NIST 800-172 Product Mapping

Product Summary

McAfee Product	NIST 800-172 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 3.1.2e, 3.1.3e Section 3.5 - Ident & Auth 3.5.1e, 3.5.3e Section 3.11 - Risk Assessment 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e, 3.13.4e Section 3.14 - Sys & Info Integrity 3.14.2e, 3.14.6e	
MVISION Cloud - Cloud Application Security Broker (CASB) https://www.mcafee.com/enterprise/en-us/products/mvision-cloud.html	Section 3.1 - Access Control 3.1.2e, 3.1.3e Section 3.4 - Configuration Management 3.4.2e, 3.4.3e Section 3.5 - Ident & Auth 3.5.1e, 3.5.3e Section 3.6 - Incident Response 3.6.1e Section 3.11 - Risk Assessment 3.11.2e, 3.11.3e, 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e, 3.13.4e Section 3.14 - Sys & Info Integrity 3.14.2e, 3.14.6e	**MVISION Unified Cloud Edge (UCE)**
MVISION Endpoint Detection and Response (EDR) https://www.mcafee.com/enterprise/en-us/products/mvision-edr.html	Section 3.6 - Incident Response 3.6.1e Section 3.11 - Risk Assessment 3.11.2e, 3.11.3e, 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e Section 3.14 - Sys & Info Integrity 3.14.2e, 3.14.6e	**MVISION Protect Plus and EDR for Endpoint**

McAfee Product	NIST 800-172 Mapping	Product Suite
MVISION Insights https://www.mcafee.com/enterprise/en-us/products/mvision-insights.html	Section 3.6 - Incident Response 3.6.1e Section 3.11 - Risk Assessment 3.11.2e, 3.11.3e, 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e Section 3.14 - Sys & Info Integrity 3.14.2e, 3.14.6e	**MVISION Protect Plus and EDR for Endpoint**
Enterprise Security Manager (ESM) https://www.mcafee.com/enterprise/en-us/products/enterprise-security-manager.html	Section 3.6 - Incident Response 3.6.1e Section 3.11 - Risk Assessment 3.11.2e, 3.11.3e, 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e Section 3.14 - Sys & Info Integrity 3.14.2e, 3.14.6e	
Threat Intelligence Exchange (TIE) http://www.mcafee.com/us/products/threat-intelligence-exchange.aspx	Section 3.6 - Incident Response 3.6.1e Section 3.11 - Risk Assessment 3.11.2e, 3.11.3e, 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e Section 3.14 - Sys & Info Integrity 3.14.2e, 3.14.3e, 3.14.6e	**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 3.6.1e Section 3.11 - Risk Assessment 3.11.2e, 3.11.3e, 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e Section 3.14 - Sys & Info Integrity 3.14.2e, 3.14.3e, 3.14.6e	

McAfee Product	NIST 800-172 Mapping	Product Suite
McAfee Web Gateway (MWG) https://www.mcafee.com/enterprise/en-us/products/web-gateway.html	Section 3.1 - Access Control 3.1.2e, 3.1.3e Section 3.5 - Ident & Auth 3.5.1e, 3.5.3e Section 3.11 - Risk Assessment 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e, 3.13.4e	**MVISION Unified Cloud Edge (UCE)**
Network Security Platform (NSP) https://www.mcafee.com/enterprise/en-us/products/network-security-platform.html	Section 3.1 - Access Control 3.1.3e Section 3.5 - Ident & Auth 3.5.1e, 3.5.3e Section 3.11 - Risk Assessment 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e, 3.13.4e Section 3.14 - Sys & Info Integrity 3.14.2e, 3.14.3e, 3.14.6e	
ePolicy Orchestrator (ePO) https://www.mcafee.com/enterprise/en-us/products/epolicy-orchestrator.html	Section 3.1 - Access Control 3.1.1e Section 3.5 - Ident & Auth 3.5.3e Section 3.6 - Incident Response 3.6.1e Section 3.11 - Risk Assessment 3.11.2e, 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e Section 3.14 - Sys & Info Integrity 3.14.3e, 3.14.6e	

