Forcepoint

Solution Brief

Forcepoint Solutions to Meet CMMC Standards

Challenge

- **CMMC Compliance Complexity:** The CMMC framework, built on NIST 800-171 standards, poses significant challenges for Defense Industrial Base organizations due to its complex, evolving requirements. The uncertainty and ambiguity surrounding CMMC remain the biggest obstacles to its widespread adoption.
- **Supply Chain Security:** Protecting the DIB supply chain is crucial for national security, yet many organizations struggle to implement robust security measures.
- **Limited Visibility and Control:** Lack of visibility and control over data flow within complex environments hinders effective security posture.

Solution

- **Zero Trust Security Framework:** Forcepoint offers a comprehensive suite of solutions built on a Zero Trust security framework, ensuring a strong security posture and solutions that are directly mapped to addressing CMMC requirements.
- **Award Winning Data-First Security:** Forcepoint is a recognized industry-leader in data security, dedicated to protecting sensitive information wherever it resides. Our solutions provide organizations with comprehensive visibility and control across all environments
- **Federal Expertise:** With extensive experience working with the federal government, Forcepoint understands the unique challenges and requirements of CMMC compliance.

Outcome

- **Enhanced Security Posture:** Forcepoint's solutions help organizations strengthen their security posture and mitigate risks associated with CMMC non-compliance.
- **Improved Supply Chain Security:** By implementing robust security measures, DIB organizations can protect their supply chains from potential breaches and disruptions.
- **Simplified Compliance:** Forcepoint's CMMC compliance platform streamlines the process, reducing the burden on organizations and ensuring adherence to regulations.
- **Data Protection:** Forcepoint's data-first approach protects sensitive information, safeguarding national security interests.

The Cybersecurity Maturity Model Certification (CMMC) is a key step in strengthening the U.S. Department of Defense's (DoD) security and safeguarding Controlled Unclassified Information (CUI) within the Defense Industrial Base (DIB) supply chain. CMMC is set to drive one of the most significant industry shifts from non-compliant to compliant services.

As its implementation unfolds over the next few years, with requirements for Organizations Seeking Assessment (OSA's), Organizations Seeking Certification (OSC's), and External Service Providers (ESP's), industries will need to adopt best practices and security controls to meet the CMMC standards.

At Forcepoint, we are committed to upholding the highest standards of product integrity and safeguarding our customers' security. We understand the serious challenges confronting our government and strongly support the CMMC as a critical initiative for the DOD to enhance national security efforts.

Ambiguity and uncertainty are the greatest barriers to the widespread adoption of CMMC across the ecosystem. The Office of the Under Secretary of Defense for Acquisition and Sustainment has emphasized that DIB organizations must strengthen their security posture to mitigate the significant loss of CUI, which poses national security risks. The DoD is expected to establish CMMC certification requirements for any ESP that processes, stores, or transmits sensitive data. Forcepoint's solutions are here to remove this uncertainty, offering clarity and tools to support CMMC compliance.

What is CMMC?

The CMMC program is aligned with the DoD's information security requirements for DIB partners. It is designed to ensure the protection of sensitive unclassified information shared by the Department with its contractors and subcontractors. This program gives the DoD greater assurance that its contractors and subcontractors are meeting the necessary cybersecurity standards for acquisition programs and systems that handle controlled unclassified information.

Based on the US Department of Commerce's National Institute of Standards and Technology (NIST) 800-171 standards, the CMMC advances the existing Defense Federal Acquisition Regulation Supplement (DFARS) regulations by adding a cybersecurity verification component.

Every business, regardless of size, that sells directly or indirectly to the DoD will need some level of CMMC compliance. The DoD's stated goal is for CMMC to be cost-effective and affordable for smaller businesses to implement at the lower CMMC levels.

Strengthening the Security in the Supply Chain

The CMMC is about strengthening and maturing cybersecurity policies and processes for all DIB members. Strengthening the security of the supply chain is a key requirement.

