carahsoft The Trusted Government IT Solutions Provider®

Zero Trust Buyer's Guide **for Government**

Discover Solutions to Strengthen Cyber Defenses, Safeguard Critical Data, and Navigate Compliance Requirements for a Secure Government Network

FEATURING: ***Solution Areas*** • ***Success Stories*** ***Zero Trust Policies*** • ***Contract Vehicles*** • ***Upcoming Events***

carahsoft

Zero Trust
Network Solutions

Government agencies require security solutions that focus on protecting critical information and reducing risk to national security. Zero Trust cybersecurity approaches treat all network traffic as untrusted in an effort to prevent unauthorized access to essential data and services.

Carahsoft and our vendor partners have assembled a portfolio of products and services to help government organizations operationalize Zero Trust networks. Our partners provide solutions that align with Zero Trust maturity models that have emerged in the public sector.

Scan to learn more about our Zero Trust Solutions

Welcome to the Zero Trust Buyer's Guide!

The Zero Trust market stands out due to its transformative approach to security. It replaces the traditional "trust but verify" model with the more rigorous "never trust, always verify" framework. This shift is especially relevant today; utilization of new technologies and cloud computing have highlighted the need for a more diverse cybersecurity portfolio. Organizations must now navigate the complexities of managing multiple devices and locations while ensuring secure, verified access to network resources. Zero Trust provides a modern framework to meet these needs, emphasizing security regardless of where users are accessing the network.

This approach provides a framework that supports higher levels of security and resilience ensuring that the right people have access to the right data at the right time, seamlessly and from anywhere in the world. With the rise of sophisticated threats such as ransomware, insider attacks, phishing, and advanced persistent threats, traditional perimeter-based security models need to be augmented with advanced technology. The Zero Trust model directly addresses the modern threat landscape by enforcing strict verification policies, safeguarding organizations from both internal and external risks.

Government agencies and organizations are all at different levels of maturity in their ZTA journey. Carahsoft has a comprehensive portfolio of leading cybersecurity vendors and reseller and integration partners who are equipped to help you determine the best course of action for Zero Trust implementation. Together, we can help you maximize the value of your existing technology investments, making sure you get the most out of the tools and systems you already own. At the same time, helping you build a Zero Trust model, enhancing security and ensuring compliance across your organization.

We offer a wide range of educational events, case studies, whitepapers, webinars and more to help you understand Zero Trust and achieve compliance. Stay ahead of cybersecurity challenges and build a strong foundation for proactive security.

Steve Jacyna
Director of Innovative Cybersecurity Solutions
Carahsoft

Table of Contents:

Zero Trust Solution Areas

Agencies across the Federal Government are implementing Zero Trust strategies to meet sophisticated threats. Zero Trust security solutions focus on protecting critical information and reducing risk to national security. Zero Trust cybersecurity approaches treat all network traffic as untrusted in an effort to prevent unauthorized access to essential data and services.

Carahsoft and our vendor partners have assembled a portfolio of products and services to help government organizations operationalize Zero Trust networks. Our partners provide solutions that align with Zero Trust maturity models that have emerged in the public sector, including initiatives from the NIST, DoD and CISA.

Identity

Agencies should ensure and enforce that the right users and entities have the right access to the right resources at the right time. Identity will form a core component of an agency's ZTA. Least privilege access, which underpins zero trust, depends on the ability to assure the identity of the entity receiving access. The Zero Trust Maturity Model moves away from simply using passwords to validate identity and instead uses a combination of factors to validate and continuously verify that identity throughout the duration of their interactions with services or data.

Device

Devices are a core component of Zero Trust Architecture. Zero Trust models demand an inventory of all devices connecting to the network, validation of the integrity and security of those devices, and controlled access of devices to services and data. Select a technology vendor below to learn more about their products for the Device Pillar of Zero Trust:

Network/Environment

Network and Environment are core components of Zero Trust Architecture. Zero Trust models call for organizations to rethink methods of network connection and protections deployed. Organizations should not implicitly trust traditional network segmentation, but rather realign their network segments and protections to better secure application workflows. Select a technology vendor below to learn more about their products for the Network/Environment Pillar of Zero Trust:

Application Workload

Application Workload is a core component of Zero Trust Architecture. Zero Trust models require organizations to secure and manage the application layer, software containers, application delivery, and the application development lifecycle. Select a technology vendor below to learn more about their products for the Application Workload Pillar of Zero Trust.

Data

Data is a core component of Zero Trust Architecture. Zero Trust Models encourage a shift to "data-centric" approaches to cybersecurity. Organizations should inventory, categorize, and protect data at rest and in transit, prioritizing protections for the most critical data assets. Select a technology vendor below to learn more about their products for the Data Pillar of Zero Trust:

Adobe	ANJUNA	appgate	AvePoint	Commvault	DELL Technologies
DIGITAL GUARDIAN	ENTRUST	Fortanix	GOLD COMET	Informatica	mimecast
netskope	noname	PATERO QUANTUM SECURE COMMUNICATION	rubrik	Secude	THALES
Trellix	Trustwave Government Solutions	VAST FEDERAL	VERITAS	vmware by Broadcom	

Visibility & Analytics

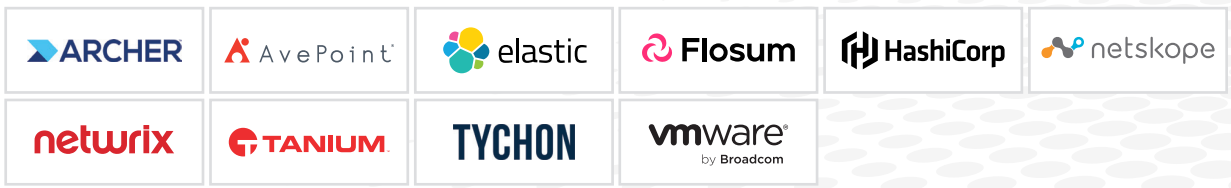
Visibility and Analytics are core components of Zero Trust Architecture. Zero Trust models require inventory and analysis of user activity, devices on the network, network traffic, application health and security, and critical data assets. Select a technology vendor below to learn more about their products for the Visibility and Analytics Pillar of Zero Trust:

