BROADCOM

WHITE PAPER

From Walls to Webs

Building Zero Trust Architecture for a Connected Government

WHITE PAPER

From Walls to Webs

Building Zero Trust Architecture for a Connected Government

TABLE OF CONTENTS

Executive Summary

The U.S. Federal Government is advancing significant cybersecurity reforms under Executive Order 14028 and Office of Management and Budget (OMB) Memorandum M-22-09. The objective of these reforms is to establish the Zero Trust security model as a foundation to defend against sophisticated cyber threats targeting government missions, infrastructure, and citizen data. Traditional perimeter-based defenses are no longer sufficient. Agencies must continuously authenticate and authorize every user, device, network, application, and transaction. Operations must be performed under the assumption of breach and least privilege at every access point must be enforced.

Federal Zero Trust security mandates require the deployment of phishing-resistant multi-factor authentication, continuous identity management, device compliance assurance, network encryption and segmentation, application access controls, and data protection. Frameworks such as NIST SP 800-207, CISA guidance, and the Federal Zero Trust Data Security Guide specify five architecture pillars: identity, devices, network, applications and workloads, and data. All of these pillars must be supported by automation, visibility, and governance.

Broadcom® solutions empower agencies to meet these mandates comprehensively. Symantec® advanced security platforms and Symantec Identity and Access Management (IAM) solutions deliver strong user authentication, privileged access management, FIDO-compliant MFA, endpoint protection, network segmentation, cloud and edge workload defense, data loss prevention, encryption, and full auditability. Designed to integrate with federal ICAM standards natively, support cloud migration, and automate compliance, these products enable secure IT modernization and ongoing risk reduction.

By aligning product capabilities with federal requirements, Broadcom provides a resilient foundation for agencies to accelerate Zero Trust security maturity, streamline compliance, and protect data and operations confidently in a constantly evolving threat environment.

The Federal Zero Trust Security Imperative

Federal agencies face an unprecedented surge in sophisticated cyber threats targeting mission-critical systems, citizen data, and government services. Traditional perimeter-based security models, reliant on hardened network boundaries, can no longer effectively protect against advanced attackers, insider threats, and supply chain vulnerabilities. Recognizing this critical challenge, the U.S. government has mandated a strategic shift toward Zero Trust security. Zero Trust security is an approach where no user, device, or network is automatically trusted, and access is continually verified based on context and risk.

Executive Order 14028, *Improving the Nation's Cybersecurity*, directs federal agencies to modernize their IT environments by adopting Zero Trust security architectures. Complementing Executive Order 14028, the OMB Memorandum M-22-09 offers detailed guidance and deadlines for implementing Zero Trust security principles. These principles focus on strong identity authentication, network segmentation, continuous device and workload validation, and data-centric security controls. Additionally, NIST SP 800-207 provides the technical framework for Zero Trust architecture, defining five key pillars: identity, devices, networks, applications and workloads, and data.

Additional federal mandates such as, the *Federal Zero Trust Data Security Guide* by the CIO Council, Directive-Type Memorandum 25-003 by the Department of Defense (DoD), *Trusted Internet Connections (TIC)* 3.0 by CISA, and FedRAMP and FISMA compliance requirements shape this imperative. These mandates require agencies to implement phishing-resistant multi-factor authentication, maintain continuous monitoring, enforce automated policy compliance, apply encryption and microsegmentation, and ensure detailed audit trails.

Together, these directives position Zero Trust architectures as the foundational security model for digital government. Agencies must abandon implicit trust assumptions and adopt adaptive, data-centric, and verifiable controls across all users, devices, applications, networks, and data. These controls provide resilient and secure delivery of government services in today's evolving threat landscape.

Federal Zero Trust Architecture Pillars

The Broadcom software portfolio addresses federal Zero Trust security mandates across the five core pillars defined by NIST SP 800-207 and subsequent federal guidance:

Identity Pillar

The foundation of Zero Trust security is to establish continuous and sufficient trust in a user's identity. Each access request must include real-time reassessment of the user's identity and transaction context. IAM delivers five key capabilities to enable this trust:

1. Context-driven and dynamic authentication of users accessing applications and data.
2. Continuous and real-time authorization based on risk and data sensitivity.
3. Automated adjustments to access as threats evolve: allowing, restricting, or blocking.
4. Risk-based monitoring to detect and respond to suspicious behaviors.
5. Entitlement management to ensure that users have only the minimum necessary access.

