McAfee CIS CSC20 Product Mapping

Objective

The aim of this document is to outline the CIS CSC20 v7.1 security control and map the McAfee® product platforms across it. The document maps our products, system integration alliance (SIA) products, and professional services capabilities across the control categories listed in the CIS CSC20 control framework.

Introduction to CIS CSC20 and Why Use It

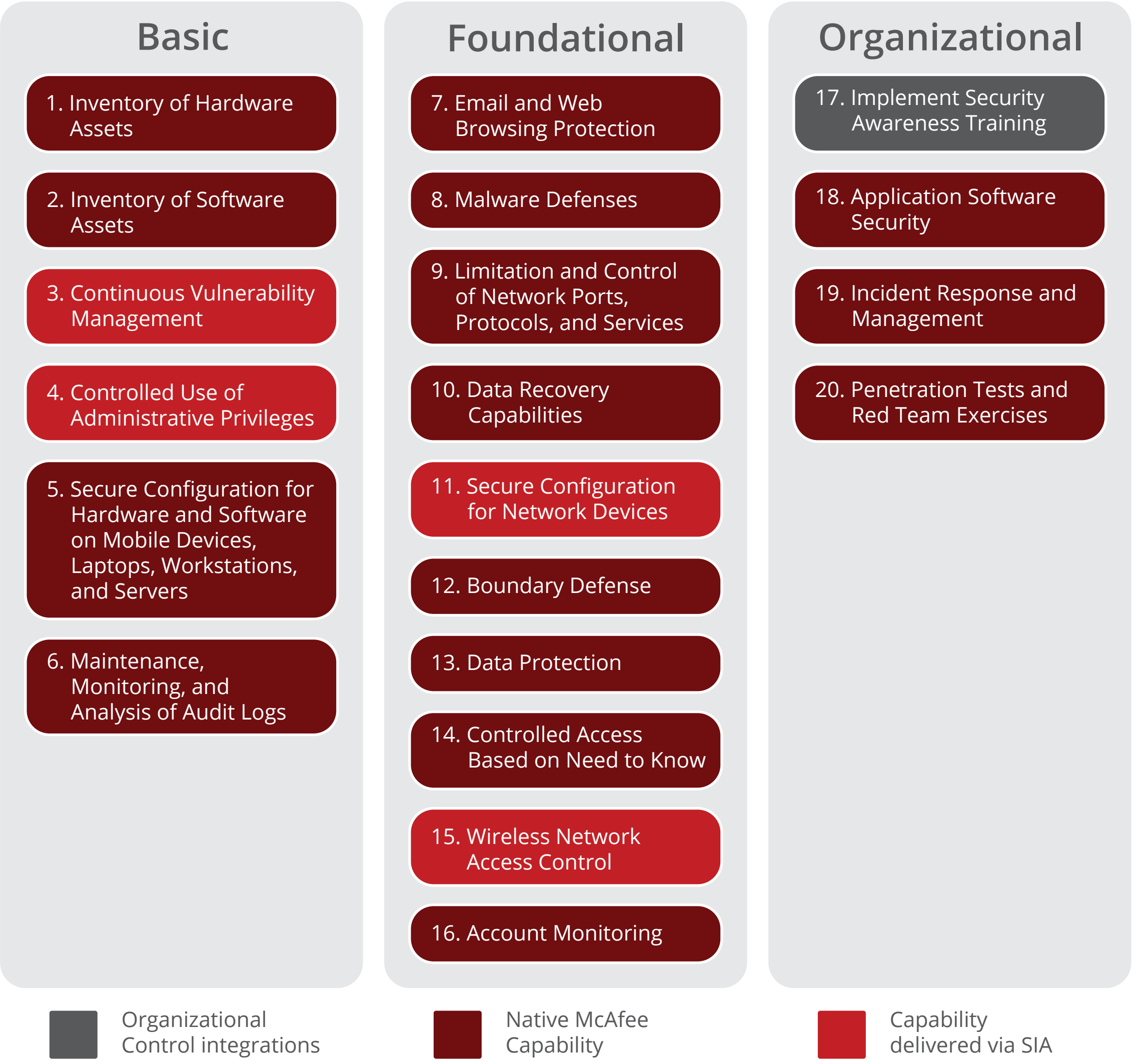
The Center for Internet Security (CIS) provide a list of Critical Security Controls (CSC) that have been cherry picked to be most effective against most common attacks. It offers layered protection via a defense in depth approach to cybersecurity and has been developed using firsthand experiences of cyber-defenders across various industry verticals such as retail, manufacturing, healthcare, government, etc.

