



Acronis

WHITE PAPER

Doing the Essential: How **Acronis** helps organisations implement Essential Eight strategies



In 2010, the Australian Signals Directorate (ASD), which provides intelligence support to Australian military operations, [developed a series of strategies](#) designed to help organisations mitigate cybersecurity incidents.

Over the course of the next seven years, the ASD determined that eight strategies were the most effective and critical for organisations to implement. Thus, the [Essential Eight](#) were born. This white paper will explore the overarching principles of the Essential Eight and provide a guide to how Acronis can help organisations implement critical elements of the strategies.

The strategies that make up the Essential Eight represent exactly what their name suggests — eight processes every organisation should absolutely adopt. There are other strategies in the Australian government's [Information security manual](#), a broad guide to cybersecurity. Some are highly recommended, others suggested.

The basics of the Essential Eight

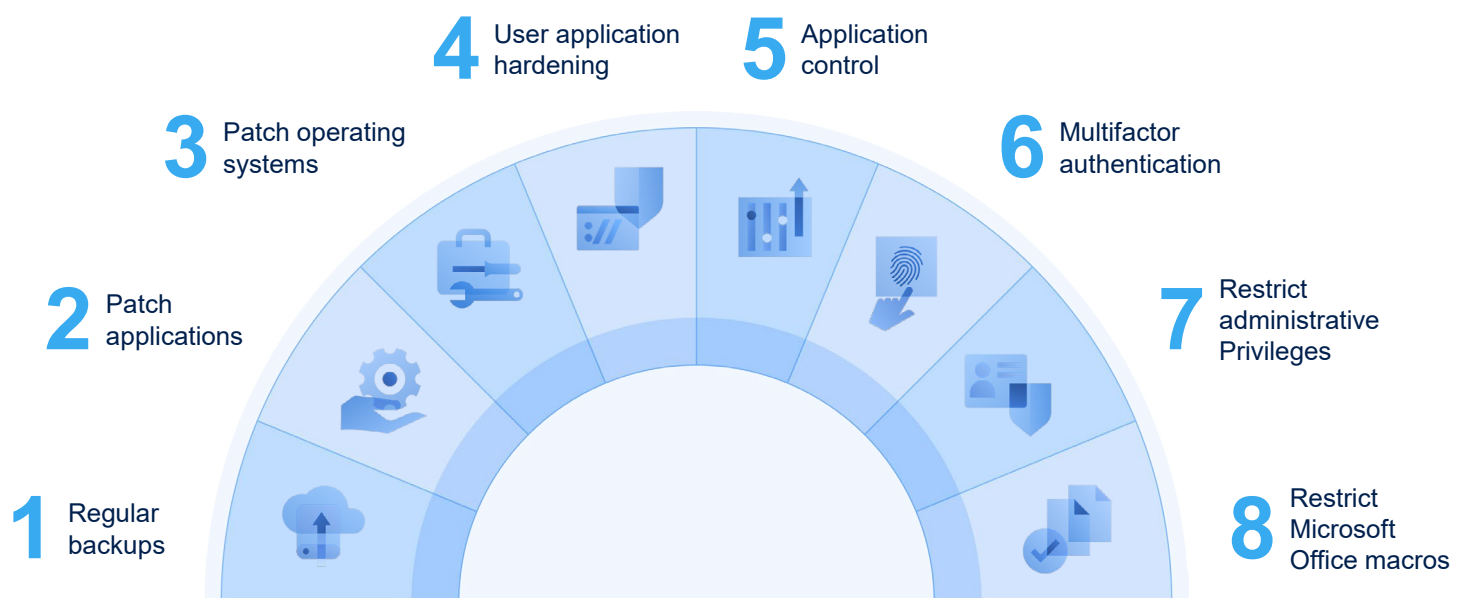
The details of the Essential Eight run deep. There are eight core strategies:

- Regular backups
- Patch applications
- Patch operating systems
- User application hardening
- Application control
- Multifactor authentication
- Restrict administrative privileges
- Restrict Microsoft Office macros



There are also large sets of sub requirements within each strategy, and those requirements change from time to time.

The Essential Eight mitigation strategies



Essential Eight maturity levels and what they mean

There are also [four levels of Essential Eight maturity](#), each of which focuses on an organisation's ability to fend off cyberattacks of varying levels of sophistication.



