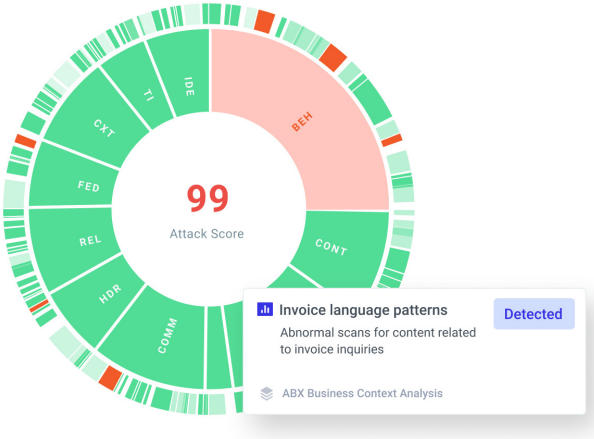
Abnormal Integrated Cloud Email Security

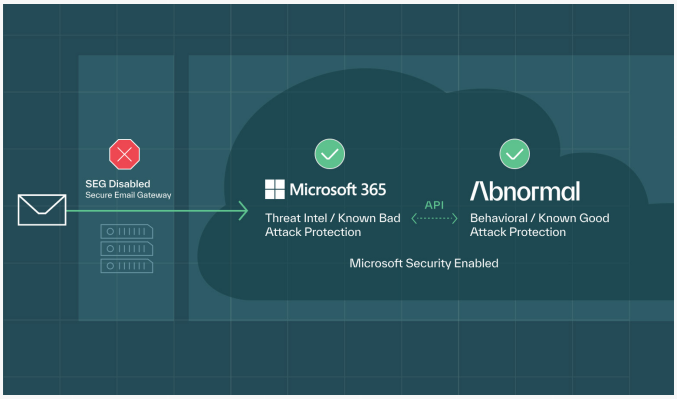
Protect your organization from advanced email threats, unwanted email, and account takeover attacks.

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. Detect and remediate compromised accounts. 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. The Abnormal Integrated Cloud Email Security (ICES) platform 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.



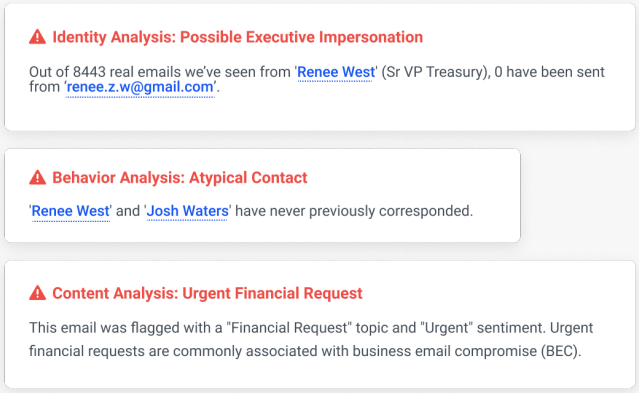


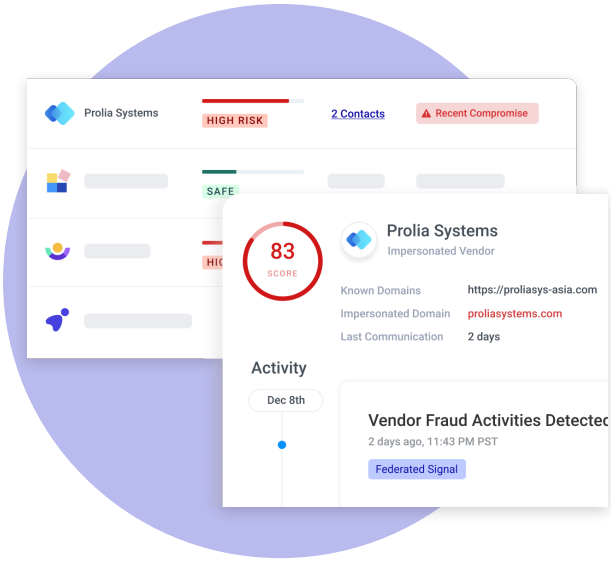
Remove Your Secure Email Gateway and Simplify Your Email Security Architecture

Organizations that require comprehensive inbound email protection are stuck with multiple products, incompatible architectures, unnecessary expense, and management overhead. With ICES, you can simplify your stack by eliminating the redundant email gateway layer and re-enabling and enhancing Microsoft'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 ICES precisely detects anomalies and blocks attacks that regularly evade Microsoft, Google, and secure email gateways.



