How Virtru Supports the Department of Defense Zero Trust Strategy

Virtru Data Security Platform

Table of Contents

Department of Defense Zero Trust Strategy

The Department of Defense (DoD) Zero Trust Strategy and Roadmap is a comprehensive approach to cybersecurity that assumes no user, network, or system is inherently trusted. The strategy envisions a DoD Information Enterprise secured by a fully implemented, Department-wide Zero Trust cybersecurity framework that will reduce the attack surface, enable risk management and effective data-sharing in partnership environments, and quickly contain and remediate adversary activities.

To ensure a consistent approach, the DoD implements Zero Trust under a framework of seven Zero Trust pillars and their supporting elements. These pillars form the foundational framework for the DoD Zero Trust Security Model and Architecture:

- User
- Device
- Applications and workloads
- Data
- Network
- Automation and orchestration
- Visibility and analytics

The Zero Trust security model relies on dynamic policies encompassing authentication assurance, ongoing verification of user and endpoint identities, and applications/services and their respective assets. Each pillar's capabilities must synergize to safeguard this model's central data pillar.

The data pillar is crucial in this strategy, focusing on securing the most valuable asset: the data itself. Virtru's data-centric security platform and applications align most directly with this pillar, providing robust protection for sensitive information throughout its lifecycle.

How Virtru Supports the Department of Defense Zero Trust Strategy

This document provides guidance and recommendations on how the Virtru Data Security Platform can help achieve key elements of the DoD Zero Trust Strategy. While the Virtru Data Security Platform aligns to helping meet the DoD Zero Trust Strategy's data pillar requirements, it also enhances security across multiple pillars, including User, Device, Network, Automation and Orchestration, and Visibility and Analytics.

Data Pillar

This section includes Virtru guidance and recommendations for DoD Zero Trust activities in the data pillar.

4.2 DoD Enterprise Data Governance

Virtru facilitates interoperability across Allied and NATO partners through the ZTDF metadata standard. This enables DoD to establish flexible, enterprise-wide data standards, meeting current requirements while adapting to future needs in a Zero-Trust environment.

The Virtru Data Security Platform — built upon the open-source data-centric security platform OpenTDF — supports ODNI's ACES/ACRE encoding specifications, ensuring standardized, cryptographically secure classification.

This approach aligns with DoD's Zero Trust Strategy while enhancing data protection.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 4.2.1 Define Data Tagging Standards The DoD Enterprise works with organizations to establish data tagging and classification standards based on industry best practices. Classifications are agreed upon and implemented in processes. Tags are identified as manual and automated for future activities. Outcomes: • Enterprise data classification and tagging standards are developed • Organizations align to enterprise standards and begin implementation	Virtru Data Security Platform The Virtru Data Security Platform addresses DoD's data tagging needs by supporting ACES/ACRE and the Zero Trust Data Format (ZTDF) data encoding specifications. Developed collaboratively with NATO and industry leaders, ZTDF cryptographically binds classifications to data, ensuring true Zero Trust security. This approach standardizes data tagging and provides a verifiable mechanism for validating classifications.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 4.2.2 Interoperability Standards The DoD Enterprise collaborating with the organizations develops interoperability standards integrating mandatory Data Rights Management (DRM) and Protection solutions with necessary technologies to enable ZT target functionality. Outcome: • Formal standards are in place by the enterprise for the appropriate data standards	Virtru Data Security Platform The Virtru Data Security Platform supports ZTDF and TDF metadata standards, ensuring interoperability across Allied and NATO partners. Based on ACES/ACRE specifications, the Virtru Data Security Platform allows for the incremental implementation of standards and non-disruptive normalization of data classification. This flexibility enables DoD to integrate externally-defined standards and facilitate data sharing across diverse systems.

4.3 Data Labeling and Tagging

The Virtru Data Security Platform offers DoD-compliant data tagging and classification capabilities and supports integration with third-party data classification and tagging tools. Virtru partners with industry leaders and working groups to ensure its platform supports current and future DoD requirements within the Zero Trust framework.

