ivanti

SOLUTION BRIEF

Patching for the Data Center

Daily news about vulnerabilities and other threats—plus fear of the unknown or falling victim to those threats—keeps organizations on edge. You do all you can to keep users' system software up to date and secure. But what about the servers in your data centers? In today's world where hackers can access pre-written exploit code, organizations need an effective means to protect their data-center servers without exhausting IT resources.

Your security practices must include patch management to help keep servers hardened, data secure and available, and your business reputation intact. You've got to deploy the latest security patches—while continuing to devote time to core business goals.

You need precise control and reporting over the entire patch process: patch discovery and inventory and deployment of all available patches to your environment continuously—and on a schedule that suits your organization.

But many organizations struggle to keep their server software up to date with the latest software updates for operating systems and third-party applications, such as Microsoft Windows® and VMware vSphere® Hypervisor systems. The problem is that data centers present more and different server patch management issues than client systems.

Detection and Remediation for the Entire Data Center

To provide a high degree of patch accuracy in your environment, you must be able to easily find system scans for missing patches and deploy patches aligned to policy throughout your entire environment. Without a clear view of your environment and the in-depth information to know which systems are the most vulnerable, it's impossible to understand the risks to your organization. But that's not an easy task due to the multiple configurations available in modern data centers.

Time and budget concerns associated with a virtual data-center environment—waiting for virtual machines (VMs) to boot up, patch, and then power back down—lead some to ignore virtual environments and take on unnecessary risk. Focusing solely on physical servers leaves the business exposed and in danger of failing an audit. You need to be able to find vulnerabilities, scan for missing patches, and deploy those patches on physical servers and virtual systems easily—and without disrupting server workloads or the business. And when it comes to compliance, offline systems can't be ignored. You must ensure patch compliance and deliver software updates, whether a system is on the network or disconnected.

Reduce Time to Patch

With all that in mind, how long do your data-center software update processes currently take? Months or weeks? To reduce your exposure, that needs to drop to days and hours.

Historically, 50% of exploits occur within two to four weeks from release. A self-imposed, 14-day patch SLA will put you ahead of the majority of exploits. But manual processes, practices, and multiple tools that can't support your entire environment add to your management complexity, as does the time it takes to discover, define, and deliver software-update packages and apply those critical patches.

No matter whether your systems are online or offline, you need to save time and direct your scarce resources to actions with an immediate and high-value payoff.

There are many ways that will help you reduce that time and risk. For example, patching templates save time and reduce your risk each time a new server is built. The ability to quickly find all your offline VMs and then patch offline VMs and templates can save up to an hour per system. Keeping offline images in a constant state of readiness to be deployed will ensure you can deploy a virtual machine without having to worry about whether it's up to date.

The most impactful way to save time is to automate every part of the server patching process. Consider how you currently deal with vulnerability assessments from vendors. Finding all the patches related to Common Vulnerabilities and Exposures (CVEs) and building patch groups of updates automatically would be a huge time-saver.

Finally, you need to simplify compliance with reporting by cutting through the mass of information across your environment and accessing data on demand. Getting the right kinds of data into the hands of executives, directors, and application owners easily provides visibility to support audits and up-to-the-minute information about your security posture for effective decision making.

A Patch Management Checklist

Automating your patch management process—from discovery to assessment to deployment—across your workstations and physical and virtual servers online and offline will help decrease the delivery time of critical security patches. To find the right patching solution, the table below lists what to look for.

Ivanti Can Help

With robust and simple server patching to meet all your requirements, Ivanti can help protect your data center so that you can save time and money and stay focused on supporting core business initiatives. Ivanti tools can be up and running in minutes to help you discover, assess, and remediate your systems across your data center automatically, based on policies you define. Our tools simplify patching across your physical and virtual systems. Find online and offline workstations and servers, scan for missing patches, and deploy them. Then patch everything from the OS and apps to virtual machines, virtual templates, and even the ESXi hypervisor with our deep integration with VMware.

Capability	Description
Administration	Single, role-based management point
Automated Discovery, Inventory, and Patching	Protect client workstations, physical servers, virtual servers, hypervisors, and templates
OS Updates	Windows and Linux operating systems
Application Patching	Third-party and custom applications
Automate CVE-to-Patch List	Import any vulnerability vendor assessment list
Patch Content	Access to an extensive patch catalog
Patch Deployment	Agentless, agent, and cloud-based agent
Rollback Support	Ability to take pre-patch snapshots
Automation Enabler	APIs for automation and orchestration
Collaboration	Share status and verify patch compliance with others
Reporting	Real-time dashboards and customizable reports

IVI-2336 11/19 BB/MK/DL

Learn More www.ivanti.co.uk ☎ +44 (0)1344 442100 ✉ sales@ivanti.com