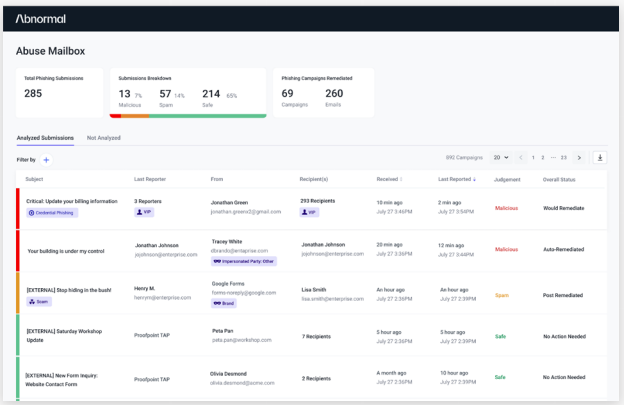


Profiles All Your Vendors For Potential Threats

Your organization's security posture is only as strong as the security posture of your vendors. Soon after integration, ICES 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.

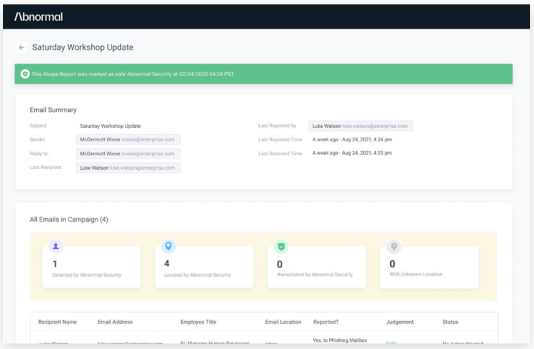
Automate Your Abuse Mailbox

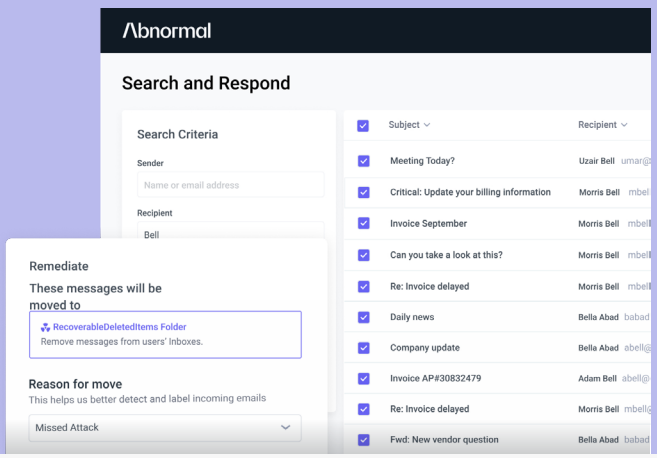
Abnormal ICES centralizes user-reported phishing attacks, and automatically investigates, remediates, and notifies reporters on the results. Approximately 90% of submissions are known to be safe emails, and this automation saves security teams many hours each week.



Fully Automate SOC Operations

Fully automate triage, investigation, remediation, and reporting, for both auto-detected and user-reported email threats. Abnormal natively integrates with SIEM and SOAR tools to enrich insights and to orchestrate workflows.



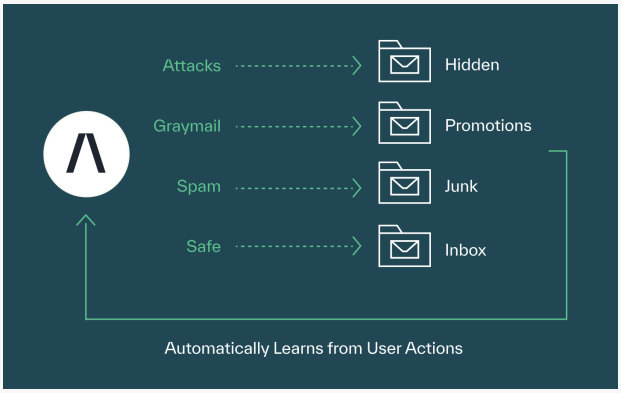


Search and Respond

Use Search and Respond to rapidly contain missed attacks or misdirect emails with sensitive information. Detection 360° provides an opportunity to have false negatives or false positives reviewed and remediated promptly, by the Abnormal team.

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.



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

Threat Intelligence Based Protection

Abnormal Behavioral AI Protection

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