Virtru's platform integrates with DoD's manual data tagging initiative, interpreting manually marked tags and offering a basic attribute policy. It allows for manual and automatic tagging and is extensible to accommodate evolving DoD needs in the Zero Trust environment.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 4.3.1 Implement Data Tagging & Classification Tools DoD organizations utilize the enterprise standard and requirements to implement data tagging and classification solution(s). Organizations ensure that future ML and AI integrations are supported by solutions through DoD enterprise requirements. Outcomes: • A requirement of Data classification and tagging tools must include integration and/or support of Machine Learning (ML) • Data classification and tagging tools are implemented at org and enterprise levels	Virtru Data Security Platform The Virtru Data Security Platform offers comprehensive data tagging and classification tools that are compliant with the latest Source Classification Guide. The platform interfaces with Forta (formerly called Titus and BoldenJames) and includes Virtru's classification tool for extensive coverage, including Windows Desktop. This modular design allows for easy expansion to accommodate industry-specific needs and enhanced AI/ML tagging, meeting DoD's current and future classification requirements in the Zero Trust framework.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 4.3.2 Manual Data Tagging Pt1 Using the DoD enterprise data tagging and classification policy and standards, manual tagging starts using basic data level attributes to meet ZT target functionality. Outcome: • Manual data tagging begins at the enterprise level with basic attributes	Virtru Data Security Platform The Virtru Data Security Platform works with leading classification vendors and can interpret manually marked data tags in documents. It includes a boilerplate policy featuring three basic attributes, aligning with the DoD's enterprise-level tagging requirements. These attributes can be applied manually or through automatic tagging, offering flexibility in implementation. Moreover, Virtru's platform allows for easy creation of additional attributes or attribute values, ensuring scalability as the DoD's tagging needs evolve beyond basic functionality in the Zero Trust framework.

.

4.4 Data Monitoring and Sensing

The Virtru Data Security Platform enhances DoD's DLP and DRM enforcement capabilities with flexible deployment options and standardized logging across enforcement points. It supports file activity monitoring for critical data classifications and integrates with SIEMs like Splunk for comprehensive threat analysis and incident response.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 4.4.1 DLP Enforcement Point Logging and Analysis DoD Organizations identify data loss prevention (DLP) enforcement points such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD organizations ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage. Outcomes: • Enforcement points are identified • Standardized Logging schema is enforced at the enterprise and org levels	Virtru Data Security Platform Virtru emits logs in standard formats compatible with SIEM/SOAR systems, adhering to standardized logging schemas at enterprise and organizational levels. The platform's consistent audit schema enhances traceability. Flexible deployment options allow enforcement points to be placed strategically at email gateways, web applications, endpoints, and backend services, providing comprehensive coverage for protection, detection, and response use cases in the Zero Trust framework.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 4.4.2 DRM Enforcement Point Logging and Analysis DoD Organizations identify data rights management (DRM) enforcement points such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD organizations ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage. Outcomes: • Enforcement points are identified • Standardized Logging schema is enforced at the enterprise and org levels	Virtru Data Security Platform The Virtru Data Security Platform helps in DRM enforcement and logging. Virtru's consistent audit schema across products ensures standardized logging at enterprise and organizational levels, aligning with DoD's cybersecurity incident response standards. The Data Security Platform's flexible deployment allows strategic placement of enforcement points at email gateways, web applications, endpoints, and backend services.
(Target) 4.4.3 File Activity Monitoring Pt1 DoD Organizations utilize File Monitoring tools to monitor the most critical data classification levels in applications, services, and repositories. Analytics from monitoring are fed into the SIEM with basic data attributes to accomplish ZT Target functionality. Outcomes: • Data and files of critical classification are actively being monitored • Basic Integration is in place with monitoring system such as the SIEM	Virtru Data Security Platform The Virtru Data Security Platform logs audit events for all data policy updates, ensuring comprehensive tracking of sensitive information across applications, services, and repositories. Audit events can be shipped to enterprise SIEM solutions such as Splunk. This integration allows audit events from Virtru's monitoring tools to feed directly into the SIEM, allowing admins to monitor data and file actions in real time. This results in greater visibility and analysis of critical data activities, enhancing overall security posture and incident response capabilities.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 4.4.4 File Activity Monitoring Pt2 DoD Organizations utilize File Monitoring tools to monitor all regulatory protected data (e.g., CUI, PII, PHI, etc.) in applications, services, and repositories. Extended integration is used to send data to appropriate inter/intra-pillar solutions such as Data Loss Prevention, Data Rights Management/Protection and User & Entity Behavior Analytics. Outcomes: • Data and files of all regulated classifications are actively being monitored • Extended integrations are in place as appropriate to further manage risk	Virtru for Windows Files Services The Virtru Data Security Platform extends its file monitoring capabilities through our Virtru for Windows File Services, establishing policy enforcement for collaborative files within a Windows file system. This component actively monitors collaborative file types, ensuring policy enforcement for any regulatory protected data types, including CUI, PII, and PHI. Virtru for Windows File Services provides crucial oversight for regulated classifications, supporting the DoD's data protection requirements.

