

Advanced Email Security and Anti- Phishing Platform (Cloud Based)

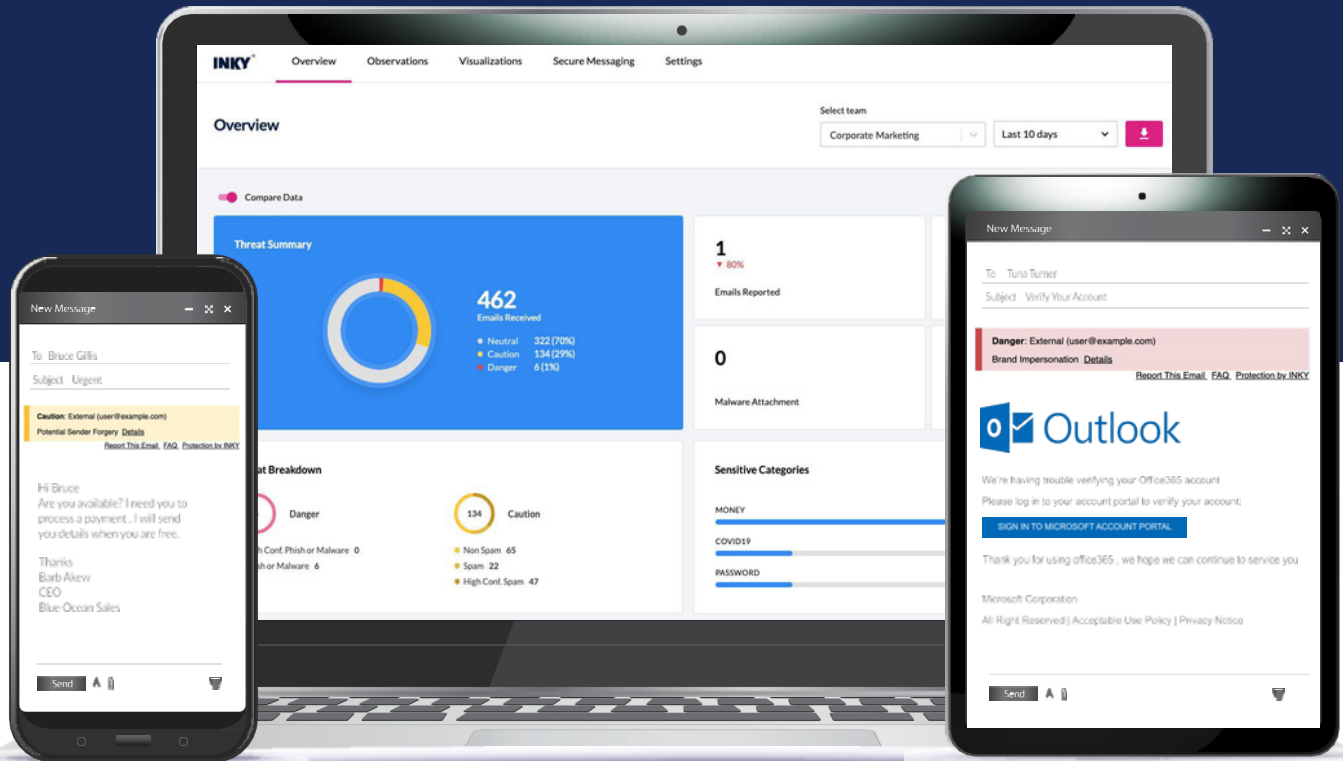
G-Cloud 15

IT Auxilium Ltd

E: hello@gpitservices.co.uk

T: 01223 827 410

Modern Email Security Built for MSPs



Stay secure with INKY in your corner.

Outsmarting malicious actors takes nothing less than agility and ceaseless innovation. INKY combines the power of generative AI and human shield to continuously adapt and stay ahead of the game. Our partners know INKY's got their back.

Email Security that Works

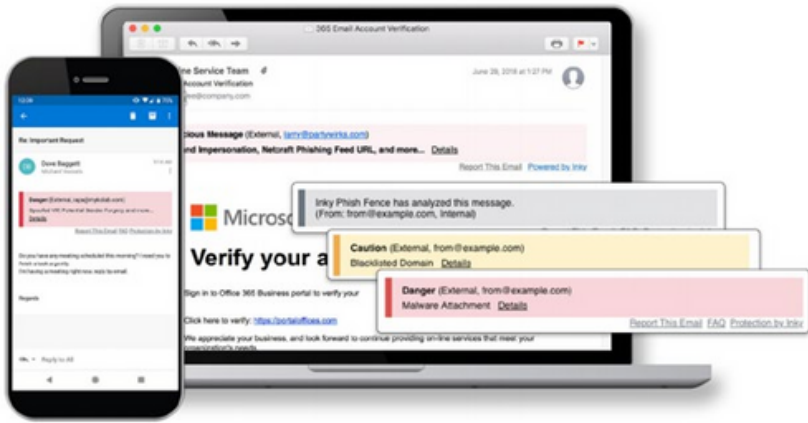
Leverage cutting-edge technology that continuously advances to stay ahead of sophisticated attackers, safeguarding your brand against forgery and protecting against account takeovers.