Automation & Orchestration

Automation and Orchestration are core components of Zero Trust Architecture. Zero Trust models deploy automation and orchestration of identity credentials, devices provisioning and access, network change management, application hosting, and enforcement of data management policy. Select a technology vendor below to learn more about their products for the Automation and Orchestration Pillar of Zero Trust:

Governance

Governance is a core component of Zero Trust Architecture. Zero Trust models demand audit and enforcement of policies for identity and permissions, device posture and lifecycle, network discovery and traffic, software development and application delivery, and data protection. Select a technology vendor below to learn more about their products for the Governance Pillar of Zero Trust:



The Defender's Advantage

A guide to activating cyber defense

Get your copy
of the ebook today:
carah.io/DefendersAdvantage

Google Cloud

Success Stories

FORESCOUT

Defense Information Systems Agency Selects Forescout to Protect Millions of Mission Critical Devices Across Global Networks

Forescout Technologies, Inc., the leader in Enterprise of Things security, announced the Defense Information Systems Agency (DISA) awarded its channel partner Carahsoft a contract for Forescout licenses to expand cybersecurity across its global enterprise as the initial phase of a multi-million dollar contract award through 2020. Through a phased approach, DISA chose Forescout technology as the foundation of the DoD's "Comply to Connect" (C2C) initiative, a security framework to provide the highest level of assurance for authentication, authorization, compliance assessment and automated remediation of devices connecting to the DoD Information Network (DoDIN).

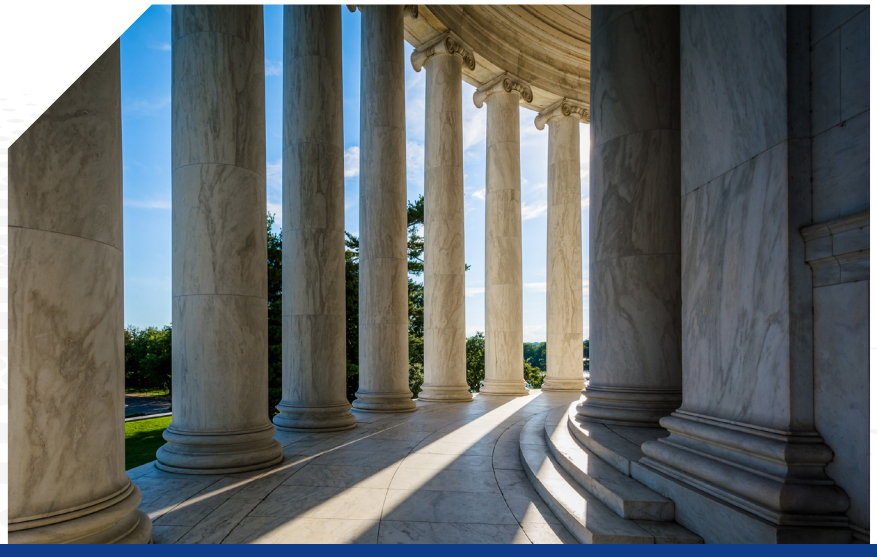
The Challenge:
C2C is a cybersecurity initiative that ensures trusted, authorized devices are rigorously inspected for malicious code, prohibited software, noncompliance and other risks. This wider array of mission-critical systems defined by U.S. Cyber Command and protected by Forescout includes Internet of Things (IoT) devices and Platform Information Technology (PIT) such as industrial control systems (ICS), weapons systems, autonomous vehicles and medical gear.

The Solution:
Forescout has supported the C2C program from its pilot and early adopter phases at DoD enterprises including DISA, the Marine Corps, the Navy's Next Generation Enterprise Network (NGEN) and Army Medical Command (MEDCOM). These first C2C pilots have also proven efficiencies in their administration workflows through Forescout's policy-based orchestration with existing security and management tools.

Key Takeaways:
Forescout Technologies, Inc. actively defends the Enterprise of Things by identifying, segmenting and enforcing compliance of every connected thing. Fortune 1000 companies trust Forescout as it provides the most widely deployed, enterprise-class platform at scale across IT, IoT and OT managed and unmanaged devices. Forescout arms customers with more device intelligence than any other company in the world, allowing organizations across every industry to accurately classify risk, detect anomalies and quickly remediate cyberthreats without disruption of critical business assets. Don't just see it. Secure it.

"We are proud and excited to be at the core of helping the DoD transition to complete visibility and continuous monitoring of its many large and complex networks and millions of devices"

Greg Clark, *Chief Executive Officer and Co-Chairman of the Board*, Forescout



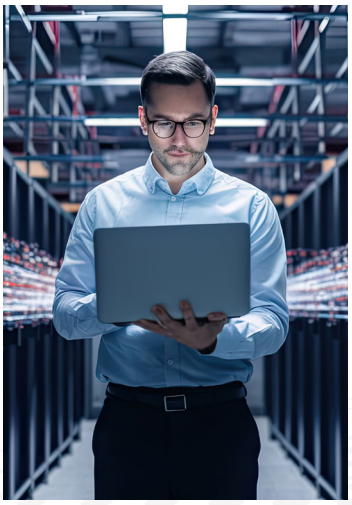
FORTINET FEDERAL

West Virginian County Commission Helps Keep Local Public Service IT Systems Up and Running with Fortinet

The Berkeley County Commission is the governing body of Berkeley County, West Virginia. The county is also the fastest growing in West Virginia. The county's budgets have increased, too, from $26 million in 2005 to around $52 million in 2023. The Berkeley County Commission manages these funds and distributes them to the county's constitutionally elected offices.

