

— SOLUTION OVERVIEW



Garrison: AI-Enabled Security Platform

Context

Federal security operations centers (SOCs) manage complex, multi-classification environments that require continuous monitoring, zero trust identity verification, and runtime threat containment.

The Problem

Legacy cybersecurity architectures create dynamic vulnerabilities:

- **Dashboard Fragmentation:** Security teams run 6–12 disjointed tools (identity, eBPF, SOAR, threat intel), each with separate auth models and audit trails.
- **Credential Risk:** Standing keys and long-lived credentials represent the primary initial breach vector for attackers.
- **Manual Containment:** Threat correlation and containment are time-consuming, manual races against time.
- **AI Agent Vulnerability:** Unbounded AI agents introduce risk if compromised, lacking guardrails on what an agent can cost or execute across system planes

The Solution

Garrison is a modular, AI-enabled security platform organized into four interconnected pillars—**Identity**, **Fabric**, **Intelligence**, and **Defense**—that work independently or compound together.

- **Identity (Trust):** Enforces CAC/PIV (EDIP) auth and issues short-lived, Just-In-Time (JIT) SPIFFE credentials for AWS STS, K8s, and Vault.
- **Fabric (Enforce):** Operates below the application layer using Linux kernel BPF-LSM/eBPF to enforce network egress, process execution, and file access policies.
- **Intelligence (Learn):** Uses auto-behavioral learning and Trivy SBOM baselines to auto-generate signed kernel policies and detect supply chain drift.
- **Defense (Detect):** Features a SOC workbench with automated SOAR playbooks, SentinelMap attack graphs, and a cascading kill switch.

Differentiation

- **One Identity, One Audit, One Revoke:** Replaces fragmented point solutions with a single SPIFFE identity fabric and a single action that revokes access across all four planes simultaneously.
- **Agent-Native Safety:** Built-in safeguards bound the blast radius and financial impact of compromised AI agents, ensuring every action is attributable to a human.
- **Air-Gapped & Sovereign:** CAC/PIV-rooted architecture engineered for regulated, air-gapped, and defense-grade environments meeting M-21-31 EL3 logging standards.

Your mission is our commitment

Contact us at build@bridgephase.com to inquire about working together.