

SENTRIS®

Sensitive Data
Security - Empowering
Your Zero Trust
Journey

Sentris®: Empowering Zero Trust Data Security

In today's security landscape, **data is your most valuable asset**. The Department of Defense (DoD)'s **Zero Trust Reference Architecture (ZTA)** emphasizes a **data-first approach**, making the **Data Pillar** a cornerstone of comprehensive security.

Sentris®, a ManTech-developed Microsoft Windows-based platform for implementing attribute-based security classification services within network environments that require a high degree of data security and confidentiality, is designed to align with the 7 goals of the **DoD Zero Trust Data Pillar**.

4.1 Data Catalog and Risk Assessment

Sentris® utilizes customizable **usage rule sets** to define and govern application behavior, ensuring your organization's unique security needs are met.

4.2 Data Governance

Centralized management via the **Sentris® Administration Tool** applies and enforces security policies across the entire environment, maintaining compliance and security integrity.

4.3 Data Labeling & Tagging

Sentris® is a data labeling and tagging solution, providing users with easy-to-use tools to label and secure content using common applications such as **Windows, Office, SharePoint, Skype for Business, and Outlook**.

Capable of tagging almost any filetype, Sentris® ensures consistent classification and security throughout your environment.

4.4 Data Monitoring & Sensing

All Sentris®-related activity is logged to the **Windows Event Viewer** and **Sentris® logs**. Sentris® can be configured for verbose logging or to log information only, and users can view the log files in the Sentris® Log Viewer.

3rd party logging tools like **Splunk** can be configured to pull Sentris® logs, enabling real-time monitoring and threat analysis.

DoD Zero Trust Capabilities DATA PILLAR

4.1 Data Catalog Risk Assessment

4.2 DoD Enterprise Data Governance

4.3 Data Labeling and Tagging

4.4 Data Monitoring and Sensing

4.5 Data Encryption & Rights Mgmt

4.6 Data Loss Prevention (DLP)

4.7 Data Access Control



4.5 Data Encryption & Rights Management

Sentris® v5 supports encryption for virtually any filetype, ensuring that sensitive data remains secure from unauthorized access.

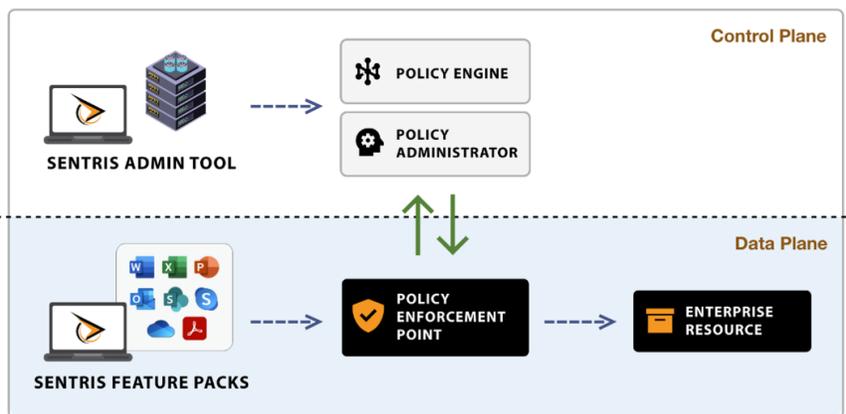
4.6 Data Loss Prevention

Leveraging the Sentris® API Documentation, organizations can create custom solutions, enhancing their ability to prevent data loss and protect critical assets.

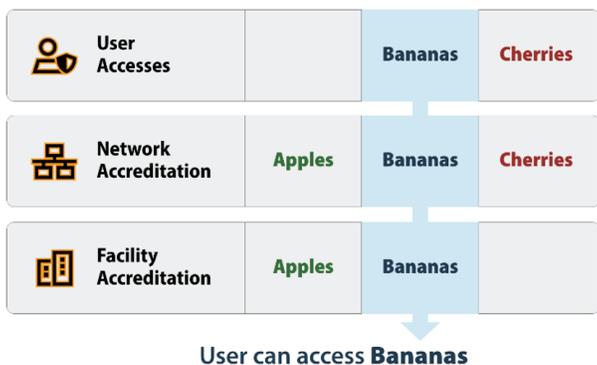
4.7 Data Access Control

For a comprehensive ZT approach, integrated protection of data is essential. Using the Sentris® ADP Synchronization Service, organizations can sync personnel accesses from an external authoritative data source with Sentris®.

Sentris® Roles within the Data and Control Planes



Sentris® Security Paradigm



Sentris® is unique in its capability to control access to data based on three criteria. **1. who is accessing the data; 2. from where; and 3. using what system?** This innovative approach to criteria-based access control allows agencies to manage access information in complex, high-security environments where traditional access control mechanisms can be ineffective and cumbersome.

Why Choose Sentris®?

Integrating with your existing infrastructure, Sentris® serves as a turn-key solution to support marking and access governance for classified environments. With its **Zero Trust-aligned capabilities**, Sentris® is ideal for enterprises seeking to:

- Quickly implement advanced data protection policies.
- Securely manage sensitive information.
- Confidently meet the demands of high-security and compliance-driven environments.

In business more than 55 years, ManTech excels in cognitive cyber, AI, data collection & analytics, enterprise IT, systems engineering and software application development solutions that support national and homeland security.

LEARN MORE - www.mantech.com/commercial-services

Chris Hassett, Sr. Executive Director, Commercial Software & Services | commercial.services@mantech.com



ManTech