Fidelis® Cybersecurity

Fidelis Elevate™

For Accelerated Delivery of Advanced Threat Visibility and Orchestrated Defenses of the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program

www.fidelissecurity.com

Contents

Executive Summary

With very little effort and expense, adversaries in cyberspace leverage automation to evade large and expensive deployments of commodity network and system security stacks (e.g., firewalls, antivirus, HIPS and IDPS). Federal organizations of all sizes report new cyber intrusions every day, and defeating these attacks is one of the most important national security challenges. In response, the Department of Homeland Security (DHS) developed the Continuous Diagnostics and Mitigation (CDM) program to provide adequate, risk-based, and cost-effective cybersecurity with more efficient allocation of cybersecurity resources.

In order to successfully execute the CDM program, industry must deliver capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts to operations, and mitigate risks automatically based upon pre-defined cyber incident response playbooks. A side benefit of this approach frees critical analyst resources to investigate and respond to the remaining cyber events. The challenge today is the unwieldy stacks of layered defense products provide lots of alerts yet do not provide true, complete visibility. With a rapidly expanding attack surface, federal agencies need solutions that detect and empower hunting for real threats, as well as prioritizing the right responses -- opposed to floods of alerts that ultimately slow down cyber missions.

Automated platforms must provide integration of data and analysis through distributed sensors and agents throughout the enterprise, including:

- **Network traffic inspection** that includes full session reassembly, deep content inspection, and process examination to provide tangible cyber efficiency and eliminate "maneuver space" for malicious activity
- **Deception technology** that discovers and classifies network assets and provides visibility of lateral movement, with high fidelity alerts
- **Endpoint detection and response** that captures rich event and process metadata for real-time and retroactive analysis, along with threat intelligence, behavioral rules and an indicator library stocked with IOC and YARA indicators, as well as prevention capabilities – all in a single agent

Fidelis Elevate™ fortifies government networks and systems by arming cyber mission operators with visibility and automation to detect and respond to adversary activity at cyber speed. Fundamentally, Elevate™ creates a rich source of metadata for real-time and retrospective analysis (with network data loss prevention, deception, and endpoint detection and response) into one, unified solution for automated threat detection and response. Although Elevate™ modules may be integrated in existing security stacks to improve visibility and threat intelligence with content and context, deployment of the Elevate™ unified platform maximizes the effectiveness of hunt missions and address cyberattacks across the entire threat lifecycle.

This whitepaper addresses the reasons that malicious cyber actors, and malicious/unwitting insiders, continue to succeed despite significant investments in the standard commodity security capabilities, and examines how Fidelis Cybersecurity delivers critical technologies and services to help federal organizations accelerate full implementation with operational focus on the mission to automatically detect, deter and defeat adversaries on every level.

Introduction

The CDM Program is organized by capabilities, as identified in the diagram shown here and further described below. Each capability consists of several capabilities, with the goal of establishing a system that will continually monitor an IT environment, identify and remediate threats, and roll up data to agency and government-wide management dashboards. This white paper gives an overview of how Fidelis supports aspects of CDM and enables agencies to achieve the security objectives of the program.

