‹Thales eSecurity›

Addressing continuous diagnostics and mitigation requirements

How Thales eSecurity's Vormetric Data Security Platform enables effective compliance

White Paper

Contents

CDM Program Executive Summary 3

CDM Phases - Strategic View........ 4

Thales eSecurity's Vormetric product line 5

Thales's Vormetric data security platform alignment to CDM functional tool areas 8

CDM Program Executive Summary

Cyber-attacks on federal government networks are growing more sophisticated, frequent, and dynamic. It is paramount that the government protects networks, systems, and information – including citizen and mission data – from unauthorized access or disruption while providing essential services. Congress established the Continuous Diagnostics and Mitigation program (CDM) to provide a strong, consistent cyber defense designed to protect more than 70 civilian agency networks.

CDM will provide these agencies with tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

Congress has tasked both the Department of Homeland Security and GSA to establish and manage the CDM initiative. CDM is a multi-year, multi-billion-dollar program being deployed in several phases. The program initially defined 15 tool functional areas (TFAs) to address the reporting and protection goals. In addition, the program defined 11 service task areas for installation and support.

Due to the size and scope of CDM, it is being rolled out in phases, each covering multiple TFAs and service task areas. The phases are focused on specific technologies that together build the solution. The tools are grouped together within each phase, based on security control grouping:

Phase 1: 'What is on the network'

Phase 2: 'Who is on the network'

Phase 3: 'What is happening on the network' Phase 3 includes three "BOUND" sections, which correspond to Blanket Purchase Agreement (BPA) Tool Functional Area (TFA) 5 – Manage Network Access Controls. This includes "BOUND-E: Monitor and Manage Encryption Mechanisms Controls"

Phase 4: 'Protecting the data on the network'

This paper offers a detailed look at many of the CDM requirements that pertain to securing sensitive government data, and reveals how the Vormetric Data Security Platform can help agencies achieve or exceed many of the functional tool area requirements within CDM.

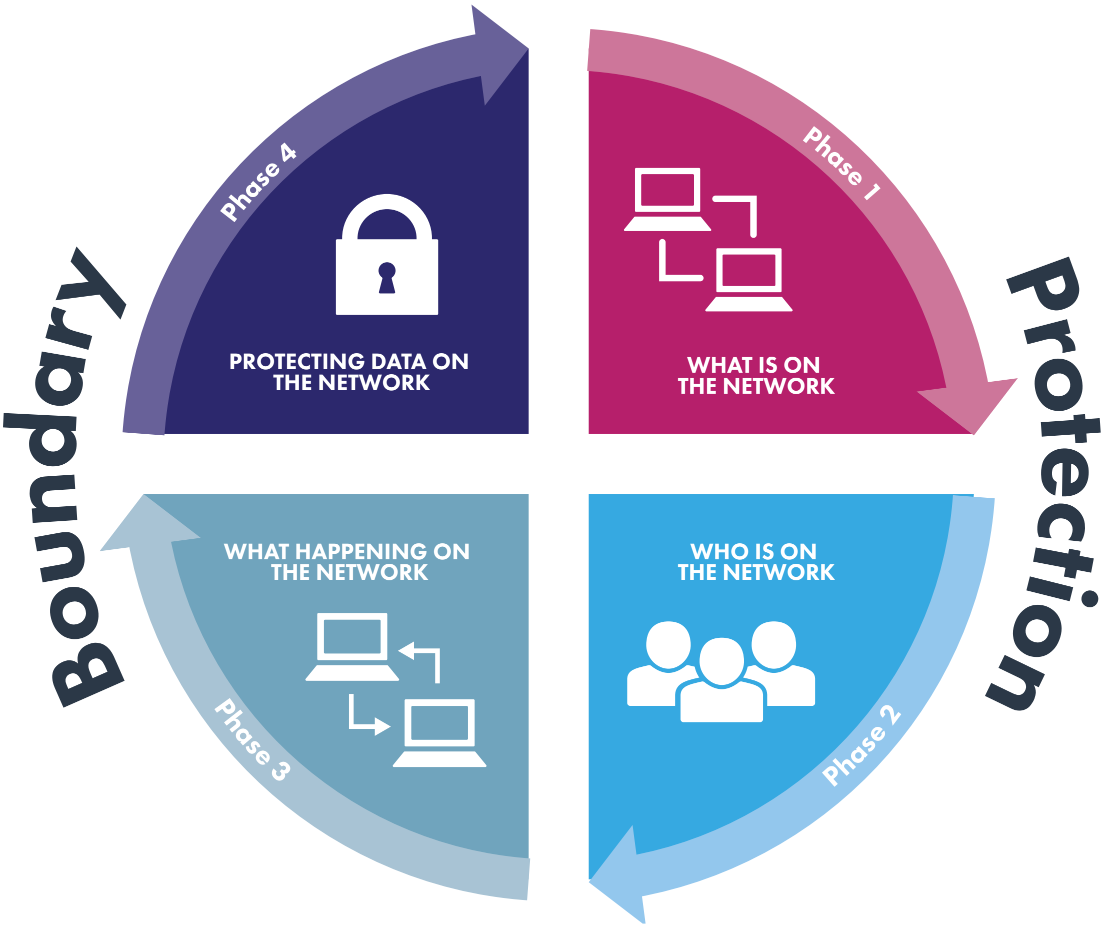
> Congress established the Continuous Diagnostics and Mitigation program (CDM) to provide a strong, consistent cyber defense designed to protect more than 70 civilian agency networks.

