









Raven AI-Email Security & Email DLP Datasheet





Raven is fully ISO 27001 and SOC 2 compliant, ensuring the highest standards of information security for regulated and fast-growing organizations alike.

Module	Feature	Details
<div> Threat Detection</div>	Phishing protection	<ul style="list-style-type: none">→ Domain fraud / spoofing prevention→ Contextual AI analysis→ SaaS tools phishing prevention→ Credential phishing prevention→ Bulk mail / grey mail detection
	BEC protection	<ul style="list-style-type: none">→ Social engineering→ Financial fraud→ Attorney fraud detection
	URL scanning	<ul style="list-style-type: none">→ Malicious URL detection→ CTA based deep-scan→ Suspicious trackers, redirects, shorteners detection
	Malware	<ul style="list-style-type: none">→ Defense in depth on malware scanning→ Sandbox reports available on-demand
	Impersonation & spear phishing protection	<ul style="list-style-type: none">→ CXO & Employee impersonation protection→ Personal ID detection→ Free mail detection
	Vendor Risk Management (TPRM) <div>★ Industry First</div>	<ul style="list-style-type: none">→ Automatic vendor detection→ Vendor invoice finger printing & bank anomaly detection→ Vendor impersonation / spoofing detection→ Continuous vendor infra monitoring (email + web infra changes)→ Compromised vendor identification→ Thread hijacking and unauthorised IDs in threads detection→ TPRM alerts & recommendation reports <div>★</div> <div>★</div>
	Internal Risk	<ul style="list-style-type: none">→ Internal alerts that carry risk→ Employees circulating malicious files / URLs→ Anomaly detection
	Group ID abuse monitoring	<ul style="list-style-type: none">→ Automatic monitoring of group IDs
	Adaptive Security	<ul style="list-style-type: none">→ LLM based threat rules update on new tactics

Module	Feature	Details
 Incident Management & Remediation	Attack Analysis	<ul style="list-style-type: none">→ AI insights about the incident→ Key detections across email meta data→ Default privacy view applied→ Preview email available only for RBAC→ Email alerts to admin
	Remediation	<p>Remediation Modes</p> <ul style="list-style-type: none">→ Automatic & Manual <p>Available Actions</p> <ul style="list-style-type: none">→ One click pull from inbox→ Junk or Quarantine folder movement→ User account reset from incident→ Block domains / users from incident
 Inbound Rules	Block and allow lists	<ul style="list-style-type: none">→ Maintain block lists & allow lists→ Domain level, user level, IP→ Address level block / allow rules
 Analytics	Dashboard	<ul style="list-style-type: none">→ Easy to view incidents across timeline→ Detection methods
 Account Monitoring	Single window for internal and external users	<ul style="list-style-type: none">→ Single view of all mail IDs internally & externally→ Reset accounts→ Tag VIP / Finance from Account monitoring→ Block external Ids→ Add vendors / regulators manually or searching
 RBAC	Admin management	<ul style="list-style-type: none">→ RBAC based controls→ oAuth based login
 Integrations	Supported Platforms	<ul style="list-style-type: none">→ Google workspace→ Microsoft 365
	SIEM	<ul style="list-style-type: none">→ Splunk
	GRC platforms	<ul style="list-style-type: none">→ Scrut, Sprinto (In pipeline) <div>Coming Soon</div>






Module	Feature	Details		
<div> Email DLP (Outbound)</div>	Policy management	<div>Data Scope</div> <div><div>→ 40+ predefined data types and growing</div><div>→ Dev data like codes/ tokens / auth access / credentials detection★</div><div>→ Custom data types / IP for business / industry on request can be developed★</div><div>→ True file type detection (70 common types)</div><div>→ No restrictions on data type groupings</div></div> <div>Detection Scope</div> <div><div>→ Email body, attachments, inline images, password protected files, zip files</div><div>→ Context aware detection★</div><div>→ No regex configuration</div><div>→ File type blocking</div><div>→ Instant policy changes with no lag</div><div>→ Severity assignment</div><div>→ Risky vendor blockingComing Soon★</div><div>→ Prefilled for complianceComing Soon★</div></div> <div>User Scope</div> <div><div>→ Google groups / Azure groups Integration / custom groups</div><div>→ Internal CUG definitions</div><div>→ External Partner groups</div><div>→ Global exclusion list / global block list</div></div> <div>Detection Mode</div> <div><div>→ Policy level block mode</div><div>→ Policy level monitor mode</div></div>	Incident Management	<div>Management modes</div> <div><div>→ Log event, block event, alerts</div><div>→ Mail alerts to admin / user / manager</div></div> <div>Incident Dashboard</div> <div><div>→ Policy triggered</div><div>→ Incident summary with data detected across content, attachment, images</div><div>→ Preview mail (RBAC based) - Sender / receiver</div><div>→ Release requests management</div></div>

Module	Feature	Details
 Email DLP (Outbound)	Deployment	<ul style="list-style-type: none"> → Relay server based → No changes to MX → 10 mins deployment time → All users or select users based deployment
	Secure User Portal	<ul style="list-style-type: none"> → Request release / purpose → Secure portal for password-based file scanning → oAuth based login

 Security & Compliance	Data residency	<ul style="list-style-type: none"> → India
	Hosting	<ul style="list-style-type: none"> → India
	AI-Models hosting	<ul style="list-style-type: none"> → India
	Compliances	<ul style="list-style-type: none"> → SoC2 (completed) → ISO 27001 (undergoing with TUV)
	Encryption	<ul style="list-style-type: none"> → Data at rest and transit
	Access Management	<ul style="list-style-type: none"> → Zero-Trust Access with Continuous Security Controls



AI Native Context-aware email security for M365 & Google Workspace



Raven is fully ISO 27001 and SOC 2 compliant, ensuring the highest standards of information security for regulated and fast-growing organizations alike.