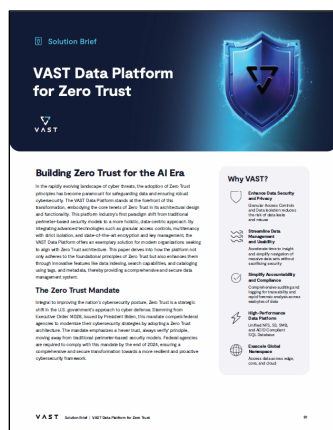# VAST Data Platform for Zero Trust

Thank you for downloading this Vast Data Solution Brief.

To learn how to take the next step toward acquiring VAST Data's solutions, please check out the following resources and information:

For additional resources:
carah.io/vastdataresources

For upcoming events:
carah.io/vastdataevents

For additional VAST Data solutions:
carah.io/vastdatasolutions

For additional Cyber solutions:
carah.io/Cybersecurity

To set up a meeting:
VASTData@carahsoft.com
888-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/vastdatacontracts

VAST Data Platform
for Zero Trust

Building Zero Trust for the AI Era

In the rapidly evolving landscape of cyber threats, the adoption of Zero Trust principles has become paramount for safeguarding data and ensuring robust cybersecurity. The VAST Data Platform stands at the forefront of this transformation, embodying the core tenets of Zero Trust in its architectural design and functionality. This platform industry's first paradigm shift from traditional perimeter-based security models to a more holistic, data-centric approach. By integrating advanced technologies such as granular access controls, multitenancy with strict isolation, and state-of-the-art encryption and key management, the VAST Data Platform offers an exemplary solution for modern organizations seeking to align with Zero Trust architecture. This paper delves into how the platform not only adheres to the foundational principles of Zero Trust but also enhances them through innovative features like data indexing, search capabilities, and cataloging using tags, and metadata, thereby providing a comprehensive and secure data management system.

The Zero Trust Mandate

Integral to improving the nation's cybersecurity posture, Zero Trust is a strategic shift in the U.S. government's approach to cyber defense. Stemming from Executive Order 14028, issued by President Biden, this mandate compels federal agencies to modernize their cybersecurity strategies by adopting a Zero Trust architecture. The mandate emphasizes a 'never trust, always verify' principle, moving away from traditional perimeter-based security models. Federal agencies are required to comply with this mandate by the end of 2024, ensuring a comprehensive and secure transformation towards a more resilient and proactive cybersecurity framework.

Why VAST?

Enhance Data Security and Privacy

Granular Access Controls and Data Isolation reduces the risk of data leaks and misuse

Streamline Data Management and Usability

Accelerate time to insight and simplify navigation of massive data sets without sacrificing security

Simplify Accountability and Compliance

Comprehensive auditing and logging for traceability and rapid forensic analysis across exabytes of data

High-Performance Data Platform

Unified NFS, S3, SMB, and ACID Compliant SQL Database

Exascale Global Namespace

Access data across edge, core, and cloud

Platform Alignment with Zero Trust

The VAST Data Platform's robust architecture and comprehensive features demonstrate a profound commitment to the principles of Zero Trust security. With granular access control, secure data segregation, advanced encryption, compliance with standards, auditing, and sophisticated data management capabilities, the platform stands as a beacon of modern cybersecurity solutions. By providing these capabilities, the VAST Data Platform ensures that organizations can not only meet the stringent requirements of the Zero Trust mandate but also pave the way for future advancements in data security and management.

The Data Pillar	VAST Data Platform Alignment
Authorize	Attribute Based Authentication (ABAC) in-conjunction with Role Based Authentication
Categorize	Catalog: Index, search, and query data in real-time
Log	Audit Logging: Console Access, Admin, and Protocol Access (S3, NFS, SMB)
Tag	Tag any object/file with a unique tag for categorization or authorization
Respond	Event Forwarding to Syslog, Splunk, ArcSight, QRadar, Elastic, Sumologic, etc
Encrypt	At rest & At Flight: FIPS 140-2 Validated & FIPS 140-3 Capable
Automate	K8S CSI, Manilla, Cinder Plugins for OpenStack, Rest API, Python SDK
Monitor	Telemetry: System, Capacity, Performance, Health, and data flow