



Achieving the Pillars of Zero Trust at Federal Agencies

eBook



carahsoft.

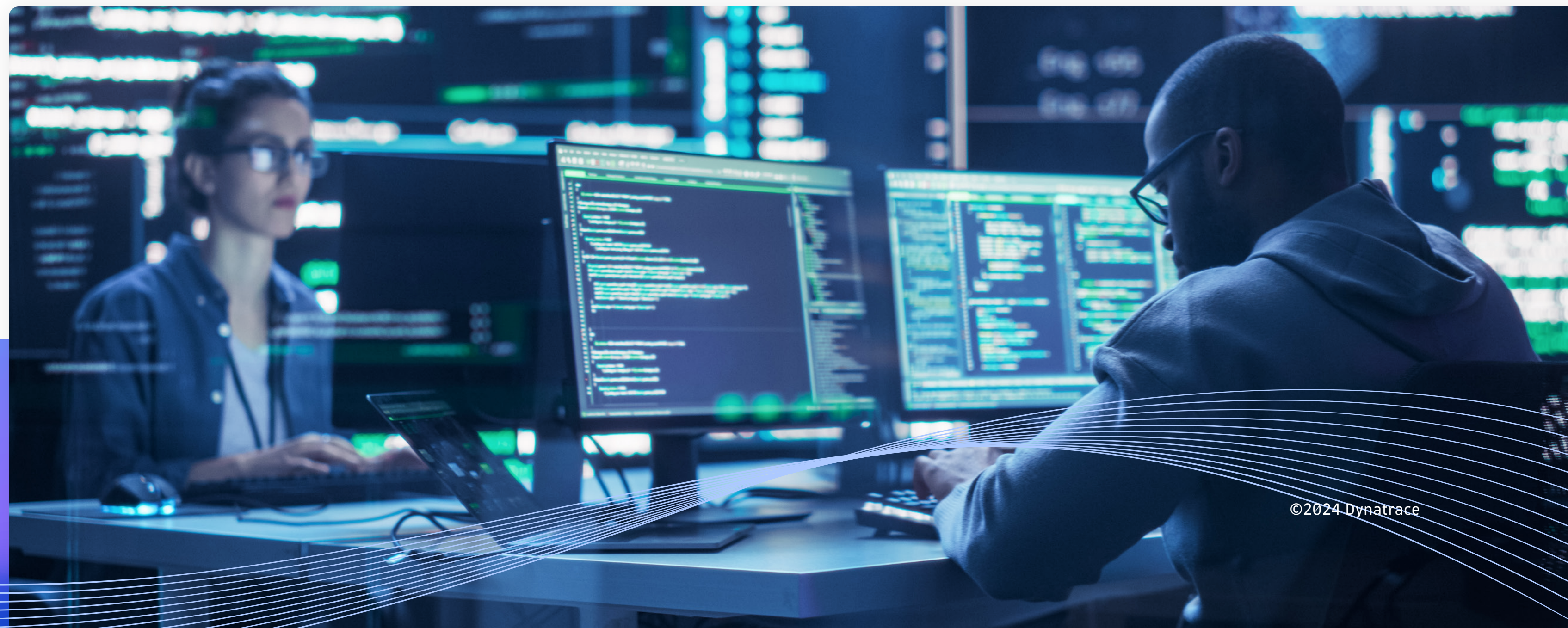
For more information, contact Carahsoft or our reseller partners:

Dynatrace@carahsoft.com | 877-742-8468



Achieving the pillars of zero trust at federal agencies

How Dynatrace allows government customers to transition from basic visibility and analytics to automatic and intelligent observability — ensuring a state of optimal cyber protection



INTRODUCTION

Optimal cyber protection requires zero trust

For government leaders, the time to implement zero trust is now: The White House [“Executive Order on Improving the Nation’s Cybersecurity”](#) has directed federal agencies to advance toward a zero trust architecture which “eliminates implicit trust in any one element, node or service and instead requires continuous verification.”

Expanding upon the executive order, the Office of Management and Budget (OMB) memo, [“Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,”](#) states agencies must meet specific zero trust goals based upon the five pillars of the [Cybersecurity and Infrastructure Security Agency \(CISA\) Zero Trust Maturity Model](#): identity, devices, networks, applications/workloads and data.

