Defender for Endpoint Configuration Baseline

Legato Security Partners, Inc.

Defender for Endpoint Policy Baseline - Servers

1. Purpose

This document will help Defender for Endpoint users to setup a Microsoft Defender Antivirus properly.

2. Scope

Defender for Endpoint Clients

3. Prerequisites

Microsoft E5 license

4. Procedure

Go to Endpoints > Configuration Management > Endpoint Security Policies | Microsoft Defender Antivirus. Enable:

Allow Archive Scanning - Allowed. Scans the archive files.

Allow Behavior Monitoring - Allowed. Turns on real-time behavior monitoring.

Allow Cloud Protection - Allowed. Turns on Cloud Protection.

Allow Email Scanning - Allowed. Turns on email scanning.

Allow Full Scan Removable Drive Scanning - Allowed. Scans removable drives.

Allow scanning of all downloaded files and attachments - Allowed.

Allow Realtime Monitoring - Allowed. Turns on and runs the real-time monitoring service.

Allow Scanning Network Files - Allowed. Scans network files.

Allow Script Scanning - Allowed.

Allow User UI Access - Not allowed. Prevents users from accessing UI.

Avg CPU Load Factor – 50

Archive Max Depth – 5

Archive Max Size – 50

Check For Signatures Before Running Scan – Enabled

Cloud Block Level – High

Cloud Extended Timeout – 30

Days To Retain Cleaned Malware – 30

Disable Catchup Full Scan – Enabled

Disable Catchup Quick Scan – Enabled

Enable Low CPU Priority – Enabled

Enable Network Protection - Enabled (block mode)

PUA Protection - PUA Protection on. Detected items are blocked. They will show in history along with other threats.

Real Time Scan Direction - Monitor incoming files.

Scan Parameter - Full scan

Signature Update Interval – 1

Submit Samples Consent - Send safe samples automatically.

Allow On Access Protection - Allowed.

Remediation action for Severe threats
Quarantine. Moves files to quarantine.

Remediation action for Low severity threats
Quarantine. Moves files to quarantine.

Remediation action for Moderate severity threats
Quarantine. Moves files to quarantine.

Remediation action for High severity threats
Remove. Removes files from system.

Allow Network Protection Down Level - Network protection will be enabled down-level.

Allow Datagram Processing On Win Server - Datagram processing on Windows Server is enabled.

Disable Dns Over Tcp Parsing - DNS over TCP parsing is enabled

Disable Http Parsing - HTTP parsing is enabled

Disable Ssh Parsing - SSH parsing is enabled

Disable Tls Parsing - TLS parsing is enabled

Engine Updates Channel - Not configured (Default). The device will stay up to date automatically during the gradual release cycle. Suitable for most devices.

Metered Connection Updates - Not Allowed

Platform Updates Channel - Not configured (Default). The device will stay up to date automatically during the gradual release cycle. Suitable for most devices.

Security Intelligence Updates Channel - Not configured (Default). The device will stay up to date automatically during the gradual release cycle. Suitable for most devices.

5. References

https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-defender