At its core, the Symantec SiteMinder™ access management solution performs a multi-step access assessment. SiteMinder verifies the protection status of resources, authenticates users, validates sessions, and authorizes access. Trusted for over 25 years and protecting thousands of federal applications, SiteMinder supports HSPD-12 PIV and DoD CAC credentials, and FIDO2-compliant passwordless, phishing-resistant authentication through Symantec Identity Security Platform (formerly VIP Authentication Hub). The platform is available as a free entitlement to customers who have licensed the SiteMinder All Agent SKU. Access control and security for the API channel is provided by the Broadcom Layer7™ API Gateway software. Layer7 API Gateway enforces authorization policies on behalf of your APIs. Identity Security Platform also embeds a risk engine that analyzes the user's endpoint device and normal login behavior to determine the likelihood that the attempt comes from a known, uncompromised, and legitimate user. The solution can also easily integrate with external risk engines and leverage their risk scores in authentication policy decisions.

Privileged access, a critical attack vector, is addressed by Symantec Privileged Access Management (PAM) software. PAM removes administrative credentials from the hands of multiple users and non-human identities, and it stores them in an encrypted data store to enable the following security requirements:

- Uses two-factor authentication to ensure that users are whom they claim to be before granting access to privileged credentials.
- Enforces policy-based access control over which credentials a privileged user might access to ensure the least privileged access and superuser containment.
- Monitors all privileged activity, and links that activity back to an individual user to improve accountability and address regulatory compliance.
- Rotates privileged passwords automatically on a configured basis to comply with internal policies and security mandates.

PAM also combats the insider threat through user and entity behavior analytics. It monitors and analyzes privileged user activity in real-time to quickly identify abnormal behavior. PAM assesses the risk associated with this activity and can trigger automated mitigation actions to proactively prevent a potential attack.

Entitlements need to be managed and governed. Access management tools such as SiteMinder and PAM grant or deny access to protected resources, but they do not ask the question, "Should the user have this access at all?" Symantec Identity Governance and Administration (IGA) software addresses this challenge by automating the provisioning and deprovisioning of access entitlements to users, and it streamlines the processes associated with reviewing and certifying user access. The automation ensures that users are only granted the level of access that they absolutely need.

Together, these IAM products provide a comprehensive, federal-ready identity fabric that supports continuous authentication, adaptive access, robust monitoring, and granular governance. IAM enables agencies to realize Zero Trust security securely and efficiently.

Device Pillar

Device integrity and continuous posture validation are fundamental requirements for a robust Zero Trust security strategy. Federal agencies must ensure that every device is securely managed, compliant, and continuously monitored before granting access to sensitive systems and data. The Broadcom Symantec security portfolio provides a comprehensive, multilayered approach to address these needs.

Symantec Endpoint Protection (SEP) software offers advanced threat prevention, detection, and response capabilities across traditional and cloud endpoints. SEP provides industry-leading intrusion prevention capabilities through the Intrusion Prevention System (IPS). The IPS inspects all traffic to eliminate 90% of threats before they ever get into your network. SEP also includes adaptive protection which serves as an attack surface reduction solution. It baselines your environment and blocks apps that are not widely needed for business purposes and could be used by attackers. A dedicated on-premises appliance can be deployed to quickly integrate EDR capabilities with SEP. Finally, the solution provides host integrity to ensure that devices are in compliance with the security policies. SEP monitors devices that join the network as the first *integrity* check, and it then evaluates all devices on an ongoing basis to ensure they continue to meet your agency's security standards. If the endpoints are out of compliance, they can be quarantined. Analysts could also be alerted to take necessary actions to bring the device into compliance, allowing it to join the network. SEP ensures that only trusted and compliant devices can access critical federal resources.

Maintaining secure device configurations and swiftly remediating vulnerabilities are essential for minimizing risk:

- Symantec Control Compliance Suite (CCS) quickly identifies misconfigurations and vulnerabilities. CCS automates IT security assessments across more than 75 platforms, with over 15,000 configuration checks. It simplifies audits and ensures regulatory adherence by providing automated compliance reporting that is aligned with federal frameworks (NIST, HIPAA, PCI DSS, and GDPR).
- Symantec IT Management Suite (ITMS) delivers automated endpoint lifecycle management, including near-real-time visibility, patch management, and vulnerability remediation. ITMS helps agencies enforce strict security and patch compliance policies, significantly reducing risk from unmanaged devices.