To help our federal customers successfully adopt policies and practices required for the five pillars, Dynatrace enables a transition from basic visibility and analytics to automatic and intelligent observability, which provides precise answers about the performance and security of every device, application and user — no matter where they are.

What's inside

CHAPTER ONE

Government going “all in” on zero trust

CHAPTER TWO

Too much too soon?

CHAPTER THREE

Reaching optimal zero trust through Dynatrace observability

CHAPTER FOUR

How Dynatrace enables the achievement of CISA’s five pillars

CHAPTER FIVE

Covering all pillars with ideal integration

CHAPTER SIX

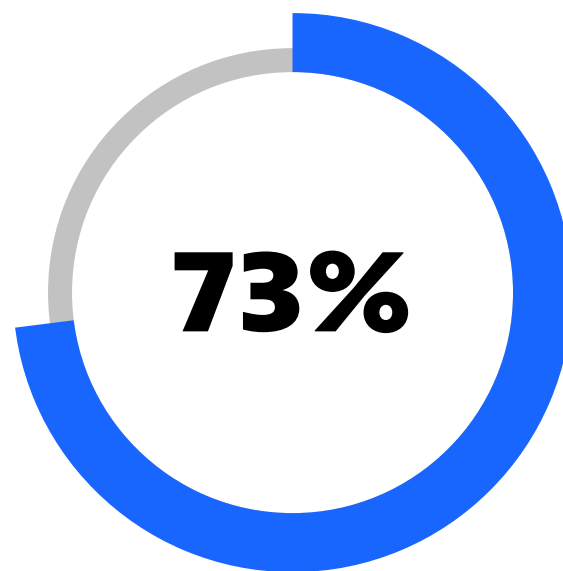
Dynatrace products and capabilities usher in a new age of cyber defense

CHAPTER ONE

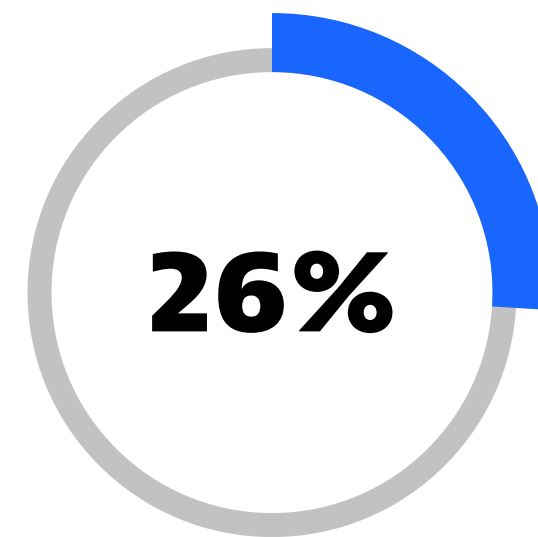
Government going “all in” on zero trust

The OMB memo stresses that agencies can no longer depend upon conventional, perimeter-focused cyber defenses. Instead, they must establish architectures that trust no person, system, network or service, verifying “anything and everything” to allow access.

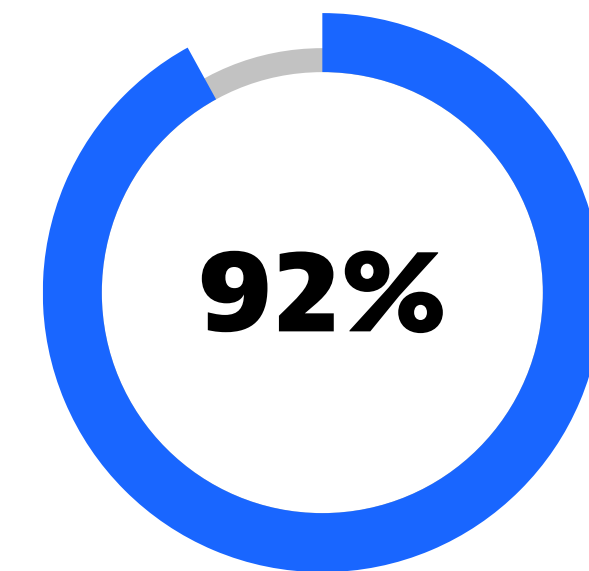
Subsequently, as [the numbers](#) show, there is no stopping zero trust in the public sector:



of federal cybersecurity decision-makers report their agency is aggressively adopting zero trust principles.



are adopting zero trust principles where they feel it makes sense.