Level zero

The first is level zero and, as the name suggests, it refers to “weaknesses in an organisation’s overall cybersecurity posture” that threat actors can easily exploit. At level zero, an organisation is open to even the simplest of cyberattacks and is doing little to stop them.



Level one

This level refers to the ability to fend off increasingly sophisticated types of attacks. At level one, organisations can defend themselves against, for example, cyberattackers who use unpatched vulnerabilities.



Level two

Level one is too simple for most managed service providers (MSPs) and small to midsize enterprises (SMEs). It might be fine for the smallest businesses, but bigger organisations should aspire to level two, in which they can defend against cyberattackers “targeting credentials using phishing and employing technical and social engineering techniques to circumvent weak multifactor authentication,” according to Essential Eight documentation.



Level three

The third level focuses on the ability to stave off the most sophisticated attacks, mostly on critical infrastructure, such as electricity and water systems. These are the types of attacks that make news and can last for months or longer without being detected. The Essential Eight says of these attacks: “Once a foothold is gained on a system, malicious actors will seek to gain privileged credentials or password hashes, pivot to other parts of a network, and cover their tracks.”

A high-level guide to Acronis and the Essential Eight

For most MSPs and organisations, reaching level two is a reasonable goal to set. Level one is the bare minimum, probably not enough to ensure that the organisation can survive an attack. MSPs and organisations can always strive to reach level three, but it’s not a necessity for most of them. Level three goes beyond what most businesses need, although there is certainly no harm in an organisation setting out to reach the highest level of protection. For most organisations, though, level two is a very safe level that involves having multiple sub measures in place within the greater framework of the Essential Eight strategies.

This white paper is not intended to provide a reference for every detail of the Essential Eight. The ASD [offers copious documentation](#) of the eight strategies. Instead, this white paper looks at the high-level concept for each strategy at maturity level two. It also explains how Acronis enables MSPs and organisations implement some critical elements of the Essential Eight strategies. Acronis provides solutions that are essential to the implementation of four of the Essential Eight, which are listed here first.

How Acronis enables implementation of four of the Essential Eight

Acronis plays a critical role in enabling MSPs and business to implement four of the Essential Eight strategies.

1 Regular backups

The Essential Eight strategy defines regular backups as enabling efficient recovery following a cyber incident. These activities include backing up important data and assets. The Essential Eight also require admin privilege restrictions to limit access to backups, monitor and protect event logs from unauthorised deletion or modification, and other stipulations.

If a business or MSP gets hit with ransomware, backups ensure important data, software and configuration settings are not lost and can be recovered in a timely manner. With backup in place, the business can stay up and running no matter what kind of incident occurs. Performing regular backups is a proactive approach that safeguards against unforeseen disruptions to operations and strengthens business continuity.

The Essential Eight stipulate that:

- Backups of important data, software and configuration settings are performed and retained with a frequency and retention time frame in accordance with business continuity requirements.
- Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time.
- Backups of important data, software and configuration settings are retained in a secure and resilient manner.
- Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises.
- Unprivileged accounts cannot access backups belonging to other accounts.
- Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.
- Unprivileged accounts are prevented from modifying and deleting backups.
- Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.

Those can be difficult processes to put in place without the right solution. Organisations need flexible but powerful functionality to ensure that data is easily and rapidly recoverable.

Acronis and regular backups

Acronis solutions perform immutable backups to ensure critical data is secure and cannot be altered, deleted

or changed — an essential capability. At the same time, Acronis ensures that your system remains free from malware and other cyberthreats. You have the flexibility to set immutable backups to either Governance Mode or Compliance Mode. Acronis delivers file-level, disk-level, image and application backups of popular workloads including Mac, Windows, Linux, Microsoft 365 and Hyper-V, Google Workspace, VMware and more.

Acronis Cyber Protect Cloud with Advanced Backup is a comprehensive cyber protection solution for MSPs that enhances data protection services by combining cloud backup with cyber protection features like anti-malware and antivirus. It protects over 20 platforms from a single console, including Microsoft Exchange, SQL Server, Oracle DBMS and SAP HANA. Advanced Backup offers

continuous data protection, ensuring minimal data loss with near-zero RPOs and includes features like data protection maps, compliance reporting and off-host data processing.

