Qualys.

WHITEPAPER

A Simple and Effective Approach to Zero Trust Security

Contents

The presidential Executive Order on Improving the Nation's Cybersecurity issued in 2021 declared Zero Trust as a fundamental tenet for securing federal systems and critical infrastructure. In January 2022, the Office of Management and Budget (OMB) published more details about the new federal strategy in Memorandum-22-09, which expanded Zero Trust beyond its original emphasis on identity and access control. The Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model Version 2.0 was published in April 2023 and provides a five-pillar strategy. The Department of Defense (DoD) Zero Trust Reference Architecture, published in July 2022, has similar components but recommends seven pillars.

Implementing Zero Trust

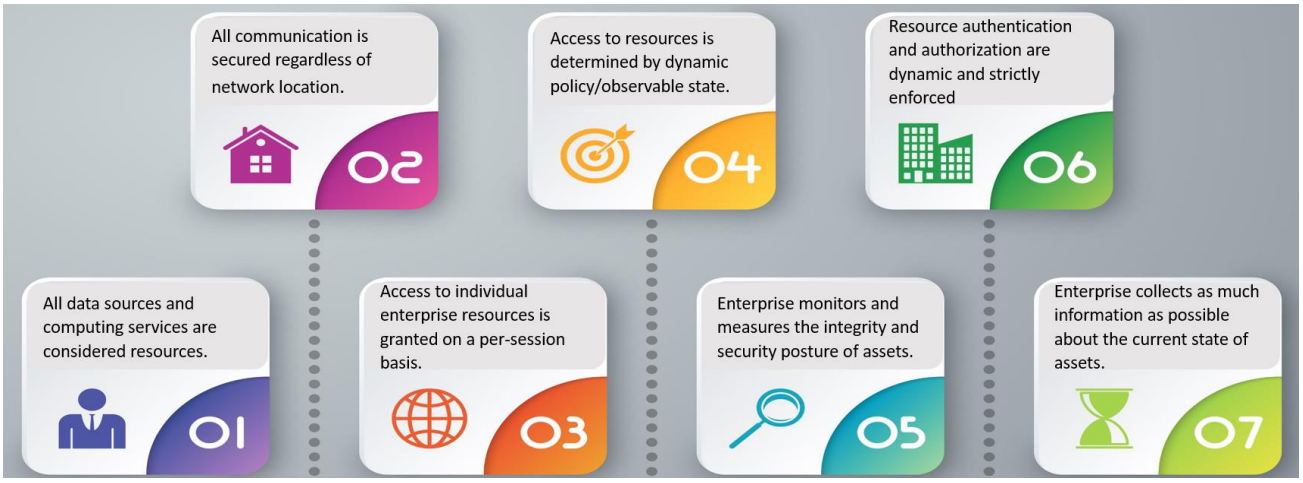
This white paper presents a simple and effective approach to zero trust security. Its precepts follow the lead of the Department of Homeland Security's CISA Zero Trust Maturity Model Version 2.0 and the DoD Zero Trust Maturity Model Version 2.0, as well as the National Institute of Standards and Technology (NIST) Zero Trust Architecture (ZTA) special publication (SP) 800-207. Emphasis has been placed on the CISA model as it offers best practices that provide a less complicated implementation to address the challenges adherent with achieving a zero trust maturity.

While no single vendor or solution addresses all ZTA requirements, this white paper also connects CISA and NIST best practices to a range of security and compliance solutions integrated by the Qualys GovCloud Platform. The integrated platform approach is valuable to both federal agencies and civilian enterprises that are committed to adopting ZTA. Moreover, while many organizations view ZTA as applicable solely to identity and access management (IAM), CISA and NIST guidelines clearly specify going well beyond IAM to adopt a zero trust approach for all endpoints and assets.

