Meeting Zero Trust Controls Natively in stackArmor's Armory on Google Cloud

stackArmor

A TYTO ATHENE COMPANY

As cyber threats grow increasingly sophisticated and persistent, federal agencies and their partners must evolve their security postures to align with modern defense paradigms. The Department of Defense (DoD) Zero Trust Reference Architecture (ZTRA) v2.0 outlines a transformational shift away from perimeter-based defenses toward a "never trust, always verify" model that enforces least privilege, continuous validation, and policy-based enforcement across every aspect of the digital enterprise.

stackArmor's *The Armory* is a secure-by-design General Support System (GSS) purpose-built to streamline FedRAMP and DoD Impact Level (IL) authorizations for Independent Software Vendors (ISVs), and Mission workloads. Agencies are seeking accelerated and lower cost pathways to meeting mission needs in a secure and compliant manner. The cloud, security and compliance experts at stackArmor have developed the Armory on Google Cloud to incorporate zero-trust architecture elements that are validated by the implementation of zero-trust control overlays that are directly integrated into the architecture as opposed to being a "bolt-on." Our design is uniquely zero-trust native implementation.

This white paper provides an in-depth overview of The Armory's system architecture, as detailed in its System Security Plan (SSP), against the seven foundational pillars of the DoD's Zero Trust framework. The Armory™ not only meets but often exceeds the "optimal" capability tier envisioned by the DoD ZTRA, providing defense, federal customers and ISV partners with a secure, scalable foundation for mission-critical operations.

User Pillar

The Armory's identity and access management strongly aligns with Zero Trust principles. It employs high-assurance user authentication (meeting NIST SP 800-63 IAL3/AAL3 requirements for FedRAMP High) and integrates a robust Identity-as-a-Service platform. This pillar was specifically architected to align with DoD ZTRA guidance which requires enforcing strict user verification and least privilege access. ISVs deployed to The Armory can leverage:

- **High-Assurance Identity Management:** provided via **Okta Government High Cloud (GHC)** as a centralized IdP for all users, providing strong multi-factor authentication (MFA) and single sign-on (SSO) at Authenticator Assurance Level 3 (AAL3). All administrative and security applications leverage Okta SSO via SAML/LDAPS federation, ensuring unified identity enforcement across the environment. This meets DoD ZTRA's emphasis on strict identity verification (person and non-person) for every access request.
- **Adaptive and Token-Based Authentication:** The use of Okta's adaptive MFA (aMFA) and Okta Verify tokens mean authentication can adjust to context/risk and uses phishing-resistant factors (per AAL3). Hardware-based authenticators are provided through Okta FastPass or Yubico's YubiKey 5 Series hardware tokens.
- **Privileged Access Controls:** The Armory strictly governs administrator access. All privileged infrastructure users authenticate via Okta which has been integrated with Google's Identity Aware Proxy (IAP). This ensures all privileged users connect via a secure software-defined perimeter, tying network session access to verified user identity. Additionally, partners/customers have no direct access to core management planes or security functions of the GSS, preventing privilege misuse.
- **Least Privilege & Role-Based Access:** By design, the system limits user access to only required resources. For example, each tenant's administrators are confined to their own project/landing zone with role-based privileges, and connections to projects and Virtual Private Clouds (VPCs) are governed by defined information flow authorizations. This reflects ZT principles of explicit authorization per request and minimal implicit trust.
- **Continuous Identity Analytics:** After strong initial authentication, The Armory monitors real-time user behavior, incorporating User and Entity Behavior Analytics (UEBA) to monitor anomalous account activity (e.g. unusual times, locations, or actions) to ensure privileged users are performing under expected and known good rulesets.
- **Non-Person Entity (NPE) Identity Management:** Achieving optimal ZT means treating service accounts and application identities with the same rigor as human users and ensuring all machine-to-machine interactions use strongly authenticated, least-privilege service identities (with short-lived credentials and auditable use). The Armory manages all machine-to-machine interactions though Google Cloud's Identity and Access Management (IAM) and Key Management Service (KMS) services to ensure that both user and service accounts are managed in accordance with ZTA requirements.

