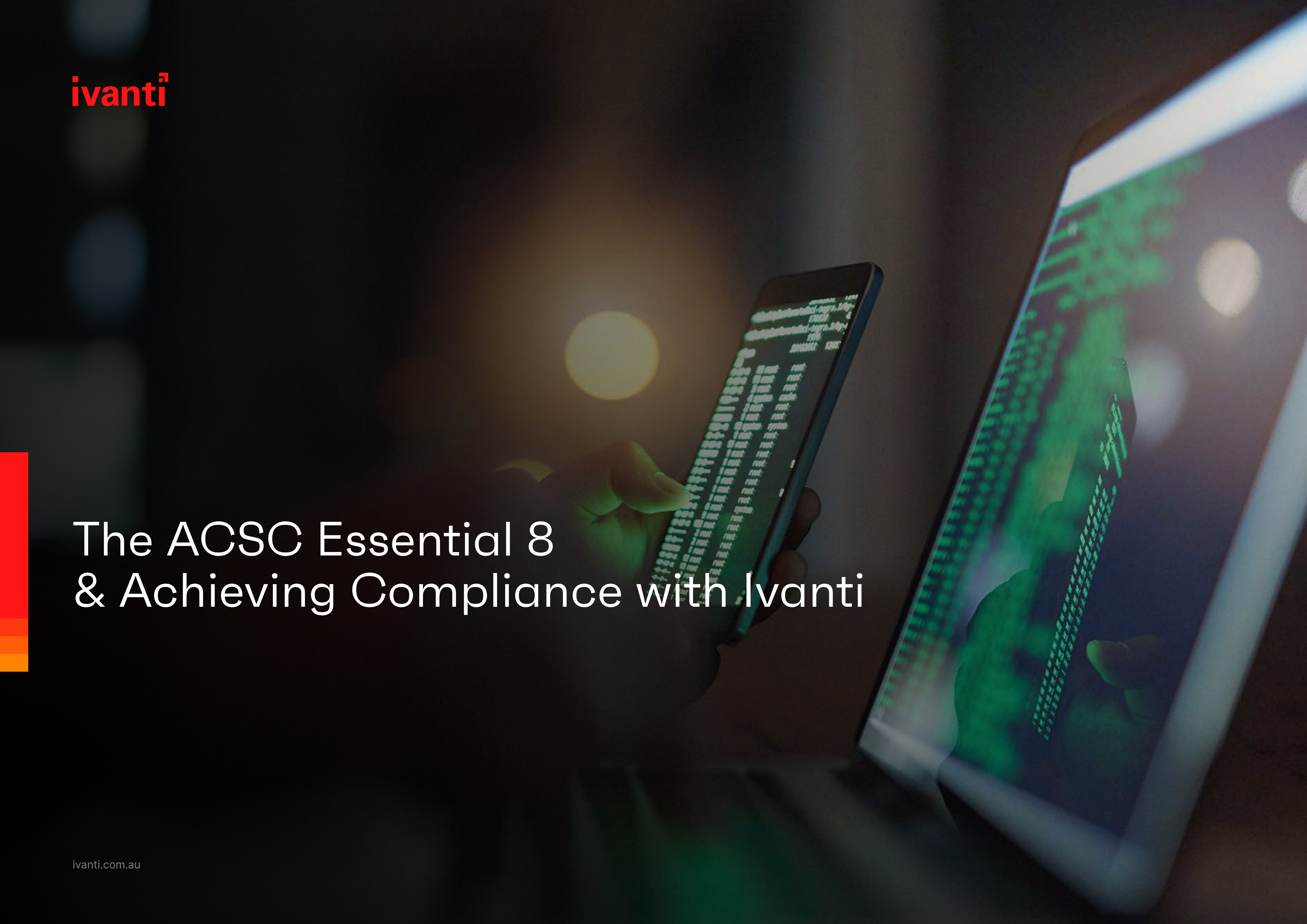
ivanti



The ACSC Essential 8 & Achieving Compliance with Ivanti

ivanti.com.au

Table of Contents

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”),and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit ivanti.com.au

What It Is, Why It Matters, How We Help

What Is the Essential 8 as Defined by the ACSC?

