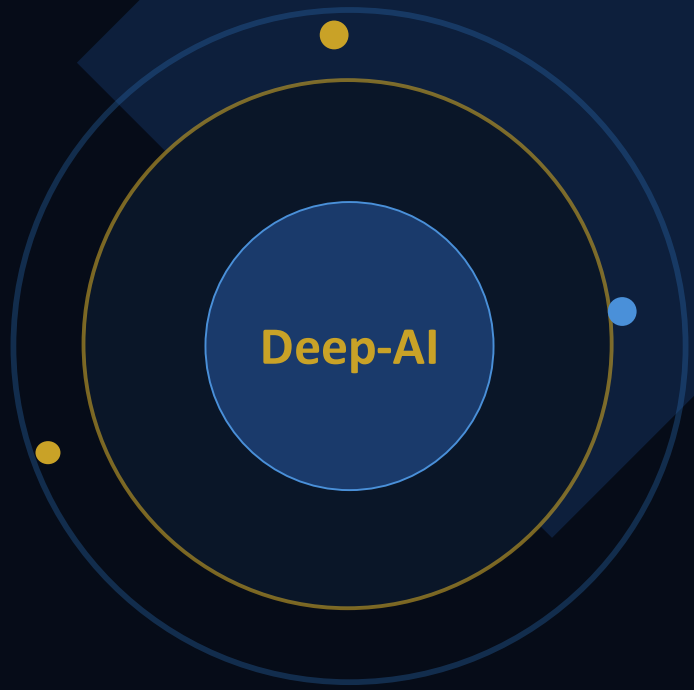
GC | CYBERSECURITY

★ WORLD'S PIONEERING AUTONOMOUS PLATFORM ★

SOLUTION SHEET

AUTONOMOUS EMAIL DATA PROTECTION

Complete, Provable Control Over Sensitive Data Movement in Email



$10.2M
Avg. U.S. Breach Cost

#1
Email: Top Breach Vector

GC | CYBERSECURITY

AUTONOMOUS EMAIL DATA PROTECTION

The First System to Give Enterprises Complete, Provable Control Over Data Movement in Email.

THE GC ADVANTAGE

The only platform satisfying both simultaneously:

CISO
Prevention & Control

↔

GENERAL COUNSEL & AUDIT

"Does your organization have autonomous control over sensitive data in email — or is legacy DLP still leaving you exposed?"

Enterprise Email: The #1 Breach Vector Your Board Has Not Contained.

Enterprise email (Microsoft 365, Google Workspace) — the **primary vector for sensitive data exfiltration** by insiders, attackers, and automated systems alike. Legacy DLP covers fewer than 2 of 9 critical exfiltration vectors. The gap is not a feature gap — it is an architectural failure.

$10.2M	$4.4M	4%	#1
Avg. U.S. Breach Cost	**Global Avg. Breach Cost**	**Global Revenue at Risk**	**Email: Top Breach Vector**
IBM 2025	*IBM 2025*	*GDPR/NIS2/DORA*	*Verizon DBIR*

BUSINESS CONTINUITY RISK

- Intellectual Property & Trade Secrets — AI-driven theft & inadvertent leaks in regulated verticals
- Healthcare & Financial Records — High-sensitivity PII & PHI crossing email perimeters undetected
- Privileged Legal Communications — Breach of attorney-client privilege via email exfiltration

REGULATORY LIABILITY

- GDPR / HIPAA / PCI-DSS / CCPA / DORA / DPDP — multi-jurisdictional fines up to 4% global revenue
- Cross-Border Data Transfer Violations — automated workflows moving regulated data across jurisdictions
- SOX Executive Liability — inadequate internal controls; $5M+ fines + prison for executives

LEGACY SOLUTION GAPS — Why Incumbent Tools Cannot Solve This

EMAIL DLP
Static policies, false positives, manual tuning — zero real exfiltration control

SECURE EMAIL GATEWAYS
Inbound threat focus only — zero authority over outbound data movement

COMPLIANCE / GRC
Post-event documentation — no real-time data protection capabilities

RESULT Uncontrolled insider risk, IP leakage, regulatory exposure & cross-border violations — **all undetected until after the damage is done.**

GC | CYBERSECURITY

COVERS ALL MAJOR EMAIL SERVICES

- Microsoft 365 — E1 / E3 / E5 / E7
- Google Workspace
- MS-Exchange
- Domino
- Icewarp / Skyconnect
- Zoho / Zymra

TRUSTED ACROSS ALL MAJOR SECTORS

- Banking & Financial Services
- Insurance
- Healthcare & Pharma
- Government
- Hi-Tech & Manufacturing
- Retail / Oil & Gas

TRUSTED BY THE GLOBAL 2000

10+ INDUSTRY VERTICALS
5 CONTINENTS

GC CYBERSECURITY · www.gccybersecurity.ai

OUR SOLUTION & QUANTIFIABLE PROOF

A continuous, Deep-AI driven governance loop — replacing manual intervention with autonomous classification, prevention, compliance, and defensibility.