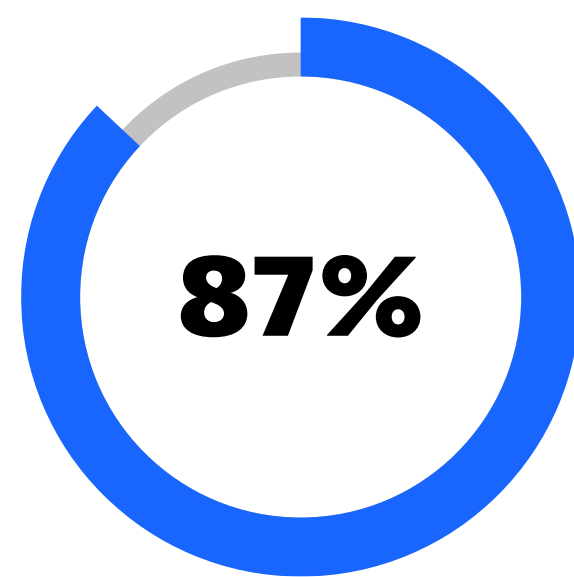


say recent initiatives such as the EO, OMB’s strategy and CISA’s maturity model have increased their confidence in their agency’s ability to implement zero trust.

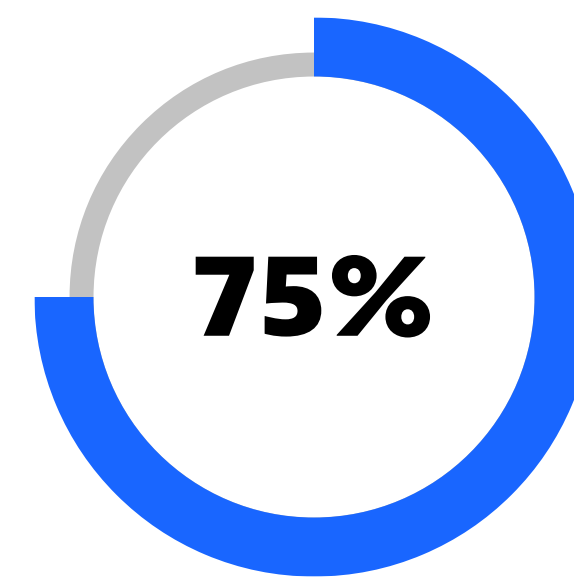
CHAPTER TWO

Too much too soon?

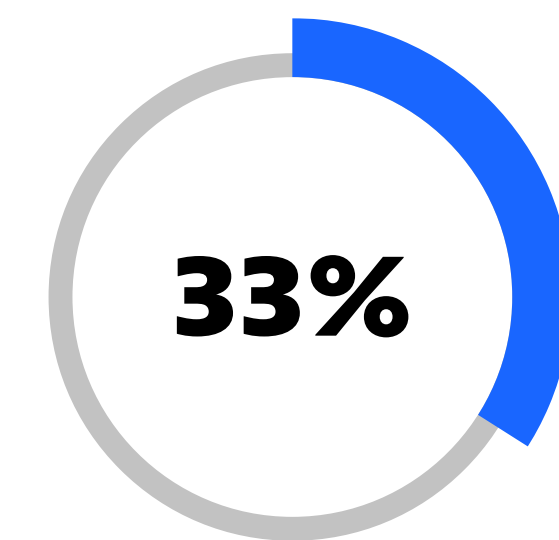
That said, the same decision-makers cite several challenges in adopting zero trust:



feel the EO/OMB is pushing agencies to move too fast for effective zero trust implementation.



When it comes to achieving the CISA pillars of zero trust, three out of four say reaching optimum maturity will be a challenge.