The Australian Cyber Security Centre (ACSC) Strategies to Mitigate Cyber Security Incidents is a prioritised list of practical actions organisations can take to make their computers more secure. The advantage of this guidance is that it is customisable to each organisation based on their risk profile and the threats they are most concerned about.

Implementing the ACSC Essential 8 effectively helps you achieve a baseline cybersecurity posture – a level that prevents many attacks, including ransomware.

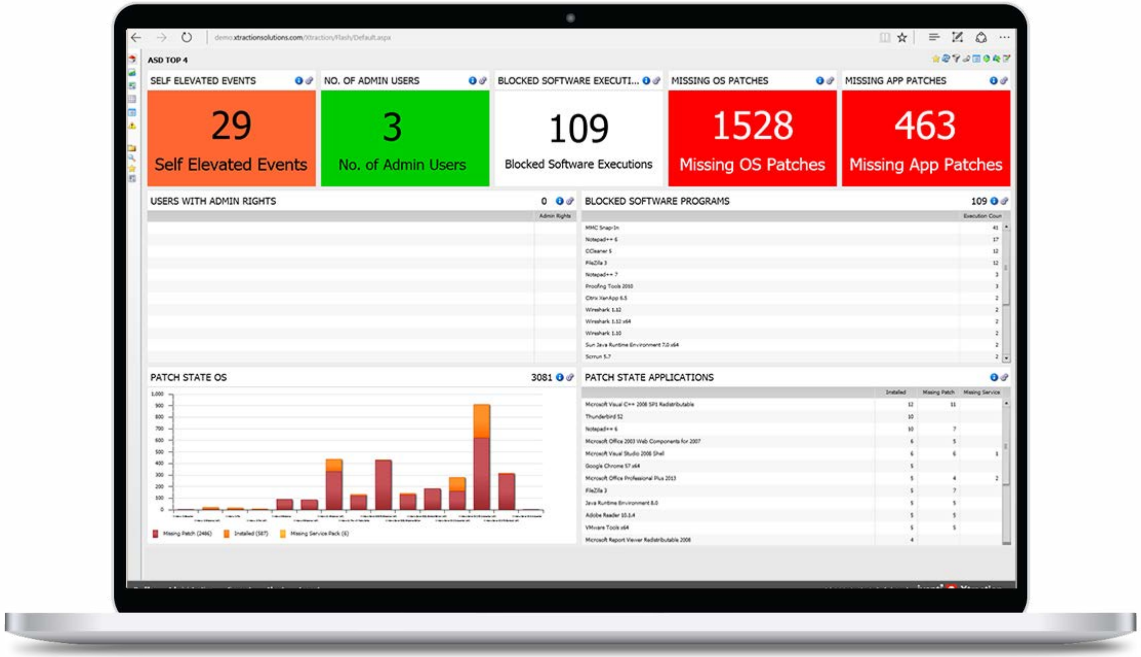
In this document, we'll discuss the importance of each control that makes up the Essential 8, the pitfalls companies fall into with each, and Ivanti's approach to solving them.

Taking a Step Back

As threats evolve, we must adjust to meet them, so building a strong cybersecurity program is not a set-it-and-forget-it process. It's a journey, and as you move forward you need to adapt, evolve, and reassess.

The Essential 8 is a critical part of this journey. Without a solid foundation, your cybersecurity program may be doomed to fail, or at the very least meet insurmountable tasks along your journey.

If you leave your attack surface exposed at 50 metres, there is no way your SecOps team can be successful, so you need to reduce that attack surface to give your detect-and-response capabilities and SecOps team a chance. Enter the Essential 8 and the need for that baseline cyber security posture.



demo.xtractionsolutions.com/Xtraction/Flash/Default.aspx

ASD TOP 4

SELF ELEVATED EVENTS	NO. OF ADMIN USERS	BLOCKED SOFTWARE EXECUTI...	MISSING OS PATCHES	MISSING APP PATCHES
29 Self Elevated Events	3 No. of Admin Users	109 Blocked Software Executions	1528 Missing OS Patches	463 Missing App Patches

