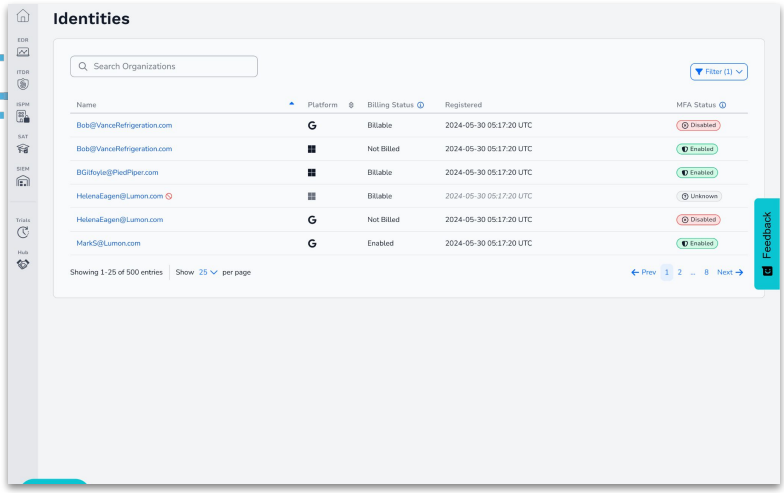
Huntress Managed Identity Threat Detection & Response (ITDR) for Google Workspace

Stop identity-based attacks across GWS with fully managed detection and response

Google Workspace (GWS) has become a primary attack surface for modern cyber threats - from business email compromise (BEC) and phishing to malicious inbox rules and unauthorized access. But most security teams lack the time, visibility, or expertise required to detect these attacks early and respond quickly.

Huntress Managed ITDR for Google Workspace delivers continuous monitoring, detection, investigation, and response for your Google identities and email environment. Backed by the Huntress 24/7 SOC, we stop identity-driven attacks before they turn into business-impacting incidents.



Key Outcomes

Identity Resilience

Continuously monitor Google Workspace authentication activity to detect suspicious sign-ins, unauthorized access attempts, and identity takeover behavior. Huntress identifies and investigates abnormal login activity before attackers establish persistence.

Email Security Against BEC

Detect attacker manipulation of inbox rules, email forwarding, and mailbox behaviors commonly used in business email compromise (BEC). Our SOC identifies and investigates suspicious rule changes designed to exfiltrate data or redirect communications.

Rapid Incident Response

When identity attacks occur, Huntress analysts investigate the activity, validate threats, and provide clear remediation guidance. Our team helps organizations quickly disable compromised accounts, remove malicious rules, and contain attacker access.

HUNTRESS

24/7 SOC protection for Google Workspace identities

Google Workspace + Huntress Managed ITDR

Huntress ingests and analyzes Google Workspace telemetry to identify attack patterns targeting identities and mailboxes. Our platform detects threats such as:

Location-based & VPN Anomalies

Expose unusual login locations and VPNs to ensure only authorized users have access to your data.

Shady Inbox & Forwarding Rules

Identify attacker-created Gmail filters used to hide security alerts, delete MFA emails, or suppress victim replies.

Malicious Datacenter Infrastructure

Track when identities authenticate from new data center providers, prioritizing the “usual suspects” that are most abused by threat actors.

Huntress by the Numbers

4.9/5
G2 customer rating

100%
Of customers would recommend[1]

3-minute
Mean-time-to-respond (MTTR)

10M+
Identities protected

> **As we increasingly rely on Google Workspace as our identity hub, we’ve realized traditional email security simply isn’t enough. Huntress Managed ITDR for GWS gives us confidence that identity threats will be investigated and handled by experts, not surfaced as yet another alert for our team to chase.**
>
> Blair Compton | IT Director | BizStream

[1]https://uevi.co/1546QIJX

HUNTRESS