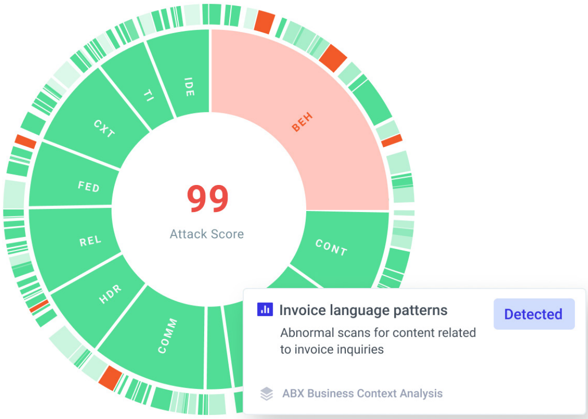
Abnormal Inbound Email Protection

Protect your organization from all types of advanced email threats and unwanted email.

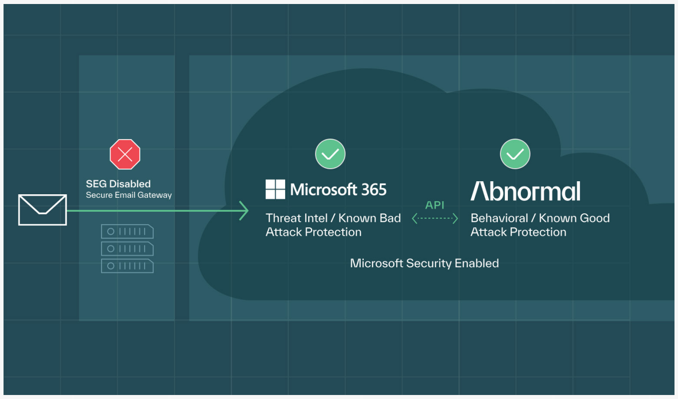
Protect your end users from the full spectrum of targeted email threats: phishing, ransomware, fraud, social engineering, supply chain attacks, executive impersonation, spam, and graymail. Integrate with Microsoft 365 and Google Workspace via a one-click API without disrupting mail flow. No MX record changes, configuration, or custom policies are needed.

Highest-Precision Protection Against All Attacks

Secure email gateways struggle to block socially-engineered attacks that pass reputation checks, have no links or attachments, and appear to come from trusted sources. Abnormal profiles known good behavior and analyzes over 45,000 signals to detect anomalies that deviate from these baselines, and then precisely blocks all socially-engineered and unwanted emails—both internal and external—and detects and remediates compromised accounts.



Abnormal scans for content related to invoice inquiries

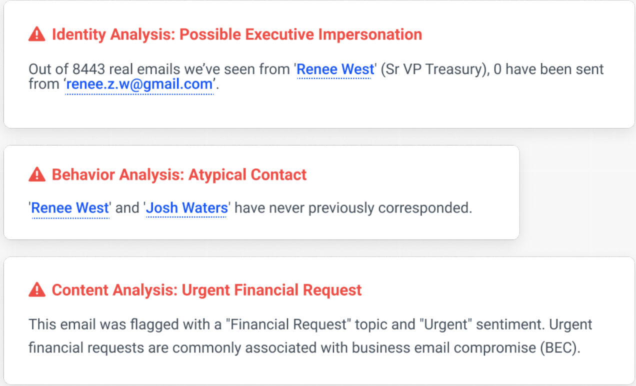

SEG Disabled
Secure Email Gateway
Microsoft 365
Threat Intel / Known Bad Attack Protection
API
Abnormal
Behavioral / Known Good Attack Protection
Microsoft Security Enabled

Remove Your Secure Email Gateway and Simplify Your Email Security Architecture

Organizations that require comprehensive inbound email protection are stuck with multiple products, incompatible architectures, unnecessary expense, and management overhead. Simplify your stack by eliminating the redundant email gateway layer and re-enabling and enhancing Microsoft's and Google's cloud gateway capabilities.

Enhance Microsoft, Google, and Email Gateway Security with Behavioral AI

By deeply understanding entities—users and vendors, their behavior, relationships, and tone and content shared—Abnormal precisely detects anomalies and blocks attacks that regularly evade Microsoft, Google, and secure email gateways.



⚠ Identity Analysis: Possible Executive Impersonation

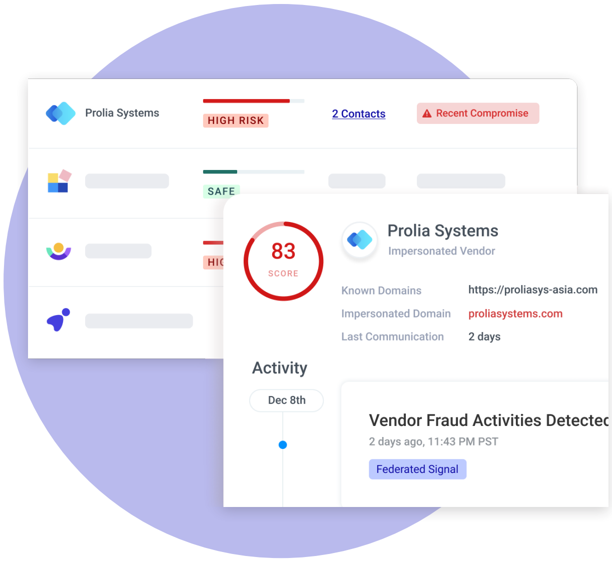
Out of 8443 real emails we've seen from 'Renee West' (Sr VP Treasury), 0 have been sent from 'renee.z.w@gmail.com'.