It is important to recognize that since the federal government will leverage DIB suppliers infrastructure, data, systems, or information to contribute to the federal government supply chain, that espionage, sabotage, or other malicious activities are targeted at the supply chain can be used to disrupt or exploit the federal government.

Establishing standardized security practices and robust third-party risk management is essential for safeguarding the DIB supply chain. The U.S. Congress has mandated supply chain best practices and recommended legislative or policy changes to encourage their adoption by the private sector. Forcepoint is committed to helping DIB members implement these practices, ensuring their supply chains are secure and compliant with CMMC.

NIST's cybersecurity frameworks continue to provide guidance and best practices, DIB members must continue to leverage NIST's guidance. The private sector DIB members must focus security policies and processes on end-to-end risk management; strong supplier management; hardware manufacturing and order fulfillment to allow for management of personnel, facility, and product security.   The DIB members must have active security engagements in the public-private partnerships. Forcepoint's solutions align with these frameworks, helping organizations implement NIST's guidance and meet CMMC requirements.

Zero Trust by Design

Zero Trust is a philosophy that assumes every request to access IT resources may be a threat. No person, application, or machine is automatically trusted in a Zero Trust system. Every time access is requested, the user, device and connection must be authenticated or re-authenticated, whether it originates from inside or outside the network.

Forcepoint's portfolio of data-first security solutions is designed on Zero Trust principles, this approach helps organizations prevent sensitive data exfiltration and ensure regulatory compliance everywhere employees work and anywhere data resides.

The Zero Trust approach is a strong fit for highly distributed networks and hybrid cloud environments where IT resources may physically reside anywhere in the world. Zero Trust also is ideally suited for a hybrid workplace where users often need to connect to applications and data from remote locations on unsecured connections. By requiring authentication on every access request, a Zero Trust environment can help prevent attacks and limit the damage that attackers can do if they successfully penetrate defenses in one part of the network.

Zero Trust solutions operate on a "default deny" basis, barring access to IT resources until a user, device, or process has been authenticated. Zero Trust environments verify access requests based on context, including user identity, location, type of device, and the content and application being requested. Adaptive policies continually reassess the risk associated with each user and device as the context changes.

Security teams in a Zero Trust environment don't wait until an attack sets off alarms. Instead, they assume a breach has already happened and constantly seek to identify and remediate it. This practice allows them to find violations faster and limit the damage.

In a Zero Trust system, legitimate users, devices and processes receive permission to access only the resources they need to perform a specific function and nothing more. This helps to limit the risk exposure of each request and minimizes the chance of a potential breach.

DIB members within the supply chain who meet CMMC requirements play a key role in enabling Zero Trust security for DoD solutions. The federal government's Zero Trust requirements are unique and more stringent compared to other industries. By adopting Zero Trust as part of their cybersecurity strategy, DIB members enhance their security capabilities, providing stronger, more mature defenses. Forcepoint's solutions deliver this level of security, helping DIB members not only meet CMMC requirements but also protect their critical assets through a robust Zero Trust framework.

Forcepoint's Federal Focus

Forcepoint is the industry-leading user and data security cybersecurity company, entrusted to safeguard organizations and the federal government while driving digital transformation and growth. Our solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value.

Forcepoint provides Data-first security with converged capabilities that protect from endpoint to cloud. We provide threat and behavior intelligence research, applying up-to-date threat and behavior intelligence for stronger cyber protection solutions. And use AI and data science, leveraging machine learning and analytics for behavioral understanding.

The Forcepoint portfolio consists of these main solutions

DATA SECURITY EVERYWHERE	DATA-FIRST SASE
Forcepoint ONE Data Security	Forcepoint ONE Cloud Access Security Broker
Forcepoint DSPM	Forcepoint ONE Web Security
Risk Adaptive Protection	Forcepoint ONE Cloud Firewall
Enterprise DLP	Forcepoint ONE ZTNA
Data Classification	Remote Browser Isolation
DLP for Email	Secure SD-WAN and NGFW