4.5 Data Encryption and Rights Management

Virtru's Data Security Platform offers file-level DRM tools with granular control, surpassing volume-level solutions. It provides automatic encryption key management compliance with FIPS standards and HSM support. The platform enables customized protection across all in-scope data repositories, meeting DoD's diverse security needs.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 4.5.1 Implement DRM and Protection Tools Pt1 DoD Organizations procure and implement DRM and Protection solution(s) as needed following the DoD Enterprise standard and requirements. Newly implemented DRM and protection solution(s) are implemented with high risk data repositories using ZTA target level protections. Outcome: • DRM and protection tools are enabled for high-risk data repositories with basic protections	Virtru Data Security Platform The Virtru Data Security Platform natively supports file-level DRM tools, offering greater granular control. This approach allows for the precise implementation of DRM and protection measures for high-risk data repositories, aligning with DoD Enterprise standards and Zero Trust Architecture (ZTA) target level protections. The platform's flexible policy configuration enables tighter security and DRM controls for higher-risk data repositories, ensuring that the most sensitive information receives appropriate protection.
(Target) 4.5.2 Implement DRM and Protection Tools Pt2 DRM and protection coverage is expanded to cover all in scope data repositories. Encryption keys are automatically managed to meet best practices (e.g., FIPS). Extended data protection attributes are implemented based on the environment classification. Outcome: • DRM and protection tools are enabled for all possible repositories	Virtru Data Security Platform The Virtru Data Security Platform natively supports file-level DRM tools, providing granular control across all in-scope data repositories. Virtru's approach ensures precise protection. The platform's Key Access Service, which is included with the platform, automatically manages encryption keys adhering to best practices. Virtru Data Security Platform optionally supports BYO Hardware Security Module (HSM) for enhanced key security. The system's configurability allows for customized key storage and interaction, including key splitting, meeting diverse security needs across different environment classifications, thus enabling robust DRM and protection for all possible repositories.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 4.5.3 DRM Enforcement via Data Tags and Analytics Pt1 Data rights management (DRM) and protection solutions are integrated with basic data tags defined by the DoD Enterprise standard. Initial data repositories are monitored and have protect and response actions enabled. Data at rest is encrypted in repositories. Outcomes: • Data Tags are integrated with DRM and monitored repositories are expanded • Based on data tags, data is encrypted at rest	Virtru Data Security Platform The Virtru Data Security Platform integrates with data tags defined by DoD Enterprise standards, working with common tagging tools like Forta (formerly Titus, and BoldenJames) and Microsoft. It uniquely normalizes tagging schemas across Allies and Partners, aligning with US and NATO standards. By leveraging data tags, the platform's out-of-the-box policy enforcement capabilities result in the automatic encryption of highly sensitive data at rest in repositories. This capability enables effective DRM enforcement based on data tags, expanding monitored repositories and ensuring encrypted protection for sensitive information.