THE AUTONOMOUS CLOSED-LOOP MODEL: 4-STEP ARCHITECTURE

01 CLASSIFY

Deep-AI Contextual Intelligence

Differentiator: 90%+ autonomous accuracy — zero human intervention or manual rule-tuning required.

Impact: Automatically classifies all confidential data — structured or unstructured

02 PREVENT

Real-Time Adaptive Control

Differentiator: Neutralizes threats from any actor: employees, contractors, malware, AI agents etc.

Impact: 70%+ reduction in insider-driven and GenAI-related data leaks.

03 COMPLY

Enforcement of Regulatory Compliance

Differentiator: Native enforcement for GDPR, HIPAA, PCI-DSS, CCPA, DORA, and DPDP — zero tuning.

Impact: Shields organization from regulatory fines reaching 4% of global annual revenue.

04 AUDIT

Executive-Ready Forensic Reports

Differentiator: C4i CyberSOC dashboards bridge the gap between CISO operations and General Counsel.

Impact: 50% faster compliance and audit preparation via fully automated evidence generation.

QUANTIFIABLE IMPACT — AVERAGE REALIZED GAINS ACROSS 100+ DEPLOYMENTS

90%
Classification Accuracy
AI-driven, zero manual tuning

70%
Fewer Insider & AI Leaks
Human and non-human actors covered

50%
Faster Compliance Prep
Automated evidence generation

30%
CapEx / OpEx Savings
Avg. realized across 100+ deployments

OUTCOME

Continuous, autonomous enforcement with real-time regulatory defensibility — shifting enterprises from reactive monitoring to **proactive risk governance.**

GC | CYBERSECURITY

An Autonomous Data Protection Architecture

Built for the AI era & Unbounded Complexity

AUTONOMOUS 3-LAYER ARCHITECTURE

ENFORCEMENT LAYER
DLP · Exfiltration Prevention · Compliance Enforcement

EXECUTION LAYER
6 Autonomous AI Agents

ORCHESTRATION LAYER
Deep AI Control Core

The GC Platform operates as an autonomous control-plane — classifying, governing, enforcing data protection & providing compliance across every email vector without rip-and-replace.

Email is the breach vector. Autonomous control is the solution.

www.gccybersecurity.ai

GC | CYBERSECURITY

WHY LEGACY DLP CANNOT CATCH UP

Architectural Lock-In
Modular, additive systems can detect — but never govern. Intelligence cannot emerge. Just adding AI will not fix the problem, it will only worsen it.

Not built to handle new threats & Gen AI
Designed for human actors with static rules, they cannot deal with the explosion of new actors (malware, AI agents, bots) and amplification of data movement,

Loss of Visibility & Control
Can at best provide visibility & controls for only 20% of data (structured) and not 80% of data (unstructured)

NEXT STEPS

01 30-Day Proof of Value — zero-touch deployment on live tenant
02 Competitive TCO Analysis — custom cost model vs. your current stack
03 Executive Risk Briefing — board-ready gap analysis & compliance report
04 Phased Displacement Plan — structured migration, zero downtime

Competitive Capability Matrix & Use Case Coverage

Where Legacy DLP Fails

CAPABILITY MATRIX — GC vs. Email DLP Tools

CAPABILITY	EMAIL DLP	GC PLATFORM
AI-Native Engine	✗	✓
Data Leak Prevention	✓	✓
Data Exfiltration Prevention	✗	✓
Auto Data Classification	✗	✓
Auto Data Access Control	✗	✓
Auto Policy Generation	✗	✓
Actor & AI Agent Administration	✗	✓
Regulatory Compliance Enforcement	~	✓
CyberSOC Forensic Trails	~	✓
SaaS & On-Prem Deployments	~	✓

USE CASE COVERAGE — 9 Critical Exfiltration Vectors

Accounting for 70%+ of real-world email breaches

USE CASE	TYPE	EMAIL DLP	GC PLATFORM
Mis-Directed Emails	Accidental	~	✓
Mis-Attached Emails	Accidental	✗	✓
Mis-Typed / Wrong Recipient	Accidental	✗	✓
Cloud Draft Exfiltration	Malicious	✗	✓
Exfiltration by Encryption	Malicious	✗	✓
Exfiltration by Mis-Classification	Malicious	✗	✓
Malware Password-Protected Tx	Malware	~	✓
Bot Large-Volume Transmissions	Malware	✗	✓
GenAI Poison Email Exfiltration	GenAI	✗	✓

COVERAGE LEGEND ✓ Full Coverage ~ Partial Coverag ✗ No Coverage

GC achieves complete coverage across all 9 critical use case categories

The only solution with full coverage across every accidental leak or malicious exfiltration email vector