The User pillar is key to controlling who and what has access within the system. The Armory implements continuous identity monitoring which complements the secure identification and authorization (IA) capabilities implemented via Okta MFA and IAP. The system leverages Okta's adaptive authentication features fully for privileged users to dynamically adjust access policies based on access required. In addition, Integrated identity analytics continuously evaluates session risk and aligns with DoD's goal of *continuous validation* of user trust.

All service accounts, APIs, and CI/CD pipelines use unique identities with MFA-equivalent protections and follow strict rotation and least privilege. NPE usage patterns are constantly monitored via the Security Information and Event Manager (SIEM) for any misuse and flagged for review upon detection.

Device Pillar

The Armory's architecture imposes tight control over devices that interact with the system, especially for administrative access, with focus on ensuring a minimal level of configuration prior to allowing device access. In addition, strong host-based protections are deployed for granular control of what is allowed to run and on which devices this is allowed throughout the system's authorization boundary. The system implements:

- **Secure Access for Administrator Devices:** The requirement that all privileged users connect via Okta integrated with IAP means that administrator devices must meet enforced conditional access policies (CAPs) in order to authenticate before reaching any internal resource. This effectively acts as a DoD Comply-to-Connect mechanism: only known, authorized devices/users can form connections. Additionally, The Armory uses Google Cloud's Identity-Aware Proxy (IAP) for admin console/VM access, ensuring that administrative sessions are brokered through an identity- and policy-aware service rather than direct device network access. All admin traffic traverses a controlled ingress (Cloud Load Balancer with IAP and NGFW) and must be explicitly allowed, reducing the risk from compromised or unauthorized devices.
- **Endpoint Posture Checking:** The system performs real-time posture assessment)e.g. checking if an admin's laptop has up-to-date patches, a secure baseline, etc.) before granting access) for all privileged user devices used by system administrators. The implementation continuously validates device health (OS patch level, antivirus status, configuration compliance) prior to and during privileged user sessions.

- **Endpoint Security on Servers:** Each server and workload instance in The Armory is treated as a hardened device. The system includes host-based security agents such as Trend Micro Deep Security (for anti-malware, HIDS/HIPS) and performs regular vulnerability scanning (Tenable Nessus) on VMs. These measures align with ZT device capabilities by ensuring that every compute instance is monitored for threats and kept in a known secure state. The SSP's inventory of update sources (e.g. for Trend Micro, Nessus, etc.) shows that The Armory maintains patch and signature updates for in-boundary software, contributing to continuous device (server) compliance.
- **Device Compliance Enforcement:** Although not explicitly a user endpoint control, the Armory enforces that no unmanaged or non-FedRAMP devices can persistently connect to its environment. By disallowing any persistent connections to external systems at lower assurance levels, the architecture implicitly requires that any device or system interfacing with the Armory meets equivalent security standards. This reflects a Zero Trust mindset of not trusting devices by default – only those from known, secure environments are permitted.

By design, The Armory requires the validation of all devices before allowing communication tunnels to be established, regardless of the privilege level of the user. By incorporating device posture checks and requiring that connecting are checked for compliance (patched OS, full disk encryption, FIPS-validated Trusted Platform Module (TPM), screen lock) before tunnel establishment. This aligns with DoD's *Continuous Compliance* mandate for devices.

Network & Environment Pillar

The Armory's network architecture is designed with strong segmentation, boundary control, and least-privilege connectivity, embodying core zero trust network concepts. Each tenant/application environment is isolated, and all traffic, internal and external, is tightly governed by policy. This pillar shows comprehensive compliance with ZTRA guidance at an optimized level. The system minimizes implicit trust in the network by enforcing micro-segmentation, encryption in transit, and continuous monitoring of network traffic. Key highlights of security design within this pillar include the following.

