DARKSCOUT

Darkscout / Email - Threat Intelligence

Turning global attacker signals into real-time protection for the inbox and bg colour should be

Email attacks are costly

As a business, your inbox is one of your most targeted assets. And the repercussions of an email-borne breach are significant – and expensive.

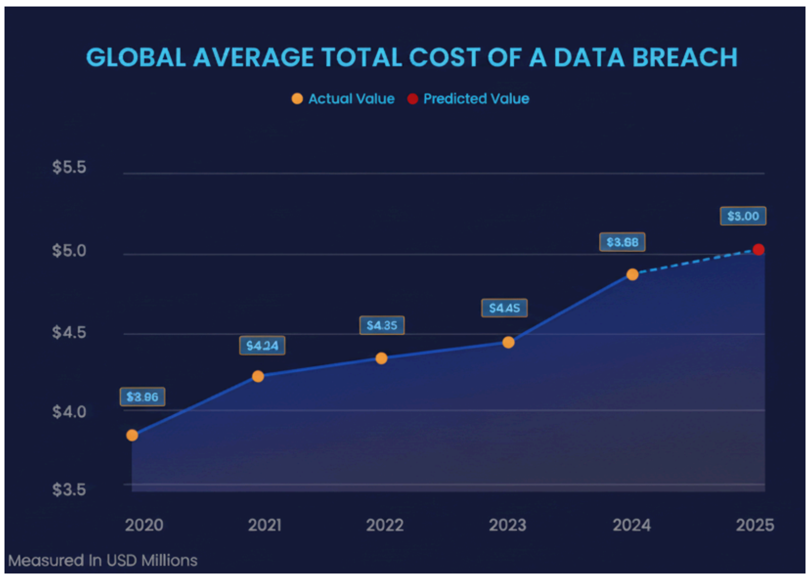
From targeted phishing and business email compromise (BEC) to account takeover and supplier fraud, a single malicious email can open the door to data theft, ransomware, and financial loss. A comprehensive email threat intelligence capability is essential to reduce your risk, protect your brand, and secure every communication.

Existing email defenses don’t cut it

Traditional email security depends on signatures, blocklists, and static rules. These controls struggle against modern attackers who:

Rapidly rotate domains, IPs, and infrastructure Use malware-free phishing and social engineering
Abuse trusted services (cloud storage, SaaS, messaging platforms)
Compromise real accounts inside your supply chain
Static filters often miss low-volume, high-impact attacks like BEC and vendor fraud. They see each message in isolation, without understanding historical communication patterns, sender-recipient relationships, or the wider attacker infrastructure behind an email.

In today’s threat environment of constantly changing domains, lures, and tools, rule-based filtering and basic reputation checks are no longer enough.



Stop email threats before they reach users, without signatures or static rules

Darkscout / EMAIL – Threat Intelligence protects your organization by understanding attacker behavior and infrastructure, not just scanning messages for known bad indicators.

Darkscout fuses global threat data, attacker infrastructure mapping, and behavioral analysis of your own email environment to identify and stop sophisticated phishing, BEC, and account-takeover attempts in real time even when they use brand new domains, clean attachments, or trusted services.

It builds a live picture of who is targeting you, how they operate, and which assets they use, then feeds that intelligence directly into your existing email security, SIEM, and SOAR stack.

Secures every email interaction

Known threats

Correlates incoming email with Darkscout’s global threat intelligence on malicious domains, IPs, and campaigns, blocking infrastructure already linked to phishing, malware, or fraud before it hits user inboxes.

Unknown & emerging threats

Uses behavioral analytics and infrastructure graphing to spot previously unseen domains, URLs, and sending patterns that resemble active attacker campaigns, stopping zero-day phishing and novel BEC attempts that bypass traditional filters.

Credential theft & phishing

Analyzes links, redirects, and landing pages including those hosted on legitimate cloud services to detect credential harvesters and MFA-phishing kits, protecting user identities and preventing account takeover.

Human layer (BEC & fraud)

Understands normal communication patterns for executives, finance teams, and suppliers. Flags anomalous payment requests, invoice changes, and impersonation attempts even when they come from apparently legitimate accounts and contain no malware.

Compromised accounts & supply chain

Correlates inbound and outbound activity, login behavior, and external intelligence to spot when a partner, vendor, or internal account has been taken over, allowing you to intervene before attackers can move laterally or exfiltrate data.

Integrated into your SOC workflows

Darkscout / EMAIL Threat Intelligence plugs directly into your existing email platforms and security stack, enriching every message with attacker context before it reaches the user. Microsoft 365, Google Workspace, and other email systems forward message telemetry and events to Darkscout for assessment; Darkscout returns risk scores, campaign tags, and IOCs that your tools can use to hold, quarantine, or flag high-risk mail and optionally alert the SOC.

Within the Darkscout console, analysts can see anomaly scores for senders and domains, mapped attacker infrastructure, and narrative summaries that explain why a message was flagged. This context makes it faster to investigate, escalate, and close email-driven incidents.

Darkscout's email intelligence also feeds your wider threat picture. Exported IOCs and risk signals integrate with SIEM, SOAR, EDR/XDR, and ticketing systems, allowing your SOC to correlate email activity with endpoint, network, and identity events for true end-to-end investigations.

Use Case coverage

Use Case	Threat Intelligence (core)	EMAIL – Intelligence + Response module
Business Email Compromise (BEC)	Detects executive and vendor impersonation using behavioral and content analysis; alerts SOC with risk scores and campaign context.	Automatically quarantines or soft-deletes high-risk messages, adds in line user warnings, and triggers SOAR playbooks for financial verification.
Targeted Phishing & Credential Theft	Identifies phishing links, credential pages, and MFA-bypass kits, even on trusted services; exports related domains/IPs as IOCs.	Enforces URL rewriting and time-of-click checks, blocks access to malicious pages, and pushes indicators to web and endpoint controls.
Account Takeover Detection	Flags anomalous sending patterns, login locations, and reply-chain hijacking indicative of compromised accounts.	Initiates automatic account containment actions via IAM/SOAR (password reset, token revocation, conditional access enforcement).
Supplier / Vendor Fraud	Detects suspicious changes in payment details and unusual requests from partner domains; correlates with external intel on compromised suppliers.	Holds suspected fraud emails from vendors, opens tickets for procurement/finance, and updates allow/deny policies when confirmed.
Ransomware & Malware Delivery	Correlates attachment behavior and URLs with known loader/C2 infrastructure; tags campaigns and surfaces related IOCs.	Blocks delivery of risky attachments/links, enriches EDR/XDR with IOCs, and launches automated containment workflows on affected endpoints.
Brand & Domain Abuse	Monitors for look-alike domains and spoofing attempts targeting your brand and key executives; alerts when they appear in inbound mail.	Automatically adds abusive domains to blocklists, updates email authentication policies, and notifies brand/legal teams.

•**About Darkscout:** Darkscout (getdarkscout.com) is a cybersecurity company focused on turning complex, fast-moving threat signals into clear, actionable intelligence. By analyzing data from email, internet-facing infrastructure, and other external sources, Darkscout helps organizations see themselves the way adversaries do and spot emerging risks before they become incidents. Its platform enriches existing security tools and workflows with context about attacker infrastructure, active campaigns, and exposed assets, enabling security teams to prioritize what matters most and respond with greater speed and confidence.