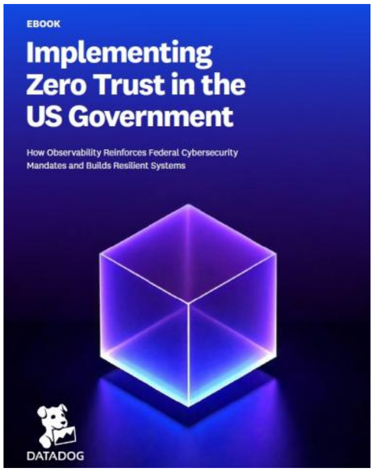
DATADOG

carahsoft



EBOOK

Implementing Zero Trust in the US Government

How Observability Reinforces Federal Cybersecurity Mandates and Builds Resilient Systems

DATADOG

Implementing Zero Trust in the Government US Government

How Observability Reinforces Federal Cybersecurity Mandates and Builds Resilient Systems

Thank you for downloading this Datadog resource. Carahsoft is the distributor for Datadog cyber solutions available via NASPO, Texas DIR-TSO-4288, MHEC, and other contract vehicles.

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

For additional resources:
carah.io/DatadogResources

For upcoming events:
carah.io/DatadogEvents

For additional Datadog solutions:
carah.io/DatadogSolutions

For additional cyber solutions:
carah.io/cyber

To set up a meeting:
Datadog@carahsoft.com
(703) 921-4160

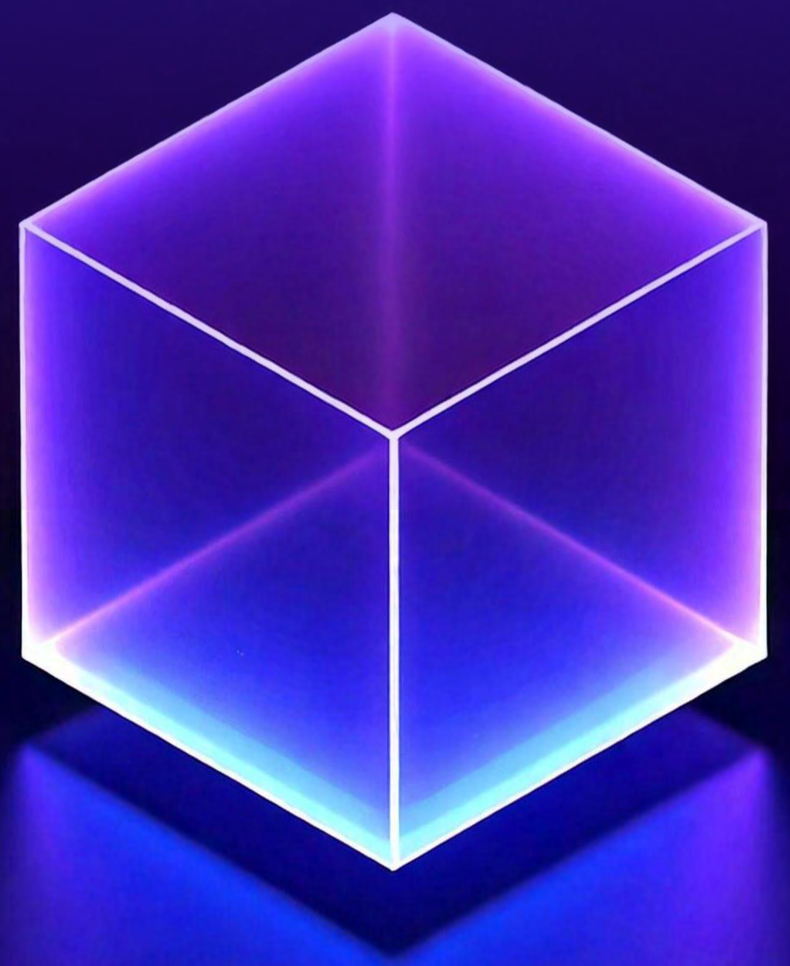
To purchase, check out the contract vehicles available for procurement:
carah.io/DatadogContracts

For more information, contact Carahsoft or our reseller partners:
Datadog@carahsoft.com | (703) 921-4160