- **Strong Segmentation of Enclaves:** The Armory uses a multi-tenant government-only cloud with VPCs and projects for each customer or application. Network access control and routing policies ensure each landing zone is completely segregated from others. In other words, there is no flat network – every application environment is a distinct segment with logically isolated subnets. This design contains any potential breach and maps to the ZT principle of micro-segmentation (down to the application/tenant level).
- **Default-Deny and Least-Privilege Traffic Policies:** All network traffic, both north-south and east-west, is subject to explicit policy whitelisting. The Armory employs Palo Alto Next-Generation Firewalls at the boundary and within a shared network hub to inspect and filter all system traffic. By policy, no traffic is allowed unless explicitly authorized. For example, even inter-service flows between components must be opened by rule, and any external inbound access (for user-facing apps) must traverse approved points. This approach aligns with DoD ZTRA's ideal that *no network traffic is implicitly trusted*. The system requires that all traffic must explicitly be allowed via traffic flow policies and whitelisting.
- **Identity-Aware Network Access:** The use of Google Cloud's Identity-Aware Proxy (IAP) integrated with load balancers means that network access to internal resources (like admin interfaces or SSH to VMs) requires user identity verification at the network layer. This tightly binds the network pillar with the user pillar – only authenticated, authorized requests get through. For privileged access, an admin's connection to a VM is not a direct network path but rather brokered by IAP and the firewall, ensuring the network never exposes listening ports unless the user is verified. This significantly reduces attack and exemplifies Zero Trust "authenticate before connect."
- **Encrypted Everywhere:** There is a significant focus on end-to-end encryption of data in transit throughout the environment. Internal service-to-service traffic is encrypted (for example, within Kubernetes clusters the guidance is to use TLS or service mesh encryption for all pod-to-pod communication). All data in transit is encrypted via FIPS-validated modules, as required by FedRAMP and DoD workloads, inside the Armory. This means even if an attacker intercepted traffic within the cloud environment, it would be cryptographically protected – aligning with zero trust tenets that the network is always treated as potentially hostile.
- **Egress Restrictions:** The Armory's environment has no persistent connections to unauthorized external systems. Outbound internet access from in-boundary components is heavily restricted; only specific update sources and trusted services are allowed (e.g., pulling security updates from known URLs over TLS). By preventing arbitrary egress, the architecture mitigates risks of data exfiltration and C2 channels. Any unexpected outbound traffic would be a notable anomaly. This whitelisting of external endpoints corresponds to optimal network tier practices, where even outgoing traffic is governed by policy.
- **Micro-Segmentation & Software-Defined Policy:** The system implements Micro-segmentation at the workload or process level via service mesh policies to restrict communications between individual microservices and/or processes, in addition what is achieved with VPC isolation. Allow lists can be dynamically orchestrated for inter-service calls to further reduce the attack surface inside each zone.

The Armory takes a "trust no workload" stance, where even if an attacker compromises one workload, there is no pathway to freely reach others. Integrated log analysis has been established for key segments to enable better clarity and to support threat hunting. Security Engineers and Analysts are provided the tools needed to monitor and act against threats in near-real time.

The established trust zones are periodically reviewed and updated to ensure they align with real-world threat vectors and evolving threat landscapes. The goal is of the system design is to eliminate any "flat" subnet where numerous services can talk without checkpoints. This aligns with DoD's goal of *segmenting and isolating everything possible* to mitigate intrusions.

Application & Workload Pillar

The Armory's architecture implements a comprehensive Secure Software Development and Deployment Framework, providing security controls for applications and workloads from development through runtime. By delivering pre-hardened environments, integrated DevSecOps tools, and continuous vulnerability management, The Armory addresses the necessary security requirements of this pillar. The Armory implements:

- **Secure Landing Zone Baselines:** Each application deployed on The Armory starts in a pre-hardened Landing Zone – a well-architected GCP project/VPC with security controls and configurations meeting FedRAMP High and DoD Impact Level (IL) 5 baseline controls. These landing zones come with predefined IAM policies, network settings, logging, and monitoring mechanisms managed as infrastructure-as-code through Terraform. Providing this secure foundation means workloads inherit strong security from inception (least privilege roles, secure network architecture, etc.), reducing misconfiguration risk. This maps to the ZT principle that workloads should "inherit secure configurations by default."
- **DevSecOps and CI/CD Integration:** StackArmor has built security into the software development lifecycle for hosted applications. Notably, The Armory's ThreatAlert Container Scanner (TCS) uses *Trivy* integrated with GitLab to scan container images for vulnerabilities on every build. Vulnerabilities are tracked through a Findings Lifecycle Manager (FLM) in GitLab and must be remediated before deployment. Additionally, static and dynamic code analysis tools are available in-boundary, and infrastructure code is tested in a staging environment via Terraform before promotion. This end-to-end integration ensures that no code or workload goes live without thorough security checks, aligning with DoD's emphasis on supply chain risk management and secure development.