The Challenge:
Since 2007, the commission's duties have also included providing IT services to Berkeley County's local government departments and agencies. Gary Wine, Berkley County Department of IT Director of IT, outlines some challenges facing the County of Berkeley Commission: "As the county has grown, so too has the demand on our team, which is today responsible for infrastructure and desktop support as well as cybersecurity."

The main concern for the Berkeley County Commission is that its network remains available at all times. Wine says, "If our network fails, that could mean that 911 calls cannot get answered or a heart monitor in an ambulance is stopped from sending pre-arrival patient data to our hospitals.



> *"As the county has grown, so too has the demand on our team, which is today responsible for infrastructure and desktop support as well as cybersecurity."*
>
> Gary Wine
> *Berkley County Department of IT Director of IT*

The Solution:
The commission has been addressing this challenge through Fortinet cybersecurity solutions for around six years. "We moved onto the Fortinet platform because our legacy firewalls were difficult to manage," comments Wine.

Today, the county has deployed four FortiGate NGFWs in its core network and 40 in high-availability pairs for redundancy and resiliency at 20 remote locations. The FortiGate NGFWs help protect the county's network from threats and enable secure VPN connectivity to remote sites.

Thanks to the FortiGate NGFWs, the Berkeley County Commission has significantly improved its security posture, helping protect its network from web-based threats. The solution is also helping to increase the resilience of the county's network.

While the FortiGate NGFWs are benefitting the county, integrating the devices with the FortiAnalyzer service is what really sets the solution apart. As a result, FortiAnalyzer is unlocking valuable insights that are helping the country improve its security footing.

Key Takeaways:
"Implementing FortiEDR is probably one of the most important things we have done in terms of security," says Wine. "It is something that no business can do without," Wine adds. "Its performance has been phenomenal. FortiEDR has been critical in identifying when a file should not run and creating an opportunity for us to resolve a potential problem before it ever got started. Add the fact that it is backed up by a SOC [security operations center] that is monitored around the clock, and you have a solution that pays for itself in no time at all."

Working with Fortinet, the Berkeley Country Commission improved the security and resilience of its network, helping to ensure that local services are delivered as citizens require. Wine concludes: "Fortinet has created a great security architecture for the county and the agencies we support. We see our relationship continuing long into the future."

carahsoft

Scan the QR to view full success story

FORESCOUT

Keep Government Operations Secure, Available & Compliant

Zero trust relies on real-time visibility of the attack surface. The Forescout Platform continuously identifies, protects and ensures the compliance of all managed and unmanaged cyber assets – IT, IoT, IoMT and OT – with least privileged access.

CONTROL LATERAL MOVEMENT
through the network with traffic flow analysis and advanced segmentation management

PRIORITIZE RISKS
and contain the weakest links before attackers do

MITIGATE THREATS
by staying ahead, own compliance, and avoiding the aftermath

Leave No Asset Unseen, *Especially The Unmanaged Ones*

The Forescout Platform provides seamless context sharing and granular workflow orchestration via ecosystem partners, helping you more effectively manage cyber risk and mitigate threats inside a Zero Trust framework.

Comply and Connect

Operate on agency-issued devices and guest devices to provide a clear view of every endpoint that touches a system. Devices that meet internal standards can connect. Those that don't are flagged and remediated.

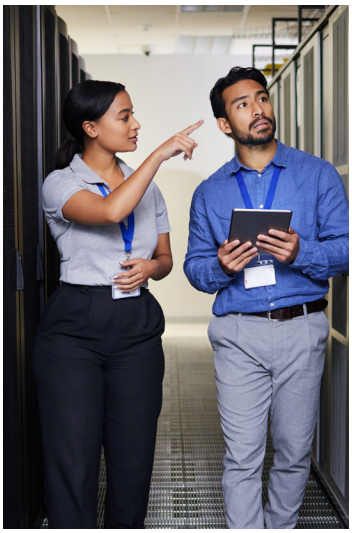
www.forescout.com/zerotrustforgov


Zero Trust
Security
Because people are the new perimeter
The traditional four walls that protected an organization's data no longer exist: More people are accessing more resources, and from more locations, than ever before. Learn how government agencies can utilize Okta as the foundation for a successful Zero Trust program now, and in the future.
Learn more at
okta.com/FedZeroTrust
okta

okta

ManTech simplifies the federal Cybersecurity Maturity Model Certification audit process with Okta

ManTech supports the Department of Defense (DoD) by adhering to stringent security requirements. To meet these demands, including the Cybersecurity Maturity Model Certification (CMMC), the company leveraged Okta to centralize identity management and simplify compliance processes.



The Challenge:
As a Federal Systems Integrator (FSI), ManTech operates in defense, intelligence, and federal civilian sectors, where it is crucial to meet stringent security standards. Compliance with the latest CMMC 2.0 model involves auditing 14 security control families and 110 security controls to ensure federal data protection. Legacy systems for Identity management posed challenges, including inefficiency, rigid processes, and lack of connectivity, making navigation cumbersome and threatening both security and productivity.

The Solution:
ManTech partnered with Okta to centralize its Identity management system, enabling a secure and seamless experience while meeting compliance requirements. Okta's cloud-native technology eliminated inefficiencies and provided a unified solution for managing Identity. Features like Universal Directory and Okta Identity Engine reduced audit times, such as completing a two-day task in just 45 minutes. Automation tools streamlined provisioning, saving engineers over 20% of their time, while granular controls restricted data access to approved devices, enhancing security.

Key Takeaways:

- **Centralized Identity Management:**
  Streamlined compliance and improved security posture by adopting a unified platform with Okta
- **Efficiency in Compliance:**
  Reduced audit times and satisfied key federal compliance standards efficiently.
- **Enhanced User Experience:**
  Improved employee experience with Single Sign-On and passwordless login options through FastPass.

The D.C. Government Enables Secure Internet and App Access with Zscaler Switching From Legacy VPNs to Zero Trust to Improve Protection and Consolidate Security

The Government of the District of Columbia (D.C. Government) oversees 70+ agencies. These include all city services, public property, police and fire protection, and more.

