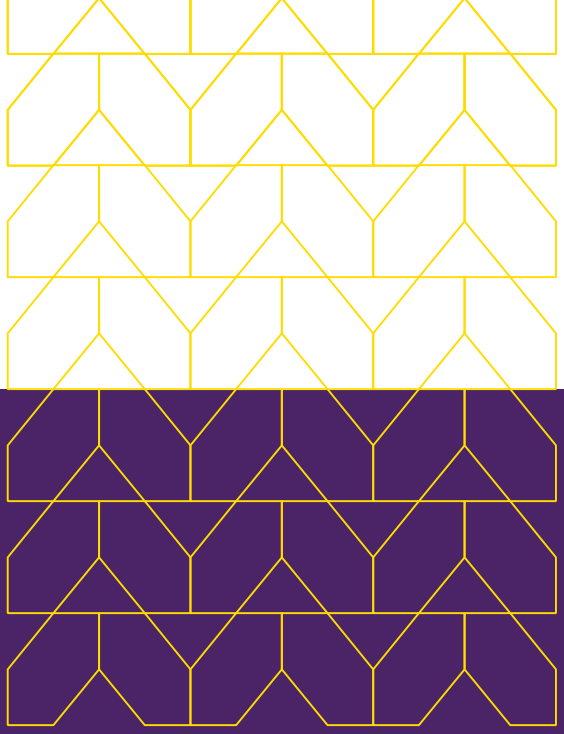
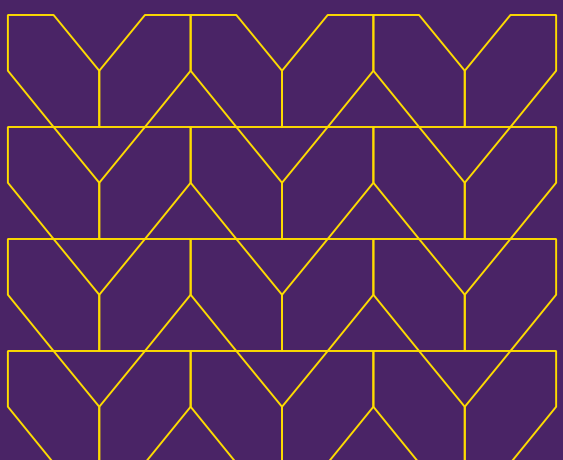


MENLO SECURITY

# How Menlo Security Supports the ACSC Essential Eight and Selected Excellent Mitigation Strategies

This document provides a summary of how the Menlo Security Isolation Platform can help organisations that are seeking to improve their security posture in accordance with the ACSC recommended mitigation strategies.



## The Power of Isolation powered security

Using isolation powered security powers an organization's ability to support ACSC's Essential Eight recommendations for mitigating risk. It does this by giving security teams visibility and control into web, email and application traffic without impacting the end user experience. Designed to thwart modern cybersecurity threats, isolation can give enterprises the protection they need to keep users, data and the organization safe—enabling organizations to implement a Secure Cloud Transformation journey.

This document provides an overview of how Menlo Security contributes towards organisations meeting these requirements, both in terms of technologies that are relevant, and with respect to the maturity level and each strategy's objectives where applicable.


When considering the implementation order as suggested in the ACSC Strategies to Mitigate Cyber Security Incidents guide, Menlo Security directly supports two of the main outcomes, specifically prevent malware delivery and execution, and limit the extent of cyber security incidents.

## Suggested Mitigation Strategy Implementation Order (start with threats of most concern to the organisation)

### Targeted cyber intrusions (advanced persistent threats) and other external adversaries who steal data:

1. Implement 'essential' mitigation strategies to:
    a. **Prevent malware delivery and execution**
    b. **limit the extent of cyber security incidents**
    c. detect cyber security incidents and respond
2. Repeat step 1 with 'excellent' mitigation strategies.
3. Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

### **Ransomware and external adversaries who destroy data** and prevent computers/networks from functioning:

1. Implement 'essential' mitigation strategies to:
    a. Recover data and system availability
    b. **Prevent malware delivery and execution**
    c. **Limit the extent of cyber security incidents**
    d. Detect cyber security incidents and respond
2. Repeat step 1 with 'excellent' mitigation strategies.
3. Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached. Note that 'Hunt to discover incidents' is less relevant for ransomware that immediately makes itself visible.

Menlo Security focuses heavily on the prevention of malware delivery and execution (including Ransomware), with the associated outcome of limiting the extent of cyber security incidents as a direct result.

# Essential Strategies

## Mitigation Strategies to Prevent Malware Delivery and Execution:

### 1. Application Control

#### The recommendation

Application control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.

