

COLLABAISHIELD

MSSP FOR YOUR COLLABORATION & AI STACK

Your infrastructure is secure. Your workforce isn't.

A fully managed, 24/7 Security Operations Center purpose-built for Google Workspace and Microsoft 365 — extending your existing SOC into the collaboration and agentic layers without replacing it. Every behavioral action your workforce takes, and every AI interaction across approved and unsanctioned tools.

THE CURRENT GAP

Employees operate daily inside Google Workspace, Microsoft 365, Copilot, Gemini, ChatGPT and dozens of other AI tools — each capable of exposing corporate, financial, PII and PHI data through a layer your SOC was never built to monitor.

Traditional SIEMs detect compromised machines. They cannot detect compromised intentions. And when cost-driven log dropping deprioritizes SaaS telemetry, the result is complete blindness to identity attacks and rogue AI integrations.

WHAT YOU GET

- ✓ MSSP coverage for collaboration and AI tools, powered by Google Security Operations SIEM/SOAR and Threat Intelligence
- ✓ Fully managed and active in hours — no analysts to retool or train
- ✓ Pre-submission prompt scanning stops data leaks before they happen
- ✓ Shadow AI discovery across unauthorized AI tool usage
- ✓ Compliance policies mapped to your business needs

ENDPOINTS SECURED. FIREWALLS CONFIGURED.

The attack surface is now human and agentic behavior — not infrastructure.

Three tiers. One managed layer.

TIER 01

SecOps for Collaboration

Telemetry from Google Workspace and Microsoft 365 into a dedicated Google SecOps tenant, with US-based analysts on 24/7/365 triage and response.

- Fills a critical void in SIEM/SOAR deployments
- Predictable per-endpoint monthly pricing
- 24/7 US-based MSSP SOC coverage
- Google Threat Intelligence integration
- Baseline compliance reporting

TIER 02

Enterprise AI Governance

Shadow AI protection and policy enforcement across embedded AI assistants and no-code agentic platforms, with real-time DLP guardrails.

- Saf3AI governance layer + 49+ connectors
- Pre-submission prompt scanning (Copilot & Gemini)
- Automated compliance mapping (OWASP, NIST, HIPAA)
- AI usage observability & cost control (FinOps)

TIER 03

Blindspot Defense

Everything in Tiers 01 and 02, plus full agentic workflow tracing and custom AI policy enforcement for regulated environments.

- Full agentic workflow tracing (OTEL-native)
- Custom AI policy enforcement via OPA engine
- EU AI Act, NIST AI RMF & OWASP LLM readiness
- Custom DLP rules: PII, PHI, PCI and more

THE DITO SOC — HUMAN-IN-THE-LOOP MSSP ENGINE

Powered by Google SecOps

Google SecOps stack

SIEM, SOAR and Google Threat Intel for rapid triage

24/7/365 monitoring

Continuous alert analysis by Dito's specialized analyst teams

100% portability

Non-locked-in architecture on Google's security ecosystem

Shadow AI detection

Unauthorized or hidden AI usage, surfaced across the organization

Data exfiltration prevention

Real-time DLP for PII, PCI and PHI during agentic interactions

Audit-ready compliance

Live reporting for NIST, HIPAA, GDPR and SOC requirements

**Your infrastructure
is secure.
Now complete the
architecture.**

Start with a Shadow AI Usage Report, a Copilot & Gemini data leakage audit, and custom behavioral monitoring in your core tools.

ditoweb.com/services/collabaishield/