The Challenge:

- VPNs extended their network to end users' computers and networks, putting agency data at risk
- Sending traffic through these tunnels was an exhausting process that taxed internal systems
- Legacy security architecture did not give admins visibility into or control over their environment

The Solution:

- Enabled secure internet access by sending user traffic directly through the Zero Trust Exchange
- Transitioned 15,000+ users away from traditional VPN, with all internal applications published through ZPA in order to ensure consistent security
- "The partnership with Zscaler has been invaluable for us. We deployed the platform at record speeds, onboarded users more effectively and enhanced the user experience." - Suneel Cheruluri, CISO, D.C. Government

Key Takeaways:

- Improves user experience by simplifying the agency's environment and seamlessly integrating with existing identity solutions
- Prioritizes governance and risk management, with emphasis on how AI-powered solutions can reduce risk

Versa Networks Selected by DISA's Thunderdome Program to Deliver SD-WAN and Zero Trust Access

Zero Trust is considered the future of security for protecting networks, systems, and data across both commercial and public sector organizations. The U.S. Department of Defense (DoD) has been making significant strides in modernizing its cybersecurity infrastructure in response to a presidential mandate to adopt Zero Trust architecture. One of the key initiatives driving this transformation is Thunderdome, a Zero Trust network access and application security architecture developed by the Defense Information Systems Agency (DISA).

Versa Networks has been selected to provide SD-WAN, Zero Trust access, and Customer Edge Security Stack (CESS) functions for Thunderdome. These functions together deliver a Zero Trust Edge capability to secure network access for both remote and on-network users.

The Challenge:

The U.S. federal government's transition towards Zero Trust has accelerated due to a growing cyber threat landscape. President Biden's 2021 "Executive Order on Improving the Nation's Cybersecurity" emphasized the need to modernize cybersecurity practices and adopt a Zero Trust Architecture.

In response, the U.S. Department of Defense (DoD) unveiled its Zero Trust Strategy and Roadmap, intending to implement these capabilities by FY27. Within the DoD, the Defense Information Systems Agency (DISA) provides command, control, information-sharing capabilities, and a globally accessible enterprise information infrastructure. In 2021, DISA delivered the initial Zero Trust cybersecurity reference architecture to help the military maintain information superiority on the digital battlefield.

Thunderdome is DISA's cutting-edge Zero Trust network access and application security architecture. It combines a range of technologies, including Identity Credentials and Access Management (ICAM), Secure Access Service Edge (SASE), and software-defined networking and security tools to offer unmatched protection and reliability.

The Solution:
Versa Networks has been selected to provide Zero Trust Edge capabilities within Thunderdome, including SD-WAN, Zero Trust access, and CESS functions. This milestone marks a significant achievement for Versa, and Kelly Ahuja, CEO of Versa Networks, expressed excitement about being part of Thunderdome.

Traditional network and security infrastructure has relied on a best-of-breed approach, stitching together multiple point products, leading to higher complexity and cost. Versa's Zero Trust Edge offers a platform-based strategy with Versa Unified SASE. This Zero Trust foundation leverages a single platform to deploy networks, with built-in threat and data protection and AI embedded in every edge. This results in faster, more comprehensive, and less error-prone threat detection, with a better user and application experience.

Versa has partnered with Booz Allen Hamilton, which was awarded a follow-on production other transaction authority (OTA) agreement for the at-scale deployment of Thunderdome. Under this agreement, Booz Allen will broadly implement and operate Thunderdome's Zero Trust network access and application security architecture.

Key Takeaways:
In an age where cybersecurity threats are ever-evolving, Thunderdome's innovative approach to delivering Zero Trust across the Department of Defense Information Network is paving the way for a more secure and resilient U.S. DoD. Versa Networks is proud to have been selected to support this important mission.

carahsoft

Scan the QR to view full success story

Advancing Government Security Through Innovation

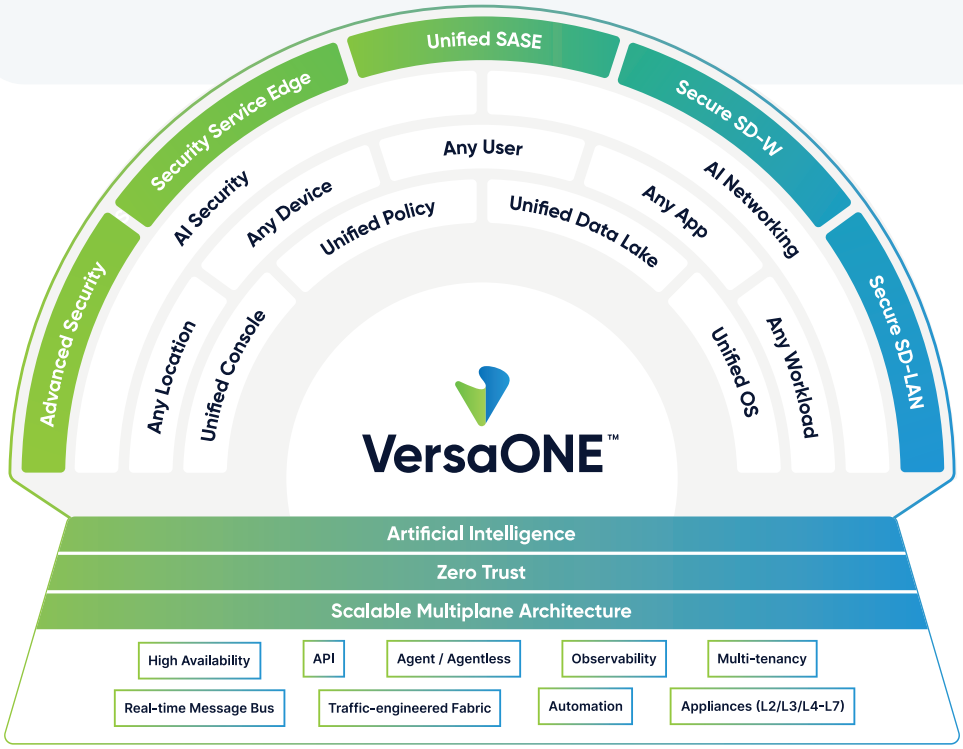
Government agencies face unique challenges in securing critical operations. VersaONE delivers a unified, AI-powered solution designed to protect, connect, and streamline your mission.