EBOOK

Implementing Zero Trust in the US Government

How Observability Reinforces Federal Cybersecurity Mandates and Builds Resilient Systems



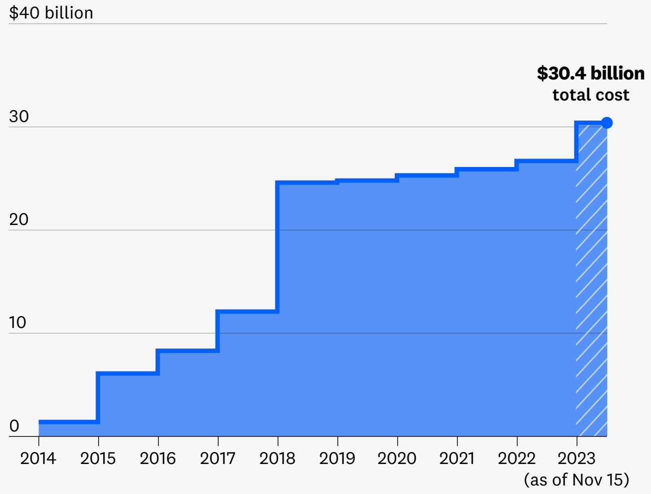
DATADOG

State of Zero Trust Architectures

US government IT leaders are navigating a pivotal era in cybersecurity as they work toward ambitious Zero Trust goals. While significant progress has been made, with CFO Act agencies reportedly achieving implementation rates in the “high 90% range,”[1] challenges persist. Agencies must balance robust security with operational productivity, address funding constraints, and develop sustainable strategies to maintain Zero Trust Architectures over the long term.

The urgency of Zero Trust adoption is underscored by an increasingly dangerous threat landscape. According to Comparitech, data breaches at local, state, and federal levels have cost US governments approximately $30.4 billion in losses from 2014 to 2023.[2]

Cumulative estimated cost of US government data breaches, since 2014



$30.4b

The estimated cost of cyber breaches impacting US government entities from 2014 to 2023.

Source: Comparitech

[1] Nihill, C. (2024, September 5). Federal CIO says agencies are nearing completion of zero-trust implementation. *FedScoop*.

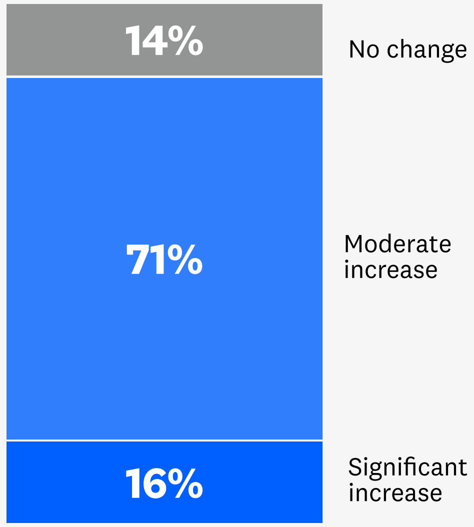
[2] Bischoff, P. (November 2023). A recent history of US Government Breaches. *Comparitech*.

This staggering figure highlights the need for comprehensive strategies to secure identities, enforce access controls, and proactively mitigate threats in today's complex digital ecosystem. While Executive Order (EO) 14028 does not provide direct funding, it has driven agencies to prioritize Zero Trust initiatives to protect their people, assets, and infrastructure. As a result, Zero Trust funding has increased significantly; following the May 2021 EO on Improving the Nation's Cybersecurity, 87% of government agencies reported budget increases to support Zero Trust efforts.[3]

As Okta's State of Zero Trust Security 2023 report states:

> **"There may be no industry under greater pressure to shore up their security with Zero Trust than the global public sector."[4]**

Reported budget changes by government agencies worldwide to support Zero Trust efforts, in 2022*



↑87%

Reported increase in budget

*Question: How has your budget changed for Zero Trust security initiatives in the past 12 months? Response options include "significant increase," "moderate increase," "no change," "moderate decrease," and "significant decrease." Figures may not sum to 100% because of rounding.