The increasing use of APIs for device-to-application communication introduces additional risks. Layer7 API Gateway secures API traffic, providing robust identity verification, policy enforcement, and protection against mobile-specific challenges, such as adaptation and integration. Its Common Criteria certifications demonstrate compliance with stringent public sector and regulatory security requirements.

PAM protects as both a proxy to the network and by providing kernel-level control. Both types of protection enhance Zero Trust security by extending least privilege enforcement directly to the operating system administrative accounts, mitigating risks even at the root level. The agents running at the kernel level limit what both human and non-human threat actors can do. For example, the agents can keep threat actors from accessing sensitive files, executing malicious commands, installing programs, starting or stopping services, changing log files, or initiating new inbound or outbound communications.

By combining SEP, CCS, ITMS, PAM, and Layer7 API Gateway, Broadcom enables federal agencies to continuously assess, manage, and protect devices. The software supports Zero Trust security mandates for secure, compliant, and least-privileged device access as critical components of the broader Zero Trust architecture.

Network Pillar

Securing network access and segmenting traffic are vital to implementing a resilient Zero Trust architecture. The Broadcom Symantec portfolio delivers a comprehensive suite of solutions designed to meet federal mandates by enforcing dynamic policy-driven access controls, continuous verification, and advanced threat protection throughout the network.

The Symantec Zero Trust Network Access (ZTNA) solution replaces traditional VPNs with granular, identity-aware access that continuously verifies users and devices before permitting connectivity. ZTNA dynamically segments network and application access according to adaptive, risk-based policies. Whether users are remote or on-premises, access is restricted based on least privilege, device posture, and contextual risk assessments. Integrated with IAM for strong authentication and unified policy enforcement that is aligned with Executive Order 14028 and OMB M-22-09, ZTNA enables federal agencies to securely migrate to hybrid and cloud environments without compromising user experience.

PAM further strengthens network security by tightly controlling access to privileged accounts within internal subnets. PAM prevents lateral movement and limits the attack surface by enforcing least privilege, while its socket filter agents block unauthorized network connections, ensuring that administrators can only access authorized systems.

Symantec Email Security offers multilayered protection across cloud and on-premises email systems, safeguarding against ransomware, spear phishing, and business email compromise (BEC) attacks. Drawing on the world's largest civilian cyber intelligence network, it integrates threat detection, sender authentication, content isolation, and user awareness to defend against sophisticated email-borne threats. For agencies preferring on-premises deployment, Symantec Messaging Gateway offers robust, appliance-based email protection.

Together, these network security solutions empower federal agencies to enforce highly segmented, continuously monitored, and tightly controlled network environments. They provide rapid detection and response capabilities that align seamlessly with the latest federal Zero Trust security requirements, ensuring secure and resilient government networks.

Applications and Workloads Pillar

As organizations adopt cloud-native applications, AI-driven services, and agent-to-agent communication protocols, APIs have become the critical communication layer of modern mission-critical infrastructure. APIs are the connective tissue that enables these capabilities, making API security a fundamental requirement. Layer7 API Gateway provides centralized policy enforcement and security controls across all APIs, enabling consistent application of Zero Trust principles regardless of where APIs are deployed. This security includes the following capabilities:

- Threat protection defense against OWASP API Security Top 10 vulnerabilities including injection attacks, broken authentication, and excessive data exposure
- Advanced API security profile support for high-value APIs exchanges
- Policy enforcement and fine-grained authorization based on user attributes, device posture, and operational context
- Rate limiting and quotas protection against API abuse and denial-of-service attacks

Automation is essential for efficient and effective Zero Trust architecture implementation within federal environments. Automation enables continuous policy enforcement, reduced manual intervention, and faster response to threats across complex workloads.

Symantec Endpoint Security leads with AI-driven automation to continuously monitor endpoint behavior through machine learning and predictive analytics. Endpoint Security detects both known and zero-day threats, including ransomware, fileless malware, and advanced persistent threats. It automatically isolates compromised devices, halts malicious processes, and triggers remediation workflows to dramatically reduce the time from detection to response. Integration with the Symantec Global Intelligence Network ensures access to evolving threat intelligence, helping federal agencies meet the OMB M-22-09 mandate for continuous monitoring and rapid incident response.

CCS and ITMS automate lifecycle management, configuration assessments, and patching workflows. CCS scans hybrid environments continuously against over 15,000 configuration benchmarks across 75+ platforms, generating compliance reports aligned to NIST and other frameworks. ITMS complements this with automated asset discovery, patch deployment, and vulnerability remediation, maintaining a robust security posture.

