

Protecting the human point.

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 [NGFW](#), [Email Security](#), [Web Security](#), [UEBA](#), [Insider Threat](#) and [DLP](#) are now available on the CDM Approved Product List for Phase Three.

FORCEPOINT PRODUCT	BOUND F - REQUIREMENT	BOUND F - REQUIREMENT	BOUND F - REQUIREMENT	BOUND E - REQUIREMENT	DETAILS	LINK
Forcepoint NGFW	Packet/Content/ Encapsulation Filtering	Proxies	Network Access Protection	Crypto+Key/CA	The Forcepoint NGFW is a next gen firewall that monitors and controls incoming and outgoing network traffic based on predetermined security policy. It features robust security enabled by 16 node active-active firewall clustering to further increase uptime and speeds and feeds on daily traffic and VPNs, while ensuring smart validity checks to administrative changes. Within the Forcepoint Security Management Console (SMC) advanced levels of inspection control with attributes, connection parameters and commands for specific proxies offer unique proxy functionality. The Forcepoint NGFW’s simple and precise firewall policies avoid errors and security holes with Smart Policies that are easy to comprehend and more efficient to maintain while pushing new policies and updates without downtime for the most critical networks.	https://www.forcepoint.com/product/network-security/forcepoint-ngfw
Forcepoint Email Security	Data Loss/Leak Prevention	Content Filter		Crypto+Key/CA	Forcepoint Email Security works in real time to accurately identify and classify network traffic, apply policies and detect threats. Unified management and reporting functions streamline work for the security team, giving them the context and insights they need to minimize the dwell time of attacks, prevent exfiltration of data, and dramatically reduce the impact of spam on the mail system.	https://www.forcepoint.com/product/cloud-security/forcepoint-email-security



FORCEPOINT PRODUCT	BOUND F - REQUIREMENT	BOUND F - REQUIREMENT	BOUND F - REQUIREMENT	BOUND E - REQUIREMENT	DETAILS	LINK
Forcepoint Web Security	Content Filter	Data Loss/Leak Prevention	Proxy	Crypto+Key/CA	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.	https://www.forcepoint.com/product/cloud-security/forcepoint-web-security
Forcepoint DLP	Data Loss/Leak Prevention	Content Filter		Crypto+Key/CA	Forcepoint DLP provides the ability to detect and secure data-at-rest across the network as well as in cloud services such as Microsoft Office 365, Citrix ShareFile and Box Enterprise. Identify and prevent malicious and accidental data exfiltration, whether originating from outside attacks or insider threats. Counter advanced threat evasion techniques with powerful OCR scanning to recognize data within an image, and use drip DLP to stop the theft of data one record at a time. Preconfigured policies allow organizations to meet compliance requirements quickly and easily.	https://www.forcepoint.com/product/data-insider-threat-protection/forcepoint-dlp
Forcepoint Web / Email Security DLP Module	Data Loss/Leak Prevention			Crypto	Forcepoint Web / Email Security DLP Module allows application of DLP policies on web /email traffic - one of the main vectors for data exfiltration. Adds enterprise-class DLP on web / email traffic (HTTP and HTTPS).	https://www.forcepoint.com/product/content-security/forcepoint-dlp-for-web-email
Forcepoint User and Entity Behaviour Analytics (UEBA)	Audit Data Collection	System and Information Integrity		Crypto	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.	https://www.forcepoint.com/product/data-insider-threat-security/forcepoint-ueba
Forcepoint Insider Threat	Incident Response Monitoring	Audit Data Collection	Ongoing Assessment Monitoring	Crypto	<p>Forcepoint Insider Threat User Activity Monitoring (UAM) software is a mature, demonstrably scalable and operationally-proven UAM solution. The host-based tool enables a policy based strategy to detect insider threats by monitoring and capturing technically-observable human behaviors on computer endpoints.</p> <p>Forcepoint Insider Threat supports a risk-managed approach to insider threat detection by providing flexibility to tailor and apply user-monitoring policies to specific desktops and user groups. Forcepoint Insider Threat provides analysts with the ability to succinctly define policy-based criteria, determining which behaviors to monitor and what information to collect. Analysts can also minimize or block the collection of sensitive information.</p>	https://www.forcepoint.com/product/data-insider-threat-protection/forcepoint-insider-threat



For more information please contact CDM@Forcepoint.com:

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance.

Forcepoint was formed in 2016 as a result of the combination of the user protection, data security and cloud expertise of Websense, the insider threat and analytics of Raytheon, the next-generation network protection capabilities of Stonesoft, the cloud application protection and visibility of Skyfence CASB (Cloud Access Security Broker) and most recently, the security analytics capabilities of RedOwl. These five businesses integrate decades of front-line experience across many domains of cybersecurity, from Fortune 100 enterprises and mid-sized businesses in every industry, to the world's most highly-secure defense, intelligence and law enforcement agencies. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.

CONTACT
cdm@forcepoint.com

© 2017 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.

[FP-DATASHEET_CDM_CAPABILITY_MATRIX_US] 100077.121917