NIST 800-171 Product Mapping

Product Summary

McAfee Product	NIST 800-171 Mapping	Product Suite
MVISION Unified Cloud Edge (UCE) https://www.mcafee.com/enterprise/en-us/solutions/unified-cloud-edge.html	Section 3.1 - Access Control 3.1.3, 3.1.5, 3.1.12, 3.1.14, 3.1.18, 3.1.22 Section 3.5 - Ident & Auth 3.5.2, 3.5.4 Section 3.6 - Incident Response 3.6.1 Section 3.8 - Media Protection 3.8.5 Section 3.13 - Sys & Comm Protection 3.13.1, 3.13.4, 3.13.8, 3.13.9, 3.13.15, 3.13.16 Section 3.14 - Sys & Info Integrity 3.14.2, 3.14.5, 3.14.6, 3.14.7	
MVISION Cloud - Cloud Application Security Broker (CASB)	Section 3.1 - Access Control 3.1.2, 3.1.3, 3.1.5, 3.1.8, 3.1.10, 3.1.11, 3.1.12 Section 3.3 - Audit & Accountability 3.3.1, 3.3.2, 3.3.5 Section 3.4 - Configuration Management 3.4.2, 3.4.9 Section 3.5 - Ident & Auth 3.5.2, 3.5.3 Section 3.6 - Incident Response 3.6.1 Section 3.8 - Media Protection 3.8.4, 3.8.5 Section 3.11 - Risk Assessment 3.11.2 Section 3.13 - Sys & Comm Protection 3.13.1, 3.13.8, 3.13.5 Section 3.14 - Sys & Info Integrity 3.14.1, 3.14.2	**MVISION Unified Cloud Edge (UCE)**

McAfee Product	NIST 800-171 Mapping	Product Suite
MVISION Endpoint Detection and Response (EDR) https://www.mcafee.com/enterprise/en-us/products/mvision-edr.html	Section 3.6 - Incident Response 3.6.1, 3.6.2 Section 3.14 - Sys & Info Integrity 3.14.2, 3.14.5, 3.14.6, 3.14.7	**MVISION Protect Plus and EDR for Endpoint**
MVISION Insights https://www.mcafee.com/enterprise/en-us/products/mvision-insights.html	Section 3.6 - Incident Response 3.6.1	**MVISION Protect Plus and EDR for Endpoint**
Enterprise Security Manager (ESM) https://www.mcafee.com/enterprise/en-us/products/enterprise-security-manager.html	Section 3.3 - Audit & Accountability 3.3.1, 3.3.2, 3.3.3, 3.3.5, 3.3.6, 3.3.8 Section 3.6 - Incident Response 3.6.1, 3.6.2 Section 3.12 - Security Assessment 3.12.3 Section 3.14 - Sys & Info Integrity 3.14.3, 3.14.7	
Threat Intelligence Exchange (TIE) http://www.mcafee.com/us/products/threat-intelligence-exchange.aspx	Section 3.6 - Incident Response 3.6.1 Section 3.14 - Sys & Info Integrity 3.14.2, 3.14.3, 3.14.4, 3.14.5, 3.14.6, 3.14.7	**MVISION Protect Plus and EDR for Endpoint**
Advanced Threat Defense (ATD) https://www.mcafee.com/enterprise/en-us/products/advanced-threat-defense.html	Section 3.6 - Incident Response 3.6.1 Section 3.14 - Sys & Info Integrity 3.14.2, 3.14.4, 3.14.5, 3.14.6, 3.14.7	
McAfee Web Gateway (MWG) https://www.mcafee.com/enterprise/en-us/products/web-gateway.html	Section 3.1 - Access Control 3.1.3, 3.1.22 Section 3.5 - Ident & Auth 3.5.4 Section 3.6 - Incident Response 3.6.1 Section 3.8 - Media Protection 3.8.5 Section 3.13 - Sys & Comm Protection 3.13.1, 3.13.8, 3.13.9, 3.13.15 Section 3.14 - Sys & Info Integrity 3.14.2, 3.14.5, 3.14.6, 3.14.7	**MVISION Unified Cloud Edge (UCE)**

