NIST 800-53 Compliance Controls

The following control families represent a portion of special publication NIST 800-53 revision 4. This guide is intended to aid McAfee, its partners, and its customers, in aligning to the NIST 800-53 controls with McAfee® capabilities. The control families are listed below.

- AC Access Control (21 controls)
- CM Configuration Management (3 controls)
- CP Contingency Planning (1 control)
- IA Identification and Authentication (28 controls)
- RA Risk Assessment (1 control)
- SC System and Communications (32 controls)
- SI System and Information Integrity (11 controls)

Each product represents various capabilities, therefore, the total number of controls listed for each family will not be a one-to-one match with the number of products as some capabilities will overlap. The chart below display each capability as it applies to a specific control family.

Capability	AC	AU	CM	CP	IA	SC	SI	Totals
McAfee Active Response	2	-	-	-	-	-	-	2
McAfee Application Control	-	-	3	-	-	3	2	8
McAfee Data Loss Prevention	1	-	-	-	-	-	-	1
McAfee Disk Encryption	-	-	-	-	-	1	-	2
McAfee Endpoint Security	-	-	-	-	-	6	1	7
McAfee Enterprise Security Manager	3	10	-	-	-	-	2	25
McAfee® ePolicy Orchestrator®	-	7	-	-	-	-	2	9
McAfee File & Removable Media Protection	-	-	-	-	-	1	-	1
McAfee Network Security Platform	-	-	-	-	-	12	-	12
McAfee Policy Auditor	15	12	-	-	8	14	4	53
None	2	1	-	1	20	6	4	34

Connect With Us

AC Access Control—21 Controls

Capabilities Summary	Number of controls
McAfee Active Response	2
McAfee Application Control	-
McAfee Data Loss Prevention	1
McAfee Disk Encryption	-
McAfee Endpoint Security	-
McAfee Enterprise Security Manager	3
McAfee ePolicy Orchestrator	
McAfee File & Removable Media Protection	-
McAfee Network Security Platform	-
McAfee Policy Auditor	15
None	2

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
AC	Account Management	Removal of Temporary/ Emergency Accounts	AC-2(2)	AC-2(2).2	Determine if the information system: ▪ Automatically removes or disables temporary and emergency accounts after the organization-defined time period for each type of account	McAfee Active Response McAfee Enterprise Security Manager
AC	Account Management	Disable Inactive Accounts	AC-2(3)	AC-2(3).2	Determine if the information system: ▪ Automatically disables inactive accounts after the organization-defined time period	McAfee Active Response McAfee Enterprise Security Manager
AC	Account Management	Automated Audit Actions	AC-2(4)	AC-2(4).3	Determine if the information system: ▪ Notifies organization-defined personnel or roles of the following account actions – Creation, modification, enabling, disabling, removal	McAfee Enterprise Security Manager
AC	Access Enforcement	Access Enforcement	AC-3	AC-3	Determine if the information system: ▪ Enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies	McAfee Policy Auditor
AC	Information Flow Enforcement	Information Flow Enforcement	AC-4	AC-4.2	Determine if the information system: ▪ Enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information flow control policies	McAfee Data Loss Prevention

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
AC	Least Privilege	Auditing Use of Privileged Functions	AC-6(9)	AC-6(9)	Determine if the information system: ▪ Audits the execution of privileged functions	McAfee Policy Auditor
AC	Least Privilege	Prohibit Non-Privileged Users from Executing Privileged Functions	AC-6(10)	AC-6(10)	Determine if the information system: ▪ Prevents non-privileged users from executing privileged functions to include: ▪ Disabling implemented security safeguards/countermeasures; ▪ Circumventing security safeguards/countermeasures; or – Altering implemented security safeguards/countermeasures	McAfee Endpoint Security with McAfee Threat Intelligence for Endpoint Security McAfee Policy Auditor
AC	Unsuccessful Login Attempts	Unsuccessful Login Attempts	AC-7	AC-7.a.3	Determine if the information system: ▪ Enforces a limit of organization-defined number of consecutive invalid logon attempts by a user during an organization-defined time period	McAfee Policy Auditor
AC	Unsuccessful Login Attempts	Unsuccessful Login Attempts	AC-7	AC-7.b.2	Determine if the information system: ▪ When the maximum number of unsuccessful logon attempts is exceeded, automatically: – Locks the account/node for the organization-defined time period; – Locks the account/node until released by an administrator; or – Delays next logon prompt according to the organization-defined delay algorithm	McAfee Policy Auditor
AC	System Use Notification	System Use Notification	AC-8	AC-8.c.1.2	Determine if, for publicly accessible systems: ▪ The information system displays organization-defined conditions before granting further access	McAfee Policy Auditor
AC	System Use Notification	System Use Notification	AC-8	AC-8.c.2	Determine if the information system: ▪ Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities	McAfee Policy Auditor
AC	System Use Notification	System Use Notification	AC-8	AC-8.c.3	Determine if the information system: ▪ Includes a description of the authorized uses of the system	McAfee Policy Auditor
AC	Concurrent Session Control	Concurrent Session Control	AC-10	AC-10.3	Determine if the information system: ▪ Limits the number of concurrent sessions for each organization-defined account and/or account type to the organization-defined number of concurrent sessions allowed	McAfee Policy Auditor