More than one-third say they struggle with competing priorities as they attempt to implement zero trust while overseeing daily operations.

CHAPTER THREE

Reaching optimal zero trust through Dynatrace observability

Dynatrace works with government customers to empower them with automatic and intelligent observability. We provide deep visibility analytics into the cloud, hosts, services, processes, containers and applications, along with automation and orchestration. This allows federal agencies to develop a zero trust architecture through the following capabilities:

- The **continuous monitoring and capturing of all data** from logs, metrics and end-to-end transactions
- The **deployment of AI** to set baselines
- The **automatic identification of anomalous and potentially threatening activity** to enforce least privilege — a core principle of zero trust that restricts access to the bare minimum needed, in order to do the job at hand.

Dynatrace understands that zero trust will involve changing a configuration or installing something new, possibly impacting user experience (UX). To avoid unwanted friction, our AI automatically identifies UX issues. We train customers to use quality gates so that if systems and software do not meet performance requirements, agency teams will roll back the security changes to resolve the issues. Leveraging Dynatrace's observability in conjunction with DevSecOps best practices, provides a robust approach to reducing unplanned system roll backs.



CHAPTER FOUR

How Dynatrace enables the achievement of CISA's five pillars

CISA's Zero Trust Maturity Model establishes guidelines for agencies to develop strategies and implementation plans. Its five pillars — identity, devices, networks, applications and workloads, and data — serve as the foundation for the adoption of the CISA model.

In the following pages of this eBook, we'll explain how teams are leveraging Dynatrace to accomplish the [objectives](#) of the five pillars, through our AI-enabled continuous observability (referred to as "visibility" in CISA graphic), analytics, automation and orchestration.

High-Level Zero Trust Maturity Model Overview

	Identity	Devices	Networks	Applications and workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as- needed automated access	• Continuous physical and virtual analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network raffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for develoopment, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based encryption • Encrypts data at rest
Initial	• MFA with strong passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement data categorization strategy • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management
Visibility and analytics			Automation and orchestration		Governance



PILLAR ONE

Identity

What CISA says

“Agencies should integrate identity, credential and access management solutions where possible throughout their enterprise to enforce strong authentication, grant tailored context-based authorization and assess identity risk for agency users and entities.”

What Dynatrace does

Dynatrace utilizes an Identity and Access Management (IAM) framework, which clearly defines the actions allowed within the Dynatrace platform. Administrators can grant [permissions](#) based strictly upon necessity and enforce the principles of least privilege. In addition, our [LDAP](#) integration can utilize an external LDAP resource to grant user and group access to the platform based on a company’s directory information.



PILLAR TWO

Devices

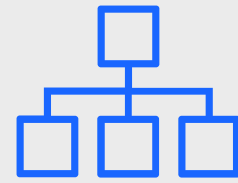
What CISA says

“Agencies should secure all agency devices, manage the risks of authorized devices which are not agency-controlled and prevent unauthorized devices from accessing resources. Device management includes maintaining a dynamic inventory of all assets including their hardware, software, firmware, etc., along with their configurations and associated vulnerabilities.”

What Dynatrace does

We conduct continuous physical and virtual asset analysis, compliance enforcement, and integrated threat protection. Resource access is enforced by real-time risk analytics of devices. For example, Dynatrace’s SmartScape technology displays applications, services, processes, hosts and data centers, along with any vulnerabilities or hosts associated with those components. Also, as a customer’s environment changes and agencies move assets to the cloud, Dynatrace will instrument those new entities on the fly.

Internally, Dynatrace protects against software supply chain attacks by utilizing security protocols within the [Software Development Life Cycle \(SDL\)](#), which automatically enforces that all developed code is scanned and tested.



PILLAR THREE

Networks

What CISA says

“(Zero Trust architectures) enable a shift away from traditional perimeter-focused approaches to security and permit agencies to manage internal and external traffic flows, isolate hosts, enforce encryption, segment activity and enhance enterprise-wide network visibility.”