McAfee Product	NIST 800-171 Mapping	Product Suite
Network Security Platform (NSP) https://www.mcafee.com/enterprise/en-us/products/network-security-platform.html	Section 3.1 - Access Control 3.1.3 Section 3.6 - Incident Response 3.6.1 Section 3.13 - Sys & Comm Protection 3.13.1, 3.13.5, 3.13.6, 3.13.15 Section 3.14 - Sys & Info Integrity 3.14.2, 3.14.5, 3.14.6, 3.14.7	
ePolicy Orchestrator (ePO) https://www.mcafee.com/enterprise/en-us/products/epolicy-orchestrator.html	Section 3.1 - Access Control 3.1.4, 3.1.5, 3.1.8, 3.1.10, 3.1.11 Section 3.3 - Audit & Accountability 3.3.8, 3.3.9 Section 3.14 - Sys & Info Integrity 3.14.4	
Endpoint Security 10.x (ENS) http://www.mcafee.com/us/products/endpoint-threat-protection.aspx	Section 3.1 - Access Control 3.1.2, 3.1.16, 3.1.20 Section 3.4 - Configuration Management 3.4.6, 3.4.7, 3.4.8, 3.4.9 Section 3.5 - Ident & Auth 3.5.1 Section 3.6 - Incident Response 3.6.1 Section 3.8 - Media Protection 3.8.2, 3.8.8 Section 3.13 - Sys & Comm Protection 3.13.7 Section 3.14 - Sys & Info Integrity 3.14.2, 3.14.7	**MVISION Protect Plus and EDR for Endpoint**
Complete Data Protection (CDP) https://www.mcafee.com/enterprise/en-us/products/complete-data-protection.html	Section 3.1 - Access Control 3.1.2, 3.1.3, 3.1.10, 3.1.19 Section 3.5 - Identity & Authentication 3.5.3, 3.5.7, 3.5.8, 3.5.9, 3.5.10 Section 3.8 - Media Protection 3.8.1, 3.8.2, 3.8.6, 3.8.9 Section 3.13 - Sys & Comm Protection 3.13.4, 3.13.11, 3.13.16	

McAfee Product	NIST 800-171 Mapping	Product Suite
Data Loss Prevention (DLP) Endpoint https://www.mcafee.com/enterprise/en-us/products/dlp-endpoint.html	Section 3.1 - Access Control 3.1.9 Section 3.3 - Audit & Accountability 3.3.2 Section 3.8 - Media Protection 3.8.1, 3.8.2, 3.8.7 Section 3.13 - Sys & Comm Protection 3.13.4, 3.13.11, 3.13.16	
Total Protection for Data Loss Prevention (DLP) https://www.mcafee.com/enterprise/en-us/products/total-protection-for-data-loss-prevention.html	Section 3.1 - Access Control 3.1.2, 3.1.3, 3.1.5, 3.1.20, 3.1.22 Section 3.3 - Audit & Accountability 3.3.1 Section 3.6 - Incident Resposne 3.6.1, 3.6.2 Section 3.8 - Media Protection 3.8.4, 3.8.5 Section 3.13 - Sys & Comm Protection 3.13.1, 3.13.8 Section 3.14 - Sys & Info Integrity 3.14.7	
McAfee Device Control (MDC) https://www.mcafee.com/enterprise/en-us/products/device-control.html	Section 3.1 - Access Control 3.1.2, 3.1.3, 3.1.21 Section 3.4 - Configuration Management 3.4.6, 3.4.7 Section 3.8 - Media Protection 3.8.1, 3.8.7, 3.8.8	**McAfee Complete Data Protection Advanced** **Total Protection for Data Loss Prevention (DLP)** **MVISION Protect Plus and EDR for Endpoint**
McAfee Application and Change Control (MAC) https://www.mcafee.com/enterprise/en-us/products/application-change-control.html	Section 3.1 - Access Control 3.1.7 Section 3.3 - Audit & Accountability 3.3.1, 3.3.4, 3.3.8 Section 3.4 - Configuration Management 3.4.1, 3.4.2, 3.4.3, 3.4.6, 3.4.7, 3.4.8, 3.4.9 Section 3.6 - Incident Response 3.6.2 Section 3.12 - Security Assessment 3.12.3 Section 3.13 - Sys & Comm Protection 3.13.13	**MVISION Protect Plus and EDR for Endpoint**

McAfee Product	NIST 800-171 Mapping	Product Suite
Policy Auditor (PA) https://www.mcafee.com/enterprise/en-us/products/policy-auditor.html	Section 3.3 - Audit & Accountability 3.3.4 Section 3.4 - Configuration Management Section 3.6 - Incident Response 3.6.2 Section 3.11 - Risk Assessment 3.11.2 Section 3.12 - Security Assessment 3.12.3 Section 3.14 - Sys & Info Integrity 3.14.1	
McAfee Product Training https://www.mcafee.com/enterprise/en-us/services/education-services/product-training.html	Section 3.2 - Training & Awareness 3.2.1, 3.2.2, 3.2.3	
McAfee Advanced Cyber Threat Services (ACTS) https://www.mcafee.com/enterprise/en-us/services/advanced-cyber-threat-services.html	Section 3.2 - Training & Awareness 3.2.1, 3.2.2, 3.2.3 Section 3.4 - Configuration Management 3.4.4, 3.4.5 Section 3.6 - Incident Response 3.6.3 Section 3.7 - Maintenance 3.7.1, 3.7.2, 3.7.3, 3.7.4, 3.7.5, 3.7.6 Section 3.11 - Risk Assessment 3.11.1 Section 3.12 - Security Assessment 3.12.1, 3.12.2, 3.12.4 Section 3.13 - Sys & Comm Protection 3.13.2	
Global Threat Intelligence (GTI) http://www.mcafee.com/us/threat-center/technology/global-threat-intelligence-technology.aspx	Section 3.14 - Sys & Info Integrity 3.14.3	
MVISION Mobile https://www.mcafee.com/enterprise/en-us/products/mvision-mobile.html	Section 3.1 - Access Control 3.1.19	