Forcepoint Solutions Mapped to CMMC

CMMC DOMAIN/ PRACTICE #	PRACTICE NAME	COMPLIANT/ ASSISTS	FORCEPOINT PRODUCTS	VALUE
ACCESS CONTROL				
AC.L1-3.1.1	Authorized Access Control	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint Next-Generation Firewalls (NGFWs) and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Role Based Access Control and Change Control functionality to limit system access to authorized users, processes acting on behalf of authorized users, or devices.
			Forcepoint NGFW	
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Role Based Access Control and Change Control functionality to limit system access to authorized users, processes acting on behalf of authorized users, or devices.
AC.L1-3.1.2	Transaction and Function Control	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN and Enterprise DLP solutions provide access control for users, devices, application, url's and files to limit information system access to the types of transactions and functions that authorized users are permitted to execute.
			Forcepoint NGFW	
			Enterprise DLP	
AC.L1-3.1.20	External Connections	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN and VPN Client and Enterprise DLP solutions provide access control for users, devices, application, url's and files to verify and control/ limit connections to and use of external information systems.
			Forcepoint NGFW	
			Enterprise DLP	
AC.L2-3.1.3	Control CUI Flow	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions provide access control for users, devices, application, url's and files to control the flow of CUI in accordance with approved authorizations.
			Forcepoint NGFW	
			Enterprise DLP	→ Forcepoint Enterprise DLP solution provides CUI detection and exfiltration prevention policies to control the flow of CUI in accordance with approved authorizations
AC.L2-3.1.4	Separation of Duties	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Role Based Access Control and Change Control functionality to employ the principle of least privilege, including for specific security functions and privileged accounts.
			Forcepoint NGFW	
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Role Based Access Control and Change Control functionality to employ the principle of least privilege, including for specific security functions and privileged accounts.

CMMC DOMAIN/ PRACTICE #	PRACTICE NAME	COMPLIANT/ ASSISTS	FORCEPOINT PRODUCTS	VALUE
ACCESS CONTROL				
AC.L2-3.1.5	Least Privilege	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Role Based Access Control and Change Control functionality to separate the duties of individuals to reduce the risk of malevolent activity without collusion.
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Role Based Access Control and Change Control functionality to separate the duties of individuals to reduce the risk of malevolent activity without collusion.
AC.L2-3.1.6	Non-Privileged Account Use	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Role Based Access Control and Change Control functionality to use non-privileged accounts or roles when accessing non-security functions.
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Role Based Access Control and Change Control functionality to use non-privileged accounts or roles when accessing non-security functions.
AC.L2-3.1.7	Privileged Functions	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Role Based Access Control and Change Control functionality to prevent non-privileged users from executing privileged functions. And SMC provides Audit Logs to capture the execution of such functions.
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Role Based Access Control and Change Control functionality to prevent non-privileged users from executing privileged functions. And FSM provides Audit Logs to capture the execution of such functions.
AC.L2-3.1.8	Unsuccessful Logon Attempts	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Administrative Access Control functionality to limit unsuccessful logon attempts.
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Administrative Brute Force Login Protection functionality to limit unsuccessful logon attempts.
AC.L2-3.1.9	Privacy and Security Notices	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's login banners functionality to provide privacy and security notices consistent with applicable CUI rules.
AC.L2-3.1.10	Session Lock	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Administrative Access Control functionality to use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Administrative Controls to use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
AC.L2-3.1.11	Session Termination	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Administrative Access Control functionality to terminate (automatically) a user session after a defined condition.
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Administrative Controls to terminate (automatically) a user session after a defined condition.

CMMC DOMAIN/ PRACTICE #	PRACTICE NAME	COMPLIANT/ ASSISTS	FORCEPOINT PRODUCTS	VALUE
ACCESS CONTROL				
AC.L2-3.1.12	Control Remote Access	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's VPN Client functionality to monitor and control remote access sessions.
AC.L2-3.1.13	Remote Access Confidentiality	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's VPN Client functionality to employ cryptographic mechanisms to protect the confidentiality of all access sessions.
		Assists	Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Administrative Controls does not have the distinction between Local Access or Remote Access but does employ cryptographic mechanisms to protect the confidentiality of all access sessions.
AC.L2-3.1.14	Remote Access Routing	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's VPN Client functionality to route remote access via managed access control points.
AC.L2-3.1.16	Wireless Access Authorization	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint "W Series" of appliances for Wireless functionality to authorize wireless access prior to allowing such connections.
Access Control AC.L2-3.1.17	Wireless Access Protection	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint "W Series" of appliances for Wireless functionality to protect wireless access using authentication and encryption.