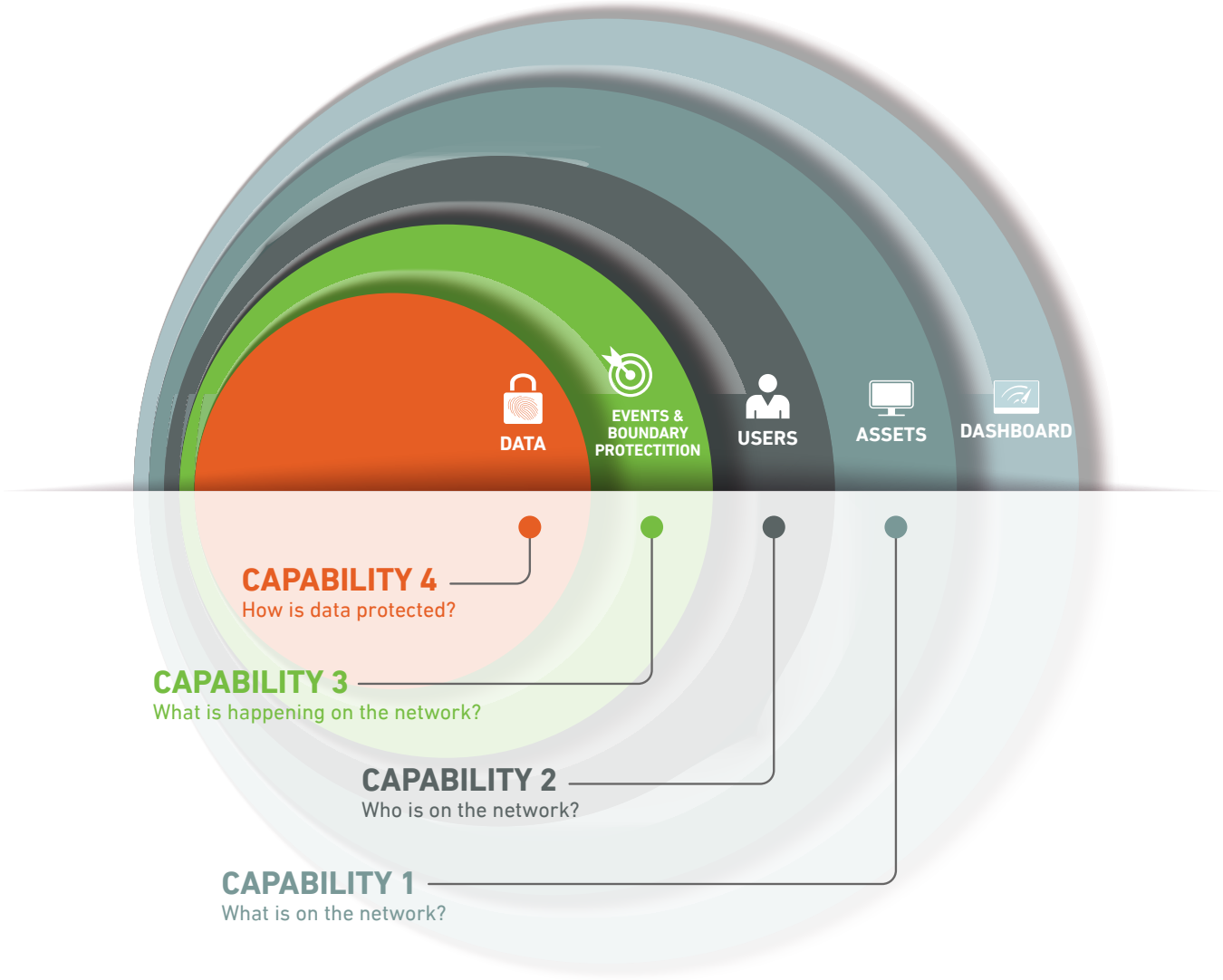


Figure 1: Capabilities of CDM

Managing "What is happening on the network?" builds on the CDM capabilities provided by "What is on the network?" and "Who is on the network?" These CDM capabilities include network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. These capabilities move beyond asset management to a more extensive and dynamic monitoring of security controls at the perimeter and on the endpoint. This includes preparing for and responding to behavior incidents, ensuring that software/system quality is integrated into the network/infrastructure, detecting internal actions and behaviors to determine who is doing what, and finally, mitigating security incidents to prevent propagation throughout the network/infrastructure.

Shifting from Prevention-Focused Defense to Fully Automated Threat Detection, Hunting, and Response at Cyber Speed

A suite of automated detection and response capabilities, like Fidelis Elevate™, fortifies enterprise defenses focused on defeating adversaries while evolving IT to support mission needs.

Today, most enterprise security investments are disproportionately weighted on "prevention" technologies.Multiple factors, however, render heavy reliance on prevention alone insufficient. A suite of automated detection and response capabilities, like Fidelis Elevate™, fortifies enterprise defenses focused on defeating adversaries while evolving IT to support mission needs. Digital transformation is the biggest business driver today, freeing employees to connect from anywhere – the office, home, coffee shops, or airport lounges – and teams in multiple time zones to collaborate as if sitting next to each other. It offers tremendous opportunities for businesses to create value and efficiencies, but it also creates new security risks. Embracing the cloud and mobile, not to mention Internet of Things (IoT) technologies, has resulted in an expanded attack surface that gives rise to multiple, multi-dimensional attack vectors.