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
AC	Session Lock	Session Lock	AC-11	AC-11.a.2	Determine if the information system: ▪ Prevents further access to the system by initiating a session lock after organization-defined time period of user inactivity or upon receiving a request from a user	McAfee Policy Auditor
AC	Session Lock	Session Lock	AC-11	AC-11.b	Determine if the information system: ▪ Retains the session lock until the user reestablishes access using established identification and authentication procedures	McAfee Policy Auditor
AC	Session Lock	Pattern-Hiding Displays	AC-11(1)	AC-11(1)	Determine if the information system: ▪ Conceals, via the session lock, information previously visible on the display with a publicly viewable image	McAfee Policy Auditor
AC	Session Termination	Session Termination	AC-12	AC-12.2	Determine if the information system: ▪ Automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect occurs	McAfee Policy Auditor
AC	Remote Access	Automated Monitoring/ Control	AC-17(1)	AC-17(1)	Determine if the information system: ▪ Monitors and controls remote access methods	N/A
AC	Remote Access	Protection of Confidentiality/ Integrity Using Encryption	AC-17(2)	AC-17(2)	Determine if the information system: ▪ Implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions	McAfee Policy Auditor
AC	Remote Access	Managed Access Control Points	AC-17(3)	AC-17(3).2	Determine if the information system: ▪ Routes all remote accesses through the organization-defined number of managed network access control points	N/A
AC	Wireless Access	Authentication and Encryption	AC-18(1)	AC-18(1)	Determine if the information system: ▪ Protects wireless access to the system using encryption and one or more of the following: – Authentication of users; and/or – Authentication of devices	McAfee Policy Auditor

AU Audit and Accountability—23 Controls

Capabilities Summary	Number of controls
McAfee Active Response	-
McAfee Application Control	-
McAfee Data Loss Prevention	-
McAfee Disk Encryption	-
McAfee Endpoint Security	-
McAfee Enterprise Security Manager	10
McAfee ePolicy Orchestrator	7
McAfee File & Removable Media Protection	-
McAfee Network Security Platform	-
McAfee Policy Auditor	12
None	1

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
AU	Content of Audit Records	Centralized Management of Planned Audit Record Content	AU-3(2)	AU-3(2).2	Determine if the information system: ▪ Provides centralized management and configuration of the content to be captured in audit records generated by the organization-defined information system components	McAfee ePolicy Orchestrator
AU	Response to Audit Processing Failures	Response to Audit Processing Failures	AU-5	AU-5.a.2	Determine if the information system: ▪ Alerts the organization-defined personnel or roles in the event of an audit processing failure	McAfee ePolicy Orchestrator McAfee Enterprise Security Manager
AU	Response to Audit Processing Failures	Response to Audit Processing Failures	AU-5	AU-5.b.2	Determine if the information system: ▪ Takes the additional organization-defined actions in the event of an audit processing failure	McAfee Policy Auditor
AU	Response to Audit Processing Failures	Audit Storage Capacity	AU-5(1)	AU-5(1).4	Determine if the information system: ▪ Provides a warning to the organization-defined personnel, roles, and/or locations within the organization-defined time period when allocated audit record storage volume reaches the organization-defined percentage of repository maximum audit record storage capacity	McAfee Policy Auditor

