DriveLock
securing your digital tomorrow

Essential Eight
An Overview

Whitepaper

DriveLock
securing your digital tomorrow

Contents

1. Introduction

1.1 DriveLock Zero Trust approach

In today's digital environment, the success of your business depends on how reliably you protect people, businesses, and your services from cyberattacks and the loss of valuable data.
Our goal is to protect the company's data, devices, and systems. To achieve this, we rely on the latest technologies, experienced security experts and Zero Trust solutions.
In today's security architecture, Zero Trust means a paradigm shift according to the maxim **"Never trust, always verify"**. This means that data can be reliably protected - even in modern business models.
Cloud-based solutions from DriveLock offer multi-layered security. They are immediately available and economically efficient with low investment costs. DriveLock is made without a back door.

1.2 Strategies to Mitigate Cyber Security Incidents and the Essential 8

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies to help cyber security professionals in all organisations mitigate cyber security incidents caused by various cyber threats.

These Mitigation Strategies are:

- Mitigation Strategies to **Prevent Malware Delivery and Execution**
- Mitigation Strategies to **Limit the Extent of Cyber Security Incidents**
- Mitigation Strategies to **Detect Cyber Security Incidents and Respond**
- Mitigation Strategies to **Recover Data and System Availability**
- Mitigation Strategy Specific to P**reventing Malicious Insiders**

While no single mitigation strategy is guaranteed to prevent cyber security incidents, organisations are recommended to implement **eight essential mitigation strategies** as a baseline. This baseline, known as the **Essential Eight**, makes it much harder for adversaries to compromise systems.

- Application Control
- Patch applications
- Configure Microsoft Office macro settings
- User application hardening
- Restrict administrative privileges
- Patch operating systems
- Multi-factor authentication
- Daily backups

To assist organizations in determining the maturity of their implementation of the Essential Eight, **three maturity levels** have been defined for each mitigation strategy.

The maturity levels are defined as:

- Maturity Level One: **Partly aligned with the intent of the mitigation strategy.**
- Maturity Level Two: **Mostly aligned with the intent of the mitigation strategy.**
- Maturity Level Three: **Fully aligned with the intent of the mitigation strategy.**

Each of the Essential 8 baseline strategies fall under the main 5 strategies in the following manner:

- **Mitigation Strategies to Prevent Malware Delivery and Execution:**
  - **Essential 8**

1. **Application control** to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
2. **Patch applications** (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computers with 'extreme risk' security vulnerabilities within 48 hours. Use the latest version of applications
3. **Configure Microsoft Office macro settings** to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
4. **User application hardening.** Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.

- **Mitigation Strategies to Limit the Extent of Cyber Security Incidents:**
  - **Essential 8**

5. **Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.
6. **Patch operating systems** Patch/mitigate computers (including network devices) with 'extreme risk' security vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
7. **Multi-factor authentication** including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

- **Mitigation Strategies to Detect Cyber Security Incidents and Respond:**
  - **Essential 8**

    None
- **Mitigation Strategies to Recover Data and System Availability:**
  - **Essential 8**

    8. **Daily backups** of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
- **Mitigation Strategy Specific to Preventing Malicious Insiders:**
  - **Essential 8**

    None

2. Further information

The **Australian Government Information Security Manual** (ISM) assists in the protection of information that is processed, stored or communicated by organizations' systems. It can be found at https://www.cyber.gov.au/ism.

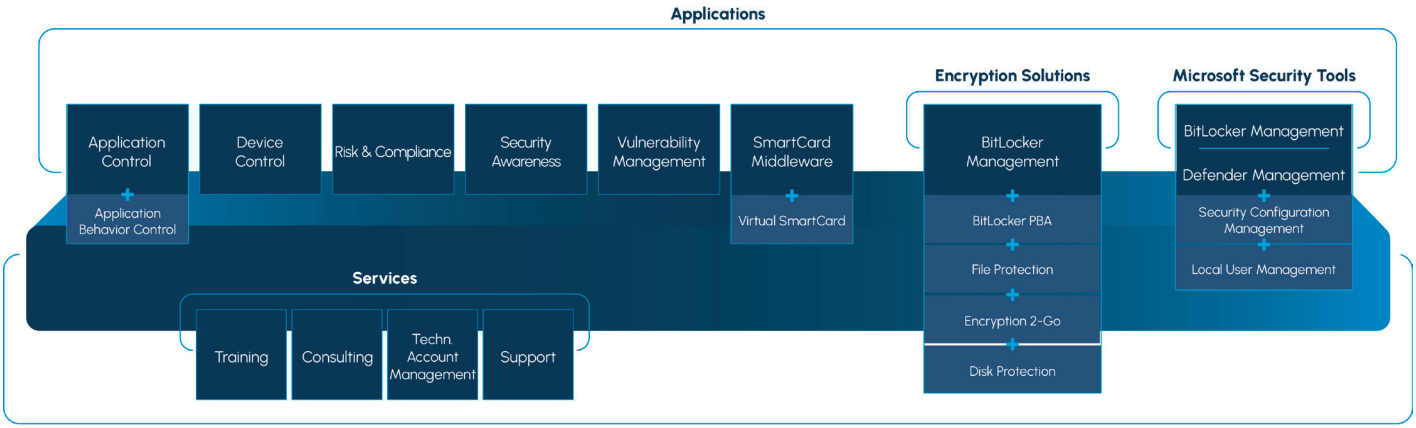
The **Strategies to Mitigate Cyber Security Incidents** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents.

