C 🗘 A L F I R E

IMPLEMENTING WINDOWS DEFENDER FOR ISO 27001, PCI, AND FEDRAMP



North America | Latin America | Europe 877.224.8077 | info@coalfire.com | coalfire.com

Coalfiresm and CoalfireOnesm are registered service marks of Coalfire Systems, Inc. All rights reserved.

INTRODUCTION

The threat of a cyber-attack is a constant factor all organizations must consider when developing their information security posture. A particular area of concern is the use of malicious code to introduce or exploit vulnerabilities within the system, or gain access to elevated privileges not readily available to the attacker. In order to provide organizations a strong, unobtrusive, and default solution to address malicious code protections, Microsoft has introduced an updated and more robust version of Windows Defender for Windows Server 2016 and the Windows 10 operating system. This new version of Windows Defender includes many features organizations have come to expect from malicious code protection programs, including auto-update capabilities, active enforcement and quarantine capabilities, and an 'on-by-default' configuration to ensure that every Windows host has built-in malicious code protections out of the box, even if an organization chooses not to implement additional host-based protections within their system environment.

In order to help customers implement this capability for compliance with ISO, PCI, or FedRAMP, Microsoft worked closely with Coalfire, a recognized third-party IT compliance firm, to define each security and compliance objective in relation to the capabilities of Windows Defender. In addition, Appendix A contains mappings between Windows Defender and the security control requirements present in ISO 27001, PCI DSS, and FedRAMP.

OVERVIEW OF WINDOWS DEFENDER

Windows Defender is a Windows program that provides anti-virus, anti-spyware, and malicious code protection for Windows Server 2016 and Windows 10 hosts that do not have a third-party anti-virus or malicious code protection program installed. Although the name Windows Defender has been around since the advent of Windows XP, it has matured into a fully-fledged malicious code protection mechanism. With Windows Server 2016 and Windows 10, Windows Defender is now used for many different system protection functions that were either provided by multiple Windows programs in the past – programs such as Microsoft Security Essentials - or were delegated to organizations to enforce with their own third-party implementations.

Windows Defender provides organizations anti-virus and malicious code protection functionality on par with many third-party industry leaders, including the following:

- Windows Defender now provides customers the ability to enforce real-time system scanning and periodic scanning. Windows Defender can be configured to scan new files and executables for malicious code signatures or anomalies that may represent malicious code prior to introduction to the system. In addition, Windows Defender can be configured to perform periodic scans of the entire system or a subset of critical system files.
- In the event a scan turns up an anomaly, Windows Defender can provide native quarantine
 protections and isolate the offending file or executable for further analysis or remediation. In addition,
 Windows Defender will write the action to the Windows Event Log to ensure organizations can identify
 the issue using their existing log collection or SIEM infrastructure and can initiate the appropriate
 response process.

- Windows Defender can be centrally managed using Group Policy, including configuring multiple instances of Windows Defender to automatically update whenever new threat signatures or new anomaly detection methods are published by Microsoft.
- Finally, Windows Defender is meant to be unobtrusive. As an 'on-by-default' component of Windows Server 2016 and Windows 10, Windows Defender is always running as a background process to ensure organizations always have a baseline set of protections in place to guard against malicious code. In the event organizations wish to implement their own alternative anti-virus or malicious code protection mechanism, including third-party implementation, Windows Defender is configured to automatically disable itself in the presence of alternative mechanisms to ensure organizations do not see a significant impact to performance.

USING WINDOWS DEFENDER FOR COMPLIANCE WITH PCI, ISO 27001, AND FEDRAMP

In addition to providing customers a default way to implement strong malicious code protections, Windows Defender can also help customers meet compliance with several common compliance frameworks. The remainder of this document is aimed at providing Windows Defender control and requirement applicability across three common compliance frameworks: ISO 27001, PCI DSS, and FedRAMP.

Although compliance does not directly equate to security, many customers are required to adhere to different compliance standards as part of doing business in organization environments. Windows Defender is broadly applicable to numerous different controls within ISO 27001, PCI DSS, and FedRAMP, and provide customers an easier and more efficient way to meet applicable control requirements that are already in place.

APPENDIX A: WINDOWS DEFENDER MAPPING TO PCI, ISO 27001, AND FEDRAMP

Windows Defender Security and Compliance Capability	ISO 27001: 2013	PCI DSS 3.2	FedRAMP; NIST 800-53 Revision 4
	A.8.3.1 - Management of Removable Media A.12.2.1 - Controls against Malware A.12.4.1 - Event Logging A.12.4.3 - Administrator and Operator Logs A.12.5.1 - Installation of Software on Operational Systems A.12.6.2 - Restrictions on Software Installation	 5.1 – Anti-Virus Software 5.1.1 – Anti-Virus Software – Detection and Prevention 5.2 – Anti-Virus Software – Updates and Monitoring 5.3 – Anti-Virus Software – Prevent Disablement or Alteration 6.6 – Implement Automated Web- Based Attack Preventions 10.2.2 – Logging actions by root privileges 10.2.5 – User changes logging 10.2.7 – Audit Object Actions 12.10.5 – Integrate Alerts into Incident Response 	AU-2 – Audit Events AU-12 – Audit Generation CM-7(2) – Least Functionality Prevent Program Execution CM-8(3) – Information System Component Inventory Automated Unauthorized Component Detection IR-4(1) – Incident Reporting Automated Reporting MA-3(2) – Maintenance Tools Inspect Media SC-7(12) – Boundary Protection Host-Based Protection SI-3 – Malicious Code Protection SI-3(1) – Malicious Code Protection Central Management SI-3(2) – Malicious Code Protection Automatic Updates SI-3(7) – Malicious Code Protection Nonsignature-based Detection SI-4 – Information System Monitoring SI-4(23) – Information System Monitoring Host-Based Devices