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
AU	Response to Audit Processing Failures	Real-Time Alerts	AU-5(2)	AU-5(2).4	Determine if the information system: ▪ Provides an alert within the organization-defined real-time period to the organization-defined personnel, roles, and/or locations when organization-defined audit failure events requiring real-time alerts occur	McAfee Policy Auditor
AU	Audit Reduction and Report Generation	Audit Reduction and Report Generation	AU-7	AU-7.a	Determine if the information system provides: ▪ An audit reduction and report generation capability that supports: – On-demand audit review – Analysis – Reporting requirements – After-the-fact investigations of security incidents	McAfee Enterprise Security Manager
AU	Audit Reduction and Report Generation	Audit Reduction and Report Generation	AU-7	AU-7.b	Determine if the information system: ▪ Provides an audit reduction and report generation capability that: – Does not alter the original content or time ordering of audit records	McAfee Enterprise Security Manager
AU	Audit Reduction and Report Generation	Automatic Processing	AU-7(1)	AU-7(1).2	Determine if the information system: ▪ Provides the capability to process audit records for events of interest based on the organization-defined audit fields within audit records	McAfee Enterprise Security Manager
AU	Time Stamps	Time Stamps	AU-8	AU-8.a	Determine if the information system: ▪ Uses internal system clocks to generate time stamps for audit records	McAfee Enterprise Security Manager
AU	Time Stamps	Time Stamps	AU-8	AU-8.b.1	Determine if the information system: ▪ Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT)	McAfee Enterprise Security Manager
AU	Time Stamps		AU-8(1)	AU-8(1).a.3	Determine if the information system: ▪ Compares the internal information system clocks with the organization-defined authoritative time source with organization-defined frequency	McAfee Policy Auditor
AU	Time Stamps		AU-8(1)	AU-8(1).b.2	Determine if the information system: ▪ Synchronizes the internal information system clocks to the authoritative time source when the time difference is greater than the organization-defined time period	McAfee Policy Auditor
AU	Protection of Audit Information	Protection of Audit Information	AU-9	AU-9.1	Determine if the information system: ▪ Protects audit information from unauthorized: – Access – Modification – Deletion	McAfee ePolicy Orchestrator McAfee Policy Auditor McAfee Enterprise Security Manager

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
AU	Protection of Audit Information	Protection of Audit Information	AU-9	AU-9.2	Determine if the information system: ▪ Protects audit tools from unauthorized: – Access – Modification – Deletion	McAfee ePolicy Orchestrator McAfee Enterprise Security Manager
AU	Protection of Audit Information	Audit Backup on Separate Physical System/ Components	AU-9(2)	AU-9(2).2	Determine if the information system: ▪ Backs up audit records, with the organization-defined frequency, onto a physically different system or system component than the system or component being audited	McAfee Policy Auditor
AU	Protection of Audit Information	Cryptographic Protections	AU-9(3)	AU-9(3).1	Determine if the information system: ▪ Uses cryptographic mechanisms to protect the integrity of audit information	McAfee ePolicy Orchestrator McAfee Enterprise Security Manager
AU	Protection of Audit Information	Cryptographic Protections	AU-9(3)	AU-9(3).2	Determine if the information system: ▪ Uses cryptographic mechanisms to protect the integrity of audit tools	McAfee ePolicy Orchestrator McAfee Enterprise Security Manager
AU	Non-Repudiation	Non-Repudiation	AU-10	AU-10.2	Determine if the information system: ▪ Protects against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation	N/A
AU	Audit Generation	Audit Generation	AU-12	AU-12.a.2	Determine if the information system: ▪ Provides audit record generation capability, for the auditable events defined in AU-2a, at organization-defined information system components	McAfee Policy Auditor
AU	Audit Generation	Audit Generation	AU-12	AU-12.b.2	Determine if the information system: ▪ Allows the organization-defined personnel or roles to select which auditable events are to be audited by specific components of the system	McAfee Policy Auditor
AU	Audit Generation	Audit Generation	AU-12	AU-12.c	Determine if the information system: ▪ Generates audit records for the events defined in AU-2d with the content in defined in AU-3	McAfee ePolicy Orchestrator McAfee Policy Auditor
AU	Audit Generation	System-Wide/Time-Correlated Audit Trail	AU-12(1)	AU-12(1).3	Determine if the information system: ▪ Compiles audit records from organization-defined information system components into a system-wide (logical or physical) audit trail that is time-correlated to within the organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail	McAfee Policy Auditor
AU	Audit Generation	Changes by Authorized Individuals	AU-12(3)	AU-12(3).5	Determine if the information system ▪ Provides the capability for organization-defined individuals or roles to change the auditing to be performed on organization-defined information system components based on organization-defined selectable event criteria within organization-defined time thresholds	McAfee Policy Auditor