Acronis Cyber Protect Cloud also offers MSPs a comprehensive disaster recovery solution that combines data protection, cybersecurity and management capabilities. It provides real-time data replication, failover clustering and automated recovery testing to ensure business continuity in the face of disasters. With features like artificial intelligence (AI)-powered threat detection, blockchain-based notarisation and proactive patching, Acronis Cyber Protect Cloud not only facilitates rapid recovery but also strengthens overall security posture.

2 Patch applications

Patching is essential for cybersecurity and a critical component of the Essential Eight. Unpatched applications leave vulnerabilities wide open for cybercriminals to attack without much effort. Regular vulnerability scans identify security flaws, and patches protect networks from exploitation. Every application you run is at risk if it's unpatched. Patching applications dramatically reduces the risk of damage from a cyberattack.

Timing is critical for patching. The second maturity level of the Essential Eight stipulates that:

- An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
- A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.
- Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 when either vulnerabilities are assessed as critical by vendors or working exploits exist.
- A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in other apps.

- Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and extensions, email clients, PDF software and security products are applied within two weeks of release, while vulnerabilities in other apps are applied within one month of release.

Patching strengthens organisational assets by getting rid of security vulnerabilities that put MSPs and businesses at risk. But staying up to date can be a costly and resource-intensive process.

Acronis and patching applications

Acronis makes that process cheaper and easier by offering tools that can identify all installed applications, scan for vulnerabilities and apply patches automatically, with no need for manual intervention. With Acronis solutions in place, security IT technicians can focus on

more critical objectives, such monitoring, investigation and incident response. Plus, MSPs and organisations have a greatly reduced need to hire expensive experts to patch systems.

For MSPs, Acronis RMM streamlines patching and inventory management through automation and comprehensive oversight. It automates patch management for Microsoft and over 300 third-party applications, featuring easy rollback options and fail-safe patching. Acronis RMM provides hardware and software inventories to track hardware for timely replacements and detect unauthorised applications. It also includes Device Sense,TM which automatically discovers, identifies and protects devices within a client's network.

3 Patch operating systems

Like applications, operating systems left unpatched are easy targets for cybercriminals. Unpatched operating systems leave security infrastructure exposed to malicious threats. The Essential Eight strategy of patching operating systems defines vulnerability scanning and patching operations.

For application patching, the Essential Eight stipulates that:

- An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
- A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
- A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.
- A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.
- Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
- Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-

facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as noncritical by vendors and no working exploits exist.

- Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.
- Operating systems that are no longer supported by vendors are replaced.

Automating these processes can help streamline vulnerability scanning and patching of operating systems to ensure the application of patches is carried out promptly and consistently.

Acronis and patching operating systems

Acronis automates those functions. Various Acronis technologies, including Acronis RMM, provide automated, user-initiated network and active directory discovery supported in Windows environments. Flexible scheduling helps you determine the frequency of vulnerability assessment scans, which run daily by default in compliance with the Essential Eight requirement. Additionally, Acronis updates collect vulnerability assessment data every three hours to ensure you have the latest information. Acronis also finds and identifies operating systems and patch levels, making it easy to remove or keep them.

4

User application hardening

User application hardening blocks users from changing web browser security settings. This Essential Eight strategy defines restrictions on users' interactions in a Windows environment, including protection from exploited vulnerabilities of unsupported software and blocking ads running malicious scripts.

Threat actors often use browsers and other standard applications to gain access to sensitive data. User application hardening reduces Microsoft Windows attack surfaces by mitigating vulnerabilities in unsupported or older versions of applications. User hardening ensures appropriate measures are in place such as removing outdated web browsers, blocking code injections and preventing browsers from processing Java and web ads from the internet.

Acronis and user application hardening

One of the Essential Eight requirements for user application hardening is the removal of Internet Explorer — a change from the previous version of the Essential Eight — which only required that Internet Explorer 11 not process content from the internet. Acronis removes the easily exploitable and outdated Internet Explorer from systems.

Acronis RMM simplifies software deployment and management for MSPs with centralised automation

across client environments using DeployPilot.™ This feature includes automatic anti-malware scans and digital signature checks for packages, ensuring security. Furthermore, Acronis RMM enhances system administration through scalable script management, enabling the creation and application of scripting plans across numerous client machines. These scripts can be scheduled based on specific conditions like machine activation or user inactivity, providing a flexible approach to software deployment and other IT tasks.