- **Secure Every User, Device, and Location.**
From federal networks to remote offices, VersaONE ensures seamless connectivity with unified policy, data, and control, tailored for the public sector's complex needs.

- **Zero Trust. Absolute Confidence.**
Built on Zero Trust principles, VersaONE empowers agencies to prevent threats, simplify compliance, and protect sensitive data without compromise.

- **Scalable Solutions for the Public Sector.**
Engineered for adaptability, VersaONE supports high availability, automation, observability, and advanced security to help agencies stay mission ready.

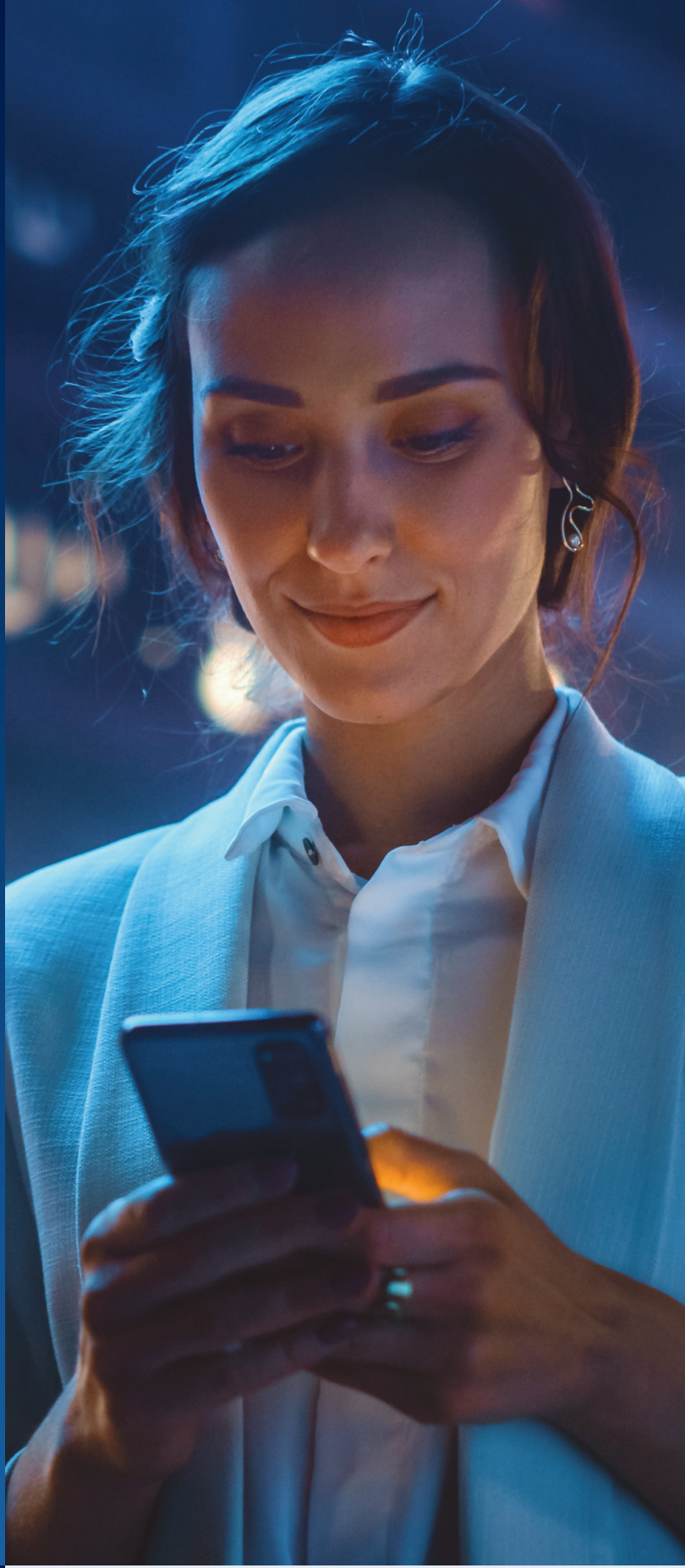
Elevate your cybersecurity strategy with a platform that delivers on the promise of innovation and resilience. Trust VersaONE to support your mission.



Learn More

zscaler™

Secure. Simplify. Transform.



Protect your agency with the most accredited security cloud in the world. FedRAMP Moderate and High, DoD IL5 and StateRAMP authorized.

- Protect data from cyberthreats
- Reduce IT cost and complexity
- Improve user experience
- Meet mandates with confidence

FedRAMP

StateRAMP

Learn more at
zscaler.com/federal

Integration with Modern Tools

Zero Trust incorporates security solutions such as Endpoint Detection and Response (EDR), cloud access security brokers (CASBs), and Security Information and Event Management (SIEM) tools to continuously evaluate risk and enforce security policies. There is no single Zero Trust solution, but rather a culmination of solutions that work together to protect against evolving cyber vulnerabilities.

Zero Trust Solutions Chart

The pillars of Zero Trust are comprised of numerous security components. The following charts identify the cybersecurity technologies needed to properly protect each of the Zero Trust pillars.