4.6 Data Loss Prevention (DLP)

Virtru's Data Security Platform optionally includes Policy Enforcement Points (PEPs) for email, file-based collaboration applications, and more.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 4.6.1 Implement Enforcement Points Data loss prevention (DLP) solution is deployed to the in-scope enforcement points. DLP solution is set to "monitor-only" and/or "learning" mode limiting impact. DLP solution results are analyzed, and policy is fine tuned to manage risk to an acceptable level. Outcome: • Identified enforcement points have DLP tool deployed and set to monitor mode with standardized logging	Virtru Data Security Platform The Virtru Data Security Platform supports diverse Policy Enforcement Points (PEPs) beyond Microsoft products, including unified communications, web based viewing and streaming data and offers structured data sources and an SDK for extending policy enforcement into other bespoke mission applications. The platform's standardized logging across various enforcement points enables comprehensive analysis of DLP results, facilitating risk management to acceptable levels. Virtru's flexible deployment options support the gradual implementation of DLP solutions across identified enforcement points.
(Target) 4.6.2 DLP Enforcement via Data Tags and Analytics Pt1 The data loss prevention (DLP) solution is updated from monitor only mode to prevention mode. Basic data tags are utilized for the DLP solution and logging schema is integrated. Outcome: • Enforcement Points to set to prevent mode integrating the logging schema and manual tags environment classification.	Virtru Data Security Platform The Virtru Data Security Platform supports diverse Policy Enforcement Points (PEPs) beyond Microsoft products, including unified communications, web based viewing and streaming data and offers structured data sources and an SDK for extending policy enforcement into other bespoke mission applications.

4.7 Data Access Control

Virtru integrates with major Identity Providers and supports Attribute-Based Access Control, enabling fine-tuned, dynamic access management. While not directly handling PAM, Virtru's approach complements existing solutions, supporting DoD's transition to dynamic privileged access and enhancing overall security posture.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 4.7.1 Integrate DAAS Access w/ SDS Policy Pt1 Utilizing the DoD enterprise SDS policy, organizational DAAS policy is developed with intended integration in mind. SDS implementation guide is developed by DoD organizations due to environment-specific nature. Outcomes: • Attribute based fine-grained DAAS policy is developed with/ enterprise and org-level support • The SDS Integration plan is developed to support DAAS policy	Virtru Data Security Platform The Virtru Data Security Platform supports Attribute-Based Access Control (ABAC), custom security groups, and dynamic security groups, mirroring and extending Microsoft capabilities. Following ACES/ACRE standards, Virtru enables the encoding of subjects and resources through flexible mapping, allowing DoD organizations to define integrations as needed. This approach facilitates the development of attribute-based, fine-grained Data as a Service (DAAS) policies with enterprise and organizational-level support. The platform's adaptability supports the creation of environment-specific Secure Data Sharing (SDS) implementation guides, enabling integration of DAAS policies within the DoD enterprise SDS framework.
(Target) 4.7.4 Integrate Solution(s) and Policy with Enterprise IDP Pt1 DoD Organizations develop an integration plan using the SDS policy and technology/functionality with the enterprise Identity Provider (IdP) solution. Outcome: • Integration plan between SDS and the authoritative Identity Provider is developed to support existing DAAS access	Virtru Data Security Platform The Virtru Data Security Platform integrates with a variety of Identity Providers (IdPs), including Microsoft ActiveDirectory, PingFederate, and Okta. Following ACES/ACRE standards, Virtru encodes subjects and resources through flexible mapping, enabling integration with multiple IdPs under a unified overarching policy. This capability supports the development of comprehensive integration plans between Secure Data Sharing (SDS) and authoritative IdPs, aligning with DoD's requirement for supporting existing Data as a Service (DAAS) access.

Data Centric Security Beyond the Data Pillar

While Virtru's Data Security Platform excels in addressing the Data Pillar of the DoD's Zero Trust Strategy, its impact extends far beyond, enhancing security across multiple pillars.

By integrating with Identity Providers, Virtru strengthens the User Pillar, enabling robust authentication and authorization. The platform's support for diverse Policy Enforcement Points bolsters the Device and Network Pillars, ensuring comprehensive protection at every access point.

Virtru's granular access controls and real-time telemetry contribute to the Visibility and Analytics Pillar, providing crucial insights for threat detection and response.

Furthermore, its flexible policy management capabilities reinforce the Automation and Orchestration Pillar, streamlining security operations.

