8 TIPS FOR BETTER

PATCH MANAGEMENT

1) KNOW YOUR ENVIRONMENT

A clear understanding of all your assets is required for a successful patch management program. Scan your environment to make sure you have proper coverage.

2) PLAN, PLAN, PLAN

Patch management often devolves into an ad hoc process without a solid, documented plan. Creating a plan will make it easier to stick to it.

3) REGULAR VALIDATION

Be careful to make sure patches are deployed with an understanding of the potential negative consequences of a technical interaction.

4) GAIN LEADERSHIP BUY-IN

Gain leadership buy-in, especially for patching of business critical applications and systems. Without this, you may be forced to leave systems unpatched due to the downtime risk if you do not have the approvals of leadership. Help your leadership team understand the benefits of patching as well as the consequences of not patching.

5) REGULAR PATCHING

Prioritize patching critical systems based on the potential risk and the criticality of security vulnerabilities in the wild. Patches that are deemed critical from a security perspective should be deployed as often and as quickly as possible.

6) SCAN EVERY DAY

Scan for antivirus and security software updates every day and patch them with priority. Functionality updates are important, however security updates are even more so.

7) AUTOMATION

Using a tool that can automate patches for Windows, Linux, and cross-platform will increase efficiency and effectiveness as well as helping with validation.

8) REGULAR REPORTING

Establish regular reporting. This will feed back into your plan and help you focus on the right patches at the right time with the right frequency.

Headquarters
7311 West 132nd St, Ste. 305
Overland Park, KS 66213
800-940-4699

UK Office
A8 Ively Road, Farnborough
Hampshire, GU14 0LX UK
+44 800-358-4915

sales@foresite.com
www.foresite.com

FORESITE CYBERSECURITY