CMMC DOMAIN/ PRACTICE #	PRACTICE NAME	COMPLIANT/ ASSISTS	FORCEPOINT PRODUCTS	VALUE
AUDIT AND ACCOUNTABILITY				
AU.L2-3.3.1	System Auditing	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Audit Logs functionality to 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.
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Audit Logs functionality to 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.L2-3.3.2	User Accountability	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Identity and various Logging functionality to ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Incidents and various Logging functionality to ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.

CMMC DOMAIN/ PRACTICE #	PRACTICE NAME	COMPLIANT/ ASSISTS	FORCEPOINT PRODUCTS	VALUE
AUDIT AND ACCOUNTABILITY				
AU.L2-3.3.4	Audit Failure Alerting	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's System Alert functionality to alert in the event of an audit logging process failure.
			Forcepoint NGFW	
		Assists	Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Incidents and various Logging functionality can be exported to Notification applications to alert in the event of an audit logging process failure.
AU.L2-3.3.5	Audit Correlation	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Reporting, Logging and Log Management Task functionality to correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
			Forcepoint NGFW	
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Incidents, various Logging, and Reporting functionality to correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
AU.L2-3.3.6	Reduction and Reporting	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Reporting, Log Filtering functionality to provide audit record reduction and report generation to support on-demand analysis and reporting
			Forcepoint NGFW	
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Incidents, various Log Filtering, and Reporting functionality to provide audit record reduction and report generation to support on-demand analysis and reporting.
AU.L2-3.3.7	Authoritative Time Source	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage Network Time Protocol across SMC, Engines and Agents for the ability to provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
			Forcepoint NGFW	
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage Network Time Protocol across Forcepoint Security Manager, Supplemental Servers and Agents for the ability to provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
AU.L2-3.3.8	Audit Protection	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Role Based Access Control and Change Control functionality to protect audit information and audit logging tools from unauthorized access, modification, and deletion.
			Forcepoint NGFW	
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Role Based Access Control and Change Control functionality to protect audit information and audit logging tools from unauthorized access, modification, and deletion.
AU.L2-3.3.9	Audit Management	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Role Based Access Control and Change Control functionality to limit management of audit logging functionality to a subset of privileged users.
			Forcepoint NGFW	
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Role Based Access Control and Change Control functionality to limit management of audit logging functionality to a subset of privileged users.

CMMC DOMAIN/ PRACTICE #	PRACTICE NAME	COMPLIANT/ ASSISTS	FORCEPOINT PRODUCTS	VALUE
CONFIGURATION MANAGEMENT				
CM.L2-3.4.2	Security Configuration Enforcement	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage STIG documentation to establish and enforce security configuration settings for information technology products employed in organizational systems.
CM.L2-3.4.3	System Change Management	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Role Based Access Control and Change Approval functionality to track, review, approve or disapprove, and log changes to organizational systems.
		Assist	Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Role Based Access Control and Change Control functionality to assist in the tracking, reviewing and provide logs for changes to organizational systems.
CM.L2-3.4.6	Least Functionality	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions by design incorporate the principle of least functionality by configuring organizational systems to provide only essential capabilities.
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions evaluate the context of data and be configured to incorporate the principle of least functionality, essentially configuring and applying DLP policy to provide only essential capabilities.
CM.L2-3.4.7	Nonessential Functionality	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions by design can restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
CM.L2-3.4.8	Application Execution Policy	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN with Endpoint Control Agent (ECA) solutions can 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.