This multi-pillar approach allows the DoD to implement a holistic Zero Trust architecture, significantly enhancing overall cybersecurity posture and operational efficiency across the entire defense ecosystem.

User Pillar

Virtru's platform integrates with various IAM solutions, supporting multi-factor authentication and PKI for critical services. It enables attribute-based access control and dynamic privilege management, complementing DoD's user inventory and access control initiatives.

1.1 User Inventory

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 1.1.1 Inventory User DoD Organizations establish and update a user inventory manually if needed, preparing for automated approach in later stages. Accounts both centrally managed by an IdP/ICAM and locally on systems will be identified and inventoried. Privileged accounts will be identified for future audit and both standard and privileged user accounts local to applications and systems will be identified for future migration and/or decommission. Outcomes: • Identified Managed Regular Users • Identified Managed Privileged Users • Identified applications using their own user account management for non-administrative and administrative accounts	Virtru Data Security Platform The Virtru Data Security Platform inventories users across its platform and Policy Enforcement Points (PEPs), similar to other vendors. However, Virtru uniquely relies on identity providers (IdPs) to supply user inventory and leverage existing infrastructure. This approach supports DoD organizations in establishing and updating user inventories, including managed regular users, privileged users, and application-specific accounts. By integrating with IdPs, Virtru facilitates the identification of centrally managed and local accounts.

1.2 Conditional User Access

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 1.2.1 Implement App Based Permissions per Enterprise The DoD enterprise working with the Organizations establishes a basic set of user attributes for authentication and authorization. These are integrated with the "Enterprise Identity Life-Cycle Management Pt1" activity process for a complete enterprise standard. The enterprise Identity, Credential, and Access Management (ICAM) solution is enabled for self-service functionality for adding/updating attributes within the solution. Remaining Privileged Access Management (PAM) activities are fully migrated to PAM solution. Outcomes: • Enterprise roles/attributes needed for user authorization to application functions and/or data have been registered with enterprise ICAM • DoD Enterprise ICAM has self-service attribute/role registration service that enables application owners to add attributes or use existing enterprise attributes • Privileged activities are fully migrated to PAM	Virtru Data Security Platform The Virtru Data Security Platform leverages IdP-provided values like Roles and Groups as attributes for real-time evaluation, enabling dynamic access control decisions and enforcement. While Virtru doesn't directly implement Just-In-Time (JIT) or Just-Enough-Administration (JEA) methods, its dynamic attribute-based system complements these approaches. The platform can adapt access to application functions and data based on appropriate enterprise attributes, supporting the DoD's transition to dynamic privileged access for high-risk user accounts and enhancing overall security posture.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target 1.2.2) Rule Based Dynamic Access Pt1 DoD Organizations utilize the rules from the "Periodic Authentication" activity to build basic rules enabling and disabling privileges dynamically. High-risk user accounts utilize the PAM solution to move to dynamic privileged access using Just-In-Time access and Just Enough-Administration methods. Outcomes: • Access to application's/service's functions and/or data are limited to users with appropriate enterprise attributes • All possible applications use JIT/JEA permissions for administrative users	Virtru Data Security Platform The Virtru Data Security Platform integrates with a variety of Identity Providers (IdPs), including Microsoft ActiveDirectory, PingFederate, and Okta. Following ACES/ACRE standards, Virtru encodes subjects and resources through flexible mapping, enabling integration with multiple IdPs under a unified overarching policy. This capability supports the development of comprehensive integration plans between Secure Data Sharing (SDS) and authoritative IdPs, aligning with DoD's requirement for supporting existing Data as a Service (DAAS) access.