3.1 – Access Control

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Not Applicable	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	AC-2	Account Management	A.9.2.1	User registration and de-registration
					A.9.2.2	User access provisioning
					A.9.2.3	Management of privileged access rights
					A.9.2.5	Review of user access rights
					A.9.2.6	Removal or adjustment of access rights
Endpoint Security 10.x (ENS) **McAfee Device Control (MDC)** **Complete Data Protection (CDP)** **Total Protection for Data Loss Prevention (DLP)** **MVISION Cloud - Cloud Application Security Broker (CASB)** **Network Security Platform (NSP)** **McAfee Security Innovation Alliance (SIA): AppGate**	3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC-3	Access Enforcement	A.6.2.2	Teleworking
					A.9.1.2	Access to networks and network services
					A.9.4.1	Information access restriction
					A.9.4.4	Use of privileged utility programs
					A.9.4.5	Access control to program source code
					A.13.1.1	Network controls
					A.14.1.2	Securing application services on public networks
					A.14.1.3	Protecting application services transactions
					A.18.1.3	Protection of records
			AC-17	Remote Access	A.6.2.1	Mobile device policy
					A.6.2.2	Teleworking
					A.13.1.1	Network controls
					A.13.2.1	Information transfer policies and procedures
					A.14.1.2	Securing application services on public networks

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
McAfee Device Control (MDC) **Complete Data Protection (CDP)** **Total Protection for Data Loss Prevention (DLP)** **MVISION Unified Cloud Edge (UCE)** **MVISION Cloud - Cloud Application Security Broker (CASB)** **McAfee Web Gateway (MWG)** **Network Security Platform (NSP)**	3.1.3	Control the flow of CUI in accordance with approved authorizations.	AC-4	Information Flow Enforcement	A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3	Segregation in networks Information transfer policies and procedures Securing application services on public networks Protecting application services transactions
ePolicy Orchestrator (ePO) **Policy Approval Workflow**	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC-5	Separation of Duties	A.6.1.2	Segregation of duties
ePolicy Orchestrator (ePO) **Total Protection for Data Loss Prevention (DLP)** **MVISION Cloud - Cloud Application Security Broker (CASB)** **MVISION Unified Cloud Edge (UCE)**	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC-6	Least Privilege	A.9.1.2 A.9.2.3 A.9.4.4 A.9.4.5	Access to networks and network services Management of privileged access rights Use of privileged utility programs Access control to program source code
			AC-6(1)	Least Privilege Authorize Access to Security Functions	No direct mapping.	
			AC-6(5)	Least Privilege Privileged Accounts	No direct mapping.	
Not Applicable	3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	AC-6(2)	Least Privilege Non-Privileged Access for Nonsecurity Functions	No direct mapping.	
McAfee Application and Change Control (MAC)	3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	AC-6(9)	Least Privilege Log Use of Privileged Functions	No direct mapping.	
			AC-6(10)	Least Privilege Prohibit Non-Privileged Users from Executing Privileged Functions	No direct mapping.	
ePolicy Orchestrator (ePO) **MVISION Cloud - Cloud Application Security Broker (CASB)**	3.1.8	Limit unsuccessful logon attempts.	AC-7	Unsuccessful Logon Attempts	A.9.4.2	Secure logon procedures

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Data Loss Prevention (DLP) Endpoint	3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	AC-8	System Use Notification	A.9.4.2	Secure logon procedures
ePolicy Orchestrator (ePO) **MVISION Cloud - Cloud Application Security Broker (CASB)** **Complete Data Protection (CDP)**	3.1.10	Use session lock with pattern- hiding displays to prevent access and viewing of data after a period of inactivity.	AC-11	Session Lock	A.11.2.8	Unattended user equipment
					A.11.2.9	Clear desk and clear screen policy
			AC-11(1)	Session Lock Pattern-Hiding Displays	No direct mapping.	
ePolicy Orchestrator (ePO) **MVISION Cloud - Cloud Application Security Broker (CASB)**	3.1.11	Terminate (automatically) a user session after a defined condition.	AC-12	Session Termination	No direct mapping.	
MVISION Unified Cloud Edge (UCE) **MVISION Cloud - Cloud Application Security Broker (CASB)**	3.1.12	Monitor and control remote access sessions.	AC-17(1)	Remote Access Automated Monitoring / Control	No direct mapping.	
Security Innovation Alliance (SIA): Appgate	3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	AC-17(2)	Remote Access Protection of Confidentiality / Integrity Using Encryption	No direct mapping.	
McAfee Web Gateway (MWG) **MVISION Unified Cloud Edge (UCE)** **Security Innovation Alliance (SIA): Appgate**	3.1.14	Route remote access via managed access control points.	AC-17(3)	Remote Access Managed Access Control Points	No direct mapping.	
Not Applicable	3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	AC-17(4)	Remote Access Privileged Commands / Access	No direct mapping.	
Endpoint Security 10.x (ENS)	3.1.16	Authorize wireless access prior to allowing such connections.	AC-18	Wireless Access	A.6.2.1	Mobile device policy
					A.13.1.1	Network controls
					A.13.2.1	Information transfer policies and procedures
Not Applicable	3.1.17	Protect wireless access using authentication and encryption.	AC-18(1)	Wireless Access Authentication and Encryption	No direct mapping.	
MVISION Unified Cloud Edge (UCE) **MVISION Mobile**	3.1.18	Control connection of mobile devices.	AC-19	Access Control for Mobile Devices	A.6.2.1	Mobile device policy
					A.11.2.6	Security of equipment and assets off-premises
					A.13.2.1	Information transfer policies and procedures