CM Configuration Management—3 Controls

Capabilities Summary	Number of controls
McAfee Active Response	-
McAfee Application Control	3
McAfee Data Loss Prevention	-
McAfee Disk Encryption	-
McAfee Endpoint Security	-
McAfee Enterprise Security Manager	-
McAfee ePolicy Orchestrator	-
McAfee File & Removable Media Protection	-
McAfee Network Security Platform	-
McAfee Policy Auditor	-
None	-

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
CM	Access Restrictions for Change	Automated Access Enforcement/ Auditing	CM-5(1)	CM-5(1).1	Determine if the information system: ▪ Enforces access restrictions for change	McAfee Application Control
CM	Access Restrictions for Change	Automated Access Enforcement/ Auditing	CM-5(1)	CM-5(1).2	Determine if the information system: ▪ Supports auditing of the enforcement actions	McAfee Application Control
CM	Access Restrictions for Change	Signed Components	CM-5(3)	CM-5(3).2	Determine if: ▪ The information system prevents the installation of organization-defined software and firmware components without verification that such components have been digitally signed using a certificate that is recognized and approved by the organization	McAfee Application Control

CP Contingency Planning—1 Control

Capabilities Summary	Number of controls
McAfee Active Response	-
McAfee Application Control	-
McAfee Data Loss Prevention	-
McAfee Disk Encryption	-
McAfee Endpoint Security	-
McAfee Enterprise Security Manager	-
McAfee ePolicy Orchestrator	-
McAfee File & Removable Media Protection	-
McAfee Network Security Platform	-
McAfee Policy Auditor	-
None	1

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
CP	Information System Recovery and Reconstitution	Transaction Recovery	CP-10(2)	CP-10(2).1	Determine if the information system: ▪ Implements transaction recovery for systems that are transaction-based	N/A

IA Identification and Authentication—28 Controls

Capabilities Summary	Number of controls
McAfee Active Response	-
McAfee Application Control	-
McAfee Data Loss Prevention	-
McAfee Disk Encryption	-
McAfee Endpoint Security	-
McAfee Enterprise Security Manager	-
McAfee ePolicy Orchestrator	-
McAfee File & Removable Media Protection	-
McAfee Network Security Platform	-
McAfee Policy Auditor	8
None	20

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
IA	Identification and Authentication (Organizational Users)	Identification and Authentication (Organizational Users)	IA-2	IA-2.1	Determine if the information system: ▪ Uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users)	N/A
IA	Identification and Authentication (Organizational Users)	Network Access to Privileged Accounts	IA-2(1)	IA-2(1).1	Determine if the information system: ▪ Implements multifactor authentication for network access to privileged accounts	N/A
IA	Identification and Authentication (Organizational Users)	Network Access to Non-Privileged Accounts	IA-2(2)	IA-2(2).1	Determine if the information system: ▪ Implements multifactor authentication for network access to non-privileged accounts	N/A
IA	Identification and Authentication (Organizational Users)	Local Access to Privileged Accounts	IA-2(3)	IA-2(3).1	Determine if the information system: ▪ Implements multifactor authentication for local access to privileged accounts	N/A
IA	Identification and Authentication (Organizational Users)	Local Access to Non-Privileged Accounts	IA-2(4)	IA-2(4).1	Determine if the information system: ▪ Implements multifactor authentication for local access to non-privileged accounts	N/A