USERS WITH ADMIN RIGHTS 0

	Admin Rights

BLOCKED SOFTWARE PROGRAMS 109

	Execution Coun
MMC Snap-In	41
Notepad++ 6	17
CCleaner 5	12
FileZilla 3	12
Notepad++ 7	3
Proofing Tools 2010	3
Citrix XenApp 6.5	2
Wireshark 1.12	2
Wireshark 1.12 x64	2
Wireshark 1.10	2
Sun Java Runtime Environment 7.0 x64	2
Scrrun 5.7	2

PATCH STATE OS 3081

PATCH STATE APPLICATIONS

	Installed	Missing Patch	Missing Service
Microsoft Visual C++ 2008 SP1 Redistributable	12	11	
Thunderbird 52	10		
Notepad++ 6	10	7	
Microsoft Office 2003 Web Components for 2007	6	5	
Microsoft Visual Studio 2008 Shell	6	6	1
Google Chrome 57 x64	5		
Microsoft Office Professional Plus 2013	5	4	2
FileZilla 3	5	7	
Java Runtime Environment 8.0	5	5	
Adobe Reader 10.1.4	5	5	
VMware Tools x64	5	5	
Microsoft Report Viewer Redistributable 2008	4		

The Essential 8 in More Detail

The ACSC Essential 8 comprises a set of security controls aimed at preventing attacks and helping organisations limit the extent of an incident and recovery.

Prevent Malware from Running	Limit the Extent of Incidents and Recover Data
Application Control	Restrict administrative privileges
Patch applications	Patch operating systems
Disable untrusted Microsoft Office macros	Multi-factor authentication
User application hardening	Daily backup of important data

The preventative measures will reduce your attack surface and the number of incidents that may occur in your environment. Layering preventative measures accounts for exceptions and gaps in a layer and short windows of time where one layer can be defeated. When you add these layers and consider their implementation, there is a tipping point where you lock down endpoints and the user has no ability to execute and the organisation has no ability to succeed. What you need is a balance between security and user needs. With the first four security controls in the Essential 8, you can focus on significantly reducing the attack surface and the number of incidents that might hit your environment.

When the inevitable security incident happens, you need to reduce the ability for the incident to spread to other systems. This is the focus of the other half of the Essential 8.

Prevent Malware from Running

Application Control

Application Control ensures only selected software applications can run on computers.	
Why do this?	All non-approved software/code is blocked, including ransomware and malware.
Challenges?	Traditional approaches can work in some cases, but many companies have tried and failed due to complexity, lack of flexibility, administration overhead and user experience impacts.
Ivanti's approach	A more dynamic approach reduces the total cost of ownership, negates performance impacts while delivering a high level of security. Flexible models allow users to get quick automated approvals for policy exemptions to ensure productivity and user experience is maximised, plus integrates with Ivanti Neurons for ITSM and ServiceNow. Privilege Management capabilities are included (see restricting administrative privileges.)
Customer example	Victoria dept of Transport needed to quickly attain Essential 8 compliance to minimise risk exposure for its 4000+ strong workforce and selected Ivanti Application Control. Implemented in under three months with no slowdown in employee productivity Ivanti solved the Department of Transport's critical security and compliance exposures while further freeing up time for IT staff for other strategic projects.
Ivanti's solution	Ivanti Application Control (Supports Windows and Linux)

> "Ivanti, in all aspects, has exceeded our expectations"

Umair Saleem
IT Team Leader, Department of Transport.