McAfee Product	NIST 800-172 Mapping	Product Suite
Enterprise Security 10.x (ENS) http://www.mcafee.com/us/products/endpoint-threat-protection.aspx	Section 3.1 - Access Control 3.1.2e, 3.1.3e Section 3.5 - Ident & Auth 3.5.1e, 3.5.3e Section 3.11 - Risk Assessment 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e, 3.13.4e Section 3.14 - Sys & Info Integrity 3.14.2e, 3.14.3e, 3.14.6e	**MVISION Protect Plus and EDR for Endpoint**
McAfee Cloud Workload Security (CWS) https://www.mcafee.com/enterprise/en-us/products/cloud-workload-security.html	Section 3.4 - Configuration Management 3.4.2e, 3.4.3e Section 3.5 - Ident & Auth 3.5.3e Section 3.11 - Risk Assessment 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e Section 3.14 - Sys & Info Integrity 3.14.6e	**McAfee Cloud Workload Security Detect and Respond** **McAfee Cloud Workload Security - Advanced**
Complete Data Protection (CDP) https://www.mcafee.com/enterprise/en-us/products/complete-data-protection.html	Section 3.1 - Access Control 3.1.3e Section 3.13 - Sys & Comm Protection 3.13.4e Section 3.14 - Sys & Info Integrity 3.14.3e	
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 3.1.3e Section 3.11 - Risk Assessment 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e, 3.13.4e Section 3.14 - Sys & Info Integrity 3.14.2e	
McAfee Device Control (MDC) https://www.mcafee.com/enterprise/en-us/products/device-control.html	Section 3.1 - Access Control 3.1.3e Section 3.13 - Sys & Comm Protection 3.13.4e	**McAfee Complete Data Protection Advanced** **Total Protection for Data Loss Prevention (DLP)** **MVISION Protect Plus and EDR for Endpoint**

McAfee Product	NIST 800-172 Mapping	Product Suite
McAfee Application and Change Control (MAC) https://www.mcafee.com/enterprise/en-us/products/application-change-control.html	Section 3.4 - Configuration Management 3.4.1e, 3.4.3e Section 3.11 - Risk Assessment 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e	**MVISION Protect Plus and EDR for Endpoint**
Policy Auditor (PA) https://www.mcafee.com/enterprise/en-us/products/policy-auditor.html	Section 3.4 - Configuration Management 3.4.1e, 3.4.2e, 3.4.3e Section 3.5 - Ident & Auth 3.5.3e	
McAfee Product Training https://www.mcafee.com/enterprise/en-us/services/education-services/product-training.html	Section 3.2 - Training & Awareness 3.2.1e, 3.2.2e	
McAfee Advanced Cyber Threat Services (ACTS) https://www.mcafee.com/enterprise/en-us/services/advanced-cyber-threat-services.html	Section 3.2 - Training & Awareness 3.2.1e, 3.2.2e Section 3.6 - Incident Response 3.6.2e Section 3.11 - Risk Assessment 3.11.1e, 3.11.4e, 3.11.5e, 3.11.7e Section 3.12 - Security Assessment 3.12.1e	
McAfee Advanced Programs Group (APG) https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-advanced-programs-group.pdf	Section 3.2 - Training & Awareness 3.2.1e, 3.2.2e	
Global Threat Intelligence (GTI) http://www.mcafee.com/us/threat-center/technology/global-threat-intelligence-technology.aspx	Section 3.6 - Incident Response 3.6.1e Section 3.11 - Risk Assessment 3.11.2e, 3.11.3e, 3.11.6e Section 3.13 - Sys & Comm Protection 3.13.1e Section 3.14 - Sys & Info Integrity 3.14.6e	

3.1 – Access Control

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
ePolicy Orchestrator (ePO) *Policy Approval Workflow*	3.1.1e	X	X		Employ dual authorization to execute critical or sensitive system and organizational operations.	AC-3(2)	Access Enforcement Dual Authorization
Unified Cloud Edge (UCE) McAfee Web Gatway (MWG) MVISION Cloud - Cloud Application Security Broker (CASB) McAfee Endpoint Security (ENS) *McAfee Client Proxy (MCP)*	3.1.2e	X			Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.	AC-20(3)	Use of External Systems *Non-Organizationally Owned Systems—Restricted Use*
Unified Cloud Edge (UCE) McAfee Web Gatway (MWG) MVISION Cloud - Cloud Application Security Broker (CASB) McAfee Endpoint Security (ENS) McAfee Client Proxy (MCP) McAfee Device Control (MDC) Total Protection for Data Loss Prevention (DLP) Network Security Platform (NSP) Complete Data Protection (CDP)	3.1.3e	X			Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems.	AC-4	Information Flow Enforcement
						AC-4(1)	Information Flow Enforcement *Object Security and Privacy Attributes*
						AC-4(6)	Information Flow Enforcement *Metadata*
						AC-4(8)	Information Flow Enforcement *Security and Privacy Policy Filters*
						AC-4(12)	Information Flow Enforcement *Data Type Identifiers*
						AC-4(13)	Information Flow Enforcement *Decomposition into Policy-Relevant Subcomponents*
						AC-4(15)	Information Flow Enforcement *Detection of Unsanctioned Information*