Source: Okta The State of Zero Trust Security 2022 Survey

[3] *Okta*. (August 2022.) The State of Zero Trust Security 2022.

[4] *Okta*. (September 2023.) The State of Zero Trust Security 2023.

While achieving 2024 milestones represents meaningful progress, the journey to fully realized Zero Trust is far from complete. As cyber threats grow more sophisticated and federal IT environments become increasingly complex, security requires a proactive, comprehensive approach. Federal agencies must deploy continuous monitoring, enterprise-wide logging, and least-privilege access controls across sprawling IT ecosystems, encompassing thousands of devices and users. However, outdated systems and processes often complicate Zero Trust adoption, necessitating extensive modernization to meet evolving security and compliance standards.

This eBook serves as a practical guide to the key authorities shaping Zero Trust Architecture in the US government, outlining the essential resources each provides. It also emphasizes the pivotal role of observability in Zero Trust strategies—enabling enhanced security, visibility, and control across government IT environments.

For IT leaders charged with deploying Zero Trust across the public sector, understanding these components is critical to building secure, resilient infrastructure that safeguards sensitive data, ensures compliance, and proactively addresses the evolving threat landscape.

Zero Trust Defined

A widely accepted definition of Zero Trust comes from the **National Institute of Standards and Technology (NIST)** in its publication, **NIST Special Publication 800-207, Zero Trust Architecture.** According to NIST, Zero Trust is:

> "...a cybersecurity paradigm focused on resource protection and the premise that trust is never implicitly granted but must be continually evaluated."[5]

This definition is widely adopted by government agencies as it establishes the foundational principles of Zero Trust, including:

01 **Never Trust, Always Verify**

Trust is never assumed; identity, access, and activity are continuously verified.

02 **Least-Privilege Access**

Users and systems are granted only the minimum access necessary to perform their tasks.

03 **Micro-Segmentation**

Networks and systems are divided into smaller, isolated segments to limit potential attack surfaces.

04 **Assume Breach Mentality**

Operate under the expectation that breaches can and will occur, focusing on containment and rapid response.

05 **End-to-End Monitoring and Visibility**

Maintain real-time monitoring of all activities across systems, users, and devices to detect anomalies and enforce policies.

These principles form the backbone of Zero Trust implementation across government agencies, ensuring robust security aligned with evolving threats. We will examine the last core principle of Zero Trust: **End-to-End Monitoring and Visibility**, highlighting how observability—which encompasses both—is essential for achieving Zero Trust in government systems.

Observability is the ability to achieve deep visibility into the internal workings of a system by analyzing the data it generates, such as metrics, traces, and logs. Unlike traditional monitoring, observability provides comprehensive insights into complex, distributed systems, enabling teams to understand system behavior, diagnose issues, and optimize performance in real time.

Before diving deeper into this focus area, we will take a broader look at the full landscape of Zero Trust, reviewing the key directives, mandates, and stakeholders that collectively shape and drive Zero Trust initiatives not only across the federal government but also within the SLED (state, local, and education) and private sectors.