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Complete Data Protection (CDP) **MVISION Mobile**	3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	AC-19(5)	Access Control for Mobile Devices Full Device / Container-Based Encryption	No direct mapping.	
Endpoint Security 10.x (ENS) **Total Protection for Data Loss Prevention (DLP)**	3.1.20	Verify and control/limit connections to and use of external systems.	AC-20	Use of External Systems	A.11.2.6	Security of equipment and assets off-premises
					A.13.1.1	Network controls
					A.13.2.1	Information transfer policies and procedures
			AC-20(1)	Use of External Systems Limits on Authorized Use	No direct mapping.	
McAfee Device Control (MDC)	3.1.21	Limit use of portable storage devices on external systems.	AC-20(2)	Use of External Systems Portable Storage Devices	No direct mapping.	
MVISION Unified Cloud Edge (UCE) **McAfee Web Gateway (MWG)** **Total Protection for Data Loss Prevention (DLP)**	3.1.22	Control CUI posted or processed on publicly accessible systems.	AC-22	Publicly Accessible Content	No direct mapping.	

3.2 – Training & Awareness

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
McAfee Product Training **McAfee Advanced Cyber Threat Services (ACTS)**	3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	AT-2	Security Awareness Training	A.7.2.2	Information security awareness, education, and training
					A.12.2.1	Controls against malware
McAfee Product Training **McAfee Advanced Cyber Threat Services (ACTS)**	3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	AT-3	Role-Based Security Training	A.7.2.2*	Information security awareness, education, and training
McAfee Product Training **McAfee Advanced Cyber Threat Services (ACTS)**	3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	AT-2(2)	Security Awareness Training Insider Threat	No direct mapping.	

3.3 – Audit & Accountability

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Enterprise Security Manager (ESM) **McAfee Application and Change Control (MAC)** **Total Protection for Data Loss Prevention (DLP)** **MVISION Cloud - Cloud Application Security Broker (CASB)**	3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	AU-2	Event Logging	No direct mapping.	
			AU-3	Content of Audit Records	A.12.4.1*	Event logging
			AU-3(1)	Content of Audit Records Additional Audit Information	No direct mapping.	
Enterprise Security Manager (ESM) **Data Loss Prevention (DLP) Endpoint** **MVISION Cloud - Cloud Application Security Broker (CASB)**	3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	AU-6	Audit Record Review, Analysis, and Reporting	A.12.4.1	Event logging
					A.16.1.2	Reporting information security events
					A.16.1.4	Assessment of and decision on information security events
			AU-11	Audit Record Retention	A.12.4.1	Event logging
					A.12.4.3	Administrator and operator logs
			AU-12	Audit Record Generation	A.12.4.1	Event logging
					A.16.1.7	Collection of evidence
Enterprise Security Manager (ESM)	3.3.3	Review and update logged events.	AU-2(3)	Event Logging Review and Updates	No direct mapping.	
McAfee Application and Change Control (MAC) **Policy Auditor (PA)**	3.3.4	Alert in the event of an audit logging process failure.	AU-5	Response to Audit Logging Process Failures	No direct mapping.	
Enterprise Security Manager (ESM) **MVISION Cloud - Cloud Application Security Broker (CASB)**	3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	AU-6(3)	Audit Record Review, Analysis, and Reporting Correlate Audit Record Repositories	No direct mapping.	
Enterprise Security Manager (ESM)	3.3.6	Provide audit record reduction and report generation to support on- demand analysis and reporting.	AU-7	Audit Record Reduction and Report Generation	No direct mapping.	
Not Applicable	3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	AU-8	Time Stamps	A.12.4.4	Clock synchronization
			AU-8(1)	Time Stamps Synchronization with Authoritative Time Source	No direct mapping.	

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Enterprise Security Manager (ESM) **ePolicy Orchestrator (ePO)** **McAfee Application and Change Control (MAC)**	3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	AU-9	Protection of Audit Information	A.12.4.2	Protection of log information
					A.12.4.3	Administrator and operator logs
					A.18.1.3	Protection of records
ePolicy Orchestrator (ePO) **MVISION Cloud - Cloud Application Security Broker (CASB)**	3.3.9	Limit management of audit logging functionality to a subset of privileged users.	AU-9(4)	Protection of Audit Information Access by Subset of Privileged Users	No direct mapping.	