CMMC DOMAIN/ PRACTICE #	PRACTICE NAME	COMPLIANT/ ASSISTS	FORCEPOINT PRODUCTS	VALUE
IDENTIFICATION AND AUTHENTICATION				
IA.L1-3.5.1	Identification	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions with Endpoint Control Agent (ECA), Forcepoint User ID Service (FUID) and Browser Based Authentication functionality to Identify information system users, processes acting on behalf of users, or devices.
		Assist	Enterprise DLP	→ Forcepoint Enterprise DLP solutions has Directory Service integration, such as integration with Active Directory, as well as Administrative Access Controls and the use of an device Agent functionality to Identify information system users, processes acting on behalf of users, or devices.
IA.L1-3.5.3	Multifactor Authentication	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions with RADIUS and TACACS+ functionality to provide multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions has Administrative Access Controls with RSA SecurID authentication to provide multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

CMMC DOMAIN/ PRACTICE #	PRACTICE NAME	COMPLIANT/ ASSISTS	FORCEPOINT PRODUCTS	VALUE
IDENTIFICATION AND AUTHENTICATION				
IA.L1-3.5.4	Replay-Resistant Authentication	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions with RADIUS and TACACS+ support enables integration with TOTP authentication server for replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
IA.L1-3.5.5	Identifier Reuse	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Administrative Access Control functionality to prevent reuse of identifiers for a defined period.
IA.L1-3.5.6	Identifier Handling	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Administrative Access Control functionality to disable identifiers after a defined period of inactivity.
IA.L1-3.5.7	Password Complexity	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Administrative Access Control functionality to enforce a minimum password complexity and change of characters when new passwords are created.
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Administrative Access Control functionality to enforce a minimum password complexity and change of characters when new passwords are created.
IA.L1-3.5.8	Password Reuse	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Administrative Access Control functionality to prohibit password reuse for a specified number of generations
IA.L1-3.5.9	Temporary Passwords	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Administrative Access Control functionality to allow temporary password use for system logons with an immediate change to a permanent password.
IA.L1-3.5.10	Identification and Authentication IA.L1-3.5.10 Cryptographically-Protected Passwords	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Administrative Access Control functionality to store and transmit only cryptographically-protected passwords.
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Administrative Access Control functionality to store and transmit only cryptographically-protected passwords.
IA.L1-3.5.11	Obscure Feedback	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Administrative Access Control functionality to obscure feedback of authentication information.
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Administrative Access Control functionality to obscure feedback of authentication information.

CMMC DOMAIN/ PRACTICE #	PRACTICE NAME	COMPLIANT/ ASSISTS	FORCEPOINT PRODUCTS	VALUE
MEDIA PROTECTION				
MP.L2-3.8.6	Media Disposal	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW Enterprise DLP	→ From behavior-centric data security policies to AI-powered data classification, securing information is at the core of what we do. Discover more about our best-in-class privacy and compliance measures, and how we're always working to improve. www.forcepoint.com/legal/forcepoint-trust-hub

CMMC DOMAIN/ PRACTICE #	PRACTICE NAME	COMPLIANT/ ASSISTS	FORCEPOINT PRODUCTS	VALUE
SYSTEM AND COMMUNICATIONS PROTECTION				
SC.L1-3.13.1	Boundary Protection	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Administrative Access Control functionality to monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the information systems.
			Forcepoint NGFW	
		Assists	Enterprise DLP	→ Forcepoint Enterprise DLP solutions provide Data Exfiltration Prevention functionality which scans the content of the data and applies policies and generates reports that provide solutions to monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the information systems.
SC.L1-3.13.3	Role Separation	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Role Based Access Control to separate user functionality from system management functionality.
			Forcepoint NGFW	
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverage the Forcepoint Security Manager's Role Based Access Control to separate user functionality from system management functionality.
SC.L1-3.13.5	Public-Access System Separation	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Administrative Access Control to separate user functionality from system management functionality
			Forcepoint NGFW	
SC.L1-3.13.6	Network Communication by Exception	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Administrative Access Control to separate user functionality from system management functionality.
			Forcepoint NGFW	
SC.L1-3.13.7	Split Tunneling	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint VPN Client to 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).
			Forcepoint NGFW	
SC.L1-3.13.8	Data in Transit	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint VPN Client and FIPS Mode to implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
			Forcepoint NGFW	
		Assists	Enterprise DLP	→ Forcepoint Enterprise DLP solutions leverages the most current versions of TLS to establish a TLS tunnel between the Agent and the Enterprise DLP solution to implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
SC.L1-3.13.9	Connections Termination	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage the Forcepoint SMC's Access Control to terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
			Forcepoint NGFW	
SC.L1-3.13.10	Key Management	Compliant	FlexEdge Secure SD-WAN	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions can import and support the use of external CA Certificate to establish and manage cryptographic keys for cryptography employed in organizational systems.
			Forcepoint NGFW	
			Enterprise DLP	→ Forcepoint Enterprise DLP solutions can import and support the use of external CA Certificate to establish and manage cryptographic keys for cryptography employed in organizational systems.