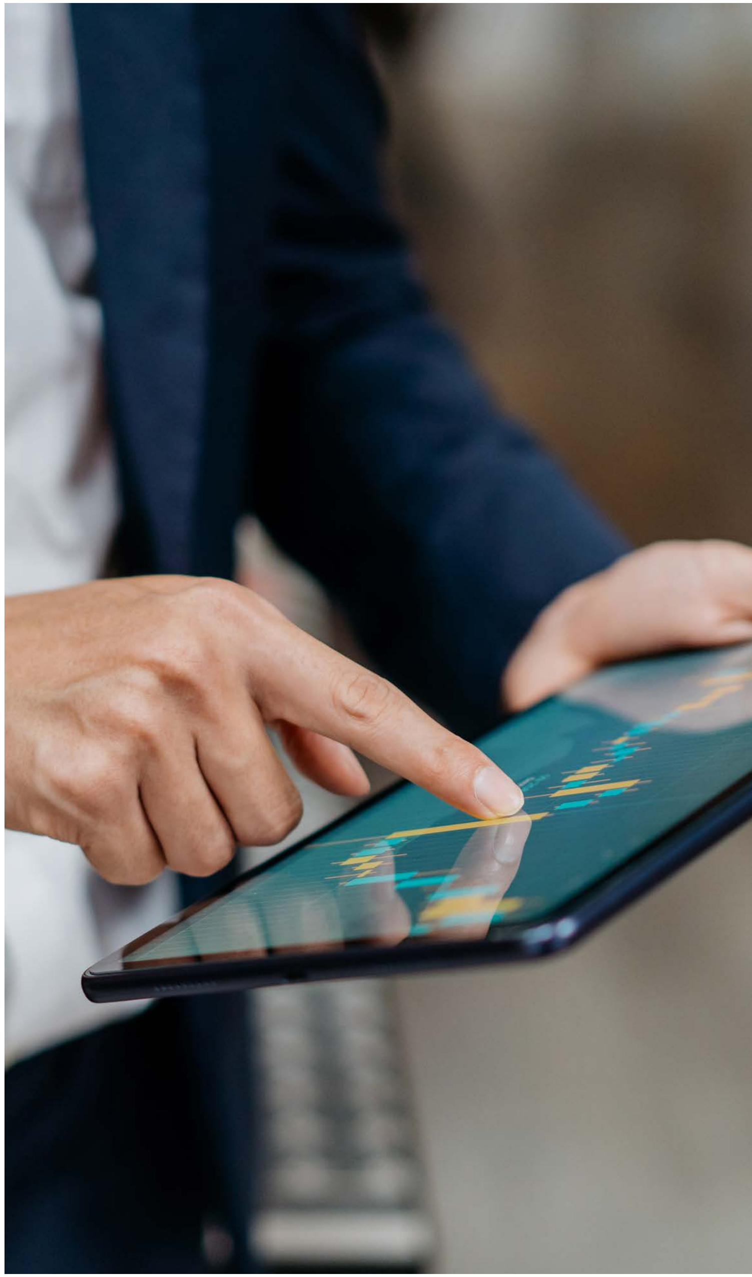
VICTORIA State Government | Department of Transport

Prevent Malware from Running

Patch Application

A patch fixes security vulnerabilities in software applications.	
Why do this?	Adversaries use known software vulnerabilities to target computers. Over 86% of known vulnerabilities do not come from Microsoft applications but from vendors such as Google, Adobe, Cisco, and Mozilla.
Challenges?	Microsoft provide highly automated approaches to patching their technology. Patching other applications is often a manual process with no clear insights to what is most important to patch. Due to this manual effort and complexity the cost is high and regular patching of these applications happens less frequently leaving organisations exposed to risk.
Ivanti's approach	The modifications to the Essential 8 maturity model for 2022 highlight the need for automated asset discovery before any vulnerability management or patch deployment occurs. Ivanti can provide customers with comprehensive asset discovery for hardware and software with the option of uploading that data to an asset management repository. Ivanti provides the largest catalogue of software updates on the market. Customers can patch applications from many vendors with the same ease they patch Microsoft products. This allows customers to reduce the cost to patch, they can patch more frequently and reduce significant risks faster. Leveraging the threat intelligence feed from Ivanti Neurons customers can see vulnerabilities that have been exploited in the wild, are associated with attack types such as ransomware and require urgent remediation. All Ivanti patch solutions integrate with vulnerability scanners to allow fast conversion of thousands of CVEs to a list of patches in seconds, this reduces manual effort speeding up the patch process.

Customer example	Ivanti Neurons for Patch Intelligence helps South Star Bank (SSB) respond to threats and resolve them more quickly by providing highly accurate data. Using patch intelligence SSB can isolate machine issues with patches, zero-day threats, and out-of-band updates.
Ivanti's solution	▪ Ivanti Neurons for Discovery ▪ Ivanti Patch for Microsoft Configuration Manager ▪ Ivanti Neurons Patch for Intune is a SaaS integration for Microsoft customers ▪ Ivanti Neurons for Patch Management supports Windows & MacOS as a SaaS offering ▪ For standalone on-premise, Ivanti Security Controls & Patch for Endpoint Manager ▪ For datacenter, Ivanti Security controls provides granular control & a full REST API ▪ Ivanti Neurons Patch Intelligence provides customers risk-based prioritisation Ivanti solutions can integrate with Microsoft Config Manager or Intune to extend automated application patching. Alternatively standalone on-premises or SaaS solutions allow customers to patch Windows, Linux and MacOS.