<table>
<tr><th>Identity</th><th>Device & Endpoint</th><th>Network & Environment</th><th>Application & Workload</th><th>Data</th></tr>
<tr><td>User Authentication</td><td>HW & SW Inventory</td><td>API Integration</td><td>DevSecOps</td><td>Data Loss Prevention</td></tr>
<tr><td>User Authorization</td><td>Device Authentication</td><td>Fully Encrypted Traffic</td><td>Application Delivery</td><td>Data Classification</td></tr>
<tr><td>Cybersecurity Access Policy</td><td>Device Authorization</td><td>Common Service Access</td><td>Micro Segmentation</td><td>Metadata Management</td></tr>
<tr><td>Privilege Access Management</td><td>Compliance Enforcement</td><td>Network Segmentation</td><td>Application Segmentation</td><td>Data Encryption</td></tr>
<tr><td>Single Identity Platform</td><td rowspan="2">Cloud-based Software Deployment & Management</td><td>Cloud Access Security Broker (CASB)</td><td>Software Chain Supply</td><td>Data Segmentation</td></tr>
<tr><td>MFA</td><td>Software Defined Networking (SDN)</td><td>Software Defined Compute</td><td rowspan="3">Dynamic Data Masking (DDM)</td></tr>
<tr><td>In-Session Monitoring</td><td rowspan="2">Cloud-based Baseline Enforcement</td><td rowspan="2">Software Defined Perimeter (Access to Apps and Data)</td><td rowspan="2">Approved/ Prohibited List</td></tr>
<tr><td>ABAC</td></tr>
<tr><td>Key Management</td><td rowspan="2">Intelligence for Endpoint Response</td><td>Application Proxy</td><td>Application Visibility & Access</td><td>Fully-automated Data Tagging via ML/AI</td></tr>
<tr><td>Transparent Authentication</td><td>Management and Monitoring</td><td>3rd-Party Application Testing</td><td>Data Rights Management (DRM)</td></tr>
</table>

Visibility & Analytics	Automation and Orchestration	Governance
Discovery & Baselining	API Standards	Threat Score
Machine Learning	Incident Response	Risk Score
Advanced Threat Protection	Artificial Intelligence	Target Valuation
Monitoring and Auditing		Triage Priority
Risk Evaluation & Dynamic Risk Scoring	Security Orchestration, Automation & Response (SOAR)	Compliance Score (snapshot & trends)
Security and Information Event Management (SIEM)		

Customer Impact

As a customer, the systems you interact with are likely using a combination of these tools to ensure continuous monitoring and security, giving you peace of mind that threats are being detected and mitigated promptly.

CROWDSTRIKE

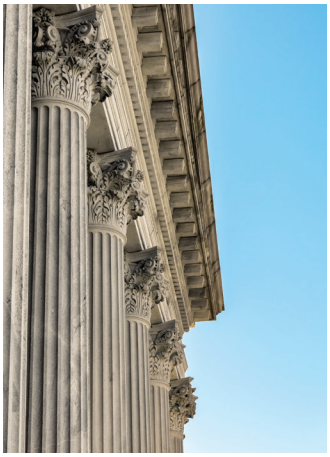
Over 80% of breaches involve compromised credentials, making identity the #1 attack vector.

CrowdStrike helps government agencies enforce Zero Trust with AI-powered solutions to stop identity-based threats.

LEARN MORE

www.crowdstrike.com

Zero Trust Progression



08. 2020

NIST published NIST.SP.800-207

05. 2021

Biden signs Executive Order 14028 on Improving the Nations Cybersecurity

08. 2021

CISA initially released Zero Trust Maturity Model (ZTMM) Version 1.0

03. 2022

Response feedback closed related to ZTMM

05. 2022

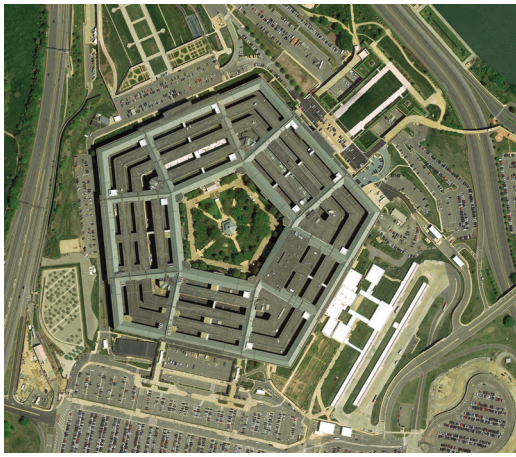
NIST published NIST.SP.800-161-r1

04. 2023

CISA releases Zero Trust Maturity Model Version 2.0

08. 2024

Deadline for Federal Civilian agencies to implement ZTA



06. 2024

DOD have implemented 91 out of the 152 target activities from the DOD's Zero Trust Strategy

08. 2027

DOD expected to reach "target level" of implementation

Computer Hardware Built for Zero Trust Architecture

ClearCube Zero Clients & Secure Endpoints That Allow Zero Trust Principles to Safeguard Your Full Environment, All the Way to End User Devices

ClearCube can help you:

Understand Zero Trust.
Assess endpoint needs.
Explore solutions.
Find the right fit.
Test easily.
Get expert implementation support.

ClearCube Technology:

TAA-compliant devices
Endpoint solution expertise
Proven innovation since 1997
U.S.-based support
Experience with latest tech

It's easy to get started with ClearCube:

1. Scan the QR code and book 15 minutes to discuss your needs
2. Receive a summary of options, expert recommendations, and a quote
3. Complete the bid and purchasing processes
   Receive your equipment, ready to deploy and with a team ready to support you

Book a Call

Clearcube.com
sales@clearcube.com
512-652-3500

CLEARCUBE

paloalto NETWORKS | PUBLIC SECTOR

We Don't Sell Products
We Sell Solutions

Learn how Palo Alto Networks can help your agency with its Zero Trust Journey.