CDM Phases - Strategic View

The first CDM phases were awarded to a set of blanket purchase agreement (BPA) holders acting as continuous monitoring as a service providers (CMaaS). A CMaaS provider would be responsible for procuring the tools, installing and operating them within the agencies defined by the award. GSA and DHS are changing to a new model in order to streamline the process and create more options for the Government. Future awards will use GSA CDM special item numbers (SIN) for competitive procurement of the tools.

Thales eSecurity's Vormetric Data Security Platform is already providing data protection with AES256 level encryption and access controls of log files for some phase 1, task order 2 agencies. This incumbency in the program ensures the Vormetric products will be included into the approved product list as GSA moves to the CDM SIN. Therefore, the technologies described below are available already for purchase for future phases of CDM.

Figure 1. CDM Phases



Thales eSecurity's Vormetric product line

The risks to data are known, but what to do to ensure data remains secure is not so clear cut. Establishing perimeter security at the endpoint and network is important, but once an adversary breaches the network, these defenses are no longer effective. Monitoring and analytics tools also enhance an agency's cyber security, but are only equipped to provide information about attacks after they have occurred. Ultimately, these approaches do not prevent data from being exfiltrated once an individual has gained access to the network.

The CDM program was implemented to help guide security efforts in government agencies. The CDM program offers a holistic approach to security, addressing the network, cyber awareness, and the actual target itself—the data that is used to run government. CDM Phase 3 includes "BOUND" -"Boundary Protection and Event Management for Managing the Security Lifecycle" – which addresses a number of approaches for securing sensitive data, including the use of data-at-rest encryption and key management.

The Vormetric Data Security Platform offers comprehensive solutions that help government agencies address these requirements.

With the Vormetric Data Security Platform, agencies can establish strong safeguards around sensitive data and minimize critical risks associated with leaving it in an unprotected state. The Vormetric solutions offer the controls required to ensure only authorized users can gain access to sensitive data at rest. These solutions can secure unstructured data, including documents, spreadsheets, images, web pages and more. These solutions can also secure structured data, such as fields in databases and applications that contain personally identifiable information, protected health information, mission data and other sensitive records.