Moreover, modern cyber-attacks are processes, not single events. Despite investments in preventive technologies, attackers routinely compromise seemingly secure organizations and steal financial assets, intellectual property, and sensitive data. To accomplish their mission, threat actors use a variety of exploitation methods and shift their approach to evade preventive defenses and remain undetectable. Traditional and non-traditional attack vectors include email phishing and business email compromise attacks, drive-by web downloads, file-less macro and script attacks, compromised IoT devices (printers, smart locks, smart lighting, and cameras to name a few), and the not-to-be-forgotten compromised identities and access credentials.

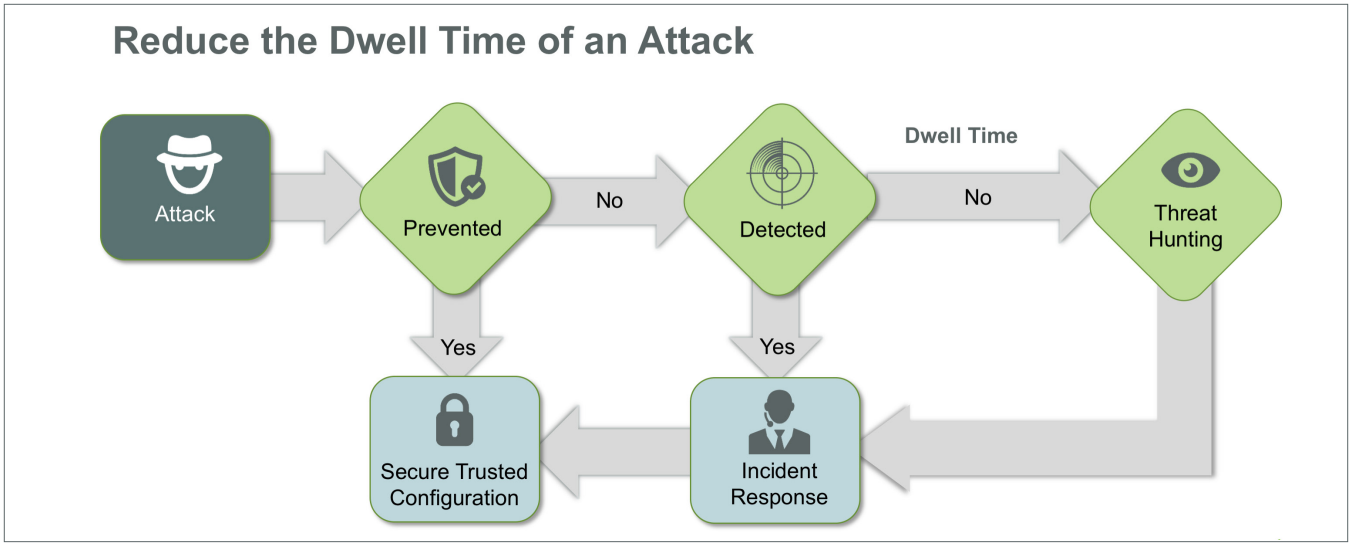
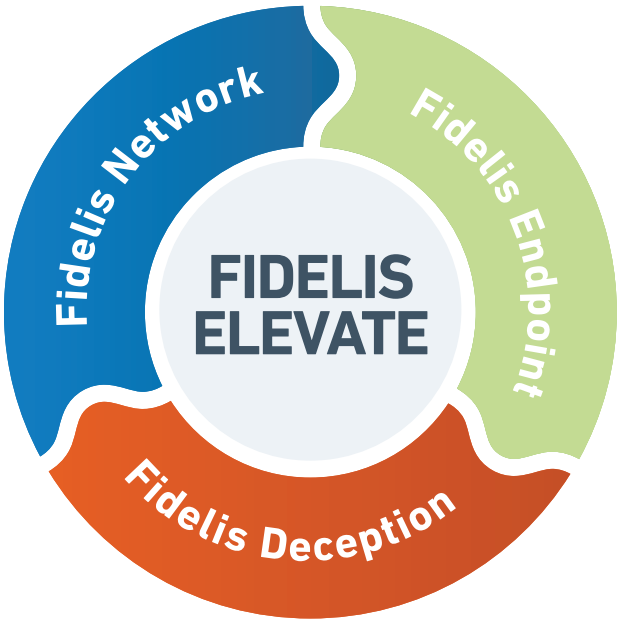