Scan to learn more

Policies and Executive Orders


2017
Binding Operational Directive to Enhance Email and Web Security (BOX 18-01): Define Technical Security Requirements
2020
Memorandum on Improving Vulnerability Identification, Management, and Remediation (M-20-32): Define Vulnerability Research Program Requirements
Memorandum on Completing the Transition to Internet Protocol Version 6 (M-21-07): Define Ipv-6 Requirements
NIST Zero Trust Architecture (NIST.SP.800-207): Define Zero Trust Capabilities
2021
NIST Guidelines on Minimum Standards for Developer Verification of Software (NIST IR 8397): Define Developer Testing Requirements
Memorandum on Protecting Critical Software Through Enhanced Security Measures (M-21-30): Define Critical Software & Requirements
DoD Zero Trust Reference Architecture: Define Zero Trust Capabilities
Memorandum on Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31): Define Investigation & Remediation Requirements
Executive Order on Improving the Nation's Cybersecurity (EO 14028): Direct to Use Cloud & Do Zero Trust
2022
Memorandum on Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (M-22-18): Enhance Security of Software Supply Chain
NIST Secure Software Development Framework (SSDF) Version 1.1 Recommendations for Mitigating the Risk of Software Vulnerabilities (NIST SP 800-218): Risk Mitigation of Software Vulnerabilities
NIST Cybersecurity Supply Chain Risk Management for Systems and Organizations (NIST SP 800-161r1): Cybersecurity Supply Chain Risk Management Practices
CISA Cloud Security Reference: Define Security for Cloud
CISA Zero Trust Maturity Model: Define Zero Trust Maturity
Memorandum on Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (M-22-01): Direction to Do EDR
Memorandum on Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (M-22-09): Define Zero Trust Strategy
NIST Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products (NIST CSWP 24): Labeling for Consumer IoT Products
2023
Memorandum on Migrating to Post-Quantum Cryptography (M-23-02): Migrating to Post Quantum Cryptography
Blinding Operational Directive on Improving Asset Visibility and Vulnerability Detection on Federal Networks (BOD 23 01): Asset Visibility and Vulnerability Detection

NIST Zero Trust Architecture (NIST.SP.800-207)

The National Institute of Standards and Technology (NIST) introduced NIST.SP.800-207 in August 2020. The publication defines Zero Trust capabilities and additionally provides guidance on migrating to a Zero Trust Architecture (ZTA). Use cases for ZTA examined include enterprise with satellite facilities, multi-cloud/cloud-to-cloud enterprise, enterprise with contracted services and/or nonemployee access, collaboration across enterprise boundaries, and enterprise with public or customer-facing services.

Executive Order 14028

Executive Order 14028 "Improving the Nation's Cybersecurity," released in May 2021, is the most influential piece of federal Zero Trust policy yet. The executive order directed agencies to implement Zero Trust Architecture and strengthen the software supply chain. It required service providers to report cyber incidents and threat information that could impact the government, instructed the NIST to publish standards for testing of vendor software source code, and created cybersecurity event log requirements for Federal departments and agencies.

Executive Order 14144

Executive Order 14028, published on May 12, 2021, provided essential foundational steps to strengthening cybersecurity within the United States and emphasized the importance of Zero Trust Architecture (ZTA). Building upon EO 14028, The Biden Administration issued Executive Order 14144 Strengthening and Promoting Innovation in the Nation's Cybersecurity on January 16th, 2025, to address the rapid evolution of cyber threats, notably those from foreign nations. The order is focused on defending digital infrastructure, securing the services and capabilities most vital to the digital domain, and building the capabilities necessary to address key threats.

NSM-8

The National Security Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems (NSM-8) was released in January 2022. The memorandum required the Committee on National Security Systems create guidance on minimum security standards for cloud migration and operations for National Security Systems (NSS). Executive departments and agencies owning an NSS must update agency plans related to cloud technology. Multifactor authentication and encryption for NSS data-at-test and data-in-transit is required for executive departments and agencies. Agencies must also report unauthorized access to NSS

M-22-09

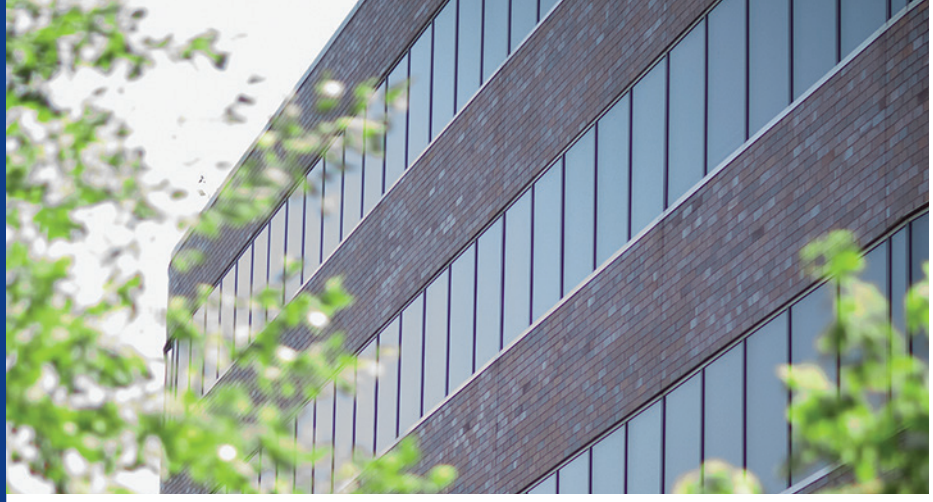
The Memorandum on Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, published in January 2022, set a Federal ZTA strategy and set additional deadlines for Federal agencies.

This memo is intended to provide a roadmap for agencies to achieve specific Zero Trust security goals, by implementing the five pillars of Zero Trust developed by the Cybersecurity and Infrastructure Security Agency (CISA), which includes Identity, Devices, Networks, Applications and Workloads, and Data by the end of FY24. The order identified top cybersecurity priorities, including the consolidation of agency identity systems, and treating all internal networks as untrusted.

BOD 23-01

CISA issued the Binding Operational Directive 23-01 (BOD 23-01) in October 2022. The directive requires Federal Civilian and Executive Branch (FCEB) agencies perform automated asset discovery every seven days, initiate vulnerability enumeration on all assets every fourteen days, apply automated upload of vulnerability enumeration results to the CDM Agency dashboard within seventy-two hours of completion, and maintain capability to perform on-demand vulnerability discovery and enumeration within seventy-two hours of CISA's request and make results available within seven days of the request.

