ivanti

DATA SHEET

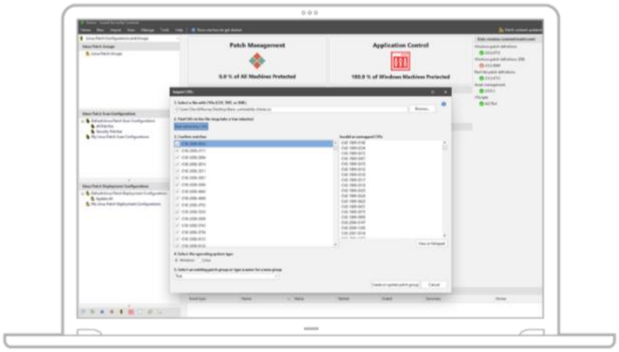
Ivanti Security Controls

With IT teams spending too much time managing security device sprawl, and Security teams suffering a labor shortage, Ivanti simplifies security with a unified solution that targets your biggest attack vectors. In Ivanti Security Controls (formerly Ivanti Patch for Windows) we've brought together the security tools global experts agree create the highest barriers to modern cyber attacks—discovery of the authorized and unauthorized software in your environment, so you can protect and defend against it; patch management for your heterogeneous OS and third-party app environment; dynamic whitelisting; and granular privilege management—as well as additional patch tools that help IT and Security work together better to better protect the business.

Patch for Windows and Linux

Ivanti Security Controls is a single automated patching solution that spans not only physical and virtual Windows servers but workstations as well. And we've added Red Hat Enterprise Linux and CentOS patch support to the leading Windows patching solution on the market—further non-Windows OSes to be added in 2019.

- **Patch your virtual servers.** 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) and even the ESXi hypervisor with the product's deep integration with VMware. It's possible to keep even offline virtual images in a constant state of readiness to be deployed. (You don't want to go through the two-step process of creating a VM and having to patch it. If offline templates are kept current all the time, you can deploy a VM without having to worry about whether it's up to date.)


Patch Management
0.0 % of All Machines Protected
Application Control
100.0 % of Windows Machines Protected

- **Patch without an agent.** Agentless technology lets you assess and deploy patches to the workstations and servers connected to your network while minimizing the impact on both your team and system workloads. Alternatively, you can use the agent to create as many different agent policies as necessary to manage your network, offering significant patching flexibility, and to provide a higher degree of patch accuracy in environments where devices are not continuously connected to the network. Assign different agent configurations to different devices in your organization.
- **Patch your Windows and Linux machines.** You need patch management software in your toolbox that can handle today's heterogenous environments. Extending patching beyond Windows is a must. And doing this efficiently, using a single interface and automated tool, not only frees up IT, but also reduces human error while enhancing your defenses.
- **Patch your applications.** Third-party applications such as Adobe Acrobat Flash and Reader, Google Chrome, Mozilla Firefox, and Oracle Java are the apps and browser add-ons hackers target most.

We provide the largest patch catalog in the industry, and our content team puts all the patches through a gauntlet of testing, so you don't have to take that on yourselves. We can save you and your team time better used to focus on core business goals.

Whitelisting and Privilege Management Done Right

Ivanti Security Controls offers a more dynamic whitelisting option as well, using trust models in place of lists, which reduces the ramp-up, cost of ownership once running, and performance impact, while still delivering a high degree of security. It also lets IT take back admin rights but still enable users to do what they need to, including easing the process of adding additional permissions if needed.

- **Simplify whitelisting.** We can provide authorized access to applications, services, and components without making IT manage extensive lists manually and without constraining users. Trusted Ownership™, for example, allows NTFS ownership of a file to simplify the process of whitelisting. Using a handful of trusted accounts to define ownership of trusted files allows easy implementation of a whitelist, and continuous addition and update of applications through your management systems, as the trusted owners are the accounts performing the install and update\upgrade efforts.
- **Control the keys to the kingdom.** There are many vulnerabilities that, if exploited, give the attacker permissions equal to the current user. Attackers can use stolen credentials and that user's admin rights to gain full access to information and systems and spread further into your network. And providing full admin rights on a server has other risks as well, like the ability to start or stop services and install or remove software in error.

  There are still companies that can enforce a policy of total lockdown of user permissions, but generally users require some ability that inevitably requires us to grant them administrative privileges on their system. Microsoft provides just two levels of control: user or a full admin. There's some variation in between, but not enough to make it a good experience for the user or administrator.

  We implement Just Enough Administration (JEA) and Just-in-Time Administration (JIT) – letting you take back your admin rights but still enable users to do what they need to, including easing the process of escalating or adding additional permissions if needed. Now you can choose. Take a full admin back down to a regular user, and provide escalation of privileges where and when needed, from access to install applications, install a printer, use PowerShell, or whatever the user may need, but nothing more than what the user should have. Or you can take that full administrator and strip away the things they should not have access to. Take PowerShell away, for example, or access to specific capabilities. Limit administrative privilege to specific consoles, applications, services, and commands, reducing the risk of admins introducing malware, halting essential services, or affecting performance of mission-critical services.

More Tools to Save You Time and Money

Ivanti Security Controls also includes the following features that make it even easier for Security and IT Ops to undertake the business of securing your organization.

- **Integrate and automate beyond Ivanti.** Patch REST APIs enable Security Controls to integrate with other products, automate shared processes, and provide remote access and control of the console.
- **Bridge the gap between Security and IT Ops with CVE to patch list creation.** Ivanti Security Controls can take a vulnerability assessment from whatever vendor the organization is using, find all the patches that relate to those Common Vulnerabilities and Exposures (CVEs), and build a patch group of updates that can be quickly approved for remediation in the environment. It's a huge time-saver replacing today's manual process.

Learn More

ivanti.com

1 800 982 2130

sales@ivanti.com

IVI-2264 06/19 AB/DL