Elements of a Zero Trust Architecture

In SP 800-207 (p. 1), NIST defined a broader concept of ZTA as follows: *"A ZT approach is primarily focused on data and service protection but can and should be expanded to include all enterprise assets (devices, infrastructure components, applications, virtual and cloud components) and subjects (end users, applications and other nonhuman entities that request information from resources)."* NIST was reluctant to describe ZTA as a *"single architecture"* and positioned it as *"a set of guiding principles for workflow, system design and operations that can be used to improve the security posture of any classification or sensitivity level."*

Notably, NIST concluded in Appendix B: *"While it is possible to use ZTA strategies to plan and deploy an enterprise environment, there is no single solution that provides all the necessary components. Also, few ZTA components available today can be used for all of the various workflows present in an enterprise."*

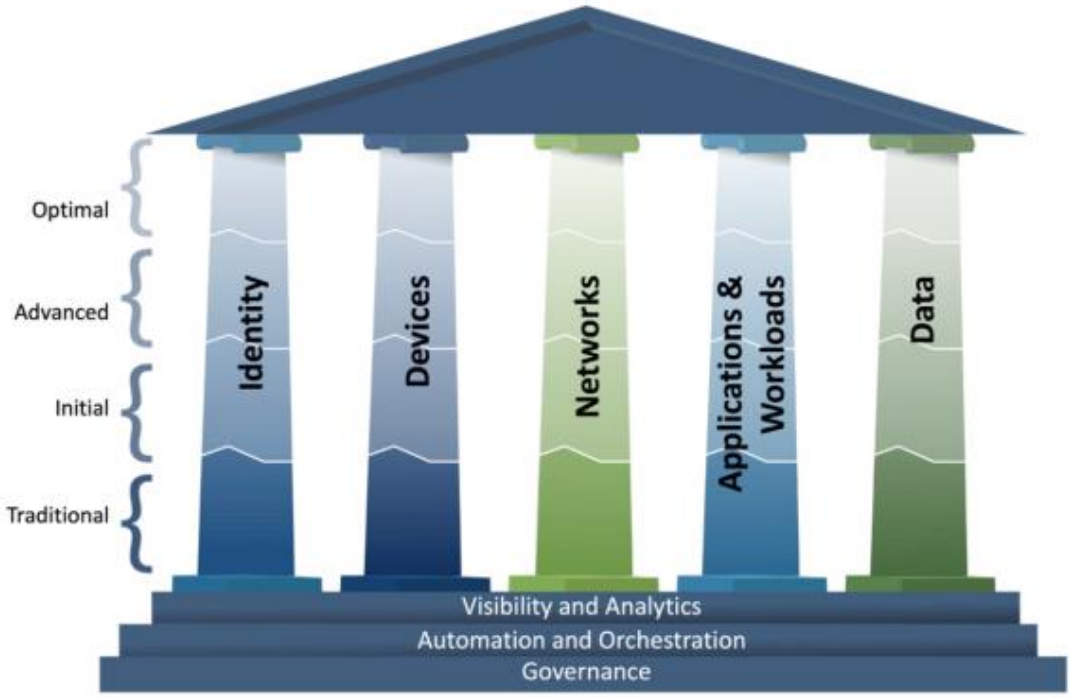


Zero Trust Basic Tenets Defined by NIST SP 800-207 (pp. 6-7). Graphic created by Qualys.

Operationalizing Zero Trust

The directive by the Office of Management and Budget, OMB Memorandum 22-09, instructed federal executive branch agencies to follow the five-pillar strategy of CISA's Zero Trust Maturity Model and comply with various implementation deadlines. Private sector firms are also encouraged to follow these best practices. Specific implementation guidance was included in the Memorandum:

A. **Identity –** Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant multifactor authentication protects those personnel from sophisticated on-line attacks.
B. **Devices** – Agencies maintain a complete inventory of every device authorized and operated for official business and can prevent, detect, and respond to incidents on those devices. This was clarified by CISA BOD 23-01, which specified requirements for continuous discovery of all IP-addressable assets and vulnerability enumeration for all assets.
C. **Networks** – Agencies encrypt all DNS requests and HTTP traffic within their environment and begin executing a plan to break down their perimeters into isolated environments.
D. **Applications and Workloads** – Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.
E. **Data** – Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies take advantage of cloud security services and tools to discover, classify, and protect their sensitive data, and have implemented enterprise-wide logging and information sharing.



