Solution Brief

Enhancing Federal Data Security with VAST Data through Zero Trust and NextLabs SkyDRM



Introduction

The federal landscape demands the highest level of security when it comes to data protection. With evolving threats and the need for inter-agency collaboration, a robust data-centric security strategy is essential. VAST Data, combined with Zero Trust principles and NextLabs SkyDRM, offers a comprehensive solution to ensure that sensitive government data remains secure throughout its lifecycle.

Key Benefits for Federal Organizations

Zero Trust Approach

VAST Data's integration with Zero Trust principles ensures that data access is never assumed safe and is continuously verified. No entity is trusted by default, reducing the risk of insider and external threats.

Persistent NextLabs SkyDRM Protection

NextLabs SkyDRM provides continuous protection that remains with the data, even as it moves outside federal boundaries or between agencies. Sensitive information is encrypted, and access is controlled at a granular level.

Regulatory Compliance

Federal agencies must meet stringent regulatory requirements (FISMA, NIST, etc.). VAST Data's solution, in tandem with NextLabs SkyDRM, helps achieve compliance through end-to-end encryption, audit trails, and access control measures.

How VAST Data and NextLabs SkyDRM Address Zero Trust in Government

Data Access Control:

VAST Data applies **attribute-based access control** (ABAC) to manage who can access sensitive data, in line with **NIST SP 800-162**. This aligns with Zero Trust by ensuring access is granted only after verifying users, devices, and contextual attributes.

Encryption at Rest and In Transit:

By encrypting data at rest and in transit with **FIPS 140-3 Level 1** validated crypto, VAST ensures that sensitive federal data remains secure, whether stored in on-premises systems or cloud platforms. This complies with **NIST SP 800-57** (Cryptographic Key Management) and **NIST SP 800-175** (Guide to Cryptographic Mechanisms).

Continuous Monitoring and Logging:

VAST provides continuous real-time monitoring of data access and usage. Integration with Security Information and Event Management (SIEM) tools allows security teams to track suspicious activities, as required by **NIST SP 800-137** (Information Security Continuous Monitoring for Federal Information Systems). This is crucial for federal compliance.

Fine-Grained Data Protection with SkyDRM:

NextLabs SkyDRM ensures that sensitive information is protected even when shared across agencies or with contractors. Data usage rights—such as viewing, editing, or sharing—are dynamically enforced and can be revoked if necessary, in accordance with **NIST SP 800-88** (Guidelines for Media Sanitization).



Use Case: Securing Inter-Agency Collaboration

When federal agencies collaborate, sharing sensitive information is necessary, yet challenging due to security concerns. VAST Data and NextLabs SkyDRM enable secure collaboration through the following:

- **Granular Permissions:** VAST Data provides Zero Trust architecture and granular access control, ensuring that only authorized personnel can access specific data. This minimizes the risk of leaks and unauthorized access. NextLabs SkyDRM enhances this with dynamic authorization technology, allowing for precise control over file permissions.
- **Secure External Sharing:** NextLabs SkyDRM ensures that even when data is shared externally, usage is tightly controlled and auditable. The solution applies digital rights to shared files, controlling exact usage permissions such as read, edit, print, and download rights. These permissions persist regardless of the file's location, ensuring protection even outside the corporate network.
- **Federated Identity Management:** User identities are managed and authenticated by each agency's identity management system and do not need to be known ahead of time. Each agency maintains their own user identity, attributes related to the user, and changes in user status. Identity and attributes of a user are dynamically used by NextLabs SkyDRM to determine access at the time of access.
- **Seamless Integration:** VAST Data's platform seamlessly integrates with existing infrastructures using standard protocols like NFS, SMB, and S3, allowing for easy adoption without significant changes. When combined with NextLabs SkyDRM's digital rights management, this integration extends to secure file sharing and collaboration, ensuring that data remains protected even when accessed externally. The platform's support for cloud-native environments and global namespace eliminates data silos, enhancing collaboration across multiple locations while maintaining stringent access controls and audit trails.



Ensuring Compliance and Control for Federal Data

The integration of Zero Trust and NextLabs SkyDRM with VAST Data ensures that federal agencies can protect their most sensitive data while adhering to government mandates:

- **FISMA Compliance:** VAST's solutions support the Federal Information Security Management Act (FISMA) by providing robust data protection and continuous monitoring capabilities.
- **NIST SP 800-53** (Security and Privacy Controls for Federal Information Systems and Organizations): VAST's offerings, in conjunction with NextLabs SkyDRM, align with NIST SP 800-53, ensuring compliance with access control, encryption, and incident response requirements.
- **NIST SP 800-207** (Zero Trust Architecture): VAST Data and NextLabs SkyDRM support NIST's Zero Trust guidelines by providing strong identity management, continuous verification, and dynamic access controls to federal data systems.

Securing the Future

VAST Data, combined with Zero Trust security and NextLabs SkyDRM, provides federal agencies with the tools necessary to protect sensitive information in a rapidly evolving digital landscape. With enhanced data protection, continuous monitoring, and strict access controls, federal agencies can confidently collaborate and safeguard critical data while adhering to NIST standards and federal regulations.

About NextLabs

NextLabs®, Inc. provides zero trust data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based zero trust policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit www.nextlabs.com

About VAST Data

VAST Data is the data platform company built for the AI era. As the new standard for enterprise AI infrastructure, organizations trust the VAST Data Platform to serve their most data-intensive computing needs. VAST Data empowers enterprises to unlock the full potential of their data by providing AI infrastructure that is simple, scalable, and architected from the ground up to power deep learning and GPU-accelerated data centers and clouds. Launched in 2019, VAST Data is the fastest growing data infrastructure company in history. For more information, please visit and follow VAST Data on X (formerly Twitter) and LinkedIn.

Scan Here learn more

©2024 VAST Data, Inc. All rights reserved. All trademarks belong to their respective owners.

11/2024