CMMC DOMAIN/ PRACTICE #	PRACTICE NAME	COMPLIANT/ ASSISTS	FORCEPOINT PRODUCTS	VALUE
SYSTEM AND COMMUNICATIONS PROTECTION				
SC.L1-3.13.11	CUI Encryption	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage FIPS Mode and FIPS Certification to employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
		Assist	Enterprise DLP	→ Forcepoint Enterprise DLP solutions can import and support the use of external CA Certificate with stronger hash function or stronger encryption to match FIPS 140-2 to establish and manage cryptographic keys for cryptography employed in organizational systems.
SC.L1-3.13.13	Mobile Code	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage Threat Prevention functionality to control and monitor the use of mobile code.
SC.L1-3.13.14	Voice over Internet Protocol	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage Access Control and the Threat Prevention functionality to control Voice over Internet Protocol.
SC.L1-3.13.15	Communications Authenticity	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW Enterprise DLP	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN and Enterprise DLP solutions leverage system communication for management connections using TLS 1.2 Encrypted and authenticated using X.509v3 Keys and Certificates to protect the authenticity of communications sessions.
SI.L1-3.14.1	Flaw Remediation	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW Enterprise DLP	→ The Forcepoint Secure Testing Methodology is a crucial part of an end-to-end process that works in lockstep with Forcepoint's Secure Software Development Lifecycle (SSDLC) - also known as our Secure Development Process to ensure security-by-design. Forcepoint's SSDLC includes elements of secure design, secure release and security education. → Forcepoint PSIRT's goal is to minimize customers' risk associated with security vulnerabilities in Forcepoint products by providing timely information, guidance and remediation of vulnerabilities. Forcepoint PSIRT is a team that manages the receipt, investigation, internal coordination, remediation and disclosure of security vulnerability information related to Forcepoint products. → Forcepoint's PSIRT is a team that coordinates security testing, vulnerability management, and vulnerability communication for products created and services provided by Forcepoint, including those that are now end-of-life (EOL). PSIRT receives reports of vulnerabilities via email to PSIRT@forcepoint.com. → Forcepoint can then ensure to identify, report, and correct information and information system flaws in a timely manner. www.forcepoint.com/legal/forcepoint-trust-hub

CMMC DOMAIN/ PRACTICE #	PRACTICE NAME	COMPLIANT/ ASSISTS	FORCEPOINT PRODUCTS	VALUE
SYSTEM AND INFORMATION INTEGRITY				
SI.L1-3.14.2	Malicious Code Protection	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage File Filtering functionality to provide Malicious Code Protection.
SI.L1-3.14.4	Update Malicious Code Protection	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage File Filtering functionality to provide updates to malicious code protection mechanisms when new releases are available
SI.L1-3.14.6	Monitor Communications for Attacks	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage Access Control and Threat Prevention functionality to monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
SI.L1-3.14.7	Identify Unauthorized Use	Compliant	FlexEdge Secure SD-WAN Forcepoint NGFW	→ Forcepoint NGFWs and FlexEdge Secure SD-WAN solutions leverage Access Control and Threat Prevention functionality to monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Forcepoint.com/contact