The Symantec CloudSOC® CASB solution extends automated policy enforcement across SaaS applications, orchestrating data classification, loss prevention, and user behavior analytics. It detects risky activities and blocks unauthorized data movement in real time which is critical for governance and risk reduction in hybrid cloud environments.

IAM enhances automation with policy-driven identity lifecycle management, including user provisioning, adaptive authentication, and continuous authorization. IAM enables agencies to uphold least-privilege access across cloud and on-premises systems.

Broadcom's integration with AI-powered orchestration platforms unifies incident response and automates remediation across endpoint, identity, email, and network security domains. This comprehensive automation fabric enables federal agencies to implement dynamic Zero Trust security controls, reduce operational costs, and enhance resilience against sophisticated cyber threats.

Data Pillar

In a world where data is increasingly distributed across hybrid, multi-cloud, and on-premises environments (often at scales that surpass those of most commercial organizations) federal agencies face the critical challenge of securing sensitive information at every stage of its lifecycle.

Broadcom addresses this challenge with the Symantec Data Loss Prevention (DLP) platform, designed to provide unified visibility and control over data regardless of where it resides or travels. Leveraging deep content inspection and context-aware detection, DLP enables agencies to precisely identify, classify, and protect sensitive data based on content, usage, and compliance requirements. DLP ensures persistent security across endpoints, storage, network, email, and cloud channels.

A core element of this strategy is data classification, supported through integrated capabilities within DLP and the broader Symantec product suite. These classifications enable organizations to categorize and manage data according to its sensitivity and regulatory requirements (such as NIST, HIPAA, PCI DSS, and GDPR), and enforce policies consistently across hybrid environments. This enforcement supports continuous compliance and audit readiness, and it ensures that sensitive information remains protected, whether it is stored locally, shared externally, or in transit.

Extending data protection into cloud applications, CloudSOC CASB provides comprehensive visibility and control over SaaS platforms, including Microsoft 365, Google Workspace, Slack, and Salesforce. CloudSOC CASB enforces real-time policies, monitors user activity, and blocks unauthorized data transfers to help agencies identify shadow IT, prevent data exfiltration, and ensure regulatory compliance without disrupting user productivity.

Despite advanced security frameworks, Zero Trust security principles assume breaches will occur, making encryption a crucial final defense line. The Broadcom Symantec PGP® Encryption portfolio provides this robust safeguard by providing the following features:

- Deliver full-disk and removable media encryption, secure email encryption automation, and end-to-end file/folder protection through the PGP Encryption Suite.
- Automate encryption through PGP Gateway Email Encryption to secure sensitive email transmission without requiring end-user involvement.
- Protect large data volumes on servers with PGP Command Line Encryption to support integration into daily operational data transfers and processing.

Together, these solutions protect sensitive data at rest, in use, and in transit while offering centralized management, automated policy enforcement, and comprehensive compliance reporting. Seamless integration with Email Security further strengthens defenses against evolving cyber threats to empower federal agencies to implement Zero Trust data security effectively and confidently.

Why Federal Agencies Should Partner with Broadcom

Broadcom is uniquely positioned to help federal agencies implement the Zero Trust cybersecurity model required by Executive Order 14028, OMB M-22-09, and related federal mandates. Its integrated Symantec security and IAM platforms secure all five Zero Trust pillars (identity, devices, network, applications and workloads, and data), enabling agencies to meet regulatory requirements and achieve cyber modernization. The Broadcom IAM solution delivers phishing-resistant authentication, adaptive access, and entitlement governance to protect privileged users, while Symantec Endpoint Security provides AI-driven threat prevention and device compliance. Network solutions such as ZTNA and PAM replace legacy VPNs with least-privilege connectivity and advanced threat defense, complemented by Symantec Email Security to protect government communications.

Data protection is powered by technologies like Symantec DLP, CloudSOC CASB, and PGP Encryption. These technologies unify policy enforcement and encryption across cloud and on-premises environments. Supported by world-class threat intelligence, automation, and seamless cross-domain integration, Broadcom enables consistent Zero Trust enforcement across modern and legacy infrastructures (including mainframe and VMware Cloud Foundation®). This cohesive ecosystem helps agencies accelerate Zero Trust maturity, reduce cyber risk, and defend critical systems and sensitive data with the speed, scalability, and resilience needed for today's evolving threat landscape.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

ZTF-FED-WP100 October 29, 2025