Figure 2: *When attacks evade preventive defenses, organizations must rely on advanced threat detection with automated remediation for high confidence policy violations; as well as threat hunting, to minimize dwell time and reduce the chance of being breached.*

How Fidelis Addresses CDM Requirements to Address Risk to the Network and Data

Fidelis Elevate™ provides a rich source of metadata for real-time and retrospective analysis by integrating network visibility with sensors for gateways, internal networks, email and web gateways, and cloud VMs (with network data loss prevention, deception, and endpoint detection and response) into one unified solution to deliver automated threat detection and response. It provides unmatched visibility and threat intelligence with content and context to help organizations quickly address cyberattacks across the entire threat lifecycle – from initial intrusion, to exploitation and lateral movement, to data theft – as well as hunting for unknown threats deep within networks and systems by hypotheses.

Detected threats are presented as conclusions determined by validation from network to endpoint, contextual enrichment, and correlated threat activity to enable analysts to take rapid, responsive, and often automated actions. By delivering comprehensive visibility, alert validation, and increased speed to respond, security teams focus on the most urgent threats and protect sensitive data rather than spending time investigating and triaging thousands of alerts.



Augment Your Security Infrastructure

A modern security platform of multiple sensors, endpoint detection and response, deception, and hunting, Fidelis Elevate™ delivers rich metadata not found in SIEM dashboards or firewall logs. Uniquely, Elevate™ delivers threat detection and defense in real-time, and retrospectively — up to 360 days!

Fidelis Elevate™

- **Collects metadata** using native data profiling for rich content and context not found in logs
- **Inclusive of email** (cloud or on-premises) and internal email sprays from attacks
- **Cloud VM visibility** of north-south and east-west communications for AWS VPCs or Azure VNETs
- **EDR lightweight agent** for Windows, macOS, and Linux systems with on and off grid defenses
- **Deception layers** for IT assets, enterprise IoT, cloud VMs, plus breadcrumbs to lure attacks
- **Threat intelligence** from Fidelis Insight, plus OpenIOC, YARA, Suricata rules, and 3rd parties
- **Highly scalable**, open APIs
- **Managed Detection Response (MDR) services** for 24/7 coverage leveraging the Elevate platform
- **Incident Response (IR)** proactive retainers and IR services for commercial and federal customers

Fidelis Elevate™ includes the following security products, which can be deployed and activated as a complete Elevate™ platform, or individually, based on an enterprise's needs:

Fidelis Network: Solves the 'my analysts are not experienced enough' problem by providing assisted and automated detection, investigation, and response. Detected advanced threats are presented as conclusions determined by automated validation, contextual enrichment, and correlated threat activity. Validated, enriched, and prioritized alerts dispel uncertainty, enabling analysts to take rapid responsive and automated actions rather than spending time to gather evidence from a variety of security systems and sources.

Fidelis Network automates threat detection and response while preventing data leakage across the network including sensors for gateways, internal traffic, cloud VMs, and email and web gateways. It bi-directionally scans all network traffic to reveal network and application protocols, files, and content; and automatically decodes and analyzes traffic to detect advanced threats and unauthorized data transfers. Patented Deep Session Inspection® (DSI) as well as Deep Packet Inspection (DPI) give unique visibility of deeply embedded content and context across all ports and protocols. It also captures and stores over 300 attributes of standard metadata, plus enhanced metadata, including custom tags, to provide rich information for automated and manual threat detection and threat hunting with up to 360 days of retrospective analysis.

Fidelis Endpoint: Provides endpoint detection and response (EDR) for visibility of all endpoint activity with automated script responses, plus the option of AV endpoint prevention (EPP) on and off networks in a single agent. Fidelis provides visibility into process actions, logged in users, registry writes, file system activity, and memory. It monitors endpoints in real-time and retrospectively, on and off the network, and records key events and processes, allowing security teams to see a timeline of suspected incidents. Fidelis Endpoint drives real-time detection using behavioral rules and indicators provided by Fidelis Insight threat intelligence. Security teams can also use third-party feeds and custom rules for threat detection, as well as hunt for threats directly on the endpoint, in both the file system and memory, using YARA and Open IOC indicators.

Fidelis Endpoint equips security teams to confidently detect, respond to, and resolve security incidents in a fraction of the time it takes using traditional approaches. Security analysts are also able to respond to endpoint activity faster by integrating with SIEMs, NGFWs, alerting tools, and more and by accessing a large library of pre-defined as well as custom response scripts. Fidelis Endpoint further aids security teams by automatically kicking off response workflows and scripts for automated remediation or deep analysis actions when suspicious activity is detected.