Organizations trying to implement security controls across their enterprise face a tough choice as a myriad of compliance and security legislations allude to different security frameworks, each bringing their own list of extensive controls. However, most of the security frameworks are adaptable as per the business needs and security maturity of the organization. For example, an organization could potentially use the core best practices of the NIST CSF (Identify, Protect, Detect, Respond, and Recover) and combine it with controls, such as the CIS CSC20, to establish a defensive and protective security baseline. The core value proposition of the CSC20 control framework is its extremely condensed nature which allows an enterprise to focus its efforts on its fundamental security needs.

Connect With Us

CSC20 Controls

The following section outlines the CSC20 Controls which are categorized into three key areas.



Basic

- 🟫 1. Inventory of Hardware Assets
- 🟫 2. Inventory of Software Assets
- 🟥 3. Continuous Vulnerability Management
- 🟥 4. Controlled Use of Administrative Privileges
- 🟫 5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- 🟫 6. Maintenance, Monitoring, and Analysis of Audit Logs

Foundational

- 🟫 7. Email and Web Browsing Protection
- 🟫 8. Malware Defenses
- 🟫 9. Limitation and Control of Network Ports, Protocols, and Services
- 🟫 10. Data Recovery Capabilities
- 🟥 11. Secure Configuration for Network Devices
- 🟫 12. Boundary Defense
- 🟫 13. Data Protection
- 🟫 14. Controlled Access Based on Need to Know
- 🟥 15. Wireless Network Access Control
- 🟫 16. Account Monitoring

Organizational

- ⬛ 17. Implement Security Awareness Training
- 🟫 18. Application Software Security
- 🟫 19. Incident Response and Management
- 🟫 20. Penetration Tests and Red Team Exercises

⬛ Organizational Control integrations

🟫 Native McAfee Capability

🟥 Capability delivered via SIA

CSC on Cloud Infrastructure

It should be noted that the un-tailored CIS Controls do not provide complete coverage of all control requirements for public/private cloud infrastructure and therefore a CIS Cloud Companion guide has been published by CIS to cover the gaps. This document covers all Cloud use cases where applicable.

CSC SANS Case Study

The following whitepaper from SANS outlines how CIS CSC could have prevented a real-world attack.

https://www.sans.org/reading-room/whitepapers/critical/case-study-cis-controls-limit-cascading-failures-attack-36957

Product Mapping Index

Summary of Product Mapping; Click on control for detailed capabilities.

Control	Product
1. Inventory of Hardware Assets	McAfee® Enterprise Security Manager (McAfee ESM) McAfee® ePolicy Orchestrator® (McAfee ePO™) McAfee® MVISION Cloud SIA Partners – Infoblox—Network Insight/NetMRI – Indegy—Industrial Cybersecurity Suite
2. Inventory of Software Assets	McAfee® Application Control (MAC) McAfee® MVISION Mobile McAfee MVISION Cloud McAfee® Threat Intelligence Exchange McAfee® Policy Auditor
3. Continuous Vulnerability Management	McAfee Policy Auditor McAfee ePO SIA Partner – Rapid 7—Nexpose
4. Controlled Use of Administrative Privileges	McAfee ePO McAfee ESM McAfee MVISION Cloud SIA Partners – Beyond Trust® – CyberArk®

Control	Product
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	McAfee Policy Auditor McAfee ePO (On-Prem/SaaS) McAfee Application Control
6. Maintenance, Monitoring, and Analysis of Audit Logs	McAfee ESM McAfee MVISION Cloud
7. Email and Web Browsing Protection	McAfee® Secure Web Gateway (On Prem) McAfee® Client Proxy (MCP) McAfee® Web Gateway Cloud Service (SaaS) McAfee® Advanced Threat Defense (McAfee ATD) McAfee® SiteAdvisor® Enterprise McAfee MVISION Cloud (SaaS Email Protection) McAfee® Security for Email Servers McAfee® MVISION Endpoint Detection and Response (MVISION EDR) SIA Partner – Cofense
8. Malware Defenses	McAfee® Endpoint Protection Platform (ENS, EDR, MVISION Endpoint, MVISION Mobile) McAfee® Network Security Platform (McAfee NSP) McAfee Secure Web Gateway McAfee® Gateway Anti-Malware Engine
9. Limitation and Control of Network Ports, Protocols, and Services	McAfee® Endpoint Security (ENS Firewall Module) SIA Partners – Checkpoint® – Fortinet®
10. Data Recovery Capabilities	Limited protection via McAfee MVISION Endpoint and McAfee Endpoint Security (ENS)
11. Secure Configuration for Network Devices	SIA Partner – Infoblox—NetMRI
12. Boundary Defense	McAfee NSP McAfee Secure Web Gateway McAfee Gateway Anti-Malware Engine

