Optimize Your Microsoft Defender for Endpoint Controls

Reach

Find and Fix Misconfigurations and Activated Unused Security Capabilities

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is an endpoint security platform that provides threat prevention, endpoint detection and response (EDR), and attack surface reduction across enterprise devices including Windows, macOS, Linux, and mobile endpoints. The platform monitors endpoint activity to detect malicious behavior, block malware, and help security teams investigate and respond to threats targeting endpoints.

Key Capabilities

Next-generation antivirus (NGAV) to prevent malware execution

EDR to detect suspicious behavior and investigate threats

Attack Surface Reduction (ASR) rules to block common attacker techniques

Automated investigation and remediation to contain and resolve threats

The Configuration Challenge

Microsoft Defender for Endpoint provides many protective capabilities, but over time, misconfigurations or incomplete deployments can significantly reduce protection. Why does this happen? Security teams are stretched thin, managing hundreds of controls while trying to keep up with newly released capabilities. Sometimes other teams change controls without security visibility. The result is configuration drift, and valuable protections left unused.

Common Misconfigurations

Incomplete device onboarding leaves portions of the environment unprotected

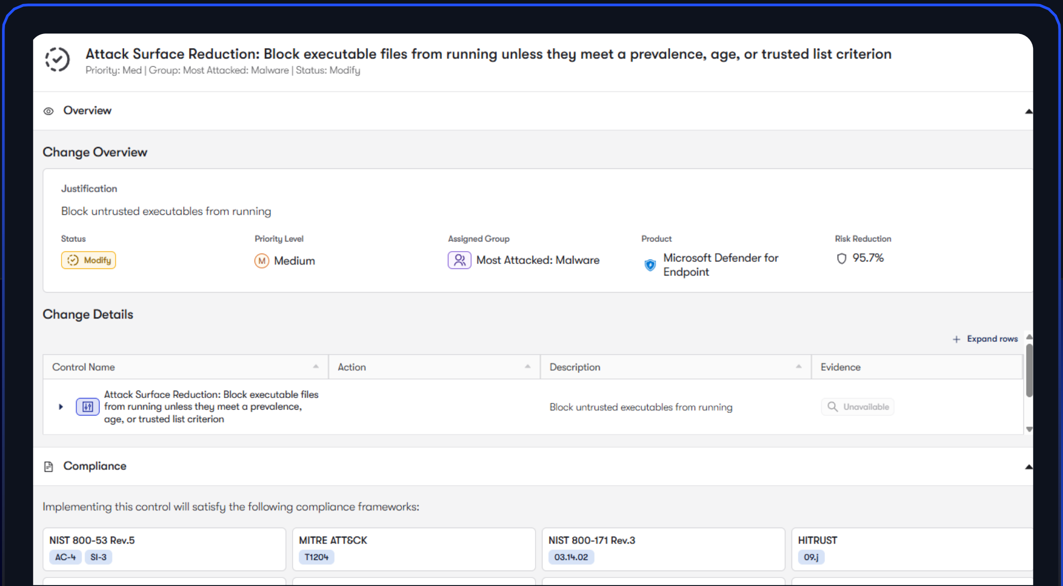
Disabled attack surface reduction rules allow common attacker techniques to get through

Inconsistent security policies across device groups lead to uneven posture across the environment.

Anti-tamper protections are not activated, allowing unauthorized disabling or uninstallation of the agent

Reach Supercharges Microsoft Defender for Endpoint

Reach connects to Microsoft Defender for Endpoint to analyze endpoint protection policies, attack surface reduction controls, and device security configurations. Reach develops a genius-level understanding of how your Microsoft tooling is being used (and misused), and then automatically identifies and remediates misconfigurations, activates unused capabilities, detects configuration drift across endpoint protection policies, and validates over time that security posture remains strong.



Attack Surface Reduction: Block executable files from running unless they meet a prevalence, age, or trusted list criterion
Priority: Med | Group: Most Attacked: Malware | Status: Modify

Overview

Change Overview

Justification
Block untrusted executables from running

Status	Priority Level	Assigned Group	Product	Risk Reduction
Modify	Medium	Most Attacked: Malware	Microsoft Defender for Endpoint	95.7%

Change Details

+ Expand rows

Control Name	Action	Description	Evidence
Attack Surface Reduction: Block executable files from running unless they meet a prevalence, age, or trusted list criterion		Block untrusted executables from running	Unavailable

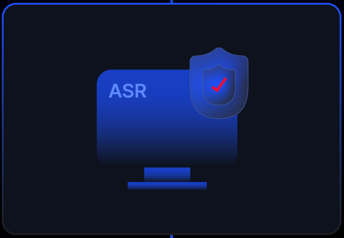
Compliance

Implementing this control will satisfy the following compliance frameworks:

NIST 800-53 Rev.5	MITRE ATT&CK	NIST 800-171 Rev.3	HITRUST
AC-4 SI-3	T1204	03.14.02	09.j

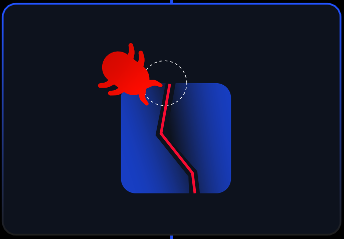
Endpoint onboarding and device protection coverage

Reach analyzes device onboarding status and identifies endpoints that are not onboarded to Defender for Endpoint or lack active protection policies. With Reach, organizations can close endpoint visibility gaps and ensure consistent threat protection across all devices.



Attack Surface Reduction (ASR) rule configuration and enforcement

Reach analyzes ASR rule configurations and identifies rules that are disabled or inconsistently enforced so that organizations can block common attacker techniques such as credential theft, ransomware behavior, and malicious script execution.

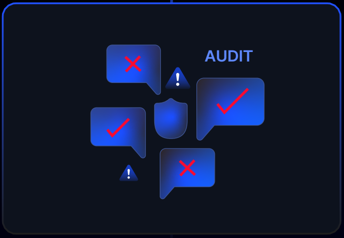


Endpoint protection policy configurations and malware prevention settings

Reach analyzes antivirus and endpoint protection settings and identifies devices operating with weakened malware protection policies. With Reach, organizations can ensure malware and malicious activity are actively blocked across endpoints.

Policy consistency across device groups and operating systems

Reach analyzes endpoint security policies applied across device groups and identifies inconsistent configurations, policy drift, or gaps in protection coverage so that organizations can maintain consistent security posture across Windows, macOS, Linux, and other managed endpoints.



Endpoint protection features operating in audit or monitoring mode

Security features may be configured in monitoring-only modes. This allows malicious activity such as ransomware, credential theft, or script-based attacks to execute on endpoints without being stopped in real time. As a result, attackers can establish persistence, move laterally, and escalate privileges, turning what should have been a prevented attack into a full incident response scenario.

Reach + Microsoft Defender for Endpoint

Together, Microsoft Defender for Endpoint and Reach help organizations ensure their endpoint security platform remains fully deployed, properly configured, and consistently enforcing protections against modern endpoint threats. By optimizing Microsoft Defender for Endpoint controls, organizations strengthen their ability to prevent and detect endpoint-based attacks, reduce endpoint attack surface, and get continuous validation of endpoint security posture.

Learn More reach.security/connect | Webpage | Demo Video