SOLUTION BRIEF

Ivanti DSM Advanced Patch Management:

Reduced risk of attack via patch installation that’s up to 80% faster

Companies today process large volumes of sensitive data — a preferred target for hackers and malware. According to industry experts, 10 new security vulnerabilities are discovered every day. Attackers mainly target the known vulnerabilities of the most popular operating systems and applications. For efficient, reliable and cost-effective protection against threats, companies need standardized, automated patch management that is always up to date.

Before installation, patches must be checked for company relevance and/or any dependencies and incompatibilities. Internal and external requirements also call for the accurate recording and transparent presentation of security issues, as well as valid proof of security compliance — even in complex, shared networks. However, all this must not be at the expense of response times, because speed is essential in patch rollout.

Automated security scan and patch download

The Ivanti DSM Advanced Patch Management solution scans the entire multi-vendor software environment for vulnerabilities automatically and informs you of the results. The solution detects security vulnerabilities in your software infrastructure — in Microsoft applications and in applications from other manufacturers — and also automatically downloads and packages necessary patches.

Before the patches go live, you can test them thoroughly (e.g. in a pilot installation). Depending on the level of urgency, patches and service packs can be automatically released, prioritized accordingly, and distributed immediately to achieve the fastest possible protection against attacks.

Policy-based installation

Because DSM Advanced Patch Management supports individual policy definitions for downloading and installing patches, entire processes can be customized and fully automated to meet the specific needs of your organization. The automation also includes the scheduled downloading of patches. This means you can shift data transfers to the times you want.

With DSM Advanced Patch Management, you can have the system perform routine tasks based on policy. You then only need to define a desired end state. An example of this type of policy-based, automated administrator task in patch management would be distributing critical Microsoft patches to the affected terminal servers immediately, without manual intervention. This is a distinct advantage over desktop and laptop computers, which only receive the patches after a specific testing and approval process due to possible incompatibilities among the applications on these devices.

The graphical user interface notifies you immediately whether or not the defined state has been reached. If necessary, deviations can be tracked down to the individual system. This means you are always accurately informed about security compliance and potential vulnerabilities. For auditing purposes, the system documents the status.

Pilot installation to minimize risk

Even though time is of the essence when installing patches, system stability and availability always come first. DSM Advanced Patch Management supports controlled change management, in which a pilot installation is used to test all new patches to prove they aren't harmful. Only when these tests have been passed successfully does DSM install the patch on computers in live operation. The solution keeps the number of necessary installations to a minimum by resolving dependencies among patches automatically.

Features

- Comprehensive protection against the most common security threats.
- Patches for operating systems, applications and virtual machines.
- Increased security through automatic detection and closing of security vulnerabilities in the system.
- Scheduled downloading of data files for new patches.
- Automation of all phases of patch management and reliable, policy-driven patch rollout.
- Automatic selection, downloading and packaging of relevant patches.
- Comprehensive reports on patch status and open security vulnerabilities.
- Integrated quality control for increased stability.

Advantages

- Reduces the risk of attack by increasing the speed of patch installation by up to 80%.
- Early identification of security vulnerabilities, even before they become apparent.
- Proactive protection measures and faster response to threats.
- Increased security through automatic detection of vulnerabilities.
- Reliable, dynamic, policy-based rollout.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com

Copyright © 2021, Ivanti. All rights reserved. IVI-2567 04/21 GV/DH

ivanti

ivanti.com/contact
epg@ivanti.com