1.3 Multi-Factor Authentication

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target 1.3.1) Organizational MFA/IDP DoD Organizations procure and implement a centralized Identity Provider (IdP) solution and Multi-Factor (MFA) solution. The IdP and MFA solution may be combined in a single application or separated as needed assuming automated integration is supported by both solutions. Both IdP and MFA support integration with the Enterprise PKI capability and enable key pairs to be signed by the trusted root certificate authorities. Mission/Task-Critical applications and services are utilizing the IdP and MFA solution for management of users and groups. Outcomes: • Component is using IdP with MFA for critical applications/services • Components have implemented an Identity Provider (IdP) that enables DoD PKI multifactor authentication • Organizational Standardized PKI for critical services	Virtru Data Security Platform The Virtru Data Security Platform integrates with various Identity and Access Management (ICAM/IdAM) solutions, such as Okta, Ping, and Keycloak, supporting multi-factor authentication. Virtru's compatibility with these solutions enables PKI multifactor authentication for critical applications and services. Additionally, Virtru offers BYO Hardware Security Module (HSM) support as an extra authentication factor, enhancing security. While not directly providing IdP or MFA, Virtru's integration capabilities support DoD organizations in implementing standardized PKI for critical services and effectively managing users and groups.

Network Pillar

Virtru supports granular data access control using ABAC and the ODNI ACES framework, aligning with DoD's network access rules. It protects data in transit and at rest, addressing coalition information sharing and cross-system boundary protection needs.

5.1 Data Flow Mapping

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 5.1.1 Define Granular Control Access Rules & Policies Pt1 The DoD Enterprise working with the Organizations creates granular network access rules and policies. Associated Concept of Operations (ConOps) are developed in alignment with access policies and ensure future supportability. Once agreed upon, DoD Organizations will implement these access policies into existing network technologies (e.g., Next Generation Firewalls, Intrusion Prevention Systems, etc.) to improve initial risk levels. Outcomes: • Provide Technical Standards • Develop Concept of Operations • Identify Communities of Interest	Virtru Data Security Platform The Virtru Data Security Platform supports Granular Data Access and Policy using ABAC and the ODNI ACES framework. It natively uses government open data standards like Trusted Data Format (TDF) and Zero Trust Data Format (ZTDF). Virtru enables granular access control for all file types and sizes, including files beyond 1GB, and controls access to information within files. This flexibility supports the development of comprehensive ConOps and helps identify Communities of Interest. While not directly implementing network technologies, Virtru's granular control enhances overall data security, complementing existing network access policies.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 5.1.2 Define Granular Control Access Rules & Policies Pt2 DoD Organizations utilize data tagging and classification standards to develop data filters for API access to the SDN Infrastructure. API Decision Points are formalized within the SDN architecture and implemented with non-mission/task critical applications and services. Outcome: • Define Data Tagging Filters for API Infrastructure	Virtru Data Security Platform The Virtru Data Security Platform utilizes ABAC and the ODNI ACES framework for Granular Data Access and Policy, supporting DoD's data tagging and classification standards. It natively employs government open data standards like TDF and ZTDF, enabling comprehensive data filters for API access. Virtru provides granular access control for all file types and sizes, including those exceeding 1GB. This capability facilitates the development of robust data filters for SDN Infrastructure API access. While not directly implementing SDN architecture, Virtru's granular control and data tagging support enhance the overall security posture, complementing API Decision Points for non-mission/task critical applications and services.

5.4 Micro Segmentation

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 5.4.4 Protect Data In Transit Based on the data flow mappings and monitoring, policies are enabled by DoD Organizations to mandate protection of data in transit. Common use cases such as Coalition Information Sharing, Sharing Across System Boundaries and Protection across Architectural Components are included in protection policies. Outcomes: • Protect Data In Transit During Coalition Information Sharing • Protect Data in Transit Across System High Boundaries • Integrate Data In Transit Protection Across Architecture Components	Virtru Data Security Platform The Virtru Data Security Platform handles data protection both in transit and at rest through tagging and encryption, aligning with DoD's mandate for data transit protection. Virtru uses the Trusted Data Format (TDF) to encrypt data which allows it to travel with the data, no matter where it goes. Virtru offers flexible deployment options for Data Security Platform, enabling protection across system boundaries. Virtru's architecture uses mappings and policy enforcement points as boundaries to implement protection policies for data transiting within and externally to system boundaries. This approach addresses common use cases like Coalition Information Sharing and protection across architectural components.