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
IA	Identification and Authentication (Organizational Users)	Network Access to Privileged Accounts—Replay Resistant	IA-2(8)	IA-2(8).1	Determine if the information system: ▪ Implements replay-resistant authentication mechanisms for network access to privileged accounts	N/A
IA	Identification and Authentication (Organizational Users)	Network Access to Non-Privileged Accounts—Replay Resistant	IA-2(9)	IA-2(9).1	Determine if the information system: ▪ Implements replay-resistant authentication mechanisms for network access to non-privileged accounts	N/A
IA	Identification and Authentication (Organizational Users)	Remote Access—Separate Device	IA-2(11)	IA-2(11).1	Determine if the information system: ▪ Implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access	N/A
IA	Identification and Authentication (Organizational Users)	Remote Access—Separate Device	IA-2(11)	IA-2(11).2	Determine if the information system: ▪ Implements multifactor authentication for remote access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access	N/A
IA	Identification and Authentication (Organizational Users)	Remote Access—Separate Device	IA-2(11)	IA-2(11).5	Determine if the information system: ▪ Implements multifactor authentication for remote access to privileged accounts such that a device, separate from the system gaining access, meets organization-defined strength of mechanism requirements	N/A
IA	Identification and Authentication (Organizational Users)	Remote Access—Separate Device	IA-2(11)	IA-2(11).6	Determine if the information system ▪ Implements multifactor authentication for remote access to non-privileged accounts such that a device, separate from the system gaining access, meets organization-defined strength of mechanism requirements	N/A
IA	Identification and Authentication (Organizational Users)	Acceptance of PIV Credentials	IA-2(12)	IA-2(12).1	Determine if the information system: ▪ Accepts Personal Identity Verification (PIV) credentials	N/A
IA	Identification and Authentication (Organizational Users)	Acceptance of PIV Credentials	IA-2(12)	IA-2(12).2	Determine if the information system: ▪ Electronically verifies Personal Identity Verification (PIV) credentials	N/A
IA	Device Identification and Authentication	Device Identification and Authentication	IA-3	IA-3.2	Determine if the information system: ▪ Uniquely identifies and authenticates organization-defined devices before establishing one or more of the following: – A local connection; – A remote connection; and/or – A network connection	N/A

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
IA	Authenticator Management	Password-Based Authentication	IA-5(1)	IA-5(1).a.5	Determine if, for password-based authentication, the information system: ▪ Enforces minimum password complexity of organization-defined requirements for case sensitivity, number of characters, mix of uppercase letters, lowercase letters, numbers, and special characters, including minimum requirements for each type	McAfee Policy Auditor
IA	Authenticator Management	Password-Based Authentication	IA-5(1)	IA-5(1).b.2	Determine if, for password-based authentication, the information system: ▪ Enforces at least the organization-defined minimum number of characters that must be changed when new passwords are created	McAfee Policy Auditor
IA	Authenticator Management	Password-Based Authentication	IA-5(1)	IA-5(1).c	Determine if, for password-based authentication, the information system: ▪ Stores and transmits only encrypted representations of passwords	McAfee Policy Auditor
IA	Authenticator Management	Password-Based Authentication	IA-5(1)	IA-5(1).d.3	Determine if, for password-based authentication, the information system: ▪ Enforces password minimum lifetime restrictions of organization-defined numbers for lifetime minimum	McAfee Policy Auditor
IA	Authenticator Management	Password-Based Authentication	IA-5(1)	IA-5(1).d.4	Determine if, for password-based authentication, the information system: ▪ Enforces password maximum lifetime restrictions of organization-defined numbers for lifetime maximum	McAfee Policy Auditor
IA	Authenticator Management	Password-Based Authentication	IA-5(1)	IA-5(1).e.2	Determine if, for password-based authentication, the information system: ▪ Prohibits password reuse for the organization-defined number of generations	McAfee Policy Auditor
IA	Authenticator Management	Password-Based Authentication	IA-5(1)	IA-5(1).f	Determine if, for password-based authentication, the information system: ▪ Allows the use of a temporary password for system logons with an immediate change to a permanent password	McAfee Policy Auditor
IA	Authenticator Feedback	Authenticator Feedback	IA-6	IA-6.1	Determine if the information system: ▪ Obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals	McAfee Policy Auditor

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
IA	Cryptographic Module Authentication	Cryptographic Module Authentication	IA-7	IA-7.1	Determine if the information system: ▪ Implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication	N/A
IA	Identification and Authentication (Organizational Users)	Identification and Authentication (Organizational Users)	IA-8	IA-8.1	Determine if the information system: ▪ Uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users)	N/A
IA	Identification and Authentication (Organizational Users)	Acceptance of PIV Credentials from Other Agencies	IA-8(1)	IA-8(1).1	Determine if the information system: ▪ Accepts Personal Identity Verification (PIV) credentials from other agencies	N/A
IA	Identification and Authentication (Organizational Users)	Acceptance of PIV Credentials from Other Agencies	IA-8(1)	IA-8(1).2	Determine if the information system: ▪ Electronically verifies Personal Identity Verification (PIV) credentials from other agencies	N/A
IA	Identification and Authentication (Organizational Users)	Acceptance of Third-Party Credentials	IA-8(2)	IA-8(2).1	Determine if the information system: ▪ Accepts only FICAM-approved third-party credentials	N/A
IA	Identification and Authentication (Organizational Users)	Use of FICAM-Issued Profiles	IA-8(4)	IA-8(4).1	Determine if the information system: ▪ Conforms to FICAM-issued profiles	N/A