Control	Product
13. Data Protection	McAfee® Data Loss Prevention (DLP) Endpoint McAfee MVISION Cloud McAfee Secure Web Gateway McAfee® DLP Prevent/Discover (Network DLP) McAfee® Database Activity Monitoring (DAM)
14. Controlled Access Based on Need to Know	McAfee MVISION Cloud McAfee Secure Web Gateway SIA Partners – Beyond Trust – CyberArk – Okta®
15. Wireless Network Access Control	SIA Partners – Aruba—ClearPass Policy Manager – Cisco—Integrated Services Engine (ISE)
16. Account Monitoring	McAfee ESM
17. Implement Security Awareness Training	Organizational Control
18. Application Software Security	McAfee® Foundstone® Security Services McAfee MVISION Mobile
19. Incident Response and Management	McAfee MVISION EDR McAfee ESM McAfee® Foundstone Incident Response (IR) Service
20. Penetration Tests and Red Team Exercises	McAfee® Advanced Programs Group (APG)

Basic Controls

1. Inventory of Hardware Assets

Product Name	Link to Solution Offering	Explanation
McAfee Enterprise Security Manager	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-siem-solutions-from-mcafee.pdf https://docs.mcafee.com/bundle/enterprise-security-manager-10.2.0-product-guide-unmanaged/page/GUID-325E7905-C6E7-43B9-821C-1E2CA514AF52.html	The Asset Manager provides a centralized location that allows you to discover, manually create, and import assets. An asset is any device with an IP address added to McAfee ESM. The Asset Manager enables you to manage the assets on your network and can allow you to discover devices that are actively communicating on the network.
McAfee ePolicy Orchestrator (McAfee ePO)	https://docs.mcafee.com/bundle/rogue-system-detection-5.0.5-product-guide-epolicy-orchestrator/page/GUID-88DB6150-6B4D-4FAC-A6AB-C0DB754216F7.html	Unprotected systems, known as rogue systems, are often the weak spot of any security strategy, creating entry points that viruses and other potentially harmful programs can use to access your network. McAfee® Rogue System Detection provides near real-time discovery of rogue systems by using Rogue System Sensors installed throughout your network. These sensors use various passive and active network discovery techniques to detect systems connected to the network.
McAfee MVISION Cloud	https://www.mcafee.com/enterprise/en-us/assets/skyhigh/data-sheets/ds-skyhigh-for-amazon-web-services-0117.pdf	McAfee MVISION Cloud allows discovery of IaaS assets and supports configuration compliance of cloud virtual machines, such as EC2, Azure Virtual machines, Storage blobs, or S3 buckets.
SIA Partners	**Infoblox—Network Insight/NetMRI** https://www.infoblox.com/wp-content/uploads/infoblox-datasheet-network-insight.pdf http://www.infoblox.com/wp-content/uploads/infoblox-datasheet-netmri.pdf **Indegy—Industrial Cybersecurity Suite** https://www.indegy.com/industrial-cyber-security/	**Infoblox** Access an authoritative, integrated database of protocol, IP address, network infrastructure device, end-host, connectivity, and port data—breaking down operational silos in IT. McAfee ePO software integrates Infoblox NIOS™ to provide comprehensive asset management and device visibility. **Indegy** Identify and discover OT assets, detect threats and maintain configuration compliance for all your mission critical OT systems. Together with the integration with the McAfee security ecosystem solutions we can protect and respond to OT threats.

2. Inventory of Software Assets

Product Name	Link to Solution Offering	Explanation
McAfee Application Control	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-application-control.pdf	McAfee Application Control prevents zero-day and APT attacks by blocking execution of unauthorized applications. Using the software inventory feature, you can easily find and manage application-related files. It groups binaries (.EXEs, DLLs, drivers, and scripts) across your enterprise by application and vendor, displays them in an intuitive, hierarchical format, and intelligently classifies them as well-known, unknown, and known-bad applications. Using whitelisting, you can prevent attacks from unknown malware by allowing only known-good whitelisted applications to run.

Product Name	Link to Solution Offering	Explanation
McAfee MVISION Mobile	https://www.mcafee.com/enterprise/en-us/products/mvision-mobile.html	McAfee MVISION mobile provides visibility of threats across mobile operating systems such as Android and iOS devices. MVISION Mobile combines signature and on device AI-based mobile threat defense against known and unknown attacks on your mobile devices, thus enabling secure BYOD for your employees. In addition, MVISION Mobile also integrates with most EMM solutions to provide automated endpoint threat remediation and containment.
McAfee MVISION Cloud	https://www.skyhighnetworks.com/product/skyhigh-for-shadow-it/	McAfee MVISION Cloud offers in-depth visibility across 20,000 cloud applications running across the enterprise irrespective of managed or unmanaged endpoints. The MVISION Cloud ground link service builds an inventory of all cloud apps running across the enterprise. This allows organizations to safely adopt sanctioned cloud apps and prevent cloud native breaches.
McAfee Threat Intelligence Exchange (TIE)	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-threat-intelligence-exchange.pdf	McAfee Threat Intelligence Exchange acts as a reputation broker to enable adaptive threat detection and response. It combines local intelligence from security solutions across your organization with external global threat data and instantly shares this collective intelligence across your security ecosystem. TIE performs adaptive checks on the running applications for global and local threat reputation, as well as check for its prevalence within the customer environment. In case of no match, the application could potentially be flagged and blocked from running by sharing context via Data Exchange Layer (DXL) with the rest of the security ecosystem.
McAfee Policy Auditor	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-policy-auditor.pdf	McAfee Policy Auditor allows an audit of all system software components, such as applications, system registry settings, etc. It automatically detects any unwarranted change in integrity of an application.