"The visibility and automation provided by Ivanti Neurons for Patch Intelligence saved SouthStar Bank several days a month researching and resolving vulnerabilities,"

said Jesse Miller, IT Specialist.

SOUTHSTAR® BANK
Banking...Texas Style

Prevent Malware from Running

Disable Untrusted Microsoft Office Macros

Microsoft Office applications can use software known as "macros" to automate routine tasks.	
Why do this?	Macros are increasingly used to enable the download of malware, compromising a system through legitimate functionality-often through phishing emails.
Challenges?	Due to lack of control, special requests, and one-time needs, macros get turned on and then left on. Organisations often lack the granularity & flexibility to control what macros can do on devices, that have a legitimate requirement for use of them.
Ivanti's approach	Ivanti provides several options to help control Office macros. Ivanti customers are able to turn macro GPO security settings on and off for devices at various times during a user's session, not just logon as with Microsoft GPO. Customers can configure a policy to enforce when a specific application start or stops, or a user connects to a specific network for example. Ivanti Application Control ensures that any file called to execute from a macro, is evaluated against the allow list policy. During an attack this is often a piece of malware or system tool that is to be used maliciously. Default rules or specific rules for Office applications can ensure system tools or scripts can never be launched from a macro.
Use case example	Administrators can build a process rule to define that whenever an application from the Office suite launches, that application cannot launch select files, examples being PowerShell, CMD and other scripting tools.
Ivanti's solution	■ Ivanti Environment Manager ■ Ivanti Application Control

Prevent Malware from Running

User Application Hardening

Block web browser access to Adobe Flash player (uninstall if possible), web ads, and untrusted Java code on the Internet.	
Why do this?	Browsers, Java, web ads, PDFs, macros and scripts have been popular ways to deliver malware to infect endpoints. Common social engineering and phishing techniques will use these to attempt to gain an initial access to a system.
Challenges?	Users run many apps and browsers, there are plug-ins to manage in each of those. If you can't easily lock down the browser or app, it's hard to manage the in-between. A lack of tooling and flexibility often means applications are banned from use or allowed with limited controls in place for specific use cases.
Ivanti's approach	Ivanti allow lockdown of Chrome, IE, and Firefox with templates, which drive configuration across all three browsers and provide self-healing capabilities. A context aware policy engine allows for dynamic application of policy based on flexible triggers, also control of child process execution from high-risk applications such as browsers, PDF readers or productivity tools. This means a customer has increased levels of flexibility and control based on the risk profile of the user device or application.
Use case example	A customer could create browser rules that when a user was logged on a device and the device was online and connected to the corporate network, with all security software running they could launch a browser with a relaxed set of policies applied. If the user connected to the same device disconnected from the network, or with a security tool disabled then the browser would run in a more locked down state, restricting capabilities.
Ivanti's solution	■ Ivanti Environment Manager ■ Ivanti Application Control

Limit the Extent of Incidents and Recover Data

Patch Operating Systems

A patch fixes security vulnerabilities in operating systems.	
Why do this?	Attackers use these vulnerabilities to move laterally through the network after gaining a foothold. Patching the OS can help limit the extent of an incident.
Challenges?	Exploits and development of new exploits have become commoditised in the past few years, and many enterprises still struggle to push updates quickly. The number of zero-day exploits identified in recent years has rapidly increased meaning out of band patches are often needed and can be complex and slow to deploy. With the increase of hybrid working post the pandemic without VPN access to remote devices often organisations do not know if patches have been deployed or the compliance status.
Ivanti's approach	The modifications to the Essential 8 maturity model for 2022 highlight the need for automated asset discovery before any vulnerability management or patch deployment occurs. Ivanti can provide customers comprehensive asset discovery for hardware and software with the option of uploading that data to an asset management repository. Many organisations will be using Microsoft tooling to help them patch Windows workloads. For those looking for more granularity, flexibility, and true edge access Ivanti provide solutions.