With the Vormetric Data Security Platform, agencies can take a comprehensive, organization-wide approach to protecting data in support of CDM. This platform offersa number of capabilities that either comply with or exceed CDM requirements:

- **Encryption and key management.** The Vormetric Data Security Platform offers strong, centrally managed file and volume encryption that is transparent to processes, applications and users. The platform also delivers capabilities for efficient, centralized key management.
- **Access controls.** The Vormetric platform delivers advanced role-based access controls that integrate with the existing security structure for efficient deployments.
- **Multi-tenant support.** The Vormetric platform provides secure multi-tenancy support in the data center, cloud environments, and autonomous servers, whether they're running on Windows, Linux or UNIX. The Vormetric solution enables each distinct data owner to have unique administrative functions on the centralized management appliance. This allows data that would otherwise have to be "air gapped" on separate storage devices to be cryptographically separated on shared infrastructure.
- **Privileged user controls.** With the Vormetric platform, security teams can establish granular controls that blind data at rest, even to individuals with privileged user account permissions, such as system administrators with root access and service account users. By leveraging these capabilities, agencies can establish strong defenses against insider threats.
- **Security intelligence.** The Vormetric Data Security Platform delivers logs that capture attempts to access protected data, providing high-value security intelligence. These logs can be used in conjunction with a security information and event management (SIEM) solution for compliance reporting.

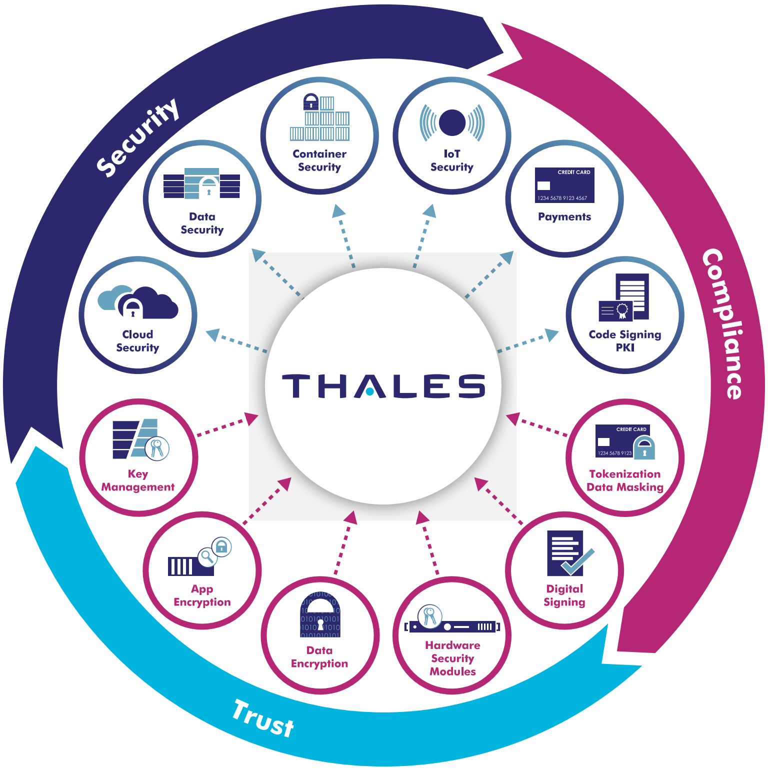
> With the Vormetric Data Security Platform, agencies can take a comprehensive, organization-wide approach to protecting data in support of CDM.

The Vormetric Data Security Platform provides strong controls while enabling fast, efficient implementation. Today, agency data can reside in a dynamic mix of environments, including in the data center, autonomous servers, and the cloud. By leveraging the Vormetric solutions, organizations can ensure that data owners retain control over access to encrypted data, no matter where it ends up residing. With the Vormetric Data Security Platform, agencies can ensure administrative controls are logically separated, so data stays secure against both internal and external threats.