- **Continuous Vulnerability Management:** The Armory performs continuous scanning of running workloads and dependencies. It leverages tools like Tenable Nessus for vulnerability scanning and scans containers at least every 30 days (with a policy that no image older than 30 days, unscanned, should be in production). Any findings are handled per FedRAMP SI-2 (flaw remediation) processes in GitLab, which functions as the system's Information Technology Service Management (ITSM) platform. These practices ensure known vulnerabilities are quickly identified and patched, which is key to a Zero Trust workload posture (assuming workloads may be targeted, one must minimize their weaknesses at all times).
- **Runtime Threat Protection:** Workloads in The Armory are instrumented with security agents and monitored. The presence of host-based IDS/IPS, anti-malware (Trend Micro Deep Security), and file integrity monitoring on servers ensures that if an application process behaves maliciously, it can be detected or stopped. Moreover, all intra-cluster communications are encrypted (FIPS mode on hosts or via service mesh), preventing attackers from intercepting sensitive data between microservices. These controls embody DoD ZTRA's guidance that workloads should be secure, continuously monitored, and resilient to compromise.
- **Isolation and Least Privilege by Design:** Each application or customer workload is not only on a separate network but also deployed in its own GCP project with separate service accounts and access controls. Partners or developers cannot change security controls of the underlying GSS, and their privileges in their landing zone are limited. This ensures a clear tenant isolation and that workloads run with only the permissions they absolutely need (enforced via Google Cloud IAM roles and service control policies). In case of a breach in one application, the blast radius is confined to that project.
- **Compliance and Security Inheritance:** For SaaS providers on the Armory, up to 80% of FedRAMP High controls are inherited from the platform's security services. This means common workload security requirements (logging, monitoring, encryption, backup, etc.) are centrally provided, and applications leverage hardened services (e.g., Cloud SQL databases with encryption, KMS for key management, etc.). Applications built on this platform automatically comply with many security controls (e.g., using approved cryptography, centralized audit logging to SIEM, etc.), reducing the chance of a workload weakening the overall posture. The Armory Tools & Services include capabilities like centralized access control, SIEM, code scanning, and more that every workload can use providing a strong architectural advantage.
- **Staging and Testing Environment:** The Armory maintains separate staging environments managed via IaC via Terraform for both GSS components and ISV applications. All changes to configurations or new deployments are validated in staging and scanned for vulnerabilities/misconfigurations before being pushed to production, with oversight by the Information System Security Manager (ISSM). This DevSecOps practice ensures that workload changes do not introduce unforeseen security issues, reinforcing a trustworthy production environment.

The Armory embodies the "secure-by-design" mindset. The stackArmor Architects and Engineers support partner applications onboarded to the system and provide them with guidelines to design their application architecture in a zero-trust manner as well. This includes building their app with strict role-based access internally, robust input validation (to prevent trusting any client data), and integrating with The Armory's centralized auth and logging. By propagating ZT principles into the application layer (not just the infrastructure), the overall system moves closer to a holistic zero trust implementation.

The system enforces that applications use cloud-managed identities and keys rather than static credentials. Google Cloud's Workload Identity Federation and KMS are leveraged so that VM instances, containers, and serverless functions each have a distinct, auditable identity and access only the secrets they require ensuring that all parts of The Armory are as secure as the next.

Through use of automated configuration scanning tools, the system ensures all workload configurations stay hardened at all times. Security Engineers work with ISVs to ensure their applications are secure not just during deployment, but throughout the system lifecycle and work with them to address any "drift" from these secure baselines as it is encountered.