Customer example	Ivanti have worked with many customers looking for more flexibility when deploying patches to the datacenter, in controlled environments with limited change windows. The full REST API available with the Ivanti patch solutions allows customers to automate the patching cycle at the click of a button. This automation was a primary driver for an ANZ insurance company managing 5000 servers who now have automated patch cycles helping to reduce time to patch, reduce manual effort and the cost of the process.
Ivanti's solution	■ Ivanti Neurons for Discovery ■ Ivanti Neurons for Patch Management supports Windows & MacOS as a SaaS ■ For standalone on-premise, Ivanti Security Controls & Patch for Endpoint Manager ■ For datacenter, Ivanti Security controls provides granular control & a full REST API ■ Ivanti Neurons Patch Intelligence provides customers risk-based prioritisation Ivanti provide on-premises or SaaS solutions allowing customers to patch Windows, Linux and MacOS.

Limit the Extent of Incidents and Recover Data

Restrict Administrative Privileges

Only use administrator privileges for managing systems, installing legitimate software, and applying software patches. Allocate them solely to those who need them.	
Why do this?	Admin accounts are the "keys to the kingdom." Adversaries use them to exploit systems, move laterally and do damage to systems.
Challenges?	Some companies can enforce total lockdown of permissions, but generally users require some ability that leads to granting them admin privileges. When these privileges are revoked its often the user experience that suffers and a push back from the user community.
Ivanti's approach	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 or access to specific capabilities.
Customer example	An architecture and design practice in Victoria approached Ivanti as many users required privileges to allow auto updating of a key design application. While this simplified the management of the application it created a significant security risk. Ivanti was able to help auto elevate the design application only when it required updating, this meant there was no change of workflow for the users, and no extra privileges were granted. The outcome was reduced cost to manage the application update process, maintaining user experience and reducing security risks.
Ivanti's solution	Ivanti Application Control

Limit the Extent of Incidents and Recover Data

Multi-Factor Authentication

A user is only granted access after successfully presenting multiple, distinct pieces of identification: typically, something you know - like a password; something you have - like a physical token; and/or something you are - like biometric data.	
Why do this?	Each level of additional authentication makes it exponentially harder for adversaries to access your organisations information and infrastructure. The theft of a set of credentials will not automatically grant an adversary access to your systems.
Challenges?	Many organisations have a level of Single Sign-On and/or basic MFA to validate their users, but the method of setup and validation is typically reliant on passwords and the human end user.
Ivanti's approach	A passwordless, context-based MFA solution that does not compromise on either security or user experience. Organisations can leverage Ivanti Zero Sign-On (ZSO) to replace passwords with multiple levels of device, user, application and network validation that is transparent to the end user – meaning better security without the pain. ZSO can also automatically be activated as part of the Ivanti UEM device client, requiring no setup or client download to rollout MFA to your organisation. Additionally, ZSO can be deployed as a standalone solution with your existing UEM and Identity stack – like Microsoft Endpoint Manager, VMWare Workspace ONE, Ivanti EPM or any other solution.
Customer example	Headquartered in Stamford, CT, Conair is one of the largest and most diversified consumer products companies in the world. The company deploys Zero Sign-On (ZSO) to provide secure, conditional access to Microsoft Office 365 on any device. With Ivanti ZSO, Conair ensures that devices comply with company security policies before granting access to critical apps such as Office 365, a customised SAP sales app, the helpdesk, or any other app that uses single sign-on (SSO) authentication.
Ivanti's recommendation	Ivanti Zero Sign-on

Limit the Extent of Incidents and Recover Data

Daily Backup of Important Data

Regularly back up all data and store it securely offline.	
Why do this?	Your organisation can access data again if it suffers a cyber security incident. Cleaning and using a compromised system is risky.
Challenges?	Reimaging and restoring a system to a known good state and then restoring the data is usually recommended.
Ivanti's approach	Today Ivanti provides no solutions to aid customers with the backup of their data.
Ivanti's recommendation	The fastest way to recover from a malware incident, especially ransomware, is to re-provision the system and restore access to user data.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com.au

ivanti

ivanti.com.au
+61 2 8966 1800
contact-anz@ivanti.com