ivanti

SOLUTION SHEET

The Right Endpoint Security—Made Easy

How can security and IT pros protect their organizations from today's sophisticated attacks?

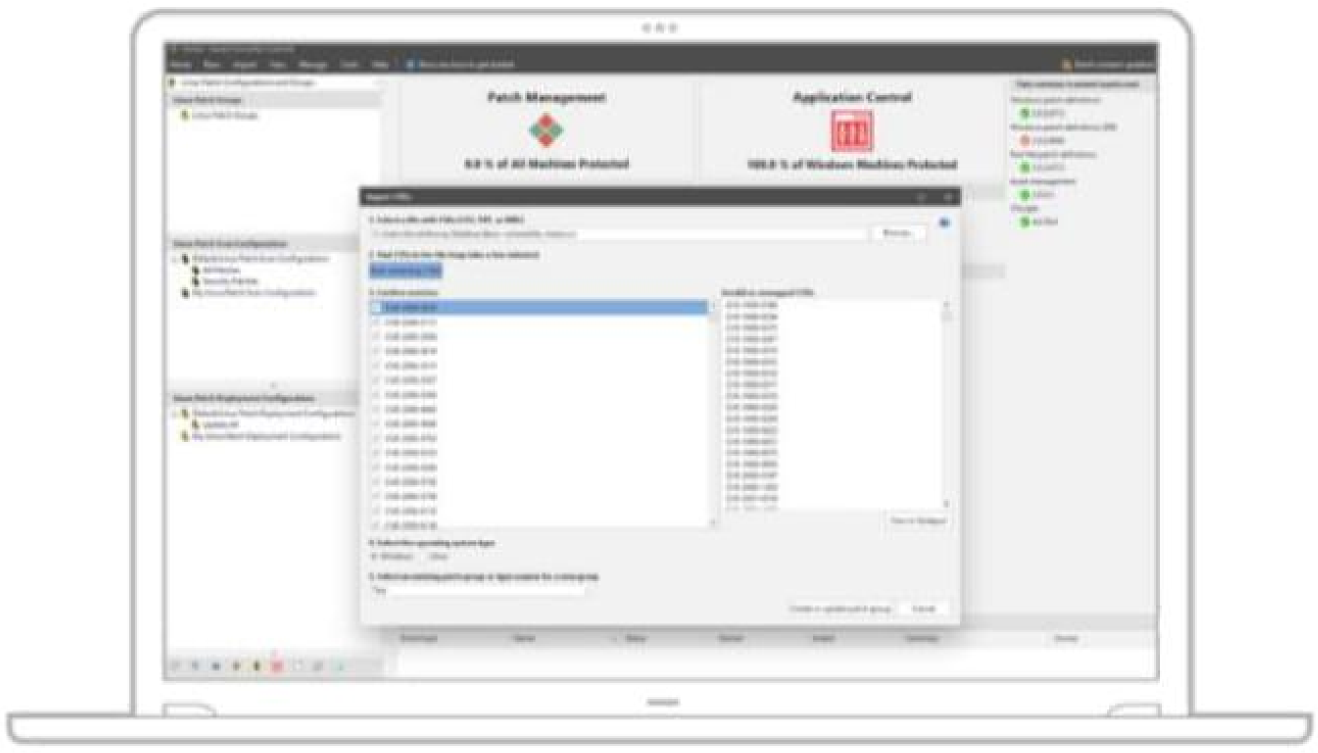
Without a focused security strategy, device sprawl is costly—and out of control. IT teams spend too much time managing these devices. Add to this a major cybersecurity labor shortage that forces companies to optimize their security personnel, and clearly a focused strategy leveraging tech that's comprehensive, simplifies management, and focuses on security basics that raise the highest barriers against real-world attacks offers a strong advantage over other solutions.

It Starts with Patching

The thing is, many vulnerabilities remain exploitable because security patches that have long been available were never implemented.

How do you keep track of and remediate all your vulnerabilities—without breaking the bank or creating headaches for IT? You must be able to research, evaluate, test, and apply patches across the organization with ease. And with the majority of vulnerabilities affecting third-party applications, patching and updating the OS just isn't enough.

Save time and money and stay focused on supporting core business initiatives. In minutes, Ivanti tools can be up and running to help you discover, assess, and remediate the Windows, macOS, Linux, and UNIX systems across your enterprise—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 (VMs), virtual templates, and even the ESXi hypervisor with our deep integration with VMware.