Data Pillar

Data within The Armory is well-protected through a combination of strong encryption, access controls, and monitoring. The platform enforces Federal standards (FIPS 140-2/3, FedRAMP High, DoD IL5) for all data at rest and in transit, aligning with DoD's data pillar objectives to encrypt and strictly control data access. The architecture provides a solid foundation for data confidentiality and integrity (via encryption and separation), while also enabling availability through backups. The Armory demonstrates mature data security measures consistent with ZTRA guidance through:

- **Universal Encryption (Data-in-Transit & At-Rest):** The Armory implements end-to-end encryption for all data flows. All data in transit is encrypted with FIPS-validated cryptographic modules within the boundary, including internal service communications. For example, internal API calls or database connections use TLS; container orchestration traffic is encrypted via FIPS mode or service mesh. Externally, TLS 1.2+/HTTPS is enforced for user connections. Data at rest in databases and storage is also encrypted using FedRAMP-approved Google Cloud services native services with KMS customer-managed encryption keys (CMEKs). This comprehensive encryption strategy meets DoD's mandate to protect data everywhere, both "in motion" and "at rest" are covered, limiting exposure in case of interception or theft.

- **Strict Cryptographic Standards:** The Armory adheres to FIPS 140-2/3 compliance for all encryption mechanisms. Only cryptographic modules validated under FIPS 140 are permitted, and verification of module certificates via the NIST CMVP database before deployment is required. Non-compliant modules are prohibited. This ensures that data protection meets DoD and federal standards (no usage of weak or unapproved algorithms), achieving a high level of assurance in data confidentiality and integrity.
- **Data Segregation by Tenant:** Each customer's data resides in their dedicated project and storage, segregated from other tenants' data by design. Access to one tenant's data is not possible from another tenant's environment which is a critical consideration for multi-tenant zero trust, where one should assume no inherent trust even within a shared platform. All partner data and services are enclosed in their own landing zone. This strong data isolation aligns with the zero-trust principle of minimizing data access scope.
- **Backups and Resilience:** The Armory includes Contingency Planning and backup capabilities as a core service. Data is regularly backed up, and services are built with high availability. This means the integrity and availability of data are maintained even in adverse events, an important aspect since zero trust also considers ransomware or destructive attacks. In addition, continuous verification of the integrity of those backups is implemented. With backups in place, encrypted, protected and validated, the system provides assurances that data can be recovered if compromised.
- **Monitoring of Data Access:** All access to data stores (e.g., database queries, file access) is logged via Cloud Audit Logs and ingested into the SIEM. The SIEM alert use-cases include data deletion or access events, meaning the security team is alerted on unusual data access patterns.
- **Data Loss Prevention at Egress:** By virtue of the egress restrictions mentioned, the platform reduces risk of unauthorized data exfiltration. There are no open channels to send sensitive data out except those explicitly allowed, all of which are monitored. Additionally, the Palo Alto NGFWs at the boundary enable inspection of outgoing traffic (to detect, for example, large data transfers or known sensitive data patterns). These patterns enforce Data Loss Prevention (DLP).

Secure data by design is one of the key pillars of the system. Ensuring data is always encrypted, be it at rest, or in transit, is a hard requirement for ISVs deployed within the GSS. The use of CMEKs ensures that data owners always have direct control over their data. This empowers data owners to protect and control their sensitive data to meet their needs and ensures that all data within the system is trusted only to those users that have explicitly been granted privileges to that data.

Automation & Orchestration Pillar

The Armory demonstrates a strong commitment to automation and orchestration, using infrastructure as code, continuous integration pipelines, and automated security responses in several areas. This pillar is well-addressed through the platform's ThreatAlert tooling and DevSecOps practices that automate monitoring, patching, and compliance tasks. The system implements the DoD's Zero Trust automation objectives via:

- **Infrastructure as Code (IaC) & Consistency:** The entire Armory environment (and customer landing zones) is deployed and managed via Terraform modules. Changes to configurations are tested in staging and require formal approval before production. This IaC approach ensures standardization and repeatability ensuring security controls are not manually applied ad hoc, but rather embedded in the templates. It also means the platform can rapidly instantiate secure environments or update configurations at scale, a key for orchestrating Zero Trust policies enterprise wide.
- **Automated Security Monitoring & Response:** The Armory's ThreatAlert(R) Security Workbench (TSW) provides real-time monitoring, and the platform includes automated alerting and responses to incidents. For example, when a potential security incident is detected, alerts are not only sent to personnel but can trigger automated actions. Additionally, Google Cloud's Monitoring/Alerting is configured as code (policy-as-code for alert definitions) and sends outputs to collaboration tools (GovSlack and GitLab issues) via the ThreatAlert(R) Serverless Relay (TSR). This integration means that the moment an alert fires, it is automatically routed to the Security Analyst team and logged for investigation, reducing response time and ensuring no alert is missed.

