

Apply ACSC Controls and Mitigate up to 85% of Endpoint Attacks

As cybersecurity breaches proliferate, targeting the user and the endpoint, the pressure on InfoSec and IT teams to protect their organization grows. Industry experts continue to highlight the basics of endpoint security in the ongoing battle to protect corporate computing resources and data.

Ivanti’s Security portfolio provides InfoSec and IT teams with capabilities essential for ransomware and other malware prevention. These include dynamic application whitelisting & endpoint privilege management, granular auditing collection, and comprehensive patch management.



This portfolio aligns with The Australian Cyber Security Centre (ACSC) Essential 8 recommendations internationally recognised as the most effective measures for preventing cyber attacks. A study by the Australian Signals Directorate found that implementing these controls can mitigate up to 85% of intrusion techniques. The Ivanti portfolio also helps organizations achieve Maturity Level 3 as recommended by the ACSC for all environments.

ACSC Security Controls	Solution
Application Whitelisting	Ivanti Application Control
Patch Applications	Ivanti Security Controls / Patch for SCCM
Patch Operating Systems	Ivanti Security Controls / Patch for SCCM
Restrict Administrative Privileges	Ivanti Application Control

Whitelisting

Ivanti® Application Control gives IT and InfoSec teams unprecedented endpoint control that reduces security risk without degrading user experience. Using Trusted Ownership™, Ivanti can deliver a dynamic approach to whitelisting and blacklisting while minimizing the traditional pain of ongoing maintenance. Ivanti deliver conditional access entitlements that can be defined per-user, based on factors such as location, device name, IP address, firewall settings, and even time of day. This

provides complete control over what can be executed from where, by whom, and when.

To support achieving ACSC Maturity Level 3 customers can whitelist servers or desktops/laptops and protect against exe,dll, msi and scripts.

Patching of OS / Applications

Ivanti patch solutions are easy-to-use solutions that discover patches missing from the environment and deploy them to the entire organisation with an agent-based or agentless approach. In addition to OS patching, Ivanti adds third-party software patching, virtual infrastructure patching, and patch scanning for all Windows systems on or off the network and network connected Linux systems. With Ivanti, your enterprise can discover, assess and remediate thousands of systems comprehensively, consistently and regularly, based on policies you define and without saturating your network or disrupting user productivity. The solution can span physical and virtual servers in the data center, find online and offline systems, scan for missing patches and then deploy them. Patch everything – the Windows OS, virtual machines (VMs), virtual templates, and even the VMware ESXi hypervisor.

To support achieving ACSC Maturity Level 3 customers can automate patching all critical systems and applications while providing detailed automated reporting of the continued protection.

Privilege Management

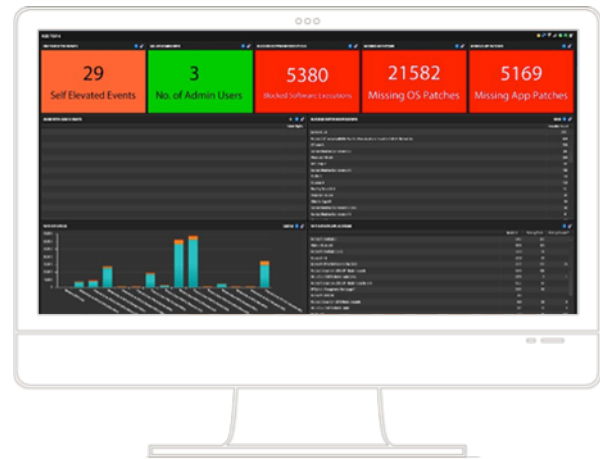
Ivanti Application Control manages user privileges and policy at a highly granular level and allows for optional, audited self-elevation. You can control end-user privileges dynamically with surgical precision, providing users with only the administrator privileges they need while keeping IT support costs from skyrocketing. By removing the need for a local administrator user account, Ivanti manages privileges at the application or individual-task level instead of at the session or account level. Privileges can be raised, lowered or even eliminated on a per-user, application, or task basis. The privilege level of a user, group, or role can be elevated or reduced for applications and control panel applets. Local administrator accounts can be removed, yet users can still access select applications or tasks that require administrator rights – all with full auditing and accountability.

To support achieving ACSC Maturity Level 3 technical controls are put in place to ensure high risk applications

never run in an elevated state, and users run with the minimum privileges they need to do their job.

Visibility & Reporting

Ivanti Xtraction is a powerful reporting solution that simplifies the aggregation of data from multiple sources. With Xtraction, users can bring together data from multiple vendors' tools and multiple enterprise applications – each with its own reporting interface – into a single, consolidated business view. Businesses can pull together and display data (in real time) from enterprise systems for security management, IT service management, IT asset management, client management, and more. IT managers and business executives can gain a visual representation of their current security stance and then drill down to focus on the more intricate needs of security analysts.



 www.ivanti.com.au

 02 8378 7201

 contact-anz@ivanti.com