Z-SHIELD CAPABILITIES

MODERN CYBERSECURITY & RANSOMWARE RESILIENCE

ZERO TRUST SECURITY ARCHITECTURE
(Continuous Verification, Least Privilege)

ENDPOINT SECURITY
Real-time Detection, EDR & Antivirus

NETWORK PROTECTION
Traffic Monitoring, Segmentation, Lateral Movement Prevention

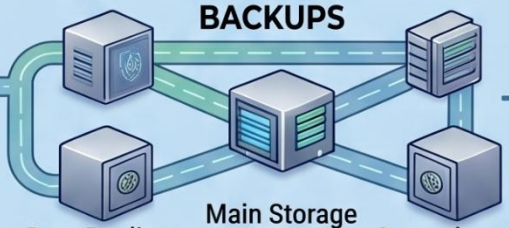
CLOUD INFRASTRUCTURE
Dynamic Auditing, Resource Control, Anomaly Detection

IDENTITY ACCESS
Conditional Access, MFA, IAM & Privileged Access

APPLICATION CONTROL
Code Signing, Vulnerability, Scanning, App Integrity

DATABASE SECURITY
Data Encryption, Access Accuting, Database Activity Monitoring

STANDBY, UPSTREAM & DOWNSTREAM IMMUTABLE BACKUPS



Data Replicas (Standby) | Main Storage (Upstream) | Secondary Site (Downstream)

IMMUTABLE & AIR-GAPPED
Read-Only Copies, Rapid Recovery

CROSS ZONES MULTI-REGION AVAILABILITY
Geo-Redundancy, Cross-Region Isolation, Disaster Recovery

RANSOMWARE RESILIENCE & MITIGATION
(Detection, Containment, Eradication, Recovery)

End-to-End Encryption

Zione Solutions, LLC

email: zshield@zionesolutions.com Phone: 248-219-8191
www.zionesolutions.com

Commit to Engineering...

Cyber Defense System Ransomware Resilience

Executive Order (EO) 14028 – Improving Nation's Cybersecurity:

Executive Order 14028 establishes a comprehensive framework to modernize the digital defenses of US government agencies by mandating a shift toward Zero Trust Architecture and the universal adoption of multifactor authentication & encryption across federal agencies. The order focuses on several key points. The EO makes it easier for IT Service Providers to share information with federal agencies and also requires that they share certain information regarding cybersecurity breaches. It also established a roadmap & timeline for government agencies to implement Zero Trust Architecture, Multi-Factor Authentication, and encryption. Another key focus of the EO is establishing common security standards for software development intended for government purchase or use, strengthening the security of the software Supply Chain. It also establishes the creation of the “Cyber Safety Review Board”, which is tasked with investigating & analyzing cybersecurity incidents to provide informed recommendations for cybersecurity going forward.

It also set up event log requirements that can be used to help detect and mitigate intrusions into an organization's systems, and have forensic data to assess the severity and extent of an incident after it has occurred, as well as the creation of a standardized playbook for Cyber Vulnerability Incidents and how agencies are expected to detect and respond to them.

Executive Order 14177:

Established a national security framework to block the large-scale transfer of personal data to adversarial nations. The order specifically targets "countries of concern" (including China, Russia, Iran, North Korea, Cuba, and Venezuela, among others) to prevent them from exploiting bulk datasets (such as genomic, biometric, health, geolocation, and financial data) for espionage, blackmail, or the refinement of AI-driven surveillance. Implementation is led by the Department of Justice, which prohibits high-risk transactions like data brokerage, and the Cybersecurity and Infrastructure Security Agency (CISA), which mandates strict security requirements for restricted vendor and investment agreements.

FIPS 140-2 & FIPS 140-3:

These are the security standards established by the National Institute of Standards and Technology (NIST) to validate the effectiveness of cryptographic modules used by the U.S. and Canadian governments to protect sensitive data. As FIPS 140-2 is phased out, FIPS 140-3 is set to replace it to better align with international ISO/IEC standards and address modern cybersecurity threats, including the need for Post-Quantum Cryptography (PQC) readiness.

FIPS 140-3's newer standard introduces more rigorous testing for physical security, stricter requirements for entropy (randomness), and a transition from "trusted paths" to "trusted channels" for secure communication. All remaining active FIPS 140-2 certificates are scheduled to be moved to the "Historical List" in September 2026, meaning that federal agencies will no longer be able to use them for new procurements, effectively mandating FIPS 140-3 compliance for any vendor seeking to do business with the federal government.

HIPAA & DFARS 252.204-7012:

For HIPAA and DFARS 252.204-7012, the U.S. government enforces rigorous encryption mandates that ensure federal agencies and their private-sector vendors protect sensitive data using FIPS-validated cryptography. Under updated 2026 HIPAA Security Rule guidelines, encryption has shifted to a functionally mandatory requirement for both covered entities and their business associates, necessitating the use of AES-256 for data at rest and TLS 1.2+ for data in transit to safeguard electronic protected health information (ePHI).