Fidelis Deception: Significantly reduces dwell time by providing a low-risk, low-friction internal alarm system to detect post-breach attacks and malicious insiders. Deception defenses provide a proactive opportunity to lure, detect, and defend early within post-breach compromise incidents with no risk to resources or data, or impact to users and operations. Fidelis Deception automatically discovers the environment and auto-generates decoys that have profiles, services, and activity matching the environment for active deception layers. It deploys decoys of key assets, services, and fake data, and then makes deception deterministic by setting up breadcrumbs on real systems likely to be compromised, thus leading attackers to decoys. High-fidelity alerts come from decoys, breadcrumbs, AD credentials, MITM, and poisoned data with network traffic analysis and telemetry data for investigations.

Fidelis Deception automatically adapts the deception environment to network changes as they occur to remain synchronized for assets, resources, and services. Deception also provides detection for legacy systems, shadow IT, and enterprise IoT devices where security agents are not possible.

Conclusion

Despite the prevalence of prevention techniques and tools at organizations' disposal, attacks are succeeding in growing numbers. The inability to see, detect, and respond to modern, complex, post-breach attacks hampers the effectiveness and efficiency of security operations teams to reduce dwell time. That's why CDM DEFEND evolved from a compliance program to provide risk-based and cost-effective cybersecurity to help federal organizations complete their missions of ensuring a secure infrastructure and ultimately sensitive data. It's also why Gartner has recommended organizations shift from a prevention-focused defense to one that prioritizes automated detection and response.

Curated security technology stacks designed for advanced threat detection, and automated detection and response, require a rich metadata model offering visibility across networks, cloud VMs, and endpoints to understand content and context of security events. Combining deep and broad visibility on both the network and endpoint with fast, comprehensive detection (with specific validation and mature response and prevention capabilities) empowers security operations teams to employ detection techniques such as network traffic analysis, endpoint forensics, and payload analysis, as well as combine techniques.

Today, by integrating Fidelis Elevate to address gaps in cybersecurity defenses, including advanced threat detection and response and preventing data loss from unwitting insiders, security teams may benefit from massive efficiency improvements and a more effective defense. Agencies will experience even greater benefits from agency Primes deploying Capabilities 3 and 4 RFS', as published by DHS https://www.dhs.gov/cdm.

Today, by **integrating Fidelis Elevate™ to address gaps in cybersecurity defenses**, including advanced threat detection and response and preventing data loss from unwitting insiders, security teams **may benefit from massive efficiency improvements and a more effective defense.**

Appendix:

The third required capability of CDM focuses on Managing "How is the network protected?" requires capabilities that limit, prevent, and/or allow the removal of unauthorized network connections/access. Such access would allow attackers to cross internal and external network boundaries and then pivot to gain deeper network access and/or capture network resident data at rest or in transit. This capability includes the use of devices such as firewalls that sit at a boundary and regulate the flow of network traffic. It also includes the use of encryption to protect traffic that must cross logical boundaries and addresses physical access systems that limit unauthorized user physical access to Federal Government facilities

Manage Network Filters and Boundary Controls (BOUND-F) network filters include devices such as firewalls and gateways that sit at the boundary between enclaves (such as a trusted internal network or subnet and an external or internal, less trusted network). The filters apply sets of rules and heuristics to regulate the flow of traffic between the trusted and less trusted sides of the boundary. The filters can also monitor tags related to information at any sensitivity level, such as PII, to ensure transmission (e.g., sharing) is restricted to authorized locations, and authorized recipients/third parties. The BOUND-F capability is further divided into the following categories:

- Content Filtering
- Packet Filtering
- Layer 2 Filtering
- Network Access Protection
- Encapsulation Filtering

BOUND-F reduces the probability that unauthorized traffic will pass through a network boundary. This includes the requirement that the boundary filtering policies are monitored, reviewed, and reauthorized per Agency policy. Network boundary security focuses on network weaknesses and vulnerabilities that can affect the network's ability to prevent the disclosure of confidential data, to determine when the integrity of the network is compromised, and to detect when malicious behavior impacts the network's availability. For the purposes of BOUND-F, network encryption points (e.g., virtual private networks) are considered network boundaries. Policies involving network encryption will have attributes associated with both BOUND-F and BOUND-E.