As articulated above, the Vormetric Data Security Platform enables security teams to employ a strategic approach to securing what adversaries are after: the data. By leveraging the Vormetric solutions, agencies can quickly realize a number of advantages:

- **Simplicity.** These solutions can easily be integrated with existing directory structures, including Active Directory and Lightweight Directory Access Protocol (LDAP), to ensure that users' access permissions are tied to their roles.
- **Low overhead.** When the Vormetric Data Security Platform is deployed, minimal changes to storage or network bandwidth are introduced. Vormetric solutions typically consume less than five percent of a system's computing resources, and they streamline ongoing administration.
- **Efficient integration.** Thales e-Security customers can take advantage of easy integration with existing SIEM platforms and other security tools, so they leverage their existing investments and more effectively secure data at rest.
- **Data protection.** The Vormetric Data Security Platform helps protect critical data from unauthorized access, offering safeguards against cyber criminals leveraging compromised credentials, contractors, and privileged users with administrative and service accounts.
- **Compliance.** The Vormetric platform offers the strong encryption and key management controls that support a range of standards, including NIST 800-53, Common Criteria, and FIPS 140-2 levels 1-3.

Figure 2. Thales Platform



Thales's Vormetric data security platform alignment to CDM functional tool areas

REQUIREMENT	TOOL FUNCTIONAL AREA	VORMETRIC PLATFORM FEATURES
Encryption shall meet or exceed the applicable federal guidance for the data as categorized. This guidance is currently contained in NIST 800-53a Rev 4 or current, and FIPS 140-2 or current.	TRUST BEHAVE CRED PRIV TFA 6,7, 8, 9	The Vormetric Data Security Platform is compliant/certified in NIST 800-53 rev 4, Common Criteria, FIPS 140-2 (levels 1-3), ATOs in DoD, and Commercial Solutions for Classified (NSA). The Vormetric Data Security Manager (DSM) is compliant as a FIPS 140-2 Level 2, FIPS 140-2 Level 3 hardware appliance and as a virtual appliance. No difference in performance regardless of configuration.
Shall encrypt data with methods that meet or exceeds the encryption requirements for the data categorization of the system while at rest.	TRUST BEHAVE CRED PRIV TFA 6,7, 8, 9	Vormetric Transparent Encryption (VTE) is compliant with the FIPS-197 AES encryption standards, such as Advanced Encryption Standard (AES) for data encryption and elliptic curve cryptography (ECC) for key exchange. The Vormetric Application Encryption library provides support for AES Encryption with 256 bit keys.

REQUIREMENT	TOOL FUNCTIONAL AREA	VORMETRIC PLATFORM FEATURES
Shall provide access control for system functions that support centralized and decentralized.	TRUST BEHAVE CRED PRIV TFA 6,7, 8, 9	The Vormetric Data Security Platform can enforce granular access policies, enabling protection of data from misuse by privileged users and APT attacks. Granular policies can be applied by user (including administrators with root privileges), process, file type, time of day, and other parameters. Enforcement options can be used to control not only whether users can access data, but which system functions are available to a particular user.
The overall purpose of the Manage Security-Related Behavior (BEHAVE) capability is to document that authorized users exhibit appropriate security-related behaviors.	BEHAVE TFA7	The Vormetric Data Security Platform produces detailed security event logs that are easy to integrate with Security Information and Event Management (SIEM) systems like Splunk, ArcSight, QRadar, and others that support syslog to produce compliance and security reports. These security logs and reports produce a non-reputable trail of permitted and denied access attempts from users and processes, providing insight into file access activities. Logging occurs at the file system level, removing the opportunity of stealthy access to sensitive data. This security information can inform of unusual or improper data access and accelerate the detection of insider and outsider threats, including the presence of APTs, and demonstrate when authorized users are performing inappropriate security-related behaviors.