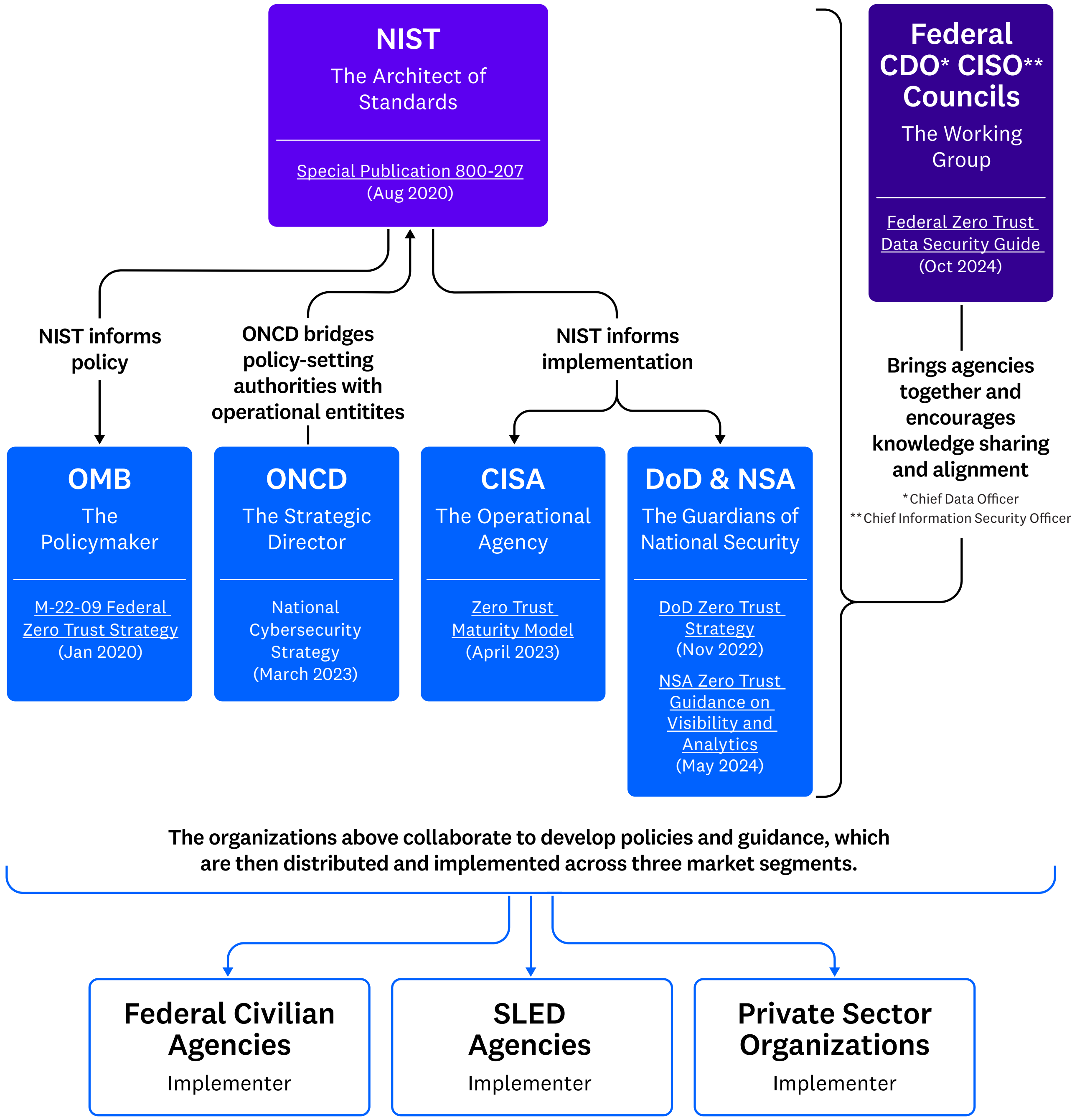
[5] Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020, August). Special Publication 800-207: Zero Trust Architecture. National Institute of Standards and Technology.

The Federal Zero Trust Ecosystem

The concept of a Zero Trust ecosystem represents a collaborative, multi-agency approach to cybersecurity, designed to protect government resources and data against sophisticated and evolving threats.

In this ecosystem, each authority plays a distinct role in setting standards, designing frameworks, turning policies into practice, and facilitating interagency collaboration.

AGENCY	ROLE IN ZERO TRUST IMPLEMENTATION
NIST	Establishes the foundational standards for Zero Trust, including the core principles and technical requirements for the entire ecosystem.
Office of Management and Budget (OMB)	Acts as the policymaker, issuing directives that establish Zero Trust standards as government-wide mandates.
Office of the National Cyber Director (ONCD)	Provides strategic leadership, coordinating policies and offering high-level oversight to ensure that Zero Trust objectives are aligned with national security priorities.
Cybersecurity and Infrastructure Security Agency (CISA)	Serves as the operational agency, translating policy into actionable guidance and tools to support federal agencies in implementing Zero Trust frameworks.
Department of Defense (DoD) and National Security Agency (NSA)	Mission owners responsible for national and international security, informing tactics to defend critical infrastructure against sophisticated cyber threats, including those posed by state-sponsored actors.
Interagency Councils (Federal CISO and CIO Councils)	Fosters collaboration across government entities and builds partnerships with the private sector, encouraging knowledge-sharing and alignment between public and private Zero Trust initiatives.