Automation and Orchestration Pillar

Virtru offers tools for defining and managing access control policies, supporting DoD's efforts to catalog and update cybersecurity policies. It can implement organization-specific and enterprise-wide security profiles, facilitating a phased approach to DAAS access control.

6.1 Policy Decision Point (PDP) and Policy Orchestration

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 6.1.2 Organization Access Profile DoD Organizations develop basic access profiles for mission/task and non-mission/task DAAS access using the data from the User, Data, Network, and Device pillars. The DoD Enterprise works with the Organizations to develop an Enterprise Security Profile using the existing Organizational security profiles to create a common access approach to DAAS. A phased approach can be used in organizations to limit risk to mission/task critical DAAS access once the security profile(s) are created. Outcomes: • Organization scoped profile(s) are created to determine access to DAAS using capabilities from User, Data, Network, and Device pillars • Initial enterprise profile access standard is developed for access to DAAS • When possible the organization profile(s) utilizes enterprise available services in the User, Data, Network, and Device pillars	Virtru Data Security Platform The Virtru Data Security Platform incorporates organizational access profiles as inputs, supporting DoD's development of basic access profiles for mission/task and non-mission/task Data as a Service (DAAS) access. Virtru's out-of-the-box policy enforcement capabilities comply with these profile requirements, integrating capabilities from the User, Data, Network, and Device pillars. While not directly creating the profiles, Virtru's system can implement and enforce the resulting access rules, supporting organization-specific and enterprise-wide security profiles. This flexibility allows for a phased approach to applying security profiles, helping limit risk to mission/task-critical DAAS access and facilitating enterprise-available services across pillars.

Visibility and Analytics Pillar

Virtru provides comprehensive event telemetry for all data interactions, integrating with SIEM/SOAR solutions for in-depth analysis. This supports DoD's threat alerting, asset identification, and Cyber Threat Intelligence program, enhancing security monitoring and threat response capabilities.

7.1 Log All Traffic

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 7.1.3 Log Analysis Common user and device activities are identified and prioritized based on risk. Activities deemed the most simplistic and risky have analytics created using different data sources such as logs. Trends and patterns are developed based on the analytics collected to look at activities over longer periods of time. Outcomes: • Develop analytics per activity • Identify activities to analyze	Virtru Data Security Platform The Virtru Data Security Platform offers comprehensive event telemetry for all data interactions through an API, supporting DoD's log analysis requirements. This capability enables integration with any SIEM/SOAR solution for in-depth inspection and analysis. While Virtru doesn't directly identify and prioritize user and device activities, the platform's detailed logging of data interactions provides crucial input for such analysis. The platform's telemetry can contribute to developing analytics for high-risk activities, helping identify trends and patterns over time.

7.2 Security Information and Event Management

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 7.2.1 Threat Alerting Pt1 DoD Organizations utilize existing Security Information and Event Management (SIEM) solutions to develop basic rules and alerts for common threat events (malware, phishing, etc.) Alerts and/or rule firings are fed into the parallel "Asset ID & Alert Correlation" activity to bring automation of responses. Outcome: • Rules developed for threat correlation	Virtru Data Security Platform The Virtru Data Security Platform provides detailed event telemetry logs via API, supporting DoD's threat alerting requirements. While not directly developing threat correlation rules, Virtru's comprehensive logging integrates with existing Security Information and Event Management (SIEM) solutions. This integration enables organizations to establish basic rules and alerts for common threats like malware and phishing. Virtru's real-time data interaction logs offer valuable input for immediate and post-mortem threat analysis. This capability enhances DoD organizations' ability to create effective threat correlation rules and supports the automation of responses through integration with the "Asset ID & Alert Correlation" activity.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 7.2.2 Threat Alerting Pt2 DoD Organizations expand threat alerting in the Security Information and Event Management (SIEM) solution to include Cyber Threat Intelligence (CTI) data feeds. Deviation and anomaly rules are developed in the SIEM to detect advanced threats. Outcome: • Develop analytics to detect deviations	Virtru Data Security Platform The Virtru Data Security Platform offers detailed event telemetry logs via API, supporting DoD's expanded threat alerting needs. While not directly incorporating Cyber Threat Intelligence (CTI) feeds or developing deviation rules, Virtru's comprehensive logging integrates with Security Information and Event Management (SIEM) solutions. This integration enables organizations to leverage Virtru's data to develop advanced threat detection analytics. The platform's real-time and historical data interaction logs provide valuable input for identifying deviations and anomalies, enhancing the SIEM's capability to detect sophisticated threats. Virtru's detailed telemetry supports immediate and retrospective threat analysis, contributing to more robust and effective threat alerting systems.
(Target) 7.2.4 Asset ID and Alert Correlation DoD Organizations develop basic correlation rules using asset and alert data. Response to common threat events (e.g., malware, phishing, etc.) are automated within the Security Information and Event Management (SIEM) solution. Outcome: • Rules developed for asset ID based responses	Virtru Data Security Platform The Virtru Data Security Platform delivers detailed event telemetry logs via API, supporting DoD's asset identification and alert correlation needs. While not directly developing correlation rules or automating responses, Virtru's comprehensive logging integrates with Security Information and Event Management (SIEM) solutions. This integration allows organizations to leverage Virtru's data to create basic correlation rules using asset and alert information. The platform's real-time and historical data interaction logs provide valuable input for identifying and responding to common threats like malware and phishing. Virtru's detailed telemetry enhances SIEM capabilities, supporting the development of asset ID-based response rules and contributing to more effective automated threat responses.