3.4 – Configuration Management

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
McAfee Application and Change Control (MAC) **Policy Auditor (PA)**	3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	CM-2	Baseline Configuration	No direct mapping.	
			CM-6	Configuration Settings	No direct mapping.	
			CM-8	System Component Inventory	A.8.1.1	Inventory of assets
McAfee Application and Change Control (MAC) **Policy Auditor (PA)** **MVISION Cloud - Cloud Application Security Broker (CASB)**	3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.			A.8.1.2	Ownership of assets
			CM-8(1)	System Component Inventory Updates During Installations / Removals	No direct mapping.	
McAfee Application and Change Control (MAC)	3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	CM-3	Configuration Change Control	A.12.1.2	Change management
					A.14.2.2	System change control procedures
					A.14.2.3	Technical review of applications after operating platform changes
					A.14.2.4	Restrictions on changes to software packages
McAfee Advanced Cyber Threat Services (ACTS)	3.4.4	Analyze the security impact of changes prior to implementation.	CM-4	Security Impact Analysis	A.14.2.3	Technical review of applications after operating platform changes

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
McAfee Advanced Cyber Threat Services (ACTS)	3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	CM-5	Access Restrictions for Change	A.9.2.3	Management of privileged access rights
					A.9.4.5	Access control to program source code
					A.12.1.2	Change management
					A.12.1.4	Separation of development, testing, and operational environments
					A.12.5.1	Installation of software on operational systems
Endpoint Security 10.x (ENS) **McAfee Application and Change Control (MAC)** **McAfee Device Control (MDC)** **Policy Auditor (PA)**	3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	CM-7	Least Functionality	A.12.5.1*	Installation of software on operational systems
Endpoint Security 10.x (ENS) **McAfee Application and Change Control (MAC)** **McAfee Device Control (MDC)**	3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	CM-7(1)	Least Functionality Periodic Review	No direct mapping.	
			CM-7(2)	Least Functionality Prevent program execution	No direct mapping.	
Endpoint Security 10.x (ENS) **McAfee Application and Change Control (MAC)**	3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by- exception (whitelisting) policy to allow the execution of authorized software.	CM-7(4)	Least Functionality Unauthorized Software / Blacklisting	No direct mapping.	
			CM-7(5)	Least Functionality Authorized Software / Whitelisting	No direct mapping.	
Endpoint Security 10.x (ENS) **McAfee Application and Change Control (MAC)** **MVISION Cloud - Cloud Application Security Broker (CASB)**	3.4.9	Control and monitor user- installed software.	CM-11	User-Installed Software	A.12.5.1	Installation of software on operational systems
					A.12.6.2	Restrictions on software installation

3.5 – Identification & Authentication

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Endpoint Security 10.x (ENS) *McAfee Client Proxy (MCP)*	3.5.1	Identify system users, processes acting on behalf of users, and devices.	IA-2	Identification and Authentication (Organizational Users)	A.9.2.1	User registration and de-registration
			IA-3	Device Identification and Authentication	No direct mapping.	
MVISION Unified Cloud Edge (UCE) **MVISION Cloud - Cloud Application Security Broker (CASB)** **Endpoint Security 10.x (ENS)** *McAfee Client Proxy (MCP)* **Security Innovation Alliance (SIA): AppGate**	3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	IA-5	Authenticator Management	A.9.2.1	User registration and de-registration
					A.9.2.4	Management of secret authentication information of users
					A.9.3.1	Use of secret authentication information
					A.9.4.3	Password management system
MVISION Cloud - Cloud Application Security Broker (CASB) **Complete Data Protection (CDP)**	3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	IA-2(1)	Identification and Authentication (Organizational Users) Network Access to Privileged Accounts	No direct mapping.	
			IA-2(2)	Identification and Authentication (Organizational Users) Network Access to Non-Privileged Accounts	No direct mapping.	
			IA-2(3)	Identification and Authentication (Organizational Users) Local Access to Privileged Accounts	No direct mapping.	
MVISION Unified Cloud Edge (UCE) **McAfee Web Gateway (MWG)**	3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	IA-2(8)	Identification and Authentication (Organizational Users) Network Access to "Privileged Accounts-Replay Resistant"	No direct mapping.	
			IA-2(9)	Identification and Authentication (Organizational Users) Network Access to Non-Privileged Accounts-Replay Resistant	No direct mapping.	