3. Continuous Vulnerability Management

Product Name	Link to Solution Offering	Explanation
McAfee Policy Auditor	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-policy-auditor.pdf	
McAfee ePO + DXL + Rapid 7 Nexpose	**McAfee ePO** https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-epolicy-orchestrator.pdf **DXL** https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-data-exchange-layer.pdf **Rapid 7 Nexpose** https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-nexpose-product-brief.pdf	This control provided in conjunction with our SIA partner Rapid7. You can't reduce risk if you can't find, validate, and contextualize it. Nexpose dynamically discovers your complete attack surface and finds vulnerabilities you are missing today. Understand your threat exposure by determining if your vulnerabilities can be exploited and if your compensating controls are deployed successfully. Contextualize the risks to get a true picture of them as they align to your modern digital business. Rapid7 is integrating Nexpose, the leading vulnerability management toolset, with McAfee ePolicy Orchestrator and Data Exchange Layer. This will enable organizations to see the risks that are present on and off their network and drive action towards remediating those risks.

4. Controlled Use of Administrative Privileges

Product Name	Link to Solution Offering	Explanation
McAfee ePO + Beyond Trust/CyberArk	McAfee ePolicy Orchestrator https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-epolicy-orchestrator.pdf DXL https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-data-exchange-layer.pdf Beyond Trust PAM https://www.beyondtrust.com/resources/datasheets/executive-summary https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-beyondtrust.pdf CyberArk PAM https://www.cyberark.com/press/cyberark-integrates-privileged-identity-management-suite-key-mcafee-enterprise-security-solutions/	BeyondTrust, a McAfee® Security Innovation Alliance partner, integrates key components of privileged access management (PAM), specifically the Password Safe privileged account and session management solution, Privilege Management for Windows solution, and Enterprise Vulnerability Management, into the enterprise-ready management functions provided by McAfee ePO software, DXL, and McAfee Enterprise Security Management (SIEM) to unite endpoint security with real-time cyberthreat protection in a single user interface. CyberArk Privileged Account Security integrated with McAfee ePolicy Orchestrator (McAfee ePO) software provides privileged account security monitoring. CyberArk sends McAfee ePO alerts regarding the usage of privileged account credentials. IT administrators can set policies for alerts to be sent to McAfee ePO software based on their most important IT. The solution generates compliance reports directly from the McAfee ePO platform. The McAfee Enterprise Security Manager and CyberArk Privileged Threat Analytics integrated solution provides unmatched privileged activity intelligence empowering organizations to quickly identify and disrupt the most critical in-progress attacks.
McAfee Enterprise Security Manager (McAfee ESM)	https://www.mcafee.com/enterprise/en-us/products/enterprise-security-manager.html https://www.mcafee.com/enterprise/en-gb/products/mcafee-connect/user-behavior-analytics.html	McAfee ESM along with its Advanced Correlation Engine (ACE) provides rapid detection of credential abuse, unusual privilege escalation activity across the infrastructure through the UBA content pack. Workflows can then be orchestrated using McAfee ePO software and DXL to trigger remedial and containment activity providing enhanced closed loop remediation of privilege related threats.
McAfee MVISION Cloud	https://www.mcafee.com/enterprise/en-gb/products/mvision-cloud.html https://www.skyhighnetworks.com/cloud-security-blog/enhancing-aws-security-hub-with-McAfee-mvision-cloud/	McAfee MVISION Cloud provides integrated API-based monitoring of IAM activity across your SaaS, PaaS, and IaaS infrastructure. MVISION Cloud ensures protection against misconfiguration of IAM privileges and monitoring of IAM activity.