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 7.2.5 User/Device Baselines DoD Organizations develop user and device baseline approaches based on DoD enterprise standards for the appropriate pillar. Attributes utilized in baselining are pulled from the enterprise wide standards developed in cross pillar activities. Outcome: • Identify user and device baselines	Virtru Data Security Platform The Virtru Data Security Platform offers detailed event telemetry logs via API, supporting DoD's user and device baseline development efforts. While not directly creating baselines, Virtru's comprehensive logging integrates with Security Information and Event Management (SIEM) solutions and other analytics tools. This integration allows organizations to leverage Virtru's data to develop user and device baselines based on DoD enterprise standards. The platform's real-time and historical data interaction logs provide valuable attributes and behavior patterns that can help identify normal user and device activities. Virtru's detailed telemetry enhances the ability to establish and monitor baselines across relevant pillars, supporting more effective security monitoring and anomaly detection.

7.5 Threat intelligence integration

DoD Activity Description and Outcome	Virtru Guidance and Recommendations
(Target) 7.5.1 Cyber Threat Intelligence Program Pt1 The DoD Enterprise works with the Organizations to develop and Cyber Threat Intelligence (CTI) program policy, standard and process. Organizations utilize this documentation to develop organizational CTI teams with key mission/task stakeholders. CTI Teams integrate common feeds of data with the Security Information and Event Management (SIEM) for improved alerting and response. Integrations with Device and Network enforcement points (e.g., Firewalls, Endpoint Security Suites, etc.) are created to conduct basic monitoring of CTI driven data. Outcomes: • Cyber Threat Intelligence team is in place with critical stakeholders • Public and Baseline CTI feeds are being utilized by SIEM for alerting • Basic integration points exist with Device and Network enforcement points (e.g., NGAV, NGFW, NG-IPS)	Virtru Data Security Platform Virtru enhances the DoD's Cyber Threat Intelligence (CTI) program by providing robust event telemetry logs through its API. This integration allows for the incorporation of Virtru's data into Security Information and Event Management (SIEM) systems, bolstering real-time alerting and response capabilities. By leveraging Virtru's detailed logs, CTI teams can conduct more comprehensive threat analyses, both in real-time and post-incident. This data integration strengthens the DoD's ability to monitor and respond to cyber threats, aligning with the goal of improved alerting and basic monitoring of CTI-driven data across various enforcement points. Virtru's contribution thus supports the DoD in achieving a more robust and responsive cyber threat intelligence posture.

TO LEARN MORE ABOUT HOW VIRTRU CAN EQUIP YOUR AGENCY TO IMPLEMENT DATA CENTRIC, ZERO TRUST SECURITY:

CONTACT federal@virtru.com

OR VISIT virtru.com/data-security-platform