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Not Applicable	3.5.5	Prevent reuse of identifiers for a defined period.	IA-4	Identifier Management	A.9.2.1	User registration and de-registration
Not Applicable	3.5.6	Disable identifiers after a defined period of inactivity.	IA-4	Identifier Management	A.9.2.1	User registration and de-registration
Complete Data Protection (CDP)	3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	IA-5(1)	Authenticator Management Password-Based Authentication	No direct mapping.	
Complete Data Protection (CDP)	3.5.8	Prohibit password reuse for a specified number of generations.				
Complete Data Protection (CDP)	3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.				
Complete Data Protection (CDP)	3.5.10	Store and transmit only cryptographically-protected passwords.				
Not Applicable	3.5.11	Obscure feedback of authentication information.	IA-6	Authenticator Feedback	A.9.4.2	Secure logon procedures

3.6 – Incident Response

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Endpoint Security 10.x (ENS) **MVISION Endpoint Detection and Response (EDR)** **MVISION Insights** **Enterprise Security Manager (ESM)** **Threat Intelligence Exchange (TIE)** **Advanced Threat Defense (ATD)** **MVISION Unified Cloud Edge (UCE)** **MVISION Cloud - Cloud Application Security Broker (CASB)** **McAfee Web Gateway (MWG)** **Network Security Platform (NSP)** **Total Protection for Data Loss Prevention (DLP)**	3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	IR-2	Incident Response Training	A.7.2.2*	Information security awareness, education, and training
			IR-4	Incident Handling	A.16.1.4	Assessment of and decision on information security events
					A.16.1.5	Response to information security incidents
Enterprise Security Manager (ESM) **McAfee Application and Change Control (MAC)** **Policy Auditor (PA)** **MVISION Endpoint Detection and Response (EDR)** **Total Protection for Data Loss Prevention (DLP)**	3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.			A.16.1.6	Learning from information security incidents
			IR-5	Incident Monitoring	No direct mapping.	
			IR-6	Incident Reporting	A.6.1.3	Contact with authorities
					A.16.1.2	Reporting information security events
			IR-7	Incident Response Assistance	No direct mapping.	
McAfee Advanced Cyber Threat Services (ACTS)	3.6.3	Test the organizational incident response capability.	IR-3	Incident Response Testing	No direct mapping.	

3.7 – Maintenance

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
McAfee Advanced Cyber Threat Services (ACTS)	3.7.1	Perform maintenance on organizational systems.	MA-2	Controlled Maintenance	A.11.2.4*	Equipment maintenance
					A.11.2.5*	Removal of assets
			MA-3	Maintenance Tools	No direct mapping.	
McAfee Advanced Cyber Threat Services (ACTS)	3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	MA-3(1)	Maintenance Tools Inspect Tools	No direct mapping.	
			MA-3(2)	Maintenance Tools Inspect Media	No direct mapping.	
McAfee Advanced Cyber Threat Services (ACTS)	3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	MA-2	Controlled Maintenance	A.11.2.4*	Equipment maintenance
					A.11.2.5*	Removal of assets
McAfee Advanced Cyber Threat Services (ACTS)	3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	MA-3(2)	Maintenance Tools Inspect Media	No direct mapping.	
McAfee Advanced Cyber Threat Services (ACTS)	3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	MA-4	Nonlocal Maintenance	No direct mapping.	
McAfee Advanced Cyber Threat Services (ACTS)	3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	MA-5	Maintenance Personnel	No direct mapping.	

3.8 – Media Protection

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Data Loss Prevention (DLP) Endpoint **Complete Data Protection (CDP)** **McAfee Device Control (MDC)**	3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	MP-2	Media Access	A.8.2.3	Handling of Assets
					A.8.3.1	Management of removable media
					A.11.2.9	Clear desk and clear screen policy
Data Loss Prevention (DLP) Endpoint **Endpoint Security 10.x (ENS)** **Complete Data Protection (CDP)**	3.8.2	Limit access to CUI on system media to authorized users.	MP-4	Media Storage	A.8.2.3	Handling of Assets
					A.8.3.1	Management of removable media
					A.11.2.9	Clear desk and clear screen policy
Not Applicable	3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	MP-6	Media Sanitization	A.8.2.3	Handling of Assets
					A.8.3.1	Management of removable media
					A.8.3.2	Disposal of media
					A.11.2.7	Secure disposal or reuse of equipment
Data Loss Prevention (DLP) Endpoint	3.8.4	Mark media with necessary CUI markings and distribution limitations.	MP-3	Media Marking	A.8.2.2	Labelling of Information
Total Protection for Data Loss Prevention (DLP) **MVISION Unified Cloud Edge (UCE)** **MVISION Cloud - Cloud Application Security Broker (CASB)** **McAfee Web Gateway (MWG)**	3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	MP-5	Media Transport	A.8.2.3	Handling of Assets
					A.8.3.1	Management of removable media
					A.8.3.3	Physical media transfer
					A.11.2.5	Removal of assets
					A.11.2.6	Security of equipment and assets off-premises
Complete Data Protection (CDP)	3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	MP-5(4)	Media Transport Cryptographic Protection	No direct mapping.	
Data Loss Prevention (DLP) Endpoint **McAfee Device Control (MDC)**	3.8.7	Control the use of removable media on system components.	MP-7	Media Use	A.8.2.3	Handling of Assets
					A.8.3.1	Management of removable media
Endpoint Security 10.x (ENS) **McAfee Device Control (MDC)**	3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	MP-7(1)	Media Use Prohibit Use Without Owner	No direct mapping.	
Complete Data Protection (CDP)	3.8.9	Protect the confidentiality of backup CUI at storage locations.	CP-9	System Backup	A.12.3.1	Information backup
					A.17.1.2	Implementing information security continuity
					A.18.1.3	Protection of records