A BOUND-F device must be capable of filtering (actively or passively) network traffic at some level per policy established by the Agency.

The BOUND-F capability provides Agencies visibility into the risk associated with boundary filtering policies, to include the use of network encryption. BOUND-F traffic filtering policies can be applied at one or more layers of the network stack. Policies at layers 4 and above typically filter based on specific applications and application content (e.g., filtering email messages and messages containing spam, malware, sensitive and PII data). Those policies would contain content filtering records that describe the content that was filtered based on rules and policies.

Collecting data associated with the boundary filtering policy and the filtering policy required for network flow across a boundary provides measurable data elements for the creation of automated security checks. These security checks provide the basis for automating the monitoring, reporting, and prioritizing of boundary filtering policy deficiencies, including those specific to sensitive information within an Agency's cyber environment. Through CDM, deficiencies are displayed for review and action.

BOUND-F helps to ensure that the filtering policies for enclaves and systems are properly implemented to secure network traffic crossing boundaries. The capability also provides insight into duplicative and/or conflicting filtering policies.

BOUND-F Operational Requirements OR-1-1	Fidelis Response
Content filtering to filter traffic based on the application content of the traffic, including both the syntax and the semantic content.	Fidelis filters traffic based upon application traffic using patented Deep Session Inspection® technology at layers 2-7 in the OSI model and can apply analytics and intelligence to alert on anomalous activity and insider communication patterns across and throughout the enterprise. Fidelis supports pre-processing at the edge to improve fidelity of activity, reduce data volume, and find risks at cyber speed before they expand laterally throughout the enterprise.
Packet filtering to filter traffic based on IP packet header information and optionally on other IP datagram externals such as datagram length or frequency. Those policies describe the datagrams and/or sessions that are filtered based on rules and policies.	Fidelis Network incorporates additional technology to perform packet-level filtering when non-content-based rules and signatures are necessary. These policies can be combined with content-based policies to address risk, reduce dwell time and improve risk-based responses.
Layer 2 filtering to filter traffic based on layer 2 header information and optionally based on other layer 2 traffic externals, such as length or frequency. For example, policies at the data link layer (layer 2) typically filter based on layer 2 header information (e.g., filtering based on source and destination Ethernet address or virtual local area network number). Those policies describe the packets that are filtered based on rules and policies.	Fidelis implements Layer 2 criteria to enforce filtering policies which provides opportunity for cyber defenses to protect data more effectively.
Encapsulation filtering to filter traffic based on the encapsulation method and traffic characteristics (e.g., IP header attributes, application, and packet content). Those policies describe the network flows that are encapsulated and filtered based on rules and policies.	Fidelis can apply filtering intelligence to all attributes and packet content at and across the session level (e.g., look at certificates and/or cipher strengths). (Note: This capability directly enhances DHS CDM BOUND-E requirements.)
Network Access Protection to ensure that a device can only connect to an enterprise network if the device is explicitly authorized to connect, and is compliant with the stated hardware, software, configuration, and patching policies. Network Access Protection policies permit access to a network only if a device is approved to access that network, and is compliant with policies regarding hardware, software, configuration, and patching. Network Access Protection also contains functions that can force the patching or upgrading of a device, and then allow connection. Network Access Protection policies describe the device connection actions that are filtered based on rules and policies.	Fidelis can identify devices and/or systems that have been modified (e.g., unpatched, reconfigured, etc.) after the access decision has been made. This is performed using the decoded session metadata to determine if known vulnerabilities or unauthorized applications and/or implementations) are in use (e.g., Heartbleed). Fidelis can also inspect the session data to determine if devices are not communicating or transmitting content in a way that is appropriate to the devices.

