Implement Windows security enhancements with Microsoft Defender for Endpoint

# Understand attack surface reduction

Attack surface Reduction is hardening the places where a threat is likely to attack.

|  |  |
| --- | --- |
| Solution | Description |
| Attack surface reduction rules | Reduce vulnerabilities (attack surfaces) in your applications with intelligent rules that help stop malware. (Requires Microsoft Defender Antivirus). |
| Hardware-based isolation | Protect and maintain the integrity of a system as it starts and while it’s running. Validate system integrity through local and remote attestation. |
| Application control | Use application control so that your applications must earn trust in order to run. |
| Exploit protection | Help protect operating systems and apps your organisation uses from being exploited. Exploit protection also works with third-party antivirus solutions. |
| Network Protection | Extend protection to your network traffic and connectivity on your organisation’s devices. (Requires Microsoft Defender Antivirus). |
| Web protection | Secure your devices against web threats and help you regulate unwanted content. |
| Controlled folder access | Help prevent malicious or suspicious apps (including file-encrypting ransomware malware) from making changes to files in your key system folders. (Requires Microsoft Defender Antivirus). |
| Device control | Protects against data loss by monitoring and controlling media used on devices, such as removable storage and USB drives, in your organisation. |

# Enable Attack Surface reduction rules

Attack surface reduction rules target certain software behaviours that are often abused by attackers. Such behaviours include:

* Launching executable files and scripts that attempt to download or run files
* Running obfuscated or otherwise suspicious scripts
* Performing behaviours that apss don’t usually initiate during normal day-to-day work

Some such software behaviours are sometimes seen in legitimate applications however these are considered risky because they are commonly abused by malware.

Each attack surface reduction rule contains one of three settings:

* **Not configured:** Disable the attack surface reduction rule
* **Block:** Enable the ASR rule
* **Audit:** Evaluate how the ASR rule would impact your organisation if enabled
* **Warn:** Enable the ASR rule but allow the end user to bypass the block