What Dynatrace does

Isolates hosts, enforces encryption and segments activity to enhance overall network visibility and better understand where traffic is coming from, and going to. [Monitoring](#) the quality of traffic passing through different servers, interfaces and processes. The Dynatrace network segmentation and configuration isolates critical workloads while supporting “just-in-time” and “just-enough” access controls. We adapt configurations based upon automated, risk-aware application profile assessments.



PILLAR FOUR

Applications and workloads

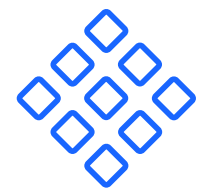
What CISA says

“Agencies should manage and secure their deployed applications and should ensure secure application delivery. Granular access controls and integrated threat protections can offer enhanced situational awareness and mitigate application-specific threats.”

What Dynatrace does

Our AI-powered observability and controls pave the path for continuous data inventorying, security testing throughout the lifecycle, authorized access for applications availability and protections against sophisticated attacks for all workflows, with context-based access controls. As agencies test parts of an application, we can determine the impact it has on the performance of their environment. We also enable agencies to integrate all of their mission-critical data, including how transactions are traversing their cloud environments, into one convenient platform.

In addition, Dynatrace’s AppSec module allows for runtime vulnerability analytics, reducing the time and cost to find and fix application vulnerabilities. Our runtime application protection reduces exposure to zero-day vulnerabilities. For example, utilizing our Software Development Life Cycle (SDL) protocols, enabled our internal security team to detect the [Log4j vulnerabilities](#) in real-time and implement immediate remediation at scale. Furthermore, our security analytics capabilities lead to quick actionable insights to support proactive security risk mitigation and remediation.



PILLAR FIVE

Data

What CISA says

“Agencies should inventory, categorize, and label data; protect data at rest and in transit; and deploy mechanisms to detect and stop data exfiltration. Agencies should carefully craft and review data governance policies to ensure all data lifecycle security aspects are appropriately enforced across the enterprise.”

What Dynatrace does

Expanded capabilities include dynamic access controls, continuous data inventorying, automated tagging and the encryption of data in use. Our Lifecycle Coverage delivers a real-time view and continuous reporting of monitored workloads, highlighting where components are running so agencies can apply zero trust rules.