BOUND-F Operational Requirements OR-1-1	Fidelis Response
Boundary filtering (a combination of multiple filtering capabilities) based on the policies and traffic characteristics. For example, boundary policies combine multiple filtering policies (e.g., IP layer and content filtering) into the overall policy for filtering traffic across a boundary (and may be implemented on one or more devices).	Fidelis is the only boundary filtering solution that can decode content at all levels of obfuscation, compression and embedding to ensure that data protection policies are evaluated on all cyber-enabled communications and enforced to reduce risk to agencies automatically at cyber speed.
BOUND-F Requirements FR-1-1	**Fidelis Response**
Content filtering that directly filters traffic based on the application and application content. Content filtering is described in terms of the applications (and the application characteristics) on which filtering can occur (e.g., URL filtering for HTTP content) and whether a proxy or translation is performed	Fidelis implements and supports IETF standards such as Internet Content Adaptation Protocol (ICAP) which extends the capability of proxy servers to thoroughly inspect HTTP traffic looking for malware transmission, data exfiltration, and other forms of malicious cyber activity. Fidelis Insight intelligence is operationalized on all network sensors to identify malicious activity occurring from the IP and session layers through to the application.
IP layer (packet) filtering that filters traffic based on the contents of IP layer protocols. Packet filtering is described in terms of what portions of the IP header are being used for the filtering decision and whether proxying or translation is being performed	Fidelis supports packet and session filtering. Further Fidelis supports X-Header extensions when proxying or address translation is being performed.
Layer 2 filtering that filters traffic at the data link layer, or layer 2, in the protocol stack. Layer 2 filtering is described in terms of which layer 2 protocol and what aspects of the protocol are being used for the filtering decision.	Fidelis can enforce content-based filters using Layer 2 criteria to enforce filtering policies.
Encapsulation filtering that shows how data from one network protocol is translated into another network protocol so that the data can continue to flow across the network. Encapsulation filtering is described in terms of the encapsulation method and the traffic characteristics (e.g., IP header attributes, application, and packet content).	Fidelis inspects IP packets and applies filtering intelligence to all attributes and packet content at and across the session level (e.g., look at certificates and/or cipher strengths). More, Fidelis rebuilds all communications at the session layer in real-time to understand the protocols and data transmitted regardless of individual packet structure and content to significantly improve risk assessment and evaluation on all cyber-enabled communications and data transfers.

BOUND-F Requirements FR-1-1	Fidelis Response
Network Access filtering that implements policy for permitting devices to connect to the network. Network Access filtering is described in terms of the types of devices the policy applies to, authentication method, and device characteristics used to make the connection decision.	Fidelis goes beyond the access decision to inspect session data between and/or among devise that have been granted access to determine if devices are not communicating or transmitting content in a way that is appropriate to the devices.
Boundary filtering of policies to determine what traffic can flow, and what traffic is blocked across a boundary. A boundary filtering policy is of the set of filtering policies for a boundary, including metadata about that policy.	Fidelis supports API integration to implement standardization of boundary policy, is the only boundary filtering solution that can extract, record, store and apply analytics to rich metadata obtained in the decoding of content at the deep session level of all content transmitted on the network.
BOUND-F Tool Functionalities	
Forward Web Proxies (or Secure Web Gateways)	Enhancing capability between client and gateway, or via ICAP.
Reverse Web Proxies	Enhancing capability between server and proxy, and/or via ICAP.
Web Application Firewalls	Enhancing capability between server and proxy, and/or via ICAP. Can monitor application behavior and content transfers.
Application Aware Firewalls (or Next Generation Firewalls)	Enhancing capability to improve detection in deeply obfuscated content; improves firewall performance by offloading intelligence, analytics to vastly improve detection accuracy.
Email Security Gateways (or Secure Email Gateways)	Fidelis Mail sensors are purpose-built to detect and combat sophisticated phishing and other APT level attacks in email (i.e., does not replace high noise SPAM filtering solutions.)
Database Firewalls	N/A
Network Access Protection or Control Devices	Fidelis Endpoint® is a key component of the Fidelis Elevate™ unified security platform that can augment NAC/NAP solutions and greatly improve enterprise device control. Fidelis uses its open API and industry standard data formats to signal risk management infrastructure to take action automatically and significantly reduce dwell time and time to respond once a threat is detected.

BOUND-F Tool Functionalities	
Intrusion Detection or Prevention Systems	Fidelis Elevate™ consists of two core technology capabilities, Endpoint and Network to provide enhanced IDS and IPS functionality beyond traditional point solution wares.

The BOUND-E capability provides visibility into risks associated with the use of cryptographic mechanisms employed on an organization's network. Agencies use cryptography to protect credentials, data at rest, and data in motion. BOUND-E provides the Agency indications of improper cryptographic behavior and/or of hardware/software misconfiguration. If cryptography is used, cryptography must be properly implemented and configured to provide the desired level of protection. BOUND-E collects policies from hardware devices, software products, and cryptographic implementation configuration settings to ensure that the right (e.g., FIPS 140-2 validated) implementations are being used and configured properly.