Simultaneously, the DFARS 252.204-7012 clause and the newly operationalized CMMC 2.0 framework require defense contractors to implement the 110 security controls of NIST SP 800-171, which specifically mandates the use of FIPS-validated modules (currently transitioning to FIPS 140-3) for protecting Controlled Unclassified Information (CUI).

OMB Memorandum M-22-09 Federal Zero Trust Strategy:

OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," serves as the formal implementation roadmap for Executive Order 14028, allowing them to meet the required Zero Trust implementation & security goals by Fiscal Year 2024. It lays the groundwork for establishing a move to agencies using centralized identity management and phishing-resistant MFA, comprehensive device tracking & security posture verification, encryption of all network traffic (with special attention to DNS and HTTP traffic) and micro-segmenting network environments, treating all applications as internet-connected & conducting rigorous testing and manual sandboxing, and moving towards a data-centric security model with automated categorization and immutable logging.

CISA's Zero Trust Maturity Model (ZTMM) 2.0:

CISA’s ZTTM 2.0 presents an overview of three broad approaches towards a gradient of Zero Trust Architecture implementation (Initial, Advanced, and Optimal), represented by five "pillars". The five pillars are Identity, Devices, Networks, Applications & Workloads, and Data. This allows for a gradual rollout, allowing the organization or agency to scale their processes over time, implementing more demanding zero trust protocols as they go, with the long-term goal being implementation of an "Optimal" Zero Trust maturity state. Broadly speaking, the core pillars involve Zero Trust Framework, Zero Data Loss and Immutable Backups, End-to-End Encryption, Micro-segmentation with fully-encrypted network traffic, Immutable workloads and continuous security testing, and continuous posture checks to ensure all devices in the environment remain fully compliant at all times.

NIST SP 800-207 Zero Trust Architecture:

Provides government agencies with a definition of Zero Trust Architecture, and seven core tenets of the concept.

1. “All data sources and computing services are considered resources.”
2. “All communication is secured regardless of network location.”
3. “Access to individual enterprise resources is granted on a per-session basis.”
4. “Access to resources is determined by dynamic policy – including the observable state of client identity, application/service, and the requesting asset – and may include other behavioral and environmental attributes.”

5. “The enterprise monitors and measures the integrity and security posture of all owned and associated assets.”
6. “All resource authentication and authorization are dynamic and strictly enforced before access is allowed.”
7. “The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.”

National Security Memorandum (NSM-8):

Establishes requirements for the National Security Systems (NSS) that are equivalent to or greater than the cybersecurity requirements mandated in EO 14028. It formally designates the Director of the National Security Agency (NSA) as the "National Manager" for NSS, granting the NSA enhanced authority to issue binding operational directives and emergency directives. Additionally, it mandates that defense and intelligence agencies modernize their digital infrastructure by adopting Zero Trust Architecture, implementing phishing-resistant multifactor authentication, and utilizing NSA-approved encryption for data both at-rest and in-transit, with a specific focus on transitioning to quantum-resistant cryptography. Additionally, NSM-8 establishes strict protocols for reporting cyber incidents to the National Manager and mandates the inventory and securing of cross-domain solutions, which are critical tools used to transfer data between classified and unclassified systems.

NIST SP 800-53 (Rev 5):

Provides a comprehensive catalog of safeguards designed to protect organizational operations, assets, and individuals from a wide range of threats and risks. This revision marks a significant shift toward a more holistic, outcome-based approach that is "entity-neutral," meaning the controls are applicable to everything from traditional IT systems to IoT and cloud-based environments. A defining feature of Revision 5 is the seamless integration of privacy into the security control catalog, treating privacy as a fundamental component of the system lifecycle rather than an afterthought. The publication organizes these safeguards into 20 control families, such as Access Control, Immutable Backups, Air-Gapped solutions, System and Communications Protection, and Supply Chain Risk Management, offering a flexible framework that allows organizations to tailor their security posture based on specific risk assessments and mission requirements.

NIST SP 800-184:

Provides a technical and strategic framework designed to help organizations transition from a state of compromise back to normal operations while minimizing the impact on mission-critical functions. Expanding on the "Recover" function of the NIST Cybersecurity Framework (CSF), this focuses on the preparation and execution of recovery playbooks tailored to specific scenarios, such as ransomware attacks or data exfiltration. It distinguishes between the tactical phase, which involves the immediate technical restoration of systems and data, and the strategic phase, which emphasizes long-term improvements to the organization’s security posture through post-event analysis and the integration of lessons learned.

By mandating the use of specific recovery metrics, such as recovery time objectives (RTOs), prioritizing the ability to restore from a "known good" state using data that has been protected from unauthorized modification (Immutability), and the efficacy of backups, the publication ensures that recovery is not just a reactive measure but a measurable, repeatable process that strengthens overall organizational resilience.