The **Essential Eight Maturity Model** complements the advice in the Strategies to Mitigate Cyber Security Incidents. It can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model.

3. Mitigation Strategies

DriveLock offers complete protection against cyberattacks for all endpoint devices.

DriveLock Zero Trust Platform



DriveLock Zero Trust Platform

DriveLock brings Zero Trust to the endpoint device and combines the following elements: Data Protection, Endpoint Protection, Endpoint Detection & Response and Identity & Access Management.

In today's security architectures, Zero Trust means a paradigm shift according to the maxim **"Never trust, always verify"**. One of the cornerstones of protecting our digital lifestyle is preventing sensitive data from being compromised. It is a core of any business strategy that is based on networked digital technologies.

To help customers with a clear structured and guided way to implement a certain set of security protections the Australian Government a suggested implementation order to build a strong cyber security posture for organizations.

The eight strategies can be grouped as the following:

ESSENTIAL 8

APPLICATION CONTROL

DriveLock's Application Control is based on "Predictive Whitelisting" and prevents the execution of all non-approved/malicious applications including .exe, DLL, & scripts, and also extends to Microsoft's latest recommended block rules.

PATCH APPLICATIONS

DriveLock's Vulnerability Management identifies, evaluates & reports all vulnerabilities and risks in the inbuilt DriveLock Console.

CONFIGURE MICROSOFT OFFICE MACROS

Our solution can control where an application can read from or write to and which child processes it can launch, with the ability to prevent execution of unwanted Microsoft Office macros even in trusted locations.

USER APPLICATION HARDENING

DriveLock can prevent web browsers from storing data outside limited locations on the local hard disk or launching child processes.

RESTRICT ADMIN PRIVILEGES

Admin accounts are the "keys to the kingdom". DriveLock's Native Security module manages local accounts and admin permissions to prevent privilege escalation.

PATCH OPERATING SYSTEMS

Using DriveLock's Vulnerability Management, all vulnerabilities are identified and reported in the DriveLock Console to alert the admin of risks and necessary patching.

MULTI-FACTOR AUTHENTICATION

DriveLock's Pre-Boot Authentication provides full support of multi-factor authentication, as well as vendor-independent smartcard middleware to prevent vendor lock-in. DriveLock's console is also integrated with Identity and Access Management for further measures.

DAILY BACKUPS

DriveLock's File Protection or Encryption 2-Go can be used to backup encrypted data on a daily basis. Data is also stored on non-rewritable / non-erasable media, where DriveLock's use of encryption makes the decommissioning process much easier.

3.1 Prevent Malware Delivery and Execution

1 Application control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts

Maturity Level:
(e.g. Windows Script Host, PowerShell and HTA) and installers.

Level 1	Level 2	Level 3
Application control is implemented on all workstations to restrict the execution of executables to an approved set. Application control is implemented on all servers to restrict the execution of executables to an approved set.	Level 2 is extended to software libraries, scripts and installers to an approved set.	Level 3 is extended to Microsoft's latest recommended block rules are implemented to prevent application control bypasses.

Why: All non-approved applications (including malicious code) are prevented from executing.

How DriveLock can help:

DriveLock's Application Control based on "Predictive Whitelisting" and Application Behavior Control can cover Maturity Level 1, 2 and 3 of the Essential 8 requirements.

2 Patch applications (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.

Maturity Level:

Level 1	Level 2	Level 3
Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	For level 2 remediation needs to be done within 2 weeks	For level 3 remediation needs to be done within 48 hours. In addition n automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place.

Why: Security vulnerabilities in applications can be used to execute malicious code on systems.

How DriveLock can help:

With DriveLock's Vulnerability Management all vulnerabilities of each device can be identified and reported on in the DriveLock Operation Centre (DOC) as well as any upcoming risk evaluated. Not every patch can be installed because existing applications may be adversely affected by the installation of a new patch, however with the DOC information regarding vulnerability risks is available to the administration team to act upon. DriveLock is able to cover Maturity Level 1, 2 and 3 of the Essential 8 requirements.