NIST
The Architect of Standards
Special Publication 800-207
(Aug 2020)

Federal CDO* CISO** Councils
The Working Group
Federal Zero Trust Data Security Guide
(Oct 2024)

NIST informs policy

ONCD bridges policy-setting authorities with operational entitites

NIST informs implementation

Brings agencies together and encourages knowledge sharing and alignment

*Chief Data Officer
**Chief Information Security Officer

OMB
The Policymaker
M-22-09 Federal Zero Trust Strategy
(Jan 2020)

ONCD
The Strategic Director
National Cybersecurity Strategy
(March 2023)

CISA
The Operational Agency
Zero Trust Maturity Model
(April 2023)

DoD & NSA
The Guardians of National Security
DoD Zero Trust Strategy
(Nov 2022)
NSA Zero Trust Guidance on Visibility and Analytics
(May 2024)

The organizations above collaborate to develop policies and guidance, which are then distributed and implemented across three market segments.

Federal Civilian Agencies
Implementer

SLED Agencies
Implementer

Private Sector Organizations
Implementer

The graphic above illustrates the key contributions of each agency and council, highlighting their collaborative roles in advancing a unified, whole-of-government approach to Zero Trust and enhancing national cybersecurity resilience.

The Role of Observability in Zero Trust

As highlighted in the Forbes article, "Why Observability Is a Foundational Element of Zero Trust,"[6] observability is recognized as a critical first step in any Zero Trust strategy.

Observability—comprehensive, end-to-end monitoring and visibility—is a core principle of Zero Trust. When paired with automation, it becomes indispensable for strengthening government cybersecurity, enabling real-time and continuous validation of infrastructure activities and access requests. This capability is especially crucial in addressing the ongoing cybersecurity skills gap by automating key monitoring and response functions, easing the burden on overstretched teams.

Beyond security, observability drives continuous modernization by delivering actionable insights to optimize and secure complex IT environments—whether on-premises, cloud-based, or hybrid. With the ability to detect, respond to, and mitigate threats in real time, observability empowers agencies to navigate an evolving threat landscape while ensuring mission success.

A key component of observability is data tagging, which provides granular context about users, devices, and transactions. This enhances precise access controls and improves monitoring and threat detection, making it an essential tool for implementing effective Zero Trust strategies.

As government IT environments increasingly adopt microservices, mobile, and remote access, AI-driven observability and search capabilities have become essential. These advanced tools not only address cybersecurity skills shortages but also support the secure implementation of Zero Trust frameworks by continuously monitoring and validating every user and device transaction. This ensures a secure, adaptive evolution of government IT systems.

[6] Eades, T. (2022, March 2). Why Observability Is A Foundational Element Of Zero Trust. *Forbes*.

US Government Authorities & Key Zero Trust Strategies

The table below outlines how US government authorities incorporate visibility, observability, and continuous monitoring into their Zero Trust strategies, focusing on essential IT layers like infrastructure, applications, and log management.