3.2 – Training & Awareness

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
McAfee Product Training McAfee Advanced Programs Group (APG) McAfee Advanced Cyber Threat Services (ACTS)	3.2.1e		X		Provide awareness training [Assignment: organization- defined frequency] focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training [Assignment: organization-defined frequency] or when there are significant changes to the threat.	AT-2	Literacy Training and Awareness
						AT-2(3)	Literacy Training and Awareness *Social Engineering and Mining*
						AT-2(4)	Literacy Training and Awareness *Suspicious Communications and Anomalous System Behavior*
						AT-2(5)	Literacy Training and Awareness *Advanced Persistent Threat*
						AT-2(6)	Literacy Training and Awareness *Cyber Threat Environment*
McAfee Product Training McAfee Advanced Programs Group (APG) McAfee Advanced Cyber Threat Services (ACTS)	3.2.2e		X		Include practical exercises in awareness training for [Assignment: organization-defined roles] that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.	AT-2(1)	Literacy Training and Awareness *Practical Exercises*
						AT-6	Training Feedback

3.3 – Audit & Accountability

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)		
Not Applicable	N/A				There are no enhanced security requirements for audit and accountability.	

3.4 – Configuration Manager

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
McAfee Application and Change Control (MAC) Policy Auditor (PA)	3.4.1e	X		X	Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.	CM-2	Baseline Configuration
						CM-3	Configuration Change Control
						CM-8	System Component Inventory
						SI-14(1)	Non-Persistence Refresh from Trusted Sources
MVISION Cloud - Cloud Application Security Broker (CASB) Policy Auditor (PA) McAfee Cloud Workload Security (CWS)	3.4.2e	X			Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [Selection (one or more): remove the components; place the components in a quarantine or remediation network] to facilitate patching, re- configuration, or other mitigations.	CM-2	Baseline Configuration
						CM-3	Configuration Change Control
						CM-3(5)	Configuration Change Control *Automated Security Response*
						CM-3(8)	Configuration Change *Control Prevent or Restrict Configuration Changes*
McAfee Application and Change Control (MAC) Policy Auditor (PA) McAfee Cloud Workload Security (CWS) MVISION Cloud - Cloud Application Security Broker (CASB)	3.4.3e	X			Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components.	CM-2(2)	Baseline Configuration *Automation Support for Accuracy and Currency*
						CM-8(2)	System Component Inventory *Automated Maintenance*

3.5 – Identification and Authentication

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
Unified Cloud Edge (UCE) McAfee Web Gatway (MWG) MVISION Cloud - Cloud Application Security Broker (CASB) McAfee Endpoint Security (ENS) McAfee Client Proxy (MCP) Network Security Platform (NSP)	3.5.1e	X			Identify and authenticate [Assignment: organization- defined systems and system components] before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.	IA-2(8)	Identification and Authentication (Organizational Users) *Access to Accounts—Replay Resistant*
						IA-3	Device Identification and Authentication
						IA-3(1)	Device Identification and Authentication *Cryptographic Bidirectional Authentication*
Not Applicable	3.5.2e	X			Employ automated mechanisms for the generation, protection, rotation, and management of passwords for systems and system components that do not support multifactor authentication or complex account management.	IA-5(18)	Authenticator Management *Password Managers*
ePolicy Orchestrator (ePO) *Policy Approval Workflow* Policy Auditor (PA) Cloud Workload Security (CWS) Unified Cloud Edge (UCE) McAfee Web Gatway (MWG) MVISION Cloud - Cloud Application Security Broker (CASB) McAfee Endpoint Security (ENS) *McAfee Client Proxy (MCP)* Network Security Platform (NSP)	3.5.3e	X			Employ automated or manual/ procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.	CM-8(3)	System Component Inventory *Automated Unauthorized Component Detection*
						IA-3(4)	Device Identification and Authentication *Device Attestation*
						SI-4(22)	System Monitoring *Unauthorized Network Services*