3.9 – Personal Security

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Not Applicable	3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	PS-3	Personnel Screening	A.7.1.1	Screening
			PS-4	Personnel Termination	A.7.3.1	Termination or change of employment responsibilities
					A.8.1.4	Return of assets
Not Applicable	3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	PS-5	Personnel Transfer	A.7.3.1	Termination or change of employment responsibilities
					A.8.1.4	Return of assets

3.10 – Physical Protection

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Not Applicable	3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	PE-2	Physical Access Authorizations	A.11.1.2*	Physical entry controls
			PE-4	Access Control for Transmission Medium	A.11.1.2	Physical entry controls
					A.11.2.3	Cabling security
Not Applicable	3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	PE-5	Access Control for Output Devices	A.11.1.2	Physical entry controls
					A.11.1.3	Securing offices, rooms, and facilities
			PE-6	Monitoring Physical Access	No direct mapping.	
Not Applicable	3.10.3	Escort visitors and monitor visitor activity.	PE-3	Physical Access Control	A.11.1.1	Physical security perimeter
					A.11.1.2	Physical entry controls
Not Applicable	3.10.4	Maintain audit logs of physical access.			A.11.1.3	Securing offices, rooms, and facilities
Not Applicable	3.10.5	Control and manage physical access devices.	PE-17	Alternate Work Site	A.6.2.2	Teleworking
					A.11.2.6	Security of equipment and assets off-premises
Not Applicable	3.10.6	Enforce safeguarding measures for CUI at alternate work sites.			A.13.2.1	Information transfer policies and procedures

3.11 – Risk Assessment

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
McAfee Advanced Cyber Threat Services (ACTS)	3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	RA-3	Risk Assessment	A.12.6.1*	Management of technical vulnerabilities
Policy Auditor (PA) **MVISION Cloud - Cloud Application Security Broker (CASB)**	3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	RA-5	Vulnerability Scanning	A.12.6.1*	Management of technical vulnerabilities
			RA-5(5)	Vulnerability Scanning Privileged Access	No direct mapping.	
Not Applicable	3.11.3	Remediate vulnerabilities in accordance with risk assessments.	RA-5	Vulnerability Scanning	A.12.6.1*	Management of technical vulnerabilities

3.12 – Security Assessment

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
McAfee Advanced Cyber Threat Services (ACTS)	3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	CA-2	Security Assessments	A.14.2.8	System security testing
					A.18.2.2	Compliance with security policies and standards
McAfee Advanced Cyber Threat Services (ACTS)	3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.			A.18.2.3	Technical compliance review
Enterprise Security Manager (ESM) **McAfee Application and Change Control (MAC)** **Policy Auditor (PA)**	3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	CA-5	Plan of Action and Milestones	No direct mapping.	
McAfee Advanced Cyber Threat Services (ACTS)	3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	CA-7	Continuous Monitoring	No direct mapping.	
			PL-2	System Security Plan	A.6.1.2	Information security coordination

3.13 – System & Communications Protection

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Total Protection for Data Loss Prevention (DLP) **MVISION Unified Cloud Edge (UCE)** **MVISION Cloud - Cloud Application Security Broker (CASB)** **McAfee Web Gateway (MWG)** **Network Security Platform (NSP)** **Advanced Threat Defense (ATD)**	3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	SC-7	Boundary Protection	A.13.1.1	Network controls
					A.13.1.3	Segregation in networks
McAfee Advanced Cyber Threat Services (ACTS)	3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.			A.13.2.1	Information transfer policies and procedures
					A.14.1.3	Protecting application services transactions
			SA-8	Security Engineering Principles	A.14.2.5	Secure system engineering principles
Not Applicable	3.13.3	Separate user functionality from system management functionality.	SC-2	Application Partitioning	No direct mapping.	
Data Loss Prevention (DLP) Endpoint **Complete Data Protection (CDP)** **MVISION Unified Cloud Edge (UCE)**	3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	SC-4	Information in Shared Resources	No direct mapping.	
Network Security Platform (NSP) **McAfee Security Innovation Alliance (SIA): Appgate**	3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	SC-7	Boundary Protection	A.13.1.1	Network controls
					A.13.1.3	Segregation in networks
					A.13.2.1	Information transfer policies and procedures
					A.14.1.3	Protecting application services transactions
Network Security Platform (NSP)	3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	SC-7(5)	Boundary Protection Deny by Default / Allow by Exception	No direct mapping.	
Endpoint Security 10.x (ENS)	3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	SC-7(7)	Boundary Protection Prevent Split Tunneling for Remote Devices	No direct mapping.	