CISA Zero Trust Maturity Model Evolution. Graphic courtesy CISA.

Implementation of the model realistically means that during the journey, agencies and other organizations will be at various stages of maturity in terms of incorporating all guidance and best practices for ZTA. The CISA model describes four stages for gauging maturity progress – each centered on the degree of *automation*:

Traditional—manually configured lifecycles (i.e., from establishment to decommissioning) and assignments of attributes (security and logging); static security policies and solutions that address one pillar at a time with discrete

dependencies on external systems; least privilege established only at provisioning; siloed pillars of policy enforcement; manual response and mitigation deployment; and limited correlation of dependencies, logs, and telemetry.

Initial—starting automation of attribute assignment and configuration of lifecycles, policy decisions and enforcement, and initial cross-pillar solutions with integration of external systems; some responsive changes to least privilege after provisioning; and aggregated visibility for internal systems.

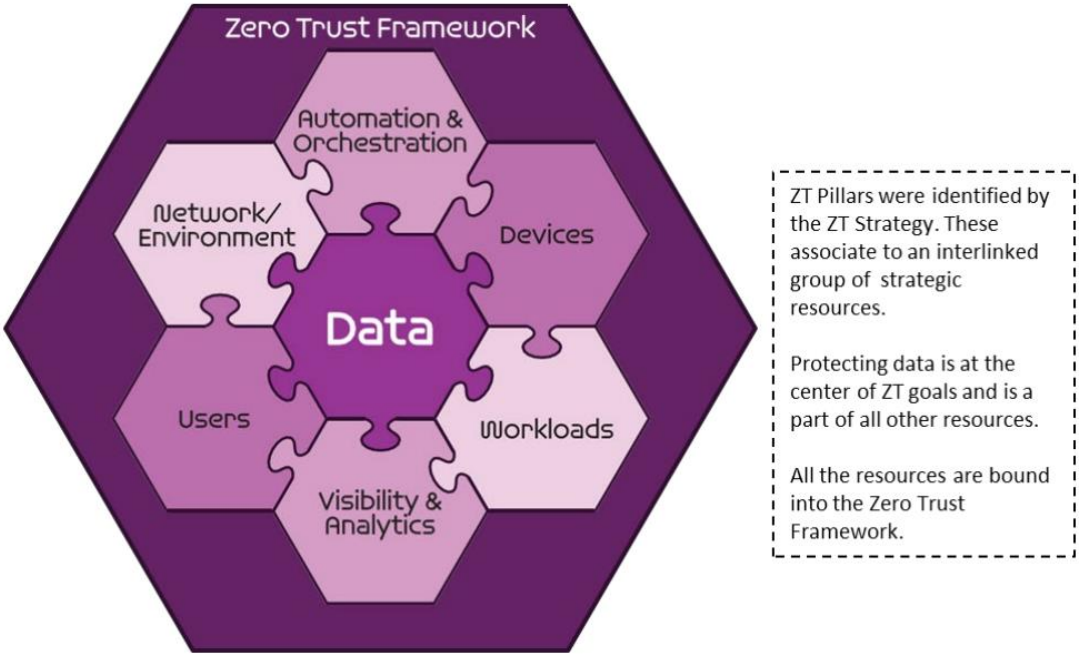
Advanced—wherever applicable, automated controls for lifecycle and assignment of configurations and policies with cross-pillar coordination; centralized visibility and identity control; policy enforcement integrated across pillars; response to pre-defined mitigations; changes to least privilege based on risk and posture assessments; and building toward enterprise-wide awareness (including externally hosted resources).