3.6 – Incident Response

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
MVISION Cloud - Cloud Application Security Broker (CASB) MVISION Endpoint Detection and Response (EDR) MVISION Insights Enterprise Security Manager (ESM) Threat Intelligence Exchange (TIE) Advanced Threat Defense (ATD) ePolicy Orchestrator (ePO) Global Threat Intelligence (GTI)	3.6.1e		X		Establish and maintain a security operations center capability that operates [Assignment: organization-defined time period].	IR-4(14)	Incident Handling *Security Operations Center*
McAfee Advanced Cyber Threat Services (ACTS)	3.6.2e		X		Establish and maintain a cyber incident response team that can be deployed by the organization within [Assignment: organization- defined time period].	IR-4(11)	Incident Handling *Integrated Incident Response Team*
						IR-7	Incident Response Assistance

3.7 – Maintenance

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)		
Not Applicable	N/A				There are no enhanced security requirements for maintenance.	

3.8 – Media Protection

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
Not Applicable	N/A				There are no enhanced security requirements for media protection.		

3.9 – Personnel Security

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
Not Applicable	3.9.1e		X		Conduct [Assignment: organization-defined enhanced personnel screening] for individuals and reassess individual positions and access to CUI [Assignment: organization- defined frequency].	PS-3	Personnel Screening
						SA-21	Developer Screening
Not Applicable	3.9.2e		X		Ensure that organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI.	PS-3	Personnel Screening
						SA-21	Developer Screening

3.10 – Physical Protection

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)		
Not Applicable	N/A				There are no enhanced security requirements for physical protection.	

3.11 – Risk Assessment

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
McAfee Advanced Cyber Threat Services (ACTS)	3.11.1e		X		Employ [Assignment: organization-defined sources of threat intelligence] as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security controls, monitoring, threat hunting, and response and recovery activities.	PM-16	Threat Awareness Program
						PM-16(1)	Threat Awareness Program Automated Means for Sharing Threat Intelligence
						RA-3(3)	Risk Assessment *Dynamic Threat Awareness*
MVISION Cloud - Cloud Application Security Broker (CASB) MVISION Endpoint Detection and Response (EDR) MVISION Insights Enterprise Security Manager (ESM) Threat Intelligence Exchange (TIE) Advanced Threat Defense (ATD) ePolicy Orchestrator (ePO) Global Threat Intelligence (GTI)	3.11.2e		X		Conduct cyber threat hunting activities [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined event]] to search for indicators of compromise in [Assignment: organization-defined systems] and detect, track, and disrupt threats that evade existing controls.	RA-10	Threat Hunting
						SI-4(24)	System Monitoring *Indicators of Compromise*
MVISION Cloud - Cloud Application Security Broker (CASB) MVISION Endpoint Detection and Response (EDR) MVISION Insights Enterprise Security Manager (ESM) Threat Intelligence Exchange (TIE) Advanced Threat Defense (ATD) Global Threat Intelligence (GTI)	3.11.3e		X		Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components.	RA-3(4)	Risk Assessment *Predictive Cyber Analytics*
						SI-4(24)	System Monitoring *Indicators of Compromise*

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
McAfee Advanced Cyber Threat Services (ACTS)	3.11.4e	X			Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination.	AC-4	Information Flow Control
						CA-3	Information Exchange
						CM-8	System Component Inventory
						PL-2	System Security and Privacy Plans
						PL-8	Security and Privacy Architectures
						SC-7	Boundary Protection
MVISION Insights McAfee Advanced Cyber Threat Services (ACTS)	3.11.5e		X		Assess the effectiveness of security solutions [Assignment: organization-defined frequency] to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.	RA-3	Risk Assessment
						RA-3(3)	Risk Assessment *Dynamic Threat Awareness*