REQUIREMENT	TOOL FUNCTIONAL AREA	VORMETRIC PLATFORM FEATURES
		The Vormetric Data Security Platform helps to provide protection across heterogeneous environments such as file systems, databases, big data implementations, VMs, cloud environments, and SAN/NAS devices. The detailed information Vormetric provides in the form of RFC5424, CEF, and LEEF logs represents essential data that can be analyzed using any SIEM solution's security intelligence capabilities to identify usage patterns that may represent threats.
Accounts that are no longer needed by a user to perform their function should be disabled or deleted since they can be targeted by attackers to gain unauthorized access.	PRIV TFA 9	Reports showing a list of "stale" accounts can be easily generated from data collected from the Vormetric Data Security Platform.
Only authorized users with authorized accounts of the correct type are accessing systems.	PRIV TFA 9	The Vormetric DSM security administrator creates policies to protect data. Policies employ two mechanisms to do this: • Data encryption. Specify that data written to a particular directory (called a "guardpoint") is encrypted, and that data will only be decrypted by properly authenticated host users. All other access attempts outside of policy are denied, logged, and sent to the SIEM.

REQUIREMENT	TOOL FUNCTIONAL AREA	VORMETRIC PLATFORM FEATURES
		• Access control. Specify which protected host users can access which files and directories in a guardpoint. Policies can furthermore specify which executables, and actions can be used and at what times. Policies govern file access and encryption in Vormetric Transparent Encryption protected directories—ensuring that only authorized accounts have access to protected data. Policies direct the logging of events based on a configurable set of criteria. These logs detail all access attempts to protected directories (successful and unsuccessfully), showing a rich set of non-reputable data including date/time, userID, process used, directory accessed, and whether or not an encryption key was invoked.
All employees have only the privileges necessary to do their jobs.	PRIV TFA 9	Vormetric policies can be used to ensure that various personnel only have the minimum amount of privileges necessary to perform their duties.
All account types employ appropriate expiration and disable policies.	PRIV TFA 9	The Vormetric polices include a "time" attribute in which one can specify: • Week Day From—To is a range of weekdays days during which access is denied or permitted. • Data From—To is a range of dates during which access is denied or permitted. • Start Time—End Time is a range of times during which access is denied or permitted.

REQUIREMENT	TOOL FUNCTIONAL AREA	VORMETRIC PLATFORM FEATURES
4.1.2 BOUND-E 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 - TFA 5	The Vormetric Data Security Platform provides protection for data-at-rest and data-in-motion. Provides data-at-rest encryption which allows access controls without changes to applications and business processes. The platform also provides a discovery process to ensure proper access is being enforced. The Vormetric Transparent Encryption allows data written to a protected volume/folder to be encrypted at rest. Thales eSecurity provides security solutions around data in transit. Vormetric Application Encryption and Tokenization address security concerns around data in transit.
4.1.2 Encryption as a Cryptography Technique: Encryption is a cryptographic technique used to protect against the improper disclosure of data. It ensures the confidentiality of information not be disclosed to unauthorized individuals. This protection applies to: • Data at rest protection□includes encryption of individual files, as well as encryption of entire volumes/ disks. Components of data at rest encryption include both the encryption software itself and the encrypted data. • Data in transit, that is, data transmitted over physical/ logical data communication links.	BOUND-E TFA 5	Vormetric encryption agents run at the file system level or volume level on a server. Agents perform encryption, decryption, access control, and logging. Agents employ logic and fine-grained policies to evaluate attempts to access protected data, and then either grant or deny access. All activities are logged.