Optimal—fully automated, just-in-time lifecycles and assignments of attributes to assets and resources that self-report with dynamic policies based on automated/observed triggers; dynamic least privilege access (just-enough and within thresholds) for assets and their respective dependencies enterprise-wide; cross-pillar interoperability with continuous monitoring; and centralized visibility with comprehensive situational awareness.

The CISA model describes three elements that are common for all five pillars. These capabilities support integration of each pillar's functions across the model, and include:

- **Visibility and Analytics**: Visibility refers to the observable artifacts that result from the characteristics of and events within enterprise-wide environments. The focus on cyber-related data analysis can help inform policy decisions, facilitate response activities, and build a risk profile to develop proactive security measures before an incident occurs.
- **Automation and Orchestration**: Zero trust makes full use of automated tools and workflows that support security response functions across products and services while maintaining oversight, security, and interaction of the development process for such functions, products, and services.
- **Governance**: Governance refers to the definition and associated enforcement of agency cybersecurity policies, procedures, and processes, within and across pillars, to manage an agency's enterprise and mitigate security risks in support of zero trust principles and fulfillment of federal requirements.
- As noted earlier, the DoD Zero Trust Framework is similar but prescribes seven pillars:

As noted earlier, the DoD Zero Trust Framework is similar to the CISA framework but prescribes seven pillars:



Department of Defense Zero Trust Framework (DISA). Graphic courtesy DoD.

How Qualys Helps Implement Zero Trust

For government agencies, associated suppliers, and private sector firms with mature Written Information Security Programs (WISPs), Qualys can play a substantial role in facilitating and simplifying the adoption of a comprehensive ZTA maturity model. Our approach simplifies ZTA compliance by using a cloud platform with a single agent to integrate controls expressly for the Devices, Networks, and Applications and Workloads pillars, with broad support for visibility and analytics, automation and orchestration, and governance across the entire model.

ZTA implementation and continuous operations are enabled to an even higher degree by using the Qualys GovCloud Platform, which is one of the only government-focused security and compliance platforms qualified for FedRAMP Ready at the High Impact level, and will soon have an Authorized to Operate (ATO) designation. Qualys was selected by the Department of Homeland Security (DHS) to support 70 federal agencies for its Continuous Diagnostics and Mitigation (CDM) program. The CDM program supports government-wide and agency-specific efforts to provide risk-based, consistent, and cost-effective cybersecurity solutions to protect federal civilian networks across all organizational tiers by:

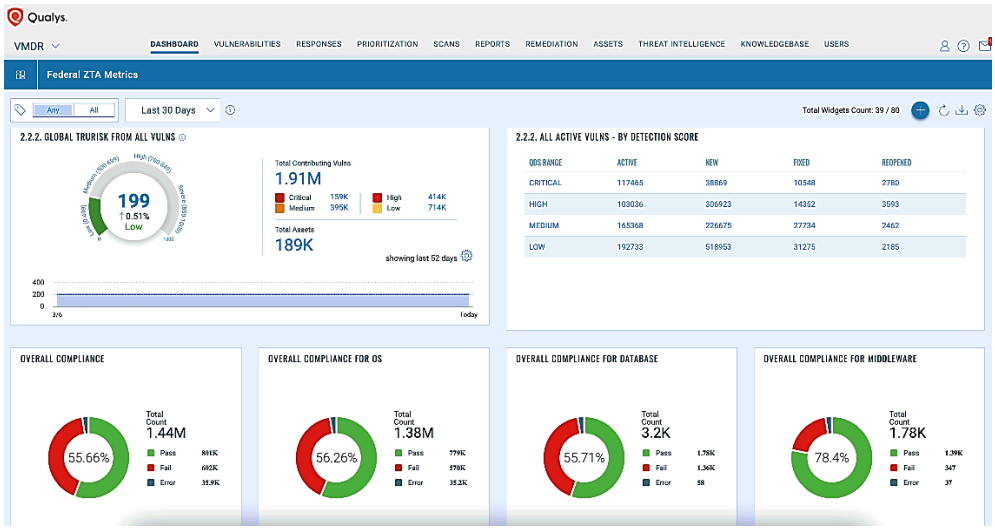
- Reducing agency threat surfaces
- Increasing visibility into the federal cybersecurity posture
- Improving federal cybersecurity response capabilities
- Streamlining Federal Information Security Modernization Act (FISMA) reporting

Mapping the Qualys GovCloud Platform to the DoD Zero Trust Maturity Model. Graphic created by Qualys.

