

FORCEPOINT CDM Capability Matrix

20+ YEARS OF EXPERTISE SUPPORTING INTELLIGENCE, DEFENSE AND CIVILIAN AGENCIES AROUND THE WORLD.

Forcepoint's application to the U.S. General Services Administration was recently accepted in the Continuous Diagnostics and Mitigation (CDM) program, which enables agencies to quickly acquire cybersecurity products. Forcepoint [Next Generation Firewall \(NGFW\)](#), [Email Security](#), [Web Security](#), [User & Entity Behavior Analytics \(UEBA\)](#), [Insider Threat](#), [Advanced Malware Detection \(AMD\)](#), [Cloud Access Security Broker \(CASB\)](#), [High Speed Guard](#) and [Data Loss Prevention \(DLP\)](#) are now available on the CDM Approved Product List.

FORCEPOINT PRODUCT	WHAT IS ON THE NETWORK?	WHO IS ON THE NETWORK?	HOW IS THE NETWORK PROTECTED?	WHAT IS HAPPENING ON THE NETWORK?	HOW IS THE DATA PROTECTED?	DETAILS	LINK
Forcepoint Next Generation Firewall (NGFW)			Bound E & Bound F			The Forcepoint NGFW monitors and controls incoming and outgoing network traffic based on predetermined security policy. It combines the best of both worlds: Forcepoint NGFW's #1 rated security and centralized manageability plus the robust protection of the government-required Sidewinder Security Proxies.	www.forcepoint.com/ngfw
Forcepoint Email Security			Bound E & Bound F			Forcepoint Email Security works in real time to accurately identify and classify network traffic, apply policies & detect threats. Unified management & reporting functions provide context & insights to minimize dwell time of attacks, prevent exfiltration of data, & dramatically reduce the impact of spam.	www.forcepoint.com/product/cloud-security/forcepoint-email-security
Forcepoint Web Security			Bound E & Bound F			Forcepoint Web Security detects threats and analyzes web content using inline, real-time composite defense assessments and predictive analysis. The web proxy component, includes TLS/SSL decryption allowing application analytics on HTTPS traffic.	www.forcepoint.com/product/cloud-security/forcepoint-web-security
Forcepoint Data Loss Prevention (DLP)			Bound E & Bound F		Data Discovery/ Classification, Data Loss Prevention	Forcepoint Data Loss Prevention (DLP) helps secure intellectual property, personally identifying information (PII), and other sensitive data – wherever it resides – on endpoints, in the cloud, or on-premises. Apply behavioral analytics and machine learning to cluster DLP incidents to find Incident Risk Ranking (IRR).	www.forcepoint.com/dlp

Forcepoint Web / Email Security DLP Module			Bound E & Bound F		Data Discovery Classification, Data Loss Prevention	Forcepoint Web / Email Security DLP Module allows application of DLP policies on web /email traffic - one of the main vectors for data extrusion. Adds enterprise-class DLP on web / email traffic (HTTP and HTTPS).	www.forcepoint.com/solutions/need/uni-fied-web-email-security
Forcepoint User and Entity Behavior Analytics (UEBA)		Trust, Behave, Cred, Priv		Audit Data Collection, System and Information Integrity		Forcepoint UEBA identifies the human risk to cyber security by monitoring and providing visibility into the cyber activity of people. Forcepoint UEBA prioritizes cyber risk and assigns a risk score for every user by analyzing large amounts of complex data from your existing IT environment and understanding the actions of users that may put critical data at risk.	www.forcepoint.com/ueba
Forcepoint Insider Threat				Incident Response Monitoring, Audit Data Collection, Ongoing Assessment Monitoring		Forcepoint Insider Threat User Activity Monitoring (UAM) enables a policy based strategy to detect insider threats by monitoring & capturing technically observable human behaviors on endpoints. Forcepoint Insider Threat provides flexibility to tailor & apply user-monitoring policies to specific desktops and user groups.	www.forcepoint.com/product/data-insider-threat-protection/forcepoint-insider-threat
Forcepoint Cloud Access Security Broker (CASB)			Bound F		Data Discovery/ Classification, Data Protection, Data Loss Prevention	Forcepoint CASB provides visibility & control for cloud applications & helps prevent the loss of critical data. It allows discovery of unsanctioned cloud applications & assess associated risk. Forcepoint CASB can be deployed in both API and inline (proxy), allowing Forcepoint CASB to quickly add custom or obscure cloud applications and detect user actions at a granular level.	www.forcepoint.com/casb
Forcepoint Advanced Malware Detection (AMD)			Bound E & Bound F			Forcepoint Advanced Malware Detection sandboxing maximizes the security efficacy of Forcepoint's products. Deep Content Inspection at multiple levels, in dormant code, and in other indicators reveals highly evasive threats often overlooked by other sandboxing technologies & eliminates false positives.	www.forcepoint.com/AMD
Forcepoint High Speed Guard			Bound E & Bound F		Data Protection	Forcepoint High Speed Guard provides network segmentation and permits highly complex, bi-directional, automated data transfers between multiple domains, specializing in real-time streaming video. High Speed Guard has demonstrated the fastest bi directional transfer rates of more than nine gigabits per second (Gb/s) on dual processor commodity servers.	www.forcepoint.com/product/cross-domain-security/forcepoint-high-speed-guard

CONTACT
cdm@forcepoint.com

© 2018 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.

[DATASHEET_CDM_CAPABILITY_MATRIX_EN] 100077FED.090418