REQUIREMENT	TOOL FUNCTIONAL AREA	VORMETRIC PLATFORM FEATURES
4.1.2 Digital Signature Design: Digital Signature Design is used to ensure the integrity of data sent between users, to ensure the authenticity that the message is from a specific user.	BOUND-E TFA 5	File signing checks the authenticity and integrity of executables and applications before they are allowed to access data protected with VTE. When file signing is initiated in the DSM Management Console, the VTE Agent calculates the cryptographic signatures of the executables that are eligible to access protected data. Files are individually signed as part of a set and that set is configured in a policy that defines the processes to allow.
4.1.2 Cryptographic Algorithm Element: NIST approved cryptographic algorithms for use in US Government systems are described in: • Cryptographic Algorithm Validation Program (CAVP). • NSA's Suite B cryptographic Program.	BOUND-E TFA 5	File signing checks the authenticity and integrity of executables and applications before they are allowed to access data protected with VTE. When file signing is initiated in the DSM Management Console, the VTE Agent calculates the cryptographic signatures of the executables that are eligible to access protected data. Files are individually signed as part of a set and that set is configured in a policy that defines the processes to allow.
4.1.2 Hash Element: Hash is a one-way cryptographic technique used to ensure the integrity of data, that is, to detect the alteration of the data at rest or in transit. The hash technique maps an input field of arbitrary size to a unique output field of a fixed size. The hash value of a given data can be used to determine if the original data was modified. Hash can be applied to either plain text data or cipher text data. Hash technique ensure the integrity of data at rest and in transit, and under certain designs be used to support data confidentiality (e.g., password hash).	BOUND-E TFA 5	Vormetric supports SHA-2 (Secure Hashing 256 bit), as well as SHA-384.

REQUIREMENT	TOOL FUNCTIONAL AREA	VORMETRIC PLATFORM FEATURES
4.1.2 Key Management Element: Key management is the entire process for generating, distributing using and destroying cryptographic key material. Keys are used to support the confidentiality, integrity, authenticity and secure communication between multiple users. The application of keys including digital certificates, protect against the disclosure of information, identify when data is altered and to verify the authenticity of the data source.	BOUND-E TFA 5	Vormetric Key Management centrally manages all Vormetric product keys as well as third party key material, including SSL certificates. The product leverages the Vormetric DSM to provide an optional high availability, standards-based, FIPS 140-2 validated key management platform that can secure keys for Microsoft SQL Server TDE, Oracle TDE, and KMIP-compliant devices. The platform can manage X.509 certificates, symmetric keys, and asymmetric keys. By consolidating key management, this product fosters consistent policy implementation across multiple systems and it reduces training and maintenance costs. Vormetric Key Management provides powerful and flexible administration capabilities, offering a Web interface, command-line interface, and API. The solution enables administrators to do bulk imports of digital certificates and cryptographic keys. Vormetric Key Management features extensive audit capabilities that can be used to report on all activities relating to key usage, including key generation, rotation, destruction, import, expiration and export. The solution can provide alerts that help administrators stay apprised of certificate and key expiration so they can more proactively manage their environments. Vormetric Key Management delivers all of the significant advantages outlined above, including high availability through system redundancy and failover.

REQUIREMENT	TOOL FUNCTIONAL AREA	VORMETRIC PLATFORM FEATURES
4.2 MNGEVT Shall have a contingency plan to restore and reconstitute full information system functionalities and the capability to apply new or additional security safeguards to prevent future compromise.	TFA 10	TFA 10 The Vormetric DSM component can operate in a clustered environment in active or standby mode, and can be added to a program's COOP/DR strategy.
4.2 MNGEVT Shall provide ongoing assessment data consolidation and assessment frequencies to deliver an effective continuous collection, analysis, and impact assessment of security policies in order to maximize automation and reduce human interaction.	TFA 11	The Vormetric Data Security Platform processes incidents at the individual component level (host system, web GUI, Vormetric DSM). These incidents and audit events are in an open syslog format that can be sent to an information system's monitoring/reporting tool, including 3rd party SIEM solutions. Log file formats can be tailored to match a program's security policy for user and application behavior.
4.3 OMI Shall collect and report information related to the implementation of methods to maintain system and information integrity and enforce system and information integrity policies.	TFA 14	Vormetric Transparent Encryption provides full audit data at the Vormetric Data Security Manager and at host agents in an open format and can integrate with a program or agency's audit reduction tool or SIEM solution.

THALES

www.thalesesecurity.com

About Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

Follow us on:

Americas – Thales eSecurity Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com