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Total Protection for Data Loss Prevention (DLP) **MVISION Unified Cloud Edge (UCE)** **MVISION Cloud - Cloud Application Security Broker (CASB)** **McAfee Web Gateway (MWG)**	3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	SC-8	Transmission Confidentiality and Integrity	A.8.2.3	Handling of Assets
					A.13.1.1	Network controls
					A.13.2.1	Information transfer policies and procedures
					A.13.2.3	Electronic messaging
					A.14.1.2	Securing application services on public networks
					A.14.1.3	Protecting application services transactions
			SC-8(1)	Transmission Confidentiality and Integrity Cryptographic or Alternate Physical Protection	No direct mapping.	
MVISION Unified Cloud Edge (UCE) **McAfee Web Gateway (MWG)**	3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	SC-10	Network Disconnect	A.13.1.1	Network controls
Not Applicable	3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	SC-12	Cryptographic Key Establishment and Management	A.10.1.2	Key Management
Data Loss Prevention (DLP) Endpoint **Complete Data Protection (CDP)**	3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	SC-13	Cryptographic Protection	A.10.1.1	Policy on the use of cryptographic controls
					A.14.1.2	Securing application services on public networks
					A.14.1.3	Protecting application services transactions
					A.18.1.5	Regulation of cryptographic controls
Not Applicable	3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	SC-15	Collaborative Computing Devices	A.13.2.1*	Information transfer policies and procedures
McAfee Application and Change Control (MAC)	3.13.13	Control and monitor the use of mobile code.	SC-18	Mobile Code	No direct mapping.	
Not Applicable	3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	SC-19	Voice over Internet Protocol	No direct mapping.	

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
MVISION Unified Cloud Edge (UCE) MVISION Cloud - Cloud Application Security Broker (CASB) McAfee Web Gateway (MWG) Network Security Platform (NSP)	3.13.15	Protect the authenticity of communications sessions.	SC-23	Session Authenticity	No direct mapping.	
Data Loss Prevention (DLP) Endpoint Complete Data Protection (CDP) MVISION Cloud - Cloud Application Security Broker (CASB)	3.13.16	Protect the confidentiality of CUI at rest.	SC-28	Protection of Information at Rest	A.8.2.3*	Handling of Assets

3.14 – System & Information Integrity

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
Policy Auditor (PA) MVISION Cloud - Cloud Application Security Broker (CASB)	3.14.1	Identify, report, and correct system flaws in a timely manner.	SI-2	Flaw Remediation	A.12.6.1	Management of technical vulnerabilities
					A.14.2.2	System change control procedures
Advanced Threat Defense (ATD) Endpoint Security 10.x (ENS) MVISION Endpoint Detection and Response (EDR) MVISION Unified Cloud Edge (UCE) MVISION Cloud - Cloud Application Security Broker (CASB) McAfee Web Gateway (MWG) Network Security Platform (NSP) Threat Intelligence Exchange (TIE)	3.14.2	Provide protection from malicious code at designated locations within organizational systems.			A.14.2.3	Technical review of applications after operating platform changes
					A.16.1.3	Reporting information security weaknesses
			SI-3	Malicious Code Protection	A.12.2.1	Controls against malware
Enterprise Security Manager (ESM) Global Threat Intelligence (GTI) Threat Intelligence Exchange (TIE)	3.14.3	Monitor system security alerts and advisories and take action in response.	SI-5	Security Alerts, Advisories, and Directives	A.6.1.4*	Contact with special interest groups

McAfee Product	C#	Requirement	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
ePolicy Orchestrator (ePO) Advanced Threat Defense (ATD) Threat Intelligence Exchange (TIE)	3.14.4	Update malicious code protection mechanisms when new releases are available.	SI-3	Malicious Code Protection	A.12.2.1	Controls against malware
Endpoint Security 10.x (ENS) Advanced Threat Defense (ATD) MVISION Endpoint Detection and Response (EDR) MVISION Unified Cloud Edge (UCE) McAfee Web Gateway (MWG) Network Security Platform (NSP) Threat Intelligence Exchange (TIE)	3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.				
Advanced Threat Defense (ATD) MVISION Endpoint Detection and Response (EDR) MVISION Unified Cloud Edge (UCE) McAfee Web Gateway (MWG) Network Security Platform (NSP) Threat Intelligence Exchange (TIE)	3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	SI-4	System Monitoring	No direct mapping.	
			SI-4(4)	System Monitoring Inbound and Outbound Communications Traffic	No direct mapping.	
Total Protection for Data Loss Prevention (DLP) Endpoint Security 10.x (ENS) Enterprise Security Manager (ESM) Advanced Threat Defense (ATD) MVISION Endpoint Detection and Response (EDR) MVISION Unified Cloud Edge (UCE) McAfee Web Gateway (MWG) Network Security Platform (NSP) Threat Intelligence Exchange (TIE)	3.14.7	Identify unauthorized use of organizational systems.	SI-4	System Monitoring	No direct mapping.	

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com