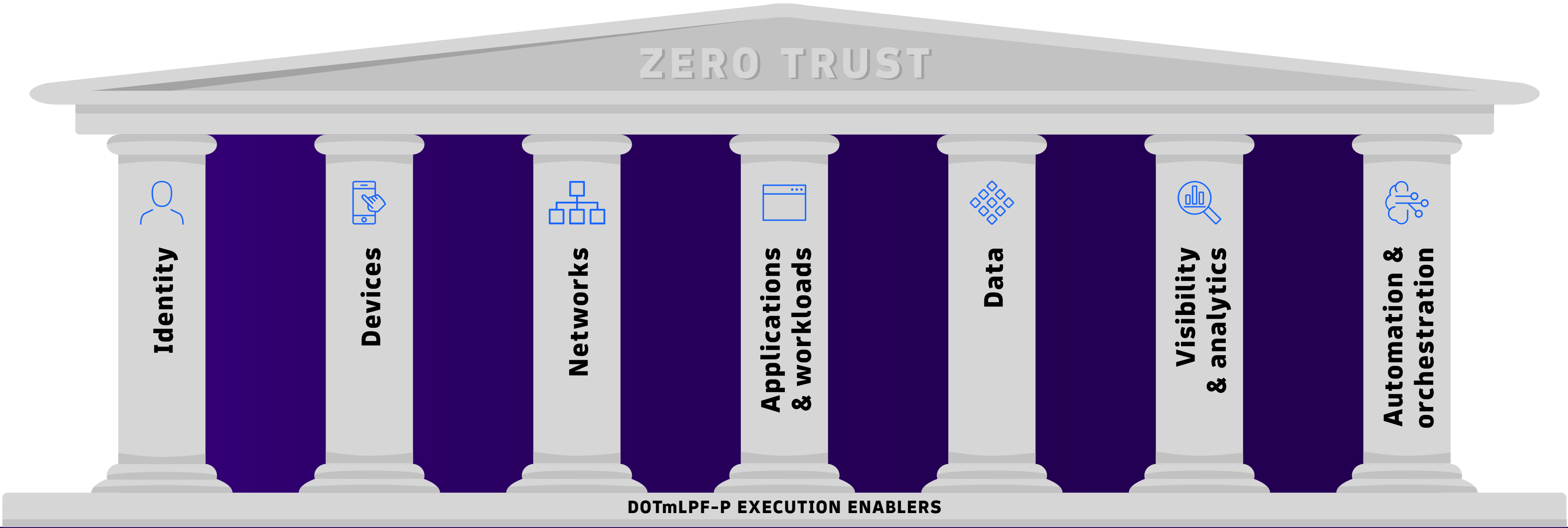
CHAPTER FIVE

Covering all pillars with ideal integration

The Department of Defense (DoD) has brought greater focus to visibility and analytics, and automation and orchestration by designating them as a [sixth and seventh zero trust pillar](#). While agencies may have achieved some or all of the CISA/DoD pillars before, they were most often conducted in silos.

But with Dynatrace, they meet these objectives in a fully integrated manner. They see all activity within context – how a transaction flows through the environment, what

services a particular page load went to, the different databases it contacted along the way, etc. – then apply our deterministic AI engine to create a descriptive architecture model in real-time. Customers can automate various scenarios to make applications more secure or comply with specific processes or zero trust pillars. All of this comes together to assemble an entirely secure cyber ecosystem with visibility and analytics as the connective glue.



CHAPTER SIX

Dynatrace products and capabilities usher in a new age of defense

Here's additional insight into how Dynatrace's products and capabilities bring unique value in supporting zero trust policies/practices and CISA's five pillars:



Dynatrace **SmartScope** maps in real-time all the components and dependencies in an agency's ecosystem, including what is expected (hosts, networks and other infrastructure) and unpredictable (website, application, services and process activity).



Dynatrace's **Apdex** rating system is calculated for each discrete user action and application.



Dynatrace **OneAgent** automatically and continuously tracks all dependencies associated with an individual host.



Our AI engine, **Davis**, scours for risk vulnerabilities within applications running in the cloud, containers, virtual machines and traditional servers, while analyzing logs, metrics and traces for additional context to immediately pinpoint the root cause of issues.



Dynatrace integrates with tools like **ServiceNow** and **Ansible** so agencies rapidly resolve problems through auto-remediation, ensuring that applications are always on and fully optimized.

Automatic and intelligent observability for hybrid multiclouds

In the not-too-distant future, there may come a day when zero trust is considered as a “given” — a concept that is just as prevalent and familiar as the cloud (remember when the cloud was something new and even abstract?) But, until then, many agencies will struggle to meet deadlines while still reaching an optimal state of CISA's five pillars.

That's why Dynatrace works with government teams to fast-track implementation and enforcement through our observability tools.

Learn more

If you are ready to learn more, please visit www.dynatrace.ai/Government/ or email us at Usfederal@dyantrace.com.



[Dynatrace](#) (NYSE: DT) exists to make the world's software work perfectly. Our unified platform combines broad and deep observability and continuous runtime application security with the most advanced AIOps to provide answers and intelligent automation from data at enormous scale. This enables innovators to modernize and automate cloud operations, deliver software faster and more securely, and ensure flawless digital experiences. That's why the world's largest organizations trust the Dynatrace® platform to accelerate digital transformation.

Curious to see how you can simplify your cloud and maximize the impact of your digital teams? Let us show you. Sign up for a [free 15-day Dynatrace trial](#).



blog



@dynatrace



Thank you for downloading this Dynatrace factsheet! Carahsoft serves as the Master Government Aggregator and Distributor for Dynatrace, offering expertise in government procurement processes and practices with purchasing available via GSA, NASA SEWP V and other contract vehicles.

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



For additional resources:
carah.io/DynatraceResources



For upcoming events:
carah.io/DynatraceEvents



For additional Dynatrace products:
carah.io/DynatraceSolutions



For additional Open Source solutions:
carah.io/OpenSourceSolutions



To set up a meeting:
Dynatrace@carahsoft.com
(877)-742-8468



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