- **Continuous Compliance & Reporting:** StackArmor has integrated machine readable compliance artifacts using open standards like Markdown and Open Security Controls Assessment Language (OSCAL) tooling and detailed compliance reporting into the Armory's operations. The system's security controls and status are automatically tracked and can generate up-to-date security posture reports in near-real time. Automating compliance evidence collection and reporting is a significant orchestration benefit, aligning with DoD's push for continuous ATO processes. The system also automates key aspects of Continuous Monitoring requirements through scheduled and automated compliance tasks, Plan of Action and Milestones (POA&M) management, and automated vulnerability and compliance scan analysis.
- **Integrated DevSecOps Pipeline:** The development pipeline itself is orchestrated for security. With GitLab as the central platform, vulnerability scans, configuration scans, and ticketing are all tied together. For instance, when the ThreatAlert(R) Container Services (TCS) finds a vulnerability, it automatically creates or updates issues in GitLab (via the ThreatAlert(R) Findings Lifecycle Manager) for developers and engineers to address. The use of GitLab for change management and the Change Control Board process is tightly coupled with the automation (tickets, merge requests, etc., drive the promotion to production). This reduces human error and ensures that security steps cannot be skipped in the deployment process, essentially orchestrating security gates into the Continuous Integration/Continuous Delivery (CI/CD) workflow.
- **Orchestrated Network and Access Control:** The Armory uses automation in network and access realms too. Cloud configurations for logging, monitoring, and IAP are managed programmatically. Alert baselines are "managed as part of IaC". Service Control Policies and firewall rules are deployed through code templates for each project. This ensures that when a new project (landing zone) is created for a customer, all necessary ZT controls (network segmentation, IAM roles, logging sinks, etc.) are automatically instantiated without lag or omission. It shows a high level of orchestration, such that security is not reliant on manual setup.

Wherever possible, system architects leverage automation to enforce security updates across the environment. If a new baseline configuration is required (due to a discovered vulnerability or new hardening guideline), Terraform and scripts are utilized to push that change to all relevant cloud resources quickly. The revision history shows active updates (e.g., replacing insecure components, updating diagrams, etc.); having an automated method to do these ensures consistency. Integrated config management tools for live state further complement Terraform to maintain a consistent system state.

The culture of stackArmor has adopted the DoD Zero Trust Culture and it mandates its teams to trust and rely on automation to enforce security, rather than trying to bypass it. As technology evolves, the system evolves to further automate and enhance these processes, ensuring The Armory is a step ahead of nefarious actors.

Visibility & Analytics Pillar

The Armory excels in providing comprehensive visibility across the environment and leveraging analytics for threat detection. It aggregates logs from every layer; cloud infrastructure, network devices, hosts, and applications into a centralized SIEM system, and has real-time dashboards and alerting. This pervasive visibility meets DoD ZTRA expectations that a zero-trust enterprise *"continuously monitors and measures the security posture"* and detects anomalies rapidly. Key aspects that provide visibility into system operations are:

- **Centralized Logging and SIEM:** All security-relevant events are centrally collected using Google Cloud Logging and Monitoring as the system SIEM. The Armory funnels logs from multiple sources; VM OS logs, VPC flow logs, firewall logs, cloud audit logs, application logs, vulnerability scanners, and security tools into a unified audit project. This comprehensive log aggregation enables correlation of events across all planes of the system. Such central visibility is a cornerstone of Zero Trust, ensuring nothing happens in isolation unseen.
- **Real-Time Alerting and Dashboards:** The Armory has configured real-time alerts and dashboards for key security events. Google Monitoring is set up with dashboards and an alerting policy baseline (managed via IaC) to detect indicators like unauthorized access attempts, DoS patterns, suspicious privileged activity, malware detections, and changes to critical resources. For example, alerts exist for attempted remote access from foreign IPs, anomalies in admin account use, and potential malware triggers. These alerts are automatically forwarded to the security team's collaboration channels for immediate triage. This capability aligns with DoD ZT goals for continuous monitoring and attack surface visibility, whereby security personnel have up-to-the-minute awareness of the system's state.
- **Continuous Monitoring Operations:** The system is continuously monitored by the Armory Security Team of Engineers and Analysts. Having dedicated analysts watching the dashboards and investigating alerts ensures that visibility leads to action. They also manage GitLab ITSM in-boundary for tracking security issues, which creates an audit trail from detection to response that exists for the life of the system which allows for historical review of all system events. This organizational commitment to continuous monitoring is exactly what the DoD ZT model calls for under the Visibility pillar, not just tooling, but people and processes actively engaged in using the telemetry.