5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Product Name	Link to Solution Offering	Explanation
McAfee Policy Auditor	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-policy-auditor.pdf	At audit time, accuracy and timeliness are critical. Whether you need to prove compliance with mounting external regulations, quickly assess system patch status to prevent exploitation of vulnerabilities or reduce liability by proving that your organization is following best practices, McAfee Policy Auditor eases the pressure. Our easy-to-manage solution automates and simplifies the process, helping you to quickly assess patch deployment progress, monitor critical security configurations, and report consistently and accurately against key industry mandates and internal policies across your entire infrastructure or on specific systems. McAfee Policy Auditor helps you stay compliant, reduce costs and manual effort, and increase visibility.
McAfee ePolicy Orchestrator (On-Prem/ SaaS)	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-epolicy-orchestrator.pdf	McAfee ePO software allows for centralized policy management and establishment of endpoint security, data governance, and threat management baseline. McAfee ePO software provides a single pane of glass across workstations, mobile devices, and private and public Cloud assets.
McAfee Application Control	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-application-control.pdf	McAfee Application Control prevents zero-day and APT attacks by blocking execution of unauthorized applications. Using the software inventory feature, you can easily find and manage application-related files. It groups binaries (.EXEs, DLLs, drivers, and scripts) across your enterprise by application and vendor, displays them in an intuitive, hierarchical format, and intelligently classifies them as well-known, unknown, and known-bad applications. Using whitelisting, you can prevent attacks from unknown malware by allowing only known-good whitelisted applications to run.

6. Maintenance, Monitoring, and Analysis of Audit Logs

Product Name	Link to Solution Offering	Explanation
McAfee Enterprise Security Manager	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-siem-solutions-from-mcafee.pdf	McAfee ESM platform provides a flexible log management architecture. It provides three options around log search (Enterprise Log Search), integrity validated long term log retention (Enterprise Log Manager), and advanced event correlation to provide effective audit log management and audit event correlation.
McAfee MVISION Cloud	https://www.mcafee.com/enterprise/en-gb/products/mvision-cloud.html	Captures a comprehensive audit trail of all user and administrator activities to support post-incident investigations and forensics.

Foundational

7. Email and Web Browsing Protection

Product Name	Link to Solution Offering	Explanation
McAfee Secure Web Gateway (On Prem) **McAfee Client Proxy (MCP)**	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-web-gateway.pdf https://www.mcafee.com/enterprise/en-us/assets/faqs/faq-client-proxy.pdf	The McAfee Secure Web Gateway provides comprehensive inbound and outbound protection for all web traffic. McAfee Client Proxy (MCP) provides flexible protection for unmanaged devices thus enforcing web protection policies on prem and off prem.
McAfee Web Gateway Cloud Service (SaaS) **McAfee Client Proxy (MCP)**	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-web-gateway-cloud-service.pdf	The McAfee Web Gateway Cloud Service (WGCS) provides a flexible deployment model to enforce web protection across remote and branch sites without the need for additional on prem hardware/software. The McAfee Web Gateway Cloud Service also provides IPSEC integration enabling integration with SD-WAN gateways.
McAfee Advanced Threat Defense (ATD)	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-advanced-threat-defense.pdf	McAfee Advanced Threat Defense enables organizations to detect advanced, evasive malware and convert threat information into immediate action and protection. Unlike traditional sandboxes, it includes additional inspection capabilities that broaden detection and expose evasive threats. Tight integration between security solutions—from network and endpoint to investigation—enables instant sharing of threat information across the environment, enhancing protection and investigation.
McAfee SiteAdvisor Enterprise	https://www.mcafee.com/enterprise/en-us/products/siteadvisor-enterprise.html	McAfee SiteAdvisor Enterprise software allows your employees to surf and search the web safely as threats like spyware, adware, and phishing scams are blocked.
McAfee MVISION Cloud (SaaS Email Protection)	https://www.skyhighnetworks.com/product/office-365-security/	McAfee MVISION Cloud Sky gateway provides active and passive protection against email data leak for O365 and Exchange Online Services.
McAfee Security for Email Servers	https://www.mcafee.com/enterprise/en-us/products/security-for-email-servers.html	Strong internal safeguards and in-depth file analysis through integration with McAfee Advanced Threat Defense detects threats that may have either slipped past your perimeter defenses or entered your network via infected laptops and internal email.
McAfee MVISION Endpoint Detection and Response (MVISION EDR)	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-mvision-edr.pdf	McAfee MVISION EDR easily plugs into security operations phishing investigation workflows. Suspicious emails can flow to MVISION EDR for inspection. If found to be malicious, MVISION EDR can quickly determine which machines across the organization may be impacted.
Cofense—Intelligence and Triage	https://www.mcafee.com/enterprise/en-us/partners/security-innovation-alliance/directory.html https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-cofense.pdf	The integration of Cofense and McAfee ESM allows you to rapidly respond to phishing. McAfee Enterprise Security Manager has one-click access to human readable reports providing detailed insight into the attacker tactics, techniques, and procedures (TTPs); email message content; malware artifacts with full threat detail.

