Deployment

MaaS360's Patch Management Service provides easy-to-use, wizard-based deployment options that simplify package distribution to relevant endpoints. After deployment, MaaS360 verifies successful completion of the patch application and reports status back to the platform for fast and easy reporting.

In addition to patch deployment and application, MaaS360 ensures that patches are properly applied and that all files are current, and if not, the patch can be automatically re-applied with no IT department, or end user interaction.

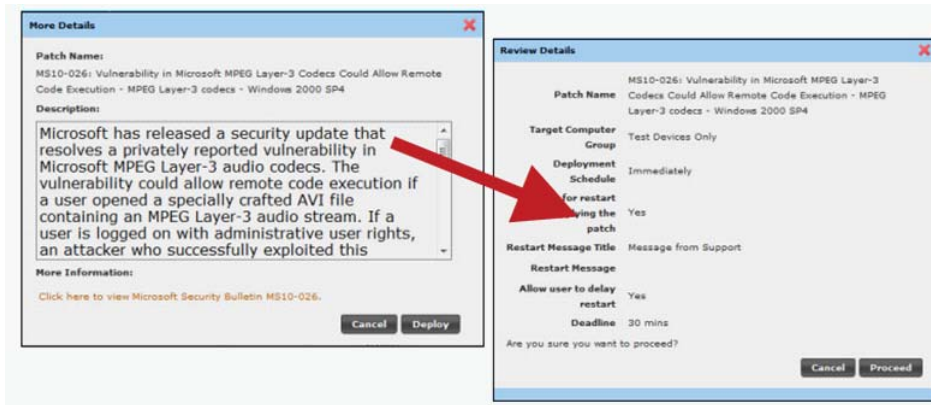


Figure 3: Easy to use deployment wizards simplify patch deployment.

Compatible with Other Services

MaaS360 Patch Management Service is available for, or can be added to, any or all of the MaaS360 Core Services: Visibility, Control or Mobile.

MaaS360 Service:	Visibility	Control	Mobile
Designed for:	All managed laptops and PCs	Laptops and PCs with confidential data	"Road warriors"
Includes:			
Visibility and reporting:	Inventory management reports Endpoint security reports Data protection reports	Inventory management reports Endpoint security reports Data protection reports Policy enforcement reports	Inventory management reports Endpoint security reports Data protection reports Policy enforcement reports Connectivity and connectivity cost reports
Control and management:		Centralized policy definition Application monitoring and remediation Anti-virus definition updates Mobile NAC	Centralized policy definition Application monitoring and remediation Anti-virus definition updates Mobile NAC VPN enforcement
Mobile connectivity:			Connectivity manager Intuitive connectivity interface Single password for mobile networking Virtual global network with 98,000 access points
Also Supports:			
Optional:	Windows Application Updates Visibility Service for Handhelds Any Connection Reporting Fiberlink Security Services Managed VPN services Patch distribution Anti-virus definition updates	Windows Application Updates Fiberlink Security Services Managed VPN services	Windows Application Updates Fiberlink Security Services Managed VPN services Access services

FOR MORE INFORMATION

For more information on MaaS360's technology and services, see www.MaaS360.com or email aholmes@fiberlink.com.

Fiberlink Communications 1787 Sentry Parkway West, Building 18 Suite 200 Blue Bell, PA 19422

Phone 215.664.1600

Fax 215.664.1601