ivanti

SOLUTION BRIEF

Continuous Vulnerability Management

When threat actors exploit weaknesses in an organization's IT infrastructure, the consequences can be devastating to productivity and reputation, as well as financially. Without treating cybersecurity as an ongoing process, hackers can find, weaponize, deploy, and attack your infrastructure faster than your team can patch the vulnerability, leaving your infrastructure exposed. Your systems may be secure today, but next week a threat actor may discover and exploit a critical vulnerability in your environment.

Continuous vulnerability management is described by the Center for Internet Security as "continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunities for attackers."

Continuous vulnerability management should be part of every organization's security practice, yet the time and manual work involved from when a vulnerability is first identified to when a software update deploys is challenging. It's recommended that the process start with scanning for vulnerabilities frequently to avoid blind spots between reports.

Security teams take vulnerability data, prioritize it, and hand it off to your IT team, which must translate those Common Vulnerabilities and Exposures (CVEs) into software updates and prioritize which titles to update. While one vulnerability is easy to identify and remediate, what if it's 10,000 detected CVEs or 100,000?

A single vulnerability assessment may find the same vulnerabilities on multiple systems in your environment, or the same vulnerability can appear on many pieces of software on one system. Deduplicating and researching CVEs to figure out what needs to be done to resolve each vulnerability can take anywhere from 5 to 8 hours each time they perform the process. One day may not seem like a lot. But when most exploits happen within 14 to 28 days of updates being made available, every day of delay leaves attackers more time to gain a foothold.

Save Time from Vulnerability to Patch Deployment

Security solutions from Ivanti provide you better insights and a better security posture. You'll stay up to date with patching across operating systems and third-party applications with automated patching of endpoints and servers. Our patching solutions integrate with vulnerability scanners, configuration management tools, and reporting to optimize the time of IT and security teams.

Achieve Continuous Vulnerability Management

Our security solutions streamline the process from identifying, classifying, and addressing vulnerabilities to avoid threat actors exploiting gaps between security vulnerability reports and remediation. IT teams can easily import vulnerability scan results taken by Security teams. Quickly view the identified CVEs and associated patches and publish or approve any missing patches for deployment and save significant time.

Whether you're patching endpoints with Ivanti Patch for SCCM, Ivanti Patch for Endpoint Manager, or are patching the data center with Ivanti Security solutions, you can take advantage of our CVE-to-Patch capability.

You'll improve the experience and productivity of IT teams that previously spent many hours researching, deduplicating, and preparing a patch group of updates manually. It's easy to import a list from a vulnerability management vendor in any format—CSV, XML, or plain-text files. Then automatically map CVEs to the right software updates that address particular vulnerabilities and gain quick visibility into which patches need to be applied. Create a patch group of what's approved in the environment and even see all the information associated with each patch.

Better Insights for Better Security Posture

How many days does it take your IT team to research, test, and roll out patches, and how do you prioritize them? Researching known issues from blog posts, vendor documentation, and other sources to determine the reliability of patch updates is yet another time-consuming activity. Prioritizing patches can also increase risk if pushing out critical patches is the current rule of thumb rather than those that are actively exploited.

Deciding which patches to prioritize, test, and roll out can extend the vulnerability management process. Ivanti lets you take advantage of our Patch Intelligence tool that combines patch data from Ivanti's third-party patch catalog with patch reliability and security metrics. Optimize the rollout of important updates by gaining insights that would take time and effort to discover otherwise.

- **Gain visibility** into issues reported by the vendor for a patch or a group of patches, or identified by Ivanti in bulletin information located with associated CVEs and patches.
- **Extend insight** into the issues experienced across Ivanti customers through anonymized peer data that reports back whether customers had to roll back the patch.
- **Determine reliability** of updates and the confidence level in rolling out quickly.
- **Identify patches** that will require more testing, fast-track patches that have a high probability of success and help prioritize testing and what can be deployed immediately based on threat scores and reliability ratings and rollout to optimize patch cycles.

Stay ahead of threat actors with continuous vulnerability management solutions from Ivanti.
For more information contact sales@ivanti.com

Learn More

www.ivanti.co.uk
+44 (0) 1344 442100
sales@ivanti.com