8. Malware Defenses

Product Name	Link to Solution Offering	Explanation
McAfee Endpoint Protection Platform (ENS, MVISION Endpoint, MVISION Mobile)	https://www.mcafee.com/enterprise/en-us/products/endpoint-protection-products.html	The McAfee protection platform includes a suite of advanced anti-malware protection which includes : - McAfee Endpoint Security provides core protection against known and advanced threats and provides AV, Host firewall, and web protection functionality. - MVISION Endpoint provides a lightweight option to centrally manage endpoint security alongside Windows Defender AV features protecting against advanced threats such as Fileless and Zero day. Combined with advanced threat remediation provides unparalleled protection against ransomware. - MVISION Mobile provides protection against evolving mobile threats across mobile operating systems such as Android and iOS and offers a true mobile threat defense solution (MTD). MVISION Mobile provides advanced mobile application forensics and analytics to protect against hidden and zero-day mobile threats.
McAfee Network Security Platform (NSP)	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-network-security-platform-ns-series.pdf	McAfee Network Security Platform (McAfee NSP) is a next-generation intrusion detection and prevention system (IDPS) that discovers and blocks sophisticated malware threats across the network. It utilizes advanced detection and emulation techniques, moving beyond mere pattern matching to defend against stealthy attacks with a high degree of accuracy. To meet the needs of demanding networks, the platform can scale to more than 40 Gbps with a single device—and up to 100 Gbps when stacked. The integrated McAfee solution portfolio streamlines security operations by combining real-time McAfee® Global Threat Intelligence feeds with rich contextual data about users, devices, and applications for fast, accurate response to network-borne attacks.
McAfee Secure Web Gateway	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-web-gateway.pdf	McAfee Web Gateway delivers comprehensive security for all aspects of web traffic in one high-performance appliance software architecture. For user-initiated web requests, McAfee Web Gateway first enforces an organization’s internet use policy. For all allowed traffic, it then uses local and global techniques to analyze the nature and intent of all content and active code entering the network via the requested web pages, providing immediate protection against malware and other hidden threats. And, unlike basic packet inspection techniques, McAfee Web Gateway can examine secure sockets layer (SSL) traffic to provide in-depth protection against malicious code or control applications that have been hidden through encryption.
McAfee Gateway Anti-Malware Engine	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-gateway-anti-malware.pdf	McAfee Gateway Anti-Malware Engine (GAM) works across both the NSP and Secure Web Gateway Platforms providing active threat emulation and protection against unknown threats at the network egress and ingress point.

9. Limitation and Control of Network Ports, Protocols, and Services

Product Name	Link to Solution Offering	Explanation
McAfee Endpoint Security (Firewall Module)	https://docs.mcafee.com/bundle/endpoint-security-10.6.0-firewall-product-guide-windows/page/GUID-0B9BDC3D-77EE-44B1-B63B-1A7E17FF0CC7.html	McAfee Endpoint security solution provides integrated firewalling and stateful packet inspection alongside host based IPS to provide protection against external threats and attacks.
Perimeter Firewall / UTM Solutions	https://www.mcafee.com/enterprise/en-us/partners/security-innovation-alliance/directory.html	McAfee SIA partners, such as Checkpoint and Fortinet provide adaptive threat defense by sharing perimeter threat data with McAfee® Threat Analytics and Intelligence platforms thus creating advanced threat protection workflows.
McAfee ESM	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-siem-solutions-from-mcafee.pdf	McAfee ESM provides network and traffic behavior analysis that can be combined with other network sensors, such as Firewalls, IPS, and routers.

10. Data Recovery Capabilities

Product Name	Link to Solution Offering	Explanation
McAfee Endpoint Security (ENS) **McAfee MVISION Endpoint**	https://www.mcafee.com/enterprise/en-gb/products/endpoint-security.html https://www.mcafee.com/enterprise/en-gb/products/mvision-endpoint.html	While McAfee doesn't provide full data backup and recovery features, MVISION Endpoint and McAfee ENS security provides advanced vaulting features which allows damage caused by ransomware to be reverted to a healthy state through its "Advanced Remediation" feature.

11. Secure Configuration for Network Devices

Product Name	Link to Solution Offering	Explanation
SIA Partner Infoblox NetMRI	https://www.infoblox.com/products/netmri/	Raise network automation to the next level with Infoblox NetMRI. It automates routine tasks such as device configuration, provisioning, and security operational tasks, enabling you to more easily achieve compliance, respond to incidents in a timely fashion, and deploy new apps faster.

