

Patching Saves Agencies Time; Aids Compliance

How do you discover and maintain control across all the IT assets in your government agency? How are you determining priority among known cybersecurity vulnerabilities? Are you still patching systems manually? Ivanti delivers the tools you need to automate, saving your organization significant time and budget.

Fast Threat Response

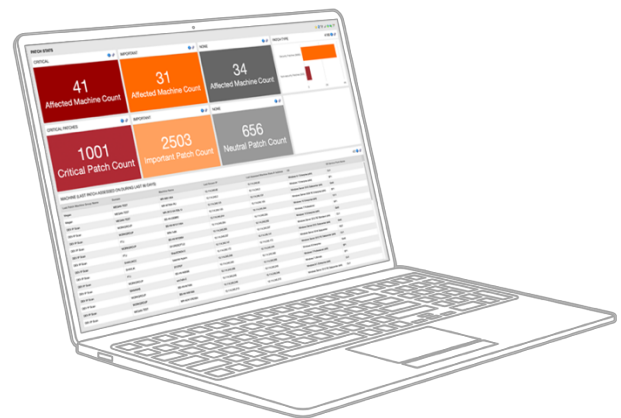
Whether you're using the public Common Vulnerabilities and Exposures (CVE) list, or the Information Assurance Vulnerability Alert (IAVA) bulletin, it can be challenging to identify the specific patches needed in your environment. Government customers using Ivanti[®] Patch for Windows benefit from access to the IAVA, and can use it to perform patch scans and prioritize listed patches for deployment.

For agencies following the MITRE Corporation-hosted CVE database, Ivanti speeds your response to identified threats. Administrators simply import their CVE file into Ivanti[®] Security Controls. Once incorporated, scanning your inventory is easy via patch groups, and machines in need of updates are targeted for deployment.

Where automation saves time, patch distribution offers efficiency. Even where customized implementations are deployed, Ivanti's agent-based patching offers simplicity. For example, where closed networks are in use, agent-based patching simplifies the lift with peer-to-peer or master agent capabilities. You can also customize distribution packages to minimize impact on network traffic, schedule policy syncs, and more.

Deployment Made Easy

Machine-by-machine patching is inefficient. And while we don't like to admit it, human error is the cause of way too many issues. The old saying "If I want it done right, I'll do it myself" doesn't apply when you're exposing your



agency to the risks a security breach can introduce. Automated patching not only makes deployment easier, but when coupled with quality dashboards and reporting, provides visibility that all patches are being applied properly.

Agency-wide Coverage

The diversity of IT that agency administrators are required to manage is increasing—and even faster as more technology comes online. With operating systems ranging from Linux and UNIX to Mac, Windows, and mobile, plus thousands of third-party applications, responsibility is shared across IT staff. While your SCCM administrator is focusing on common endpoint territory, they can also patch third-party applications. Ivanti's application patching catalog is among the most extensive, including popular applications: Adobe Reader, Apple iTunes, Google Chrome, Mozilla Firefox, as well as more challenging updates like Java. Back in the data center, your Linux admins use the same tool to ensure patches are implemented. Solutions from Ivanti help admins discover all the assets that need patching, helping agencies toward compliance and security objectives.

Unify Security and Management

Deliver the promise of Unified IT with Ivanti® Endpoint Manager and Security Controls. Your agency's IT is easily maintained, and tools like application control, blacklisting and whitelisting, and encryption are performed within a unified administrative console. From servers in the data center, to workstations in the offices and mobile devices in the field, integrated dashboards and reporting tools show you all that's deployed, and the insights that help you ensure agency IT is operating at peak performance and security.

Learn more about Ivanti Security Solutions:

www.ivanti.com/solutions/security

Learn More



ivanti.com



1 888 253 6201



sales@ivanti.com

Copyright © 2019, Ivanti. All rights reserved. IVI-2308 07/19 RD/BB/DH