3 Configure Microsoft Office macro settings to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.

Maturity Level:

Level 1	Level 2	Level 3
Microsoft Office macros are allowed to execute, but only after prompting users for approval. Microsoft Office macro security settings cannot be changed by users.	In addition to level 1 only signed Microsoft Office macros are allowed to execute. Microsoft Office macros in documents originating from the internet are blocked.	Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros. Microsoft Office macros in documents originating from the internet are blocked. Microsoft Office macro security settings cannot be changed by users.

Why: Microsoft Office macros can be used to deliver and execute malicious code on systems.

How DriveLock can help:

While the basic settings of this topic are configured using Windows Group Policy, DriveLock can go further: with Application Behavior Control DriveLock can control where an application such as Office can read from or write to and which child processes it can launch. So although a macro from a trusted location may be compromised, Application Behaviour Control is able to prevent the execution of unwanted sections of these macros. DriveLock is able to cover Maturity Level 1, 2 and 3 of the Essential 8.

4 User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.

Maturity Level:

Level 1	Level 2	Level 3
Web browsers are configured to block or disable support for Flash content.	In addition, Web browsers are configured to block web advertisements. Web browsers are configured to block Java from the internet	In addition to level 2 Microsoft Office is configured to disable support for Flash content. Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.

Why: Flash, ads and Java are popular ways to deliver and execute malicious code on systems.

How DriveLock can help:

The settings are configured using the web browser in place but DriveLock Application Behavior Control can go further: for instance it can prevent web browsers from storing data outside specific locations on the local hard disk or launching child processes. Modern web applications and browsers can access local data in ways other than Flash or Java. DriveLock covers Maturity Level 1 and 2 of the Essential 8 requirements.

3.2 Limit the extent of Cyber Threats

5 Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.

Maturity Level:

Level 1	Level 2	Level 3
Privileged access to systems, applications and data repositories is validated when first requested. Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.	Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis. Policy security controls are used	Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis. Privileged access to systems, applications and data repositories is limited to that required for personnel to undertake their duties. Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.

Why: Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.

How DriveLock can help:

The requirement is valid in general for any system and any user account, however it often starts with local users and local administrative privileges which are then escalated to a server. DriveLock's Native Security module helps with managing local accounts and local administrative permissions so it can effectively prevent privilege escalation. DriveLock can cover Maturity Level 1 and 2 of the Essential 8 requirements.

6 Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.

Maturity Level:

Level 1
Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.
Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

Level 2
Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.
Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

Level 3
Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place.
Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

Why: Security vulnerabilities in operating systems can be used to further the compromise of systems.

How DriveLock can help:

With DriveLock's Vulnerability Management all vulnerabilities of each device can be identified and reported on in the DriveLock Operation Centre (DOC) as well as any upcoming risk evaluated. Not every patch can be installed because existing applications may be adversely affected by the installation of a new patch, however with the DOC information regarding vulnerability risks is available to the administration team to act upon. DriveLock is able to cover Maturity Level 1, 2 and 3 of the Essential 8 requirements.

7 Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

Maturity Level:

Level 1
Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards, mobile app one-time password tokens, SMS messages, emails, voice calls or software certificates.

Level 2
Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smart-cards or mobile app one-time password tokens.

Level 3
Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication is used to authenticate all users when accessing important data repositories. Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smart cards.

Why: Stronger user authentication makes it harder for adversaries to access sensitive information and systems.

How DriveLock can help:

DriveLock's Pre-Boot Authentication (available for Microsoft BitLocker as well as with our own disk encryption engine) provides full support of multi-factor authentication. Thus the whole boot-process is secured with multi-factor authentication.

DriveLock provides a Vendor independant smartcard middleware platform to to prevent vendor lock in when smart cards or tokens are selected as the second factor authentication. DriveLock can cover Maturity Level 1, 2 and 3 of the Essential 8 requirements.

3.3 Recover Data and System Availability

8 Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

Maturity Level:

Level 1	Level 2	Level 3
Backups of important information, software and configuration settings are performed monthly. Backups are stored for between one to three months. Partial restoration of backups is tested on an annual or more frequent basis.	Backups of important information, software and configuration settings are performed weekly. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for between one to three months. Full restoration of backups is tested at least once. Partial restoration of backups is tested on a bi-annual or more frequent basis.	Backups of important information, software and configuration settings are performed at least daily. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for three months or greater. Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur. Partial restoration of backups is tested on a quarterly or more frequent basis.

Why: To ensure information can be accessed following a cyber security incident (e. g. a ransomware incident).

How DriveLock can help:

DriveLock's File Protection or Encryption 2-Go can be used to prevent administrators from accessing classified information while ensuring that a backup strategy is implemented as needed since the data that is backed up is encrypted.
Especially when fulfilling the level 3 requirement of storing data on non-rewritable/non-erasable media, customers should keep in mind that at some point in time this media needs to be decommissioned. When using encrypted backups the decommissioning is much easier as there is no requirement for destruction of the media.

DriveLock
securing your digital tomorrow

Contact us!

DriveLock SE
+49 (89) 546 36 49-0
info@drivelock.com

www.drivelock.com