12. Boundary Defense

Product Name	Link to Solution Offering	Explanation
McAfee NSP	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-network-security-platform-ns-series.pdf	McAfee Network Security Platform (McAfee NSP) is a next-generation intrusion detection and prevention system (IDPS) that discovers and blocks sophisticated malware threats across the network. It utilizes advanced detection and emulation techniques, moving beyond mere pattern matching to defend against stealthy attacks with a high degree of accuracy. To meet the needs of demanding networks, the platform can scale to more than 40 Gbps with a single device—and up to 100 Gbps when stacked. The integrated McAfee solution portfolio streamlines security operations by combining real time McAfee Global Threat Intelligence feeds with rich contextual data about users, devices, and applications for fast, accurate response to network-borne attacks.
McAfee Secure Web Gateway	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-web-gateway.pdf	McAfee Web Gateway delivers comprehensive security for all aspects of web traffic in one high-performance appliance software architecture. For user-initiated web requests, McAfee Web Gateway first enforces an organization's internet use policy. For all allowed traffic, it then uses local and global techniques to analyze the nature and intent of all content and active code entering the network via the requested web pages, providing immediate protection against malware and other hidden threats. And, unlike basic packet inspection techniques, McAfee Web Gateway can examine secure sockets layer (SSL) traffic to provide in-depth protection against malicious code or control applications that have been hidden through encryption.
McAfee Gateway Anti-Malware Engine	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-gateway-anti-malware.pdf	McAfee Gateway Anti-Malware Engine (GAM) works across both the NSP and Secure Web Gateway Platforms providing active threat emulation and protection against unknown threats at the network egress and ingress point.

13. Data Protection

Product Name	Link to Solution Offering	Explanation
McAfee Data Loss Prevention (DLP) Endpoint	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-dlp-endpoint.pdf	McAfee ePO platform provides a centralized console to manage and enforce your Device to Cloud Data loss prevention policies. McAfee ePO software manages the endpoint DLP policies on managed endpoints.
McAfee MVISION Cloud	https://www.skyhighnetworks.com/cloud-data-loss-prevention/	McAfee MVISION Cloud protects against cloud native breaches without impacting on end user productivity or user experience. MVISION Cloud protects Cloud to Cloud data breaches by protecting SaaS collaboration platforms such as Onedrive, Microsoft Teams, Box, etc. MVISION Cloud enforces granular permissions for activity within cloud services based on contextual factors such as the cloud service, user, device, attempted action, and location in addition to simple coarse-level policies to allow or block access. MVISION Cloud integrates with Mobile Device Management (MDM) solutions to enforce device-based access controls, such as allowing read-only access when sensitive documents are being accessed from unmanaged devices. McAfee ePO (SaaS/On-Prem) software provides the ability to extend the on prem data classification policies across the Cloud to offer a unified endpoint to Cloud DLP policy.

Product Name	Link to Solution Offering	Explanation
McAfee Secure Web Gateway	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-web-gateway.pdf	McAfee Secure Web Gateway provides integrated DLP policies for web content upload and boundary protection for confidential data leaving the enterprise network. The combination of MVISION Cloud, Secure Web Gateway (SaaS and On-Prem) provide an industry first "Unified Cloud Edge" protection service.
McAfee DLP Prevent (Network DLP)	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-dlp-prevent.pdf	McAfee DLP Prevent protects data leaving the enterprise network and provides storage for DLP activities on the enterprise network for historical forensics and eDiscovery efforts.
McAfee Database Activity Monitoring	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-database-activity-monitoring.pdf	McAfee Database Activity Monitoring, organizations gain visibility into all database activity, including local privileged access and sophisticated attacks from within the database. McAfee Database Activity Monitoring helps them protect their most valuable and sensitive data from external threats and malicious insiders. In addition to providing a reliable audit trail, McAfee Database Activity Monitoring also prevents intrusion by terminating sessions that violate security policy.

14. Controlled Access Based on Need to Know

The need to know access control principle is critical in ensuring user privileges are aligned to employee roles and responsibilities and unnecessary privileges are not available to users. While this should be part of an organization's security standards, procedures, and guidelines McAfee® products make it intuitive to configure policies that enforce the need to know principle.

Product Name	Link to Solution Offering	Explanation
McAfee MVISION Cloud	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-mvision-cloud.pdf	Supports role-based access and policies driven by AD groups and users.
McAfee Secure Web Gateway (SaaS/On-Prem)	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-web-protection.pdf	Supports role-based access and policies driven by AD groups and users.
SIA Integrations with IAM Platforms	https://www.mcafee.com/enterprise/en-us/assets/skyhigh/data-sheets/ds-skyhigh-okta-1114.pdf	McAfee integrates with a number of Idp/IAM platforms such as Okta, CyberArk, and Beyond Trust to provide further capabilities in creating a conducive security ecosystem that enforces the need to know principle.

15. Wireless Network Access Control

Product Name	Link to Solution Offering	Explanation
SIA Partners	https://www.mcafee.com/enterprise/en-us/partners/security-innovation-alliance/directory.html	McAfee integrates with leading Network Access Control Vendors (NAC) such as Cisco ISE, Aruba ClearPass, and Forescout. McAfee shares threat data collected from McAfee ESM and Endpoint Security and shares threat context to the NAC platforms to enforce network containment and isolation.