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
MVISION Unified Cloud Edge (UCE) MVISION Cloud - Cloud Application Security Broker (CASB) MVISION Endpoint Detection and Response (EDR) MVISION Insights Enterprise Security Manager (ESM) Threat Intelligence Exchange (TIE) Advanced Threat Defense (ATD) McAfee Web Gateway (MWG) Network Security Platform (NSP) Policy Orchestrator (ePO) McAfee Endpoint Security (ENS) *McAfee Client Proxy (MCP)* McAfee Cloud Workload Security (CWS) McAfee Application and Change Control (MAC) Total Protection for Data Loss Prevention (DLP) Global Threat Intelligence (GTI)	3.11.6e	X			Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.	RA-3 RA-3(1)	Risk Assessment Risk Assessment *Supply Chain Risk Assessment*
McAfee Advanced Cyber Threat Services (ACTS)	3.11.7e	X			Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan [Assignment: organization-defined frequency].	SR-2	Supply Chain Risk Management Plan

3.12 – Security Assessment

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
McAfee Advanced Cyber Threat Services (ACTS)	3.12.1e	X	X		Conduct penetration testing [Assignment: organization- defined frequency], leveraging automated scanning tools and ad hoc tests using subject matter experts.	CA-8	Penetration Testing
						SR-6(1)	Supplier Assessments and Reviews *Testing and Analysis*

3.13 – Systems and Communications

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
MVISION Unified Cloud Edge (UCE) MVISION Cloud - Cloud Application Security Broker (CASB) MVISION Endpoint Detection and Response (EDR) MVISION Insights Enterprise Security Manager (ESM) Threat Intelligence Exchange (TIE) Advanced Threat Defense (ATD) McAfee Web Gateway (MWG) Network Security Platform (NSP) ePolicy Orchestrator (ePO) McAfee Endpoint Security (ENS) *McAfee Client Proxy (MCP)* McAfee Cloud Workload Security (CWS) McAfee Application and Change Control (MAC) Total Protection for Data Loss Prevention (DLP) Global Threat Intelligence (GTI)	3.13.1e			X	Create diversity in [Assignment: organization- defined system components] to reduce the extent of malicious code propagation.	PL-8	Security and Privacy Architectures
						SA-17(9)	Developer Security and Privacy Architecture and Design *Design Diversity*
						SC-27	Platform-Independent Applications
						SC-29	Heterogeneity
						SC-29(1)	Heterogeneity *Virtualization Techniques*
						SC-47	Alternate Communications Paths

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
Not Applicable	3.13.2e			X	Implement the following changes to organizational systems and system components to introduce a degree of unpredictability into operations: [Assignment: organization-defined changes and frequency of changes by system and system component].	SC-30(2)	Concealment and Misdirection *Randomness*
McAfee Security Innovation Alliance (SIA) Partner: Attivo Networks https://attivonetworks.com/documentation/Attivo_Networks-McAfee_Partner_Brief.pdf?x68534	3.13.3e			X	Employ [Assignment: organization-defined technical and procedural means] to confuse and mislead adversaries.	SC-8(4)	Transmission Confidentiality and Integrity Conceal or Randomize Communications
						SC-26	Decoys
						SC-30	Concealment and Misdirection
						SC-30(2)	Concealment and Misdirection Randomness
						SI-20	Tainting
MVISION Unified Cloud Edge (UCE) MVISION Cloud - Cloud Application Security Broker (CASB) McAfee Web Gateway (MWG) Network Security Platform (NSP) McAfee Endpoint Security (ENS) *McAfee Client Proxy (MCP)* Complete Data Protection (CDP) Total Protection for Data Loss Prevention (DLP) McAfee Device Control (MDC)	3.13.4e	X		X	Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components.	SC-7	Boundary Protection
						SC-7(13)	Boundary Protection *Isolation of Security Tools, Mechanisms, and Support Components*
						SC-7(21)	Boundary Protection *Isolation of System Components*
						SC-7(22)	Boundary Protection *Separate Subnets for Connecting to Different Security Domains*
						SC-25	Thin Nodes
Not Applicable	3.13.5e			X	Distribute and relocate the following system functions or resources [Assignment: organization-defined frequency]: [Assignment: organization-defined system functions or resources].	SC-30(3)	Concealment and Misdirection *Change Processing and Storage Locations*