#### Menlo Security benefits

Menlo Security Private Access provides reverse browser isolation. This allows a web application to be accessed without the user's browser directly interacting with the application server. Applications are instead accessed via a remote browser. Applications can also be assigned on a granular user-by-user basis.

### Maturity level: 1

| Description | How Menlo Security addresses strategy |
|---|---|
| The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients. | For web browser-based activity, web enabled applications are accessed via reverse browser isolation, separating the user's endpoint and browser from the application server. Precise controls can be placed around what application a user can access, along with Read-Only or Read-Write access (Uploads/Downloads).<br><br>This avoids the need to run a client on the endpoint for certain applications, and also allows for control the version of browser being used. |

## 2. Patch Applications

### The recommendation

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.

### Menlo Security benefits

Menlo Security conducts all fetch and execute commands in a remote browser in the cloud—separate from users' devices. If an endpoint is not up to date with patching (e.g. OS and/or application), the vulnerabilities are not able to be exploited via web browsing as there is no direct interaction between the user's browser and web site (which may be a legitimate site that has been compromised).

## Maturity level: 1

| Description | How Menlo Security addresses strategy |
|---|---|
| Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. | Menlo Private Access (MPA) provides protection against unpatched vulnerabilities on servers, using reverse browser isolation technology. It can allow for certain internet facing servers to be relocated to a private network, specifically relevant for internal applications which may be publicly exposed. |
| Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release. | Remote Browser Isolation (RBI) provides a virtual patch, by preventing malicious or compromised web servers from running exploit code against un-patched browsers, plugins, or operating systems. Document isolation also provides a virtual patch against vulnerabilities being targeted in PDF software, Office applications, and other document applications. |
| A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. | N/A |
| A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. | N/A |
| Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed. | RBI provides a virtual patch, by preventing malicious or compromised web servers from running exploit code against un-patched browsers, plugins, or operating systems. Document isolation also provides a virtual patch against vulnerabilities being targeted in PDF software, Office applications, and other document applications. |

## 3. Configure MS Office Macro Settings

### The recommendation

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.

### Menlo Security benefits

Menlo Security executes all documents from email and the web in a remote browser in the Isolation Platform. Office documents can be viewed in browser isolation via a viewer, and a SafePDF copy may also be generated which has all active content and macros removed. No macros would be able to run on user devices if viewed via isolation or SafePDF.

If original documents (including macros) are required, Menlo Security has partnered with several Content Disarm and Reconstruction (CDR) vendors to safely deliver original files, alternatively, the files can be scanned using an AV engine and Cloud Sandbox, and only made available if they pass these checks.

### Maturity level: 2

| Description | How Menlo Security addresses strategy |
|---|---|
| Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. | Compensating control: RBI allows Office documents to be accessed via Document Isolation, eliminating the need to have the original document downloaded to the endpoint. |
| Microsoft Office macros in files originating from the Internet are blocked. | Compensating control: RBI allows Office documents to be accessed via Document Isolation, eliminating the need to have the original document downloaded to the endpoint. |
| Microsoft Office macro antivirus scanning is enabled. | RBI includes the capability of AV scanning (plus Sandbox analysis) of Office documents to detect malicious macros. |
| Microsoft Office macros are blocked from making Win32 API calls. Microsoft Office macro security settings cannot be changed by users. Allowed and blocked Microsoft Office macro executions are logged. | Compensating control: RBI allows Office documents to be accessed via Document Isolation, eliminating the need to have the original document downloaded to the endpoint. Users are not permitted to change Document Isolation policies. |
| Microsoft Office macro security settings cannot be changed by users. | Users are unable to change RBI settings. It is also possible to allow only SafePDF versions of Office documents, eliminating the possibility of a macro enabled document from being downloaded to the endpoint. |

## 4. Use Application Hardening

### The recommendation

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

### Menlo Security benefits

Menlo Security strips out all active content—such as Flash and Java—and rewrites it in HTML5. This protects users without changing the native browsing experience.

## Maturity level: 2

| Description | How Menlo Security addresses strategy |
|---|---|
| Web browsers do not process Java from the internet. | RBI separates the browser from the internet. This completely prevents Java from the server running directly in the browser. Any Java/JavaScript is processed only in the remote browser. |
| Web browsers do not process web advertisements from the internet. | RBI allows for the blocking of Web Advertisements via Category policy, and if allowed, advertisements are processed only in the remote browser. |
| Internet Explorer 11 does not process content from the Internet. | RBI can either block IE11 internet access, or separates the browser from the internet, preventing IE11 from processing content from the Internet. |
| Microsoft Office is blocked from creating child processes. | RBI allows Office documents to be accessed via Document Isolation, eliminating the need to have the original document downloaded to the endpoint. |
| Microsoft Office is blocked from creating executable content. | RBI allows Office documents to be accessed via Document Isolation, eliminating the need to have the original document downloaded to the endpoint. |
| Microsoft Office is blocked from injecting code into other processes. | RBI allows Office documents to be accessed via Document Isolation, eliminating the need to have the original document downloaded to the endpoint. |