16. Account Monitoring

Product Name	Link to Solution Offering	Explanation
McAfee ESM	https://www.mcafee.com/enterprise/en-us/products/mcafee-connect/user-behavior-analytics.html	McAfee ESM provides correlation and monitoring of all user and system account activity via multiple log sources. McAfee ESM provides correlation and monitoring of your cloud user accounts via MVISION Cloud across all your cloud services.

Organizational

17. Implement Security Awareness Training

Implementing a security awareness training is crucial to bringing the human element in the people, process, technology triad of cybersecurity. All McAfee products offer options for including feedback for end users to make them aware of any policy violations they might have caused knowingly or unknowingly. An example of such a use case would be the replacement of PII containing file with a Tombstone file when uploaded to Onedrive (and on policy violation). This provides guided education to the user as to why the file was removed, improving user experience and resulting in fewer calls to the helpdesk.

18. Application Software Security

Product Name	Link to Solution Offering	Explanation
McAfee Foundstone Security Services	https://www.mcafee.com/enterprise/en-us/services/foundstone-services/software-security.html	McAfee Foundstone Security Services provide a professional services capability that allows us to support your secure software development efforts. Our software security practice focuses on identifying security bugs and design flaws across the software development lifecycle. Our holistic approach organically combines strategic, white box (static code analysis), and black box (penetration testing) services.
McAfee MVISION Mobile	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-mvision-mobile.pdf	McAfee MVISION Mobile provides advanced AI/ML-based mobile application scanning. This can be used to review security of mobile applications as part of the enterprise mobile application compliance validation or as part of an enterprise mobile application software development lifecycle.

19. Incident Response and Management

Product Name	Link to Solution Offering	Explanation
McAfee MVISION EDR	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-mvision-edr.pdf	McAfee MVISION Endpoint Detection and Response provides AI-guided investigation for security incidents which allows analysts to cut through infrastructure noise leading to incident response in minutes rather than hours and drastically reducing the "Mean time to respond (MTTR)" and "Mean Dwell Time (MDT)". MVISION EDR combines threat IOC/IOA from multiple sources such as SIEM events (McAfee ESM), Endpoint Process Activity, McAfee Global Threat Intelligence platforms to guide an analyst to the correct conclusions with minimal efforts. Advanced threat correlation leads to detection of stealthy attacks which traditional tools would otherwise fail to detect. Built-in incident workflow means ability to perform orchestrated actions such as creating service desk ticket or automating a response action such as quarantining the endpoint.
McAfee ESM	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-enterprise-security-manager.pdf	McAfee ESM provides the fundamental security platform to integrate all security data emanating from network devices, endpoints, and from other sources to one central place allowing for storage and investigation. McAfee ESM combined with McAfee completes the next-gen SOC capabilities that can proactively fight threats.
McAfee Foundstone Incident Response (IR) Service	https://www.mcafee.com/enterprise/en-us/services/foundstone-services/incident-response.html	McAfee Foundstone Incident Response services can offer expert support in the unfortunate event that you get hit with a security incident. McAfee Incident Response (IR) Service provides a comprehensive offering that combines an IR readiness assessment and pre-paid emergency incident response hours, delivered by our seasoned security experts. Be more prepared for an attack with McAfee IR Service.

20. Penetration Tests and Red Team Exercises

Product Name	Link to Solution Offering	Explanation
McAfee Advanced Programs Group (APG)	https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-advanced-programs-group.pdf	As new threat variants, attacks, and actors appear on a daily basis, even sophisticated enterprises have difficulty getting insight into these newly developed techniques and players. The best way to combat the attacks of both today and tomorrow is through actionable threat intelligence, delivered with custom, in-depth incident analysis reporting developed for your specific needs. The Advanced Programs Group (APG) from McAfee specializes in investigating targeted intrusions performed by the most advanced threat groups. APG uses the intelligence gathered from McAfee Global Threat Intelligence (McAfee GTI) capabilities, in conjunction with the experience of intelligence professionals, to provide actionable intelligence of developing threats, trends, and vectors.

Summary

McAfee products provide comprehensive coverage across the CIS CSC controls and our integrated approach to security provides flexibility for customers to leverage their existing McAfee and non-McAfee products to establish a strong cybersecurity foundation.

References

https://www.cisecurity.org/controls/cis-controls-list/

Document Name	CIS CSC20 Product Mapping
Author	Arnab Roy, RSA UKISA
Contact	arnab_roy@mcafee.com
Document History	First Release – 30/01/2020
Document Version	1.0

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

McAfee products and services may provide features that support and enhance your industry's compliance obligations, however, they are neither designed nor intended as holistic compliance solutions. The information provided herein is for information purposes only and does not constitute legal advice or advice on how to meet your compliance obligations.