While BOD 23-01 only applies to FCEB, CISA recommends that all organizations implement the guidance to protect critical infrastructure from exploitation of unknown or under protected weaknesses.



Contract Vehicles

Carahsoft offers a number of contract options for purchasing Zero Trust solutions. Our contracts offer purchasing options for civilian, defense, state, and local government customers. Customers can purchase solutions off of these major contract vehicles:

GSA Multiple Award Schedule (MAS)

Carahsoft holds a GSA Multiple Award Schedule (MAS) that allows customers to procure a wide variety of Zero Trust solutions. Carahsoft holds Contract #47QSWA18D008F and allows customers to purchase everything from identity to automation & orchestration solutions.

ITES-SW2

The purpose of the ITES-SW 2 acquisition is to support Army, Department of Defense (DoD) and all Federal Agency enterprise Information Technology (IT) infrastructure and info-structure goals by leveraging Commercially available-Off-The-Shelf (COTS) software products and maintenance in 14 product categories in addition to related incidental services and hardware.

NASA SEWP V

The NASA SEWP V GWAC (Government-Wide Acquisition Contract) provides the latest in Information Technology (IT) products and product-based services for all Federal Agencies. SEWP provides the best value and cost savings through innovative procurement tools and processes; premier customer service and outreach; and advocation of competition and cooperation within the industry.

NASPO ValuePoint Cooperative Purchasing Organization

The NASPO ValuePoint Cooperative Purchasing Organization (formerly WSCA-NASPO) provides the highest standard of excellence in public cooperative contracting. By leveraging the leadership and expertise of all states with the purchasing power of their public entities, NASPO ValuePoint delivers best value, reliable, competitively sourced contracts.

Since 1993 NASPO ValuePoint has been the cooperative purchasing arm of NASPO (the National Association of State Procurement Officials) encouraging, fostering and guiding the nation's most significant public contract cooperative. NASPO ValuePoint is a unified, nationally focused cooperative aggregating the demand of all 50 states, the District of Columbia and the organized US territories, their political subdivisions and other eligible entities spurring best value, innovation and competition in the marketplace.

OMNIA, Partners – Cobb County

Carahsoft holds an OMNIA Partners, Cobb County, GA Technology Products, Solutions and Related Services contract (#23-6692-01) that provides full access to a portfolio of value-driven contracts, spend visibility analytics, and subject matter experts.

OMNIA, Partners – Education Software Solutions and Services

Carahsoft Technology Corp., The Trusted Government IT Solutions Provider®, today announced that it has been awarded a Region 4 Education Service Center (ESC) contract (#R191902) for Educational Software Solutions and Services available now through OMNIA Partners. This contract makes these solutions available to state and local government agencies, education institutions, non-profits, municipalities, and additional public sector organizations through Carahsoft and authorized reseller partners.

Educational Software Solutions and Services are available through this contract and Carahsoft's reseller partners to public sector organizations in all 50 U.S. states and the District of Columbia, and the contract is established for a five-year period of performance through April 30, 2025. All solutions on this contract are offered at special discounts off their manufacturer list price, and additional price reductions can be provided on a deal-by-deal basis.

Explore the benefits of how you can count on Carahsoft and our Reseller Partners

- 24x7 availability call us at 888-662-2724
- Dedicated support specializing in serving enterprise ready solutions
- Ecosystem of value-added reseller partners
- Contract Expertise: We understand your procurement needs and the outcomes you're seeking
- Quick turnaround quote: Get the IT solutions you need with the fast, accurate service you deserve
- Substantial cost savings on Zero Trust products and service portfolio from certified technology brand partners
- Advanced technology solutions including Identity, Device, Network, Application Workload, Data, Visibility and Analytics, Automation and Orchestration and Governance.

splunk>
a CISCO company

Simplify Zero Trust with Splunk

Splunk plays a pivotal role in enabling Zero Trust by providing the necessary tools for:

- Comprehensive visibility across hybrid and multi-cloud environments.
- Real-time monitoring, threat detection, and analytics to identify and respond to security incidents.
- Automation of security tasks to reduce complexity and improve response times.
- Support for compliance by ensuring proper logging, reporting, and monitoring of all access points and activities.

By leveraging Splunk, organizations can implement a robust Zero Trust framework while overcoming the challenges of complexity, cost, and compliance.

Upcoming Events

The Digital Government Institute's (DGI) Zero Trust Implementations Lessons Learned Workshop

April 24, 2025 | Virtual

The workshop will cover key topics such as the foundational principles of Zero Trust, step-by-step implementation strategies, and the unique considerations and obstacles faced by government entities. Whether you are in the planning stages or looking to refine your existing security measures, this session will provide you with the necessary knowledge and tools to navigate the complexities of Zero Trust architecture.

Featured at the Workshop will be government speakers such as Brian McKenney, Sr Cyber Security, Cyber Solutions Center from Mitre.

Scan the QR
to register now

CyberSmart 2025: From A to Z

April 3, 2025 | Reston, VA

Federal agencies understand that cybersecurity has to be the foundation of their operations, from online to back office.

For instance, the telecommunications breach by Salt Typhoon, a Chinese government-backed hacking group, targeted both U.S. political leaders and national security information. First detected in early summer, in December the Cybersecurity and Infrastructure Security Agency (CISA) said at a press conference there is no way to estimate how long it will take for the hackers' access to be shut down.

One major challenge for agencies is how to meet these requirements while looking for ways to incorporate new technologies that can streamline their operations. The biggest example of this is the explosive advent of artificial intelligence (AI) as a tool that agencies are tasked to incorporate.

Scan the QR
to register now

Symantec by Broadcom

Protecting Public Sector Agencies from Advanced Cyberattacks

Gain end-to-end protection across devices, networks, and data while maintaining compliance.

Read the Tech Spotlight

carahsoft

11493 Sunset Hills Road, Suite 100
Reston, Virginia 20190

(571) 591-6111
ZeroTrust@Carahsoft.com

carahsoft.com/solve/zero-trust