BOUND-E Requirements	
BOUND-E provides the Agency indications of improper cryptographic behavior and/or of hardware/software misconfiguration. If cryptography is used, cryptography must be properly implemented and configured to provide the desired level of protection. BOUND-E collects policies from hardware devices, software products, and cryptographic implementation configuration settings to ensure that the right implementations are being used and configured properly.	Fidelis monitors secure communications natively at the protocol decode level and creates metadata regarding the cryptography used in every secure protocol network session. This information is available in real-time and can be used to trigger filtering decisions that stop malicious and/or unauthorized communications.
BOUND-E Operational Requirements	
Shall afford protection to the confidentiality, integrity, and authenticity of data at rest, in transit, or in process via cryptography.	Fidelis monitors secure communications natively at the protocol decode level and creates metadata regarding the cryptography used in every secure protocol network session. This information is available in real-time and can be used to trigger filtering decisions that stop malicious and/or unauthorized communications. Fidelis Endpoint supports review and analysis of data-at-rest requirement
Shall collect data associated with the boundary encryption policy and the encryption policy required for a network flow across a boundary to provide measurable data elements for the creation of automated security checks.	Fidelis Network Collector is unique in its ability to monitor, decode, and record ALL session metadata to automate security inspection of encrypted data flows.

TOR Group B Additional Security Capability Requirements

C.4.3.3.1 Incident Response Automation	Fidelis Response
Incident response automation is the orchestration that is necessary to support the respond function with automated tools to the maximum extent possible.	The Fidelis Platform is the first fully-automated and complete compromise detection and response system designed to improve SOC operations. The Platform is Engineered to deliver comprehensive visibility, alert validation and increased response velocity across networks and endpoints with our unique real-time and historical compromise intelligence.
Incident response event notification Incident handling data collection Incident monitoring Incident reporting Incident response devices	Fidelis automates the functions listed in its Network- and Endpoint-based ADR Platform. Fidelis is fully open and provides opportunities for customers and solution providers to implement additional orchestration where needed in their operations.
The [IR Automation] focus is on being able to collect data, correlate that data, analyze the data, and provide notifications to the incident response staff.	Fidelis provides automated triangulation of intelligence, indicators, behaviors, signatures and heuristics eliminates the manual data investigation and collection required to enable incident response action.
Scanning for recognition of malicious content Automated malware analysis tools Aggregation of threat intelligence data	Fidelis implements multiple malware detection opportunities using content decoding and execution sandboxing. Fidelis provides threat intelligence and is able to consume third party and custom (i.e., customer-generated) threat intelligence to aggregate and process threat intelligence during real-time malware scanning and analysis processes in the Platform.
C.4.3.3.2 Ongoing Assessment	
Help achieve greater automation, accuracy and currency related to the implementation status of Agency NIST 800-53 controls (most current version) and Agency-defined parameters.	Fidelis monitors all sessions, traffic patterns and content transmissions in real-time. This data collection and information can be used to automate continuous validation of effectiveness of NIST 800-53 controls and provide real-time alerting when Agency-defined parameters are exceeded.

C.4.3.3.2 Ongoing Assessment	
Provide identification of new component weaknesses and vulnerabilities that represent unauthorized deviations to an Agency	Fidelis automatically sees attempts to exploit new component weaknesses.
C.4.3.3.6 Data-Based Perimeter Protection	
Provide capability for the identification and prevention of data exfiltration within the Agency.	For the past 2 decades, Fidelis has built unique intellectual value around content decoding and identification of data exfiltration methods. Going beyond packets, Fidelis uses real-time session building to perform patented Deep Session Inspection (and blocking) of content as it traverses and/or transits to leave the network.

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy.

By integrating bi-directional network traffic analysis across your cloud and internal networks with email, web, endpoint detection and response, and automated deception technology, the Fidelis Elevate™ platform captures rich metadata and content that enables real-time and retrospective analysis, giving security teams the platform to effectively hunt for threats in their environment. Fidelis solutions are delivered as standalone products, an integrated platform, or as a 24x7 Managed Detection and Response service that augments existing security operations and incident response capabilities. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.