RA Risk Assessment—1 Control

Capabilities Summary	Number of controls
McAfee Active Response	-
McAfee Application Control	-
McAfee Data Loss Prevention	-
McAfee Disk Encryption	-
McAfee Endpoint Security	-
McAfee Enterprise Security Manager	-
McAfee ePolicy Orchestrator	-
McAfee File & Removable Media Protection	-
McAfee Network Security Platform	-
McAfee Policy Auditor	1
None	-

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
RA	Vulnerability Scanning	Privileged Access	RA-5(5)	RA-5(5).3	Determine if: ▪ The information system implements privileged access authorization to organization-defined information system components for selected organization-defined vulnerability scanning activities	McAfee Policy Auditor

SC System and Communications—32 Controls

Capabilities Summary	Number of controls
McAfee Active Response	-
McAfee Application Control	3
McAfee Data Loss Prevention	-
McAfee Disk Encryption	1
McAfee Endpoint Security	6
McAfee Enterprise Security Manager	-
McAfee ePolicy Orchestrator	-
McAfee File & Removable Media Protection	1
McAfee Network Security Platform	12
McAfee Policy Auditor	14
None	6

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
SC	Application Partitioning	Application Partitioning	SC-2	SC-2	Determine if the information system: ▪ Separates user functionality (including user interface services) from information system management functionality	McAfee Policy Auditor
SC	Security Function Isolation	Security Function Isolation	SC-3	SC-3	Determine if the information system: ▪ Isolates security functions from nonsecurity functions	McAfee Policy Auditor
SC	Information in Shared Resources	Information in Shared Resources	SC-4	SC-4	Determine if the information system: ▪ Implements multifactor authentication for network access to non-privileged accounts	McAfee Policy Auditor
SC	Denial-of-Service Protection	Denial-of-Service Protection	SC-5	SC-5.3	Determine if the information system: ▪ Prevents unauthorized and unintended information transfer via shared system resources	N/A
SC	Boundary Protection	Boundary Protection	SC-7	SC-7.a.1	Determine if the information system: ▪ Monitors communications at the external boundary of the information system	McAfee Network Security Platform
SC	Boundary Protection	Boundary Protection	SC-7	SC-7.a.2	Determine if the information system: ▪ Monitors communications at key internal boundaries within the system	McAfee Network Security Platform

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
SC	Boundary Protection	Boundary Protection	SC-7	SC-7.a.3	Determine if the information system: ▪ Controls communications at the external boundary of the information system	McAfee Network Security Platform
SC	Boundary Protection	Boundary Protection	SC-7	SC-7.a.4	Determine if the information system: ▪ Controls communications at key internal boundaries within the system	McAfee Network Security Platform
SC	Boundary Protection	Boundary Protection	SC-7	SC-7.b	Determine if the information system: ▪ Implements subnetworks for publicly accessible system components that are either: – Physically separated from internal organizational networks; and/or – Logically separated from internal organizational networks	McAfee Network Security Platform
SC	Boundary Protection	Boundary Protection	SC-7	SC-7.c	Determine if the information system: ▪ Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture	McAfee Endpoint Security McAfee Network Security Platform
SC	Boundary Protection	Deny by Default/ Allow by Exception	SC-7(5)	SC-7(5).1	Determine if the information system, at managed interfaces: ▪ Denies network traffic by default	McAfee Endpoint Security McAfee Network Security Platform
SC	Boundary Protection	Deny by Default/ Allow by Exception	SC-7(5)	SC-7(5).2	Determine if the information system, at managed interfaces: ▪ Allows network traffic by exception	McAfee Endpoint Security McAfee Network Security Platform
SC	Boundary Protection	Prevent Split Tunneling for Remote Devices	SC-7(7)	SC-7(7)	Determine if the information system, in conjunction with a remote device: ▪ Prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks	McAfee Endpoint Security
SC	Boundary Protection	Route Traffic to Authenticated Proxy Servers	SC-7(8)	SC-7(8).3	Determine if the information system: ▪ Routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers at managed interfaces	McAfee Policy Auditor
SC	Boundary Protection	Fail Secure	SC-7(18)	SC-7(18)	Determine if the information system: ▪ Fails securely in the event of an operational failure of a boundary protection device	McAfee Endpoint Security McAfee Network Security Platform