Qualys GovCloud Platform Architecture and Components

The Qualys GovCloud Platform is the most advanced security platform for federal, state, and local agencies, as well as regulated private sector firms that need highly secure zero trust hybrid IT infrastructures to comply with the Zero Trust Security Model and broader mandates for guidelines in NIST Special Publication 800-53 v5 (see below). The Qualys GovCloud Platform is the only FedRAMP Ready status vulnerability management platform fulfilling all 421 High Baseline controls out of 1,007 controls in SP 800-53. The Qualys platform is built with the world's most comprehensive Vulnerability Management (VM) capabilities, including its own asset inventory, threat database, and attack surface management. The apps required for ZTA compliance are delivered via one platform, managed with one dashboard, and deployed with a single agent.

As an integrated solution, the Qualys GovCloud Platform includes four tiers of capabilities that simplify planning, deployment, and continuous ZTA operations for the complex, sophisticated requirements of federal agencies, suppliers, and mature private sector firms.

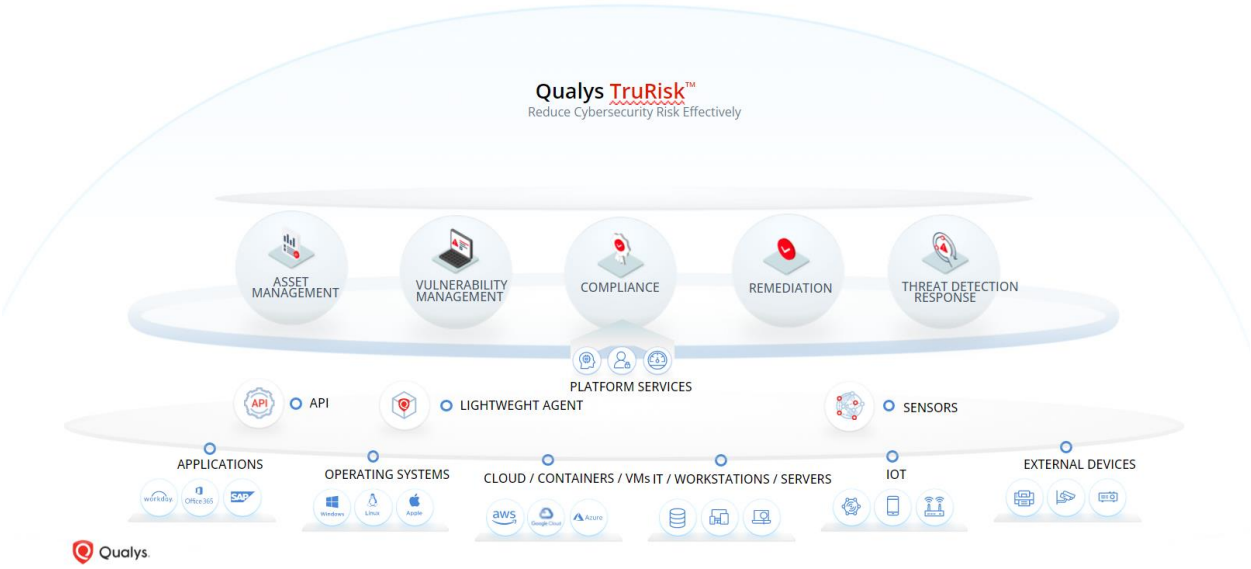


Comprehensive Application Suite – More than two dozen security and compliance applications are fully integrated within the GovCloud Platform. With a single, centralized interface, security and compliance teams are provided with an agency-wide view. Applications focused on ZTA requirements include Vulnerability Management, Detection, and Response (VMDR); Patch Management; VMDR + CyberSecurity Asset Management (CSAM) with Extended Attack Surface Management (EASM); Policy Compliance; File Integrity Monitoring; and Security Assessment Questionnaire.