Ivanti also offers a plug-in to Microsoft System Center Configuration Manager that automatically discovers and deploys your third-party app patches through the SCCM console.

An advanced API stack for our patching solutions integrates with security solutions, vulnerability scanners, configuration management tools, and reporting tools, helping you bridge the gap between Security, IT, and DevOps. For example, you can automatically import the latest vulnerability assessment into the next batch of patches to test, saving significant time and helping make IT a more effective partner in securing the organization. For its part, DevOps is all about continuous improvement and automation—and when integrated with patch management can lead to more resilient and consistent infrastructures and systems. And you can pull critical data into solutions like Splunk, Reporting Services, Archer, and Crystal Reports for faster analysis of, response to, and closure rates for critical security incidents.

Block What You Can't Patch

Patching won't protect against zero-day exploits, of course. And if you can't patch—because you're running legacy systems, for example, or you have concerns that patching will break something in your environment? You need to secure the apps that don't get patched with tools like application whitelisting.

It's also essential that users receive only the apps they need to be productive, and can't introduce unauthorized apps that could reduce desktop stability, impact security, breach licensing compliance, lead to user downtime, and increase desktop management costs.

However, while locking down desktops reduces risk, it also significantly reduces the quality of the end user experience. Users hampered by poor experiences produce less, call the help desk more, and may turn to 'shadow IT' workarounds, creating new security risks.

Ivanti offers leading solutions that help you prevent unauthorized code execution without making IT manage extensive lists manually, and without creating obstacles to user productivity. Trusted Ownership™ automatically prevents the execution of any code, even unknown, that a non-trusted owner (a typical user account, for example) introduces. You can manage user privileges and policy just as easily, at a granular level, while allowing for self-elevation when exceptions occur. We make it simple to give users just the privileges they need to fulfil their roles—no more, no less.

Prioritize Secure Configuration

The default configurations for operating systems and apps are geared to ease-of-deployment and ease-of-use—not security. At the end of the day, then, what you are looking to do is maintain a set of minimum standards for your configs.

To help stave off attacks like SamSam ransomware, we provide a security suite that can turn off Remote Desktop Protocol (RDP) if you don't need it. Similarly, after WannaCry hit, it was recommended that IT disable the Server Message Block (SMB) v1 service. We disable it by default.

You can also set a lockout policy to limit password guessing attacks And, we can provide device control—control removable device usage and enforce encryption on removable devices and hard drives—via this suite or a standalone solution.

These are a few examples of the secure configuration management Ivanti makes possible.

Level Up with a Security Suite

Ivanti also brings industry-leading automated patch management for Windows and Red Hat Linux, dynamic whitelisting, and granular privilege management together in one solution. As well as supporting CVE to patch list creation, it provides patch REST APIs to integrate with other products, automate shared processes, and provide remote access and control of the console. Throughout 2019, Ivanti Security Controls will be expanded to patch MacOS, CentOS and more and provide device control.

We also offer a security suite that's integrated with our unified endpoint management platform, so you can manage and secure your devices from one console. Ivanti Endpoint Security for Endpoint Manager adds advanced antivirus and antimalware capabilities to patch management and app control. As noted earlier, it also provides device control, as well as advanced protection against fileless attacks (disabling scripts downloaded from the Internet, learning app behavior, allowing only trusted apps to run scripts, and protecting against in-memory attacks, etc.). In addition, you can limit access to authorized networks or IP addresses, and customize firewall configurations for individual systems or groups of systems, including configuring the latest Windows firewalls. And you can detect attempts to encrypt files on the local machine, stop the encryption process, and notify all other computers on the network to blacklist the malware—effectively thwarting the attack. Powerful remote control capabilities mean you can isolate, investigate, and clean endpoints across the network.

Real-Time Dashboard Reporting

Finally, since you have no real defense without real insight into your environment, Ivanti Xtraction turns reporting into a checkbox, with data on demand about our solutions and many more, and the ability to easily create new dashboards and reports. Get the right data into the hands of executives, directors, and line-of-business (LOB) and application owners, to help them make smarter, faster decisions with ease.

IVI-1954 07/14 AB/BB/SJ

Learn More ivanti.com ☎ 1 800 982 2130 ✉ sales@ivanti.com