AUTHORITY & KEY ZERO TRUST RESOURCE	KEY POINTS ON VISIBILITY, OBSERVABILITY, AND CONTINUOUS MONITORING
NIST SP 800-207 (Zero Trust Architecture, 2020)	– Defines observability and visibility as foundational principles of Zero Trust, highlighting **continuous monitoring** across all network assets. – SP 800-207 underscores the importance of **infrastructure monitoring** to detect internal lateral movement and **application monitoring** to observe all transaction layers. – **Log management** is essential, with guidance recommending centralized logging to streamline security response and audit trails.
OMB Memorandum M-22-09 (Federal Zero Trust Strategy, 2022)	– Mandates that federal agencies implement continuous monitoring as a core Zero Trust practice by 2024, specifying that observability must cover **infrastructure, applications, and access points.** – Outlines the need for comprehensive **log management** and cross-agency visibility to reduce incident detection time and improve threat response.
ONCD National Cybersecurity Strategy (2023)	– Emphasizes the need for **continuous visibility** across federal IT systems to detect and mitigate threats early. – Calls for **unified data sharing** among agencies, with observability frameworks to monitor both internal and external risks. – Encourages agencies to prioritize **infrastructure monitoring** to reduce potential cyberattack surfaces, and suggests leveraging advanced **log management** to quicken response times.
CISA Zero Trust Maturity Model (2023)	– Highlights observability as a critical factor in the Zero Trust Maturity Model, emphasizing continuous **monitoring across infrastructure and applications.** – Calls for **log management and aggregation** to detect anomalies a nd provide timely alerts, with guidance on using telemetry to support threat detection and to enforce granular security policies across systems.
DoD Zero Trust Reference Architecture (2022)	– Recommends continuous monitoring to safeguard national security systems, detailing observability strategies for **infrastructure and application monitoring.** – Emphasizes full visibility into network segments to limit lateral movement. – **Log management** is noted as essential for both security and compliance, enabling real-time detection and response for defense infrastructure.
NSA Zero Trust Guidance on Visibility and Analytics (2024)	– Details **visibility and observability** requirements for real-time detection of threats. – Recommends agencies adopt **full-stack monitoring** of infrastructure and applications to capture complete telemetry. – Continuous monitoring is emphasized for managing east-west network traffic, and robust **log management** is advised to centralize security intelligence and improve threat detection accuracy.
CISO and CDO Councils Federal Zero Trust Data Security Guide (2024)	– Underscores the necessity of continuous monitoring and **observability** to secure data effectively. – Advocates for comprehensive **infrastructure monitoring** to detect and respond to threats in real time. – Highlights the importance of **application monitoring** to ensure data integrity and security throughout its lifecycle. – Robust **log management** practices are recommended to maintain detailed records of data access and usage, facilitating audits and compliance.

Accelerate Your Zero Trust Transformation with Datadog

Datadog excels in visibility, observability, and continuous monitoring, making it an ideal partner for organizations advancing their Zero Trust goals. With Datadog, agencies gain real-time visibility across all IT layers—monitoring infrastructure, applications, and log data through a single, integrated platform. This comprehensive observability allows for swift detection of anomalies and security threats, supporting proactive threat mitigation and compliance.

Datadog's core capabilities—Infrastructure Monitoring, Application Performance Monitoring (APM), and Log Management—are foundational for achieving Zero Trust security principles in complex IT environments.

The following table highlights how Datadog's full suite of products supports Zero Trust implementation by addressing common security and operational challenges. With capabilities like real-time security monitoring, incident management, and automation, Datadog empowers organizations to manage all facets of Zero Trust within a unified platform, ensuring compliance with federal standards while building a secure and resilient IT ecosystem.

DATADOG CORE CAPABILITIES

Infrastructure Monitoring

Continuously monitors system performance and security events, enabling real-time anomaly detection, enforcing least-privilege access policies, and verifying secure interactions across on-premises, hybrid, and multi-cloud environments.

Application Performance Monitoring

Continuously observes application behavior to detect anomalies, identify unauthorized access patterns, and resolve performance issues, supporting the Zero Trust principles of continuous monitoring and threat detection.

Log Management

Centralizes and analyzes logs in real time, providing actionable insights into user and system activities to verify access, detect threats, and ensure compliance with Zero Trust security mandates.