⚠ Behavior Analysis: Atypical Contact

'Renee West' and 'Josh Waters' have never previously corresponded.

⚠ Content Analysis: Urgent Financial Request

This email was flagged with a "Financial Request" topic and "Urgent" sentiment. Urgent financial requests are commonly associated with business email compromise (BEC).



Prolia Systems | HIGH RISK | 2 Contacts | ⚠ Recent Compromise

SAFE

HIG

83
SCORE

Prolia Systems
Impersonated Vendor

Known Domains https://proliasys-asia.com
Impersonated Domain proliasystems.com
Last Communication 2 days

Activity

Dec 8th

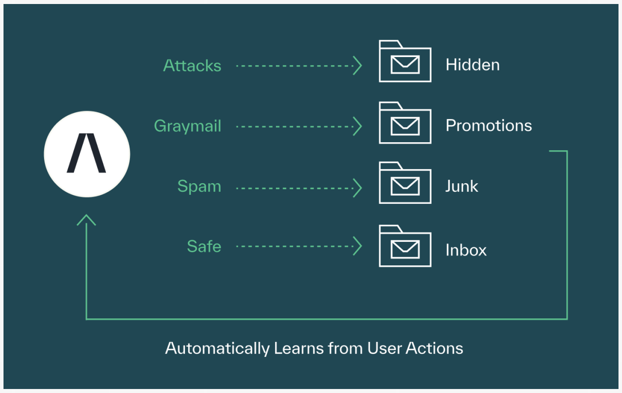
Vendor Fraud Activities Detectec
2 days ago, 11:43 PM PST
Federated Signal

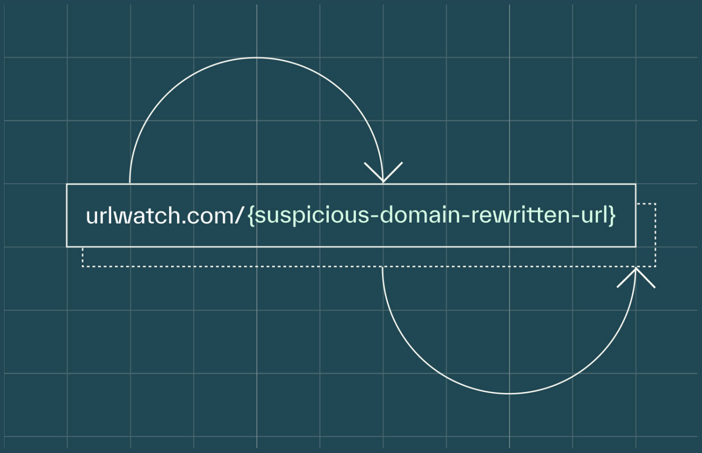
Profiles All Your Vendors for Potential Threats

Your organization's security posture is only as strong as the security postures of your vendors. Soon after integration, Abnormal reviews all your emails to extract your vendor relationships. It monitors your vendors for security risks observed across the entire enterprise ecosystem, automatically identifies when vendor accounts have been compromised, and protects your end users from them.

Improved End User Experience and Productivity

Abnormal learns end-user preferences by observing how they move messages between folders, allowing it to automatically create and manage individualized safe and blocklists, as well as deliver spam and graymail to junk and promotional folders respectively. End users no longer have to rely on spam and quarantine digests to salvage missed messages.



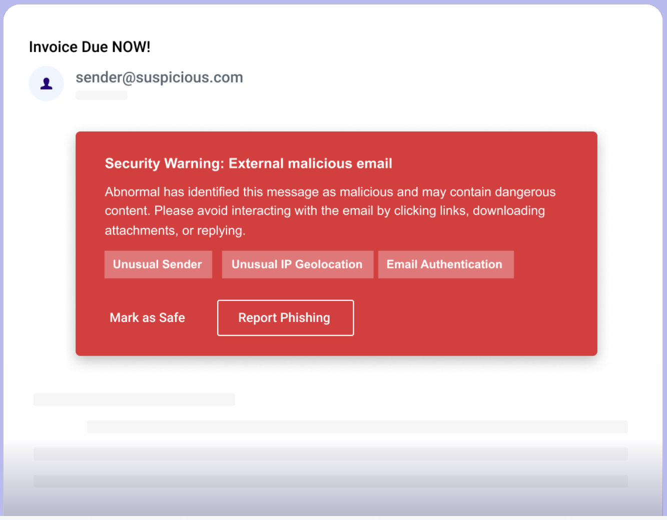


Smart URL Rewriting

Not all emails are malicious. So why rewrite every single URL within them? Abnormal scans every email to determine its risk profile, and only rewrites URLs within those emails that look suspicious.