## Maturity level: 2



| Description | How Menlo Security addresses strategy |
|---|---|
| Microsoft Office is configured to prevent activation of OLE packages. | RBI allows Office documents to be accessed via Document Isolation, eliminating the need to have the original document downloaded to the endpoint. |
| PDF software is blocked from creating child processes. | RBI allows PDF documents to be accessed via Document Isolation, eliminating the need to have the original document downloaded to the endpoint. |
| ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented. | RBI allows Office/PDF documents to be accessed via Document Isolation, eliminating the need to have the original document downloaded to the endpoint. |
| Web browser, Microsoft Office and PDF software security settings cannot be changed by users. | RBI allows Office documents to be accessed via Document Isolation, eliminating the need to have the original document downloaded to the endpoint. Users are not permitted to change Document Isolation policies. |
| Blocked PowerShell script executions are logged. | N/A |

## Mitigation Strategies to Limit the Extent of Cyber Security Incidents:

### 5. Restrict Administrative Privileges

#### The recommendation

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.

#### Menlo Security benefits

Menlo Security decouples all administrator and privileged user web and email access—eliminating the possibility that devices can be compromised, while providing additional access and controls where appropriate.

### Maturity level: 1

| Description | How Menlo Security addresses strategy |
|---|---|
| Requests for privileged access to systems and applications are validated when first requested. | Menlo Private Access allows highly granular control over users and applications they are granted access to. |
| Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services. | RBI/SWG policy can be set to prevent privileged accounts being used when accessing the Internet. |
| Privileged users use separate privileged and unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. | RBI/SWG policy can be set to prevent privileged accounts being used when accessing the internet. Alternatively a separate tenancy can be utilised to provide a separate environment for privileged user accounts. |
| Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. | N/A |

## 6. Patch Operating Systems

### The recommendation

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.

### Menlo Security benefits

Menlo Security conducts all fetch and execute commands in a remote browser in the cloud—separate from users' devices. If an endpoint is not up to date with patching (e.g. OS and/or application), the vulnerabilities are not able to be exploited via web browsing as there is no direct interaction between the user's browser and web site (which may be a legitimate site that has been compromised).

## Maturity level: 1

| Description | How Menlo Security addresses strategy |
|---|---|
| Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. | RBI<br>Menlo Private Access provides protection against unpatched vulnerabilities on servers, using reverse browser isolation technology. |
| Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release. | RBI<br>Menlo Private Access provides protection against unpatched vulnerabilities on servers, using reverse browser isolation technology. |
| A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services. | N/A |
| A vulnerability scanner is used at least fortnightly to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices. | N/A |
| Operating systems that are no longer supported by vendors are replaced. | N/A |

# Excellent

## Mitigation Strategies to Prevent Malware Delivery and Execution:

**Automated dynamic analysis of email and web content run in a sandbox,** blocked if suspicious behaviour is identified (e.g. network traffic, new or modified files, or other system configuration changes).

***How Menlo Security addresses strategy***

- Remote Browser Isolation
- Email Isolation

**Email content filtering.** Allow only approved attachment types (including in archives and nested archives). Analyse/sanitise hyperlinks, PDF and Microsoft Office attachments. Quarantine Microsoft Office macros.

***How Menlo Security addresses strategy***

- Email isolation
- Document isolation

**Web content filtering.** Allow only approved types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks and free domains.

***How Menlo Security addresses strategy***

Secure Web Gateway policies can block access to malicious domains and IP addresses, advertisements, proxy avoidance sites etc using category-based filtering.

**Deny corporate computers direct internet connectivity.** Use a gateway firewall to require use of a split DNS server, an email server and an authenticated web proxy server for outbound web connections.

***How Menlo Security addresses strategy***

Remote Browser Isolation decouples computer browsers from the Internet. Web proxy forms the baseline protection for outbound web connections, however the isolation technology separates the browser from the internet through the use of a remote browser running in the MSIP.

# Conclusion

Menlo Security Secure Web Gateway and Private Access, powered by our Remote Browser Isolation technology, can help organisations eliminate the prospect of malware delivery and execution, plus the associated cyber security incidents, from threats which originate from the Web and Email. This can either directly, or as a compensating control, support several of the Essential Eight mitigation strategies, plus also a number of Excellent mitigation strategies, and in doing so, help organisations on their Essential Eight Maturity Model journey.


MENLO SECURITY

**To find out more, contact us:**

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com


## About Menlo Security

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.