DATADOG PRODUCT	ZERO TRUST CAPABILITY
Infrastructure	
Infrastructure Monitoring	Continuously monitors system performance and security events, enabling real-time anomaly detection, enforcing least-privilege access policies, and verifying secure interactions across on-premises, hybrid, and multi-cloud environments.
Network Performance Monitoring	Delivers visibility into network traffic patterns for hybrid, multi-cloud, and on-premises environments.
Network Device Monitoring	Provides device insights to enable continuous monitoring and security policy enforcement.
Applications	
Application Performance Monitoring	Continuously observes application behavior to detect anomalies, identify unauthorized access patterns, and resolve performance issues, supporting the Zero Trust principles of continuous monitoring and threat detection.
Security	
Application Security Management	Detects, prioritizes, and responds to application threats to minimize risk across all layers.
Cloud Security Management (CSM)	Provides visibility and control over cloud environments to detect, prevent, and respond to threats, ensuring secure and compliant operations at all layers.
Cloud Security Posture Management (CSPM)	Continuous configuration scans across cloud accounts, hosts, and containers to remediate misconfigurations, enforce least privilege, and reduce threats.
Cloud Security Management (CSM) Vulnerabilities	Identifies and remediates vulnerabilities to secure assets and uphold Zero Trust principles.
Kubernetes Security Posture Management (KSPM)	Enforces security best practices in Kubernetes to uphold Zero Trust and minimize container risks.
Cloud Infrastructure Entitlement Management (CIEM)	Manages identities and privileges in dynamic cloud environments.
Software Composition Analysis	Identifies vulnerabilities in open source components to ensure secure, trusted code.
Code Security (IAST)	Detects vulnerabilities in the production application's code and fixes them quickly with observability context.
Cloud Security Information and Event Management (SIEM)	Delivers real-time security insights for continuous threat detection and response.
Log Management	
Log Management	Centralizes and analyzes logs in real time, providing actionable insights into user and system activities to verify access, detect threats, and ensure compliance with Zero Trust security mandates.
Log Forwarding	Transmits real-time event data securely for continuous monitoring and threat detection.
Audit Trail	Tracks user activities to ensure traceability and accountability for actions.
Sensitive Data Scanner	Identifies and redacts sensitive data and personally identifiable information (PII) to enforce protection and compliance policies.
Cloud Service Management	
Incident Management	Provides a system through which your organization and security teams can effectively identify and mitigate incidents.
Workflow Automation	Allows security teams to automatically run predefined task sequences when compliance or security signals are triggered.
Event Management	Automatically generates events from Datadog products like monitors, Watchdog™, and Error Tracking. Also ingests events from any source, including third-party alerts, change requests, deployments, and configuration updates.

Conclusion

Zero Trust represents a transformative shift in security, built on a foundation of interconnected pillars to achieve end-to-end protection. At the heart of this approach is observability—an essential pillar integrated across all others. By leveraging real-time network telemetry and feeding it into advanced tools, visibility enables security and network operations teams to make data-driven, informed decisions.

For US government agencies, successfully implementing Zero Trust demands a steadfast focus on visibility, observability, and continuous monitoring. This eBook has demonstrated how observability underpins key Zero Trust principles, such as constant verification, least-privilege access, and proactive threat detection. Prioritizing these elements empowers agencies to strengthen cybersecurity, maintain compliance, and safeguard sensitive data across their infrastructure, applications, and systems.

Datadog understands the challenges of adopting Zero Trust and provides a powerful observability and security platform tailored to meet the unique needs of government IT leaders. With comprehensive, real-time insights into infrastructure, applications, and user activity, Datadog enables agencies to achieve their Zero Trust objectives and enhance security in today's complex threat landscape.

Through its FedRAMP®-authorized platform, Datadog delivers a suite of integrated tools for infrastructure and application monitoring, advanced log management, and security incident response. These capabilities provide the real-time visibility essential for effective Zero Trust, equipping teams to navigate complexity, mitigate risks, and confidently meet cybersecurity mandates.

Ultimately, Datadog's secure and compliant solutions support a resilient government infrastructure, aligning with the highest security standards to protect against evolving threats and ensure mission success.

Ready to improve your security posture with observability?
With Datadog's AI-powered observability platform, organizations gain real-time visibility into their entire IT environment, enabling them to continuously monitor and validate user identities, secure devices, track network traffic, and ensure applications and data are protected. Contact us to learn how Datadog can help advance your Zero Trust objectives.

Get started with Datadog

STEP 1

Visit ddog-gov.com/signup

STEP 2

Choose the region called "United States (US1-FED) – FedRAMP Moderate Authorized" & complete the quick form

LOGGING IN

01 Tell us about your stack

02 Install your first Datadog Agent

03 Start collecting metrics & events from your systems & apps

04 Contact us anytime for support

Let's connect

Datadog has helped thousands of customers achieve observability across their technology stacks by unifying data from on-premises, hybrid, and cloud-based systems into a single source of truth. Contact us to learn about how we can help advance your mission.

Contact our Public Sector Sales team
team-enterprisepublicsector@datadoghq.com

Learn more about
Datadog for Government