Analytics and Reporting Engines – Modern security and compliance applications depend on intense operational data analytics, so the Qualys GovCloud Platform integrates the use of eight analytics and reporting engines: Apache Kafka, Ceph, Elastic, Redis, Apache Cassandra, Apache Flink, or a cloud microservice.

Distributed Scalable Sensors / Agents – To collect operational data for analytics, the Qualys GovCloud Platform enables the flexible use of six scalable sensors / agents: infrastructure, virtual, cloud, agent, passive, and API.

Flexible Deployments (Cloud and On-Premises) – Federal agencies can deploy the Qualys GovCloud Platform for cloud and on-premises environments from FedRAMP. Non-government enterprises can deploy to virtual environments including Amazon Web Service, Microsoft Azure, or Google Cloud.



The Qualys Cloud Platform

Mapping Qualys GovCloud to NIST SP 800-53

Many experts consider NIST 800-53 as the ultimate pinnacle to achieve the highest cybersecurity maturity level while also ensuring a zero trust posture. Organizations seeking to attain ZTA should consider achieving full compliance with NIST 800-53 as a worthwhile goal to mitigate security breaches, audit failures, brand damage, and litigation. The below matrix outlines how a dozen Qualys applications, delivered in a single platform with a single agent, can help you meet the requirements for all seventeen of the NIST 800-53 control families.

		Qualys Capabilities											
Sr. No.	NIST 800-53 Control Family	VMDR	PM	EDR	TP	CSAM	PC	CSA	SCA	CS	SEM	SDR	FIM	SAQ
1	Access Control						•	•	•	•	•	•		•
2	Awareness and Training													•
3	Audit and Accountability						•	•	•	•		•		
4	Security Assessment and Authorization			•	•		•	•	•	•				
5	Configuration Management					•	•	•	•	•	•	•		
6	Contingency Planning					•								•
7	Identification and Authentication						•	•	•	•	•	•		
8	Incident Response			•										•
9	Maintenance						•	•	•	•				
10	Media Protection						•	•						•
11	Physical and Environmental Protection													•
12	Planning													•
13	Personnel Security						•	•						•
14	Risk Assessment	•	•											•
15	System and Service Acquisition	•					•	•	•					
16	System and Communications Protection	•		•			•	•	•	•				
17	System and Information Integrity			•									•	

Conclusion

With the Zero Trust Architecture and Model, the U.S. government has set a high bar for securing IT and security environments for federal agencies, suppliers, and many private sector firms. Executive Order 14028 on Improving the Nation's Cybersecurity set national policy for "the prevention, detection, assessment, and remediation of cyber incidents as a top priority and essential to national and economic security." EO 14028 and other mandates prescribe ZTA as a primary path for achieving this policy goal. Requirements cross a broad range of technologies, including Identity, Devices, Networks, Applications & Workloads, and Data. As noted, no single solution addresses all these requirements. However, by using the Qualys GovCloud Platform, organizations can simplify and achieve compliance with a broad swath of ZTA requirements while leveraging many integrated security and compliance solutions with one centralized control center and agent. Whether your organization is a federal agency, supplier, or civilian enterprise with a critical infrastructure, we encourage you to learn more about the Qualys GovCloud Platform and how it can help your organization comply with national policy for cybersecurity by effectively implementing a zero trust architecture and model.

We also invite you to learn more about how you can use Qualys to achieve Zero Trust Maturity by starting your free trial today.

Contributors:

Bill Reed, Qualys Product Marketing

Dave Buerger, Qualys Product Marketing