- **Long-Term Data for Analytics:** The Armory configures log retention to align with federal guidelines – logs are kept for 30 months in object storage. This is important for forensic analysis and spotting slow-developing trends or repeated patterns over time. With extensive log history, security analysts can perform deep dives (e.g., searching if a newly discovered Indicator of Compromise (IoC) ever appeared in the past) and machine learning models are trained on a large sampling of historical data to improve anomaly detection. Retaining this volume of data shows foresight and enhances the analytical capabilities of the monitoring team.
- **Single Pane of Glass –** stackArmor has created a proprietary application called the ThreatAlert Security Workbench (TSW) to provide visualization of system state on an ongoing basis. The application provides dashboarding functionality that that maps the seven pillars and highlights security metrics for each. Data Owners also have near-real time visibility into the running system state and the status of their Continuous Monitoring requirements. Having such a dashboard aligned to DoD's Zero Trust pillars, helps analysts and leadership alike quickly grasp security posture in each are and improves overall situational awareness, which is key aim of the Visibility & Analytics pillar.
- **Periodic Red-Team Simulations:** To validate and improve visibility, regular red-teaming and adversary simulation exercises are conducted as part of continuous monitoring. The outcomes help to reveal if any blind spots exist in logging or if any malicious activity fails to trigger alerts. The stackArmor team utilizes lessons from these exercises to further tune the analytics. Over time, the continuous testing and revalidation of the system automation helps to calibrate monitoring towards an optimal state where *any* malicious or policy-violating action is noticed and responded to quickly.

As seasoned security professionals, stackArmor understands that monitoring a system and gathering data only provides value if that data is focused and actionable. The Armory was designed to ensure that data gathered in the day-to-day operations of the system is consistently being evaluated and made available to the right teams at the right times to act when action is needed.

Zero Trust Overlays Alignment

The DoD Zero Trust Overlays provide targeted, mission-specific adaptations of the Zero Trust principles, ensuring that systems apply the right controls in the right operational context. The Armory's architecture naturally aligns with these overlays by combining FedRAMP High/IL5–compliant controls with mission-tailored Zero Trust enforcement points.

By leveraging capabilities such as identity federation with strong MFA, continuous monitoring via tamper-resistant logging, and segmentation through NGFW and VPC Service Controls, The Armory implements a security posture that meets the overlay intent for cloud-based, mission-critical workloads. This alignment ensures that the system not only meets the baseline ZTA requirements but also provides the context-driven protections expected in high-assurance DoD environments.

Conclusion

The Armory exemplifies a modern, zero-trust native implementation of the DoD Zero Trust Reference Architecture, weaving together secure user and device authentication, network micro-segmentation, encrypted workloads, continuous monitoring, and policy-driven automation into a cohesive and operationalized security fabric. Every element of the system, from its pre-hardened landing zones to its integrated ThreatAlert(R) Security Workbench, reflects the core tenets of "never trust, always verify" and "assume breach."

By unifying Identity-as-a-Service, FedRAMP-compliant cloud-native controls, and automated compliance orchestration under a single secure architecture, The Armory delivers a turn-key Zero Trust environment aligned with both FedRAMP and DoD cybersecurity expectations. Its design enables ISVs to rapidly deploy secure, resilient SaaS offerings within a trusted framework that meets the rigor of national security-grade standards.

With its foundational alignment to the DoD ZTRA and its commitment to continuous innovation, The Armory not only provides an effective blueprint for Zero Trust implementation, it sets a benchmark for the future of secure cloud service enablement across the federal landscape.

https://stackarmor.com/armory/