3.14 – System and Information Integrity

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
Not Applicable	3.14.1e	X			Verify the integrity of [Assignment: organization- defined security critical or essential software] using root of trust mechanisms or cryptographic signatures.	SI-7(6)	Software, Firmware, and Information Integrity *Cryptographic Protection*
						SI-7(9)	Software, Firmware, and Information Integrity *Verify Boot Process*
						SI-7(10)	Software, Firmware, and Information Integrity *Protection of Boot Firmware*
MVISION Unified Cloud Edge (UCE) MVISION Cloud - Cloud Application Security Broker (CASB) MVISION Endpoint Detection and Response (EDR) MVISION Insights Enterprise Security Manager (ESM) Threat Intelligence Exchange (TIE) Advanced Threat Defense (ATD) McAfee Web Gateway (MWG) Network Security Platform (NSP) Total Protection for Data Loss Prevention (DLP) McAfee Endpoint Security (ENS) *McAfee Client Proxy (MCP)*	3.14.2e			X	Monitor organizational systems and system components on an ongoing basis for anomalous or suspicious behavior.	AU-6(6)	Audit Record Review, Analysis, and Reporting *Correlation with Physical Monitoring*
						SI-4(4)	System Monitoring *Inbound and Outbound Communications Traffic*
						SI-4(7)	System Monitoring *Automated Response to Suspicious Events*
						SI-4(11)	System Monitoring *Analyze Communications Traffic Anomalies*
						SI-4(13)	System Monitoring *Analyze Traffic and Event Patterns*
						SI-4(18)	System Monitoring *Analyze Traffic and Covert Exfiltration*
						SI-4(19)	System Monitoring *Risk for individuals*
						SI-4(20)	System Monitoring *Privileged Users*

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
McAfee Application and Change Control (MAC) Complete Data Protection (CDP) McAfee Endpoint Security (ENS) Advanced Threat Defense (ATD) McAfee Web Gateway (MWG) Network Security Platform (NSP) Threat Intelligence Exchange (TIE) Enterprise Security Manager (ESM) ePolicy Orchestrator (ePO)	3.14.3e	X			Ensure that [Assignment: organization-defined systems and system components] are included in the scope of the specified enhanced security requirements or are segregated in purpose- specific networks.	AC-3	Access Enforcement
						AC-4	Information Flow Enforcement
						SA-8	Security and Privacy Engineering Principles
						SC-2	Separation of System and User Functionality
						SC-3	Security Function Isolation
						SC-49	Hardware-Enforced Separation and Policy Enforcement
Not Applicable	3.14.4e	X			Refresh [Assignment: organization-defined systems and system components] from a known, trusted state [Assignment: organization-defined frequency].	SI-14	Non-Persistence
						SI-14(1)	Non-Persistence *Refresh from Trusted Sources*
						SI-14(2)	Non-Persistence *Non-Persistent Information*
						SI-14(3)	Non-Persistence *Non-Persistent Connectivity*
McAfee Professional Services	3.14.5e	X			Conduct reviews of persistent organizational storage locations [Assignment: organization-defined frequency] and remove CUI that is no longer needed.	SC-28(2)	Protection of Information at Rest *Offline Storage*
						SI-14(2)	Non-Persistence *Non-Persistent Information*

McAfee Product	C#	Defense-in-Depth Protection Strategy			Requirement	NIST SP 800-53 Relevant Security Controls	
		Penetration Resistant Architecture (PRA)	Damage Limiting Operations (DLO)	Cyber Resiliency and Survivability (CRS)			
MVISION Unified Cloud Edge (UCE) MVISION Cloud - Cloud Application Security Broker (CASB) MVISION Endpoint Detection and Response (EDR) MVISION Insights Enterprise Security Manager (ESM) Threat Intelligence Exchange (TIE) Advanced Threat Defense (ATD) McAfee Web Gateway (MWG) Network Security Platform (NSP) ePolicy Orchestrator (ePO) McAfee Endpoint Security (ENS) *McAfee Client Proxy (MCP)* McAfee Cloud Workload Security (CWS) Global Threat Intelligence (GTI) Security Innovation Alliance (SIA) Partner: ThreatQ https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-threat-quotient-tie.pdf	3.14.6e		X		Use threat indicator information and effective mitigations obtained from [Assignment: organization- defined external organizations] to guide and inform intrusion detection and threat hunting.	PM-16(1) SI-4(24) SI-5	Threat Awareness Program Automated Means for Sharing Threat Intelligence System Monitoring Indicators of Compromise Security Alerts, Advisories, and Directives
McAfee Professional Services	3.14.7e	X			Verify the correctness of [Assignment: organization- defined security critical or essential software, firmware, and hardware components] using [Assignment: organization-defined verification methods or techniques].	SA-17	Developer Security and Privacy Architecture and Design

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