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
SC	Transmission of Confidential Information	Transmission of Confidential Information	SC-8	SC-8	Determine if the information system: ▪ Protects one or more of the following: – Confidentiality of transmitted information; and/or – Integrity of transmitted information	N/A
SC	Transmission of Confidential Information	Cryptographic of Alternate Physical Protection	SC-8(1)	SC-8(1).2	Determine if the information system: ▪ Implements cryptographic mechanisms to do one or more of the following during transmission unless otherwise protected by organization-defined alternative physical safeguards: – Prevent unauthorized disclosure of information; and/or – Detect changes to information	N/A
SC	Network Disconnect	Network Disconnect	SC-10	SC-10.2	Determine if the information system: ▪ Terminates the network connection associated with a communication session at the end of the session or after the organization-defined time period of inactivity	McAfee Network Security Platform
SC	Cryptographic Protection	Cryptographic Protection	SC-13	SC-13.3	Determine if the information system: ▪ Implements the organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, executiveorders, directives, policies, regulations, and standards	McAfee Policy Auditor
SC	Collaborative Computing Devices	Collaborative Computing Devices	SC-15	SC-15.a.2	Determine if the information system: ▪ Prohibits remote activation of collaborative computing devices, except for organization-defined exceptions where remote activation is to be allowed	McAfee Endpoint Security McAfee Network Security Platform
SC	Collaborative Computing Devices	Collaborative Computing Devices	SC-15	SC-15.b	Determine if the information system: ▪ Provides an explicit indication of use to users physically present at the devices	McAfee Policy Auditor
SC	Secure Name	Address Resolution Service (Authoritative Source)	SC-20	SC-20.a	Determine if the information system: ▪ Provides additional data origin and integrity verification artifacts, along with the authoritative name resolution data the system returns in response to external name/address resolution queries	McAfee Policy Auditor
SC	Secure Name	Address Resolution Service (Authoritative Source)	SC-20	SC-20.b	Determine if the information system: ▪ Provides the means to, when operating as part of a distributed, hierarchical namespace: – Indicate the security status of child zones; – Enable verification of a chain of trust among parent and child domains(if the child supports secure resolution services)	McAfee Policy Auditor

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
SC	Secure Name	Address Resolution Service (Recursive or Caching Resolver)	SC-21	SC-21.1	Determine if the information system: ▪ Requests data origin authentication on the name/address resolution responses the system receives from authoritative sources	McAfee Policy Auditor
SC	Secure Name	Address Resolution Service (Recursive or Caching Resolver)	SC-21	SC-21.2	Determine if the information system: ▪ Requests data integrity verification on the name/address resolution responses the system receives from authoritative sources	McAfee Policy Auditor
SC	Secure Name	Address Resolution Service (Recursive or Caching Resolver)	SC-21	SC-21.3	Determine if the information system: ▪ Performs data origin authentication on the name/address resolution responses the system receives from authoritative sources	McAfee Policy Auditor
SC	Secure Name	Address Resolution Service(Recursive or Caching Resolver)	SC-21	SC-21.4	Determine if the information system: ▪ Performs data integrity verification on the name/address resolution responses the system receives from authoritative sources	McAfee Policy Auditor
SC	Architecture and Provisioning for Name	Address Resolution Service	SC-22	SC-22.1	Determine if the information systems that collectively provide name/address resolution service for an organization: ▪ Implement internal/external role separation	McAfee Policy Auditor
SC	Architecture and Provisioning for Name	Address Resolution Service	SC-22	SC-22.2	Determine if the information systems that collectively provide name/address resolution service for an organization: ▪ Are fault tolerant	McAfee Policy Auditor
SC	Session Authenticity	Session Authenticity	SC-23	SC-23	Determine if the information system: ▪ Protects the authenticity of communications sessions	McAfee Policy Auditor
SC	Fail in Known State	Fail in Known State	SC-24	SC-24.4	Determine if the information system: ▪ Fails to the organization-defined known-state for organization-defined types of failures	N/A
SC	Fail in Known State	Fail in Known State	SC-24	SC-24.5	Determine if the information system: ▪ Preserves the organization-defined system state information in the event of a system failure	N/A
SC	Protection of Information at Rest		SC-28	SC-28.2	Determine if the information system: ▪ Protects: – The confidentiality of organization-defined information at rest; and/or – The integrity of organization-defined information at rest	McAfee File & Removable Media Protection McAfee Disk Encryption
SC	Process Isolation		SC-39	SC-39	Determine if the information system: ▪ Maintains a separate execution domain for each executing process	N/A