Contextual Banners That Help End Users

Abnormal precisely assesses every email for potential threat and the type of threat, and if deliverable, automatically provides relevant information using banners. End users, as a result, are better equipped to ensure that they do not fall victim to attack.

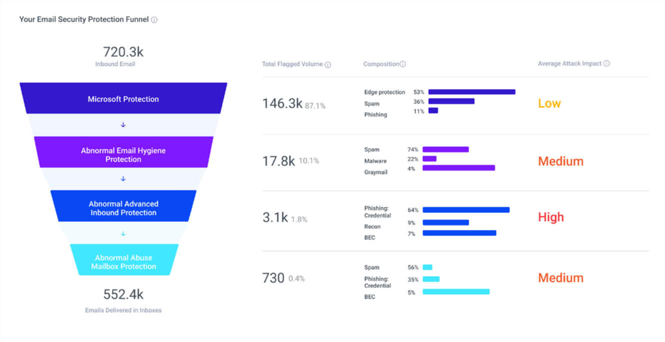


Invoice Due NOW!

sender@suspicious.com

Security Warning: External malicious email

Abnormal has identified this message as malicious and may contain dangerous content. Please avoid interacting with the email by clicking links, downloading attachments, or replying.



Your Email Security Protection Funnel ⓘ

720.3k
Inbound Email
Microsoft Protection
Abnormal Email Hygiene Protection
Abnormal Advanced Inbound Protection
Abnormal Abuse Mailbox Protection
552.4k
Emails Delivered in Inboxes

Total Flagged Volume ⓘ	Composition ⓘ		Average Attack Impact ⓘ
146.3k 87.1%	Edge protection Spam Phishing	53% 36% 11%	Low
17.8k 10.1%	Spam Malware Graymail	74% 22% 4%	Medium
3.1k 1.8%	Phishing: Credential Recon BEC	64% 9% 7%	High
730 0.4%	Spam Phishing: Credential BEC	56% 35% 5%	Medium

Integrates Insights and Reporting

Centralize metrics, insights, and actions across email security solutions, and the management of global blocklists across hundreds of tenants, from a single pane of glass.

Secure Email Gateway Vs. Defense in Depth with Abnormal

⊞ G Threat Intelligence Based Protection

Λ Abnormal Behavioral AI Protection

Capability	SEG	Microsoft 365 + Λbnormal	Google + Λbnormal
Email Hygiene			
IP & Domain Reputation	Yes	⊞	G
Sender Authentication (SPF / DKIM / DMARC)	Yes	⊞	G
Spam	Yes	⊞ + Λ	G + Λ
Graymail	Varies by Vendor	⊞ + Λ	G + Λ
Internal-to-Internal Email Scanning	No	Λ	G + Λ
Outbound Email Scanning	Yes	⊞	G
Policy Engines			
Custom Routing Rules	Varies by Vendor	⊞	G
Advanced Malware Protection			
Full Malware Attachment Scanning	Varies by Vendor	⊞ + Λ	G + Λ
Full URL Inspection	Varies by Vendor	⊞ + Λ	G + Λ
Rewrite Suspicious URLs Only	No	Λ	Coming Soon
URL Protection			
Time of Click URL Protection	Varies by Vendor	⊞ + Λ	G + Λ
Phishing Protection			
Spear-Phishing Protection	Partial	⊞ + Λ	G + Λ
Internal or Lateral Phishing Protection	Varies by Vendor	Λ	Λ
Social Engineering Protection			
Business Email Compromise (BEC) + CEO Fraud	Varies by Vendor	Λ	Λ
Vendor Email Compromise (VEC) + Invoice Fraud	No	Λ	Λ
Account Compromise Protection			
Compromised Internal Account Detection & Remediation	No	Λ	Λ
Compromised Supplier / Vendor Accounts Detection	No	Λ	Λ
Post Delivery Remediation			
Automated Abuse Mailbox Operations	No	Λ	Λ
Post-Delivery Remediation of Zero-Day Attacks	Premium License	Λ	Λ
End User Experience			
Automated Safe And Block Lists per User	No	Λ	Coming Soon
Automated Bulk Email Sorting	Digests	Mailbox	Coming Soon
Data Loss Protection (Inbound and Outbound)			
Content Control Policies	License Expansion	Yes	Coming Soon

Try Abnormal Inbound Email Protection Today

Integrate within minutes via one-click API, without any disruption to mail flow. No changes to your email configuration or custom policies required.

www.abnormalsecurity.com/risk →