Other elements of the Essential Eight

While Acronis doesn't play a direct role in enabling organisations to implement these elements of the Essential Eight, Acronis technologies work well with solutions from other vendors that aid compliance.

5 Application control

Essential Eight documentation states that application control is “a security approach designed to protect against malicious code (also known as malware) executing on systems.”

Application control largely involves developing criteria for whether an application can execute on a system. Organisations need to set up blocklists, or lists of unapproved applications, and allowlists, or lists of approved applications.

Agreeing on a list of permitted applications — or a list of prohibited applications for that matter — is a common challenge most MSPs and businesses face. Once properly set up, application control critically reduces your risk of application-based threats introduced through the execution of unvalidated programs.

6 Multifactor authentication

Multifactor authentication (MFA) provides an additional layer of protection beyond traditional username and password authentication. MFA is a method that requires users to enter two or more forms of identification before gaining access to accounts or systems. This Essential Eight strategy is designed to safeguard against risks like phishing, compromised internet access and secure access to data and software.

For small businesses, MSPs and other organisations, employing MFA prevents the unauthorised access of threat actors. This strategy offers a critical line of defence against credential stuffing, brute force, phishing and other attacks. Additionally, MFA can safeguard against potential lateral movement within a network.

7

Restrict administrative privileges

Restricting administrative privileges limits the number of administrative accounts within an organisation's IT infrastructure to only essential administrators. This Essential Eight strategy is intended to prevent cybercriminals from gaining unauthorised access to restricted accounts the criminals can then use to escalate privileges, evade detection and spread infection.

By restricting administrative privileges, MSPs and organisations can effectively harden Windows administrative access. This greatly minimises the attack surface and helps secure their network and manage cyber risk. In the event a user's account is compromised, restricting administrative privileges prevents adversaries from accessing restricted assets. As such, restricting privileges can reduce the impact of financial and operational damage from a cyberattack.

8

Configure Microsoft Office macros

This strategy involves disabling Microsoft Office macro settings to prohibit users from misusing them. Microsoft Office macro settings should be blocked on incoming emails or other methods of entry and undergo anti-malware scanning. Essential Eight specifications include event logging of macros allowed and blocked, compiling an inventory of trusted publishers and validating those lists annually.

Through configuring Microsoft macros, MSPs and businesses ensure that only trusted users, locations, document add-in catalogues and other macro settings are granted. Configuring Microsoft macro settings gives organisations and service providers control over autorun tasks that can introduce unwanted executions while maintaining user productivity and flexibility.



Acronis solutions for implementing the Essential Eight

The Acronis capabilities that facilitate implementation of the Essential Eight are available as part of one of two solutions: Acronis Cyber Protect Cloud for MSPs and Acronis Cyber Protect for IT operations in businesses and other organisations.

Acronis Cyber Protect Cloud

[Acronis Cyber Protect Cloud](#) is an integrated cyber protection solution specifically designed for MSPs. It combines cybersecurity, data protection and endpoint management into a single, unified platform, significantly reducing the complexity and overhead associated with managing multiple tools.

The solution features advanced AI-based static and behavioral heuristic antivirus, anti-malware and anti-ransomware technologies, along with data loss prevention through device control. Acronis Extended Detection and Response (XDR) further enhances endpoint protection with full-stack anti-malware, improving detection speed and accuracy while ensuring zero false positives. Additionally, Acronis Cyber Protect Cloud supports fail-safe patching, forensic backup and robust automation capabilities, all of which are aimed at simplifying the management of client environments and streamlining business operations.

Acronis Cyber Protect

[Acronis Cyber Protect](#) is a comprehensive cyber protection solution for businesses that seamlessly integrates backup and data protection with advanced cybersecurity features. It offers secure, immutable backups and rapid recovery capabilities, including cloud-to-cloud backups for major productivity suites. The software includes robust security features such as AI-enhanced behavioral heuristic antivirus, anti-malware, anti-ransomware and anti-cryptojacking technologies, as well as endpoint detection and response (EDR) and real-time threat protection.

Additionally, it provides endpoint management tools like proactive patching, automated scripts and remote access for troubleshooting, along with detailed compliance reporting and data protection maps. Centralised management through a single console simplifies the administration of cybersecurity, backup and endpoint management tasks, while AI and machine learning (ML) technologies enhance predictive alerts and anomaly detection.