SI System and Information Integrity—11 Controls

Capabilities Summary	Number of controls
McAfee Active Response	-
McAfee Application Control	2
McAfee Data Loss Prevention	-
McAfee Disk Encryption	-
McAfee Endpoint Security	1
McAfee Enterprise Security Manager	2
McAfee ePolicy Orchestrator	2
McAfee File & Removable Media Protection	-
McAfee Network Security Platform	-
McAfee Policy Auditor	4
None	4

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
SI	Information System Monitoring	System-Generated Alerts	SI-4(5)	SI-4(5).3	Determine if: ▪ The information system alerts organization-defined personnel or roles when organization-defined compromise indicators occur	McAfee ePolicy Orchestrator McAfee Enterprise Security Manager
SI	Security Function Verification	Security Function Verification	SI-6	SI-6.a.2	Determine if the information system: ▪ Verifies the correct operation of organization-defined security functions	N/A
SI	Security Function Verification	Security Function Verification	SI-6	SI-6.b.3	Determine if the information system: ▪ Performs this verification one or more of the following: – At organization-defined system transitional states; – Upon command by user with appropriate privilege; and/or – With the organization-defined frequency	McAfee Policy Auditor
SI	Security Function Verification	Security Function Verification	SI-6	SI-6.c.2	Determine if the information system: ▪ Notifies organization-defined personnel or roles of failed security verification tests	McAfee ePolicy Orchestrator McAfee Enterprise Security Manager

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
SI	Security Function Verification	Security Function Verification	SI-6	SI-6.d.2	Determine if the information system: ▪ Performs one or more of the following actions when anomalies are discovered: – Shuts the information system down; – Restarts the information system; and/or – Performs organization-defined alternative action(s)	McAfee Policy Auditor
SI	Software, Firmware, and Information Integrity	Integrity Checks	SI-7(1)	SI-7(1).4	Determine if the information system: ▪ Performs an integrity check of organization-defined software, firmware, and information one or more of the following: – At startup; – At organization-defined transitional states or security-relevant events; and/or – With the organization-defined frequency	McAfee Application Control McAfee Policy Auditor
SI	Software, Firmware, and Information Integrity	Automated Response to Integrity Violations	SI-7(5)	SI-7(5).2	Determine if the information system: ▪ Automatically performs one or more of the following actions when integrity violations are discovered: – Shuts the information system down; – Restarts the information system; and/or – Implements the organization-defined security safeguards	McAfee Policy Auditor
SI	Information Input Validation	Information Input Validation	SI-10	SI.10.2	Determine if the information system: ▪ Checks the validity of organization-defined information inputs	N/A
SI	Error Handling	Error Handling	SI-11	SI-11.a	Determine if the information system: ▪ Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries	N/A
SI	Error Handling	Error Handling	SI-11	SI-11.b.2	Determine if the information system: ▪ Reveals error messages only to organization-defined personnel or roles	N/A
SI	Information Handling and Retention	Information Handling and Retention	SI-16	SI-16.2	Determine if the information system: ▪ Implements organization-defined security safeguards to protect its memory from unauthorized code execution	McAfee Application Control McAfee Endpoint Security

Disclaimer

This document is released as-is and does not represent a complete and final product. Future products will include each control in detail and align to the NIST 800-53 rev. 4 special publication.

References

NIST SP 800-53 Full Control List. (n.d.). Retrieved from STIG Viewer:
https://www.stigviewer.com/controls/800-53

NIST Special Publication 800-53 (Rev. 4)— Security Controls and Assessment Procedures for Federal Information Systems and Organizations Control Families. (n.d.). Retrieved from National Vulnearbility Database:
https://web.nvd.nist.gov/view/800-53/Rev4/home

Security Assessment Framework Documents. (n.d.). Retrieved from FedRAMP:
https://www.fedramp.gov/resources/documents/

Security Assessment Framework Templates. (n.d.). Retrieved from FedRAMP:
https://www.fedramp.gov/resources/templates-3/

Security Technical Implementation Guides (STIGs). (n.d.). Retrieved from DISA IASE:
http://iase.disa.mil/stigs/Pages/index.aspx

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com