Easy to Deploy and Manage

INKY is super easy to use. It takes 30 minutes for the initial install followed by 15 minutes for any new customer onboarding. Most importantly, with INKY it takes less than 1 hour per month to manage 1,000 mailboxes.

Streamline Operations

INKY delivers a comprehensive email security platform, eliminating the need for single-solution vendors. Simplify management, reduce costs, and gain a more efficient, scalable solution for your business.

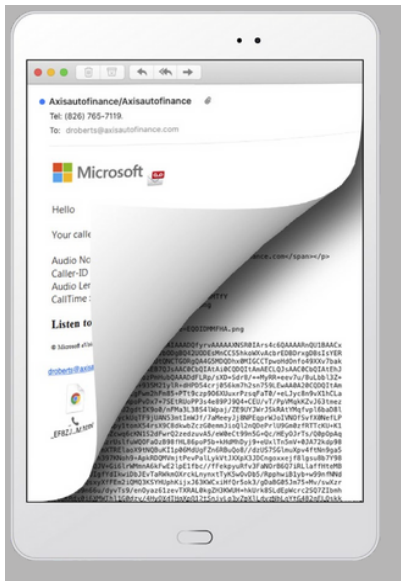
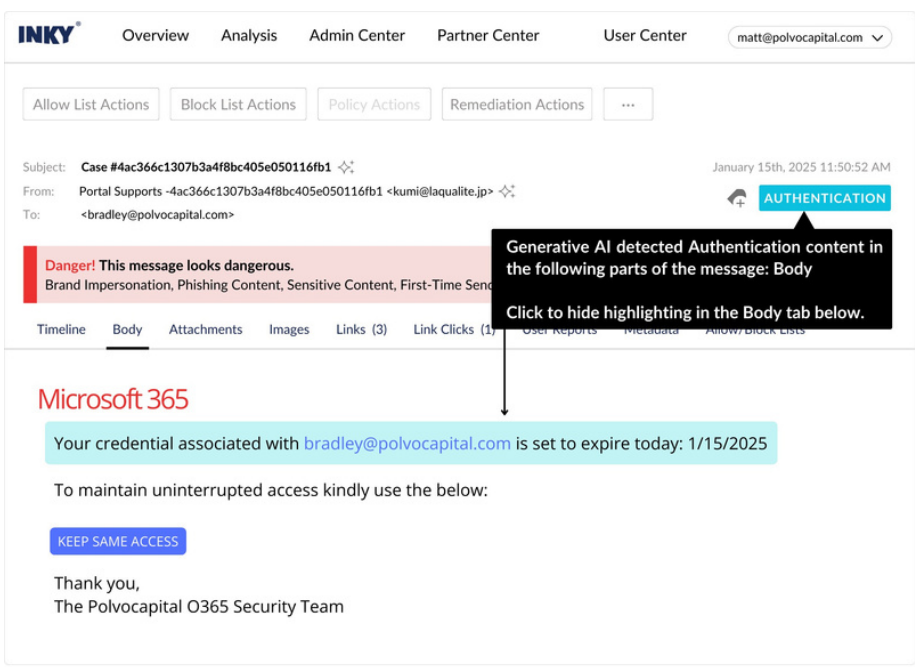


Coach users to make smart decisions –everywhere, all the time.

Periodic security training often falls short with distracted, busy users. INKY's Email Assistant provides continuous coaching, helping users make safe choices on any device or email client.

Seeing is believing with INKY GenAI.

The Dashboard visually breaks down what INKY GenAI detects, tagging threat categories, highlighting suspicious language, and providing detailed explanations. Admins gain deeper insights to track and understand threats more effectively.



Play tough defense using AI against email impersonation.

Detect the behaviors of the most sophisticated attackers with technology that's always getting smarter to keep you ahead of brand forgery and account takeovers.

MODERN EMAIL SECURITY PLATFORM

INKY's GenAI-powered email security platform detects threats that others overlook. Acting as a security coach, the INKY Email Assistant highlights suspicious behaviors with interactive banners, guiding users towards safe actions on any device or email client. IT teams are relieved from the burden of manually filtering every email or maintaining multiple systems. With its powerful technology and intuitive user engagement, INKY effectively blocks bad actors for good.



INKY ADVANCED

Inbound Mail Protection (PF)

Anti-Phishing, Anti-Malware, Spam filter
Uses AI to blocks impersonation and ransomware with intuitive user coaching

Internal Mail Protection (IMP)

Account Takeover protection with sender profiling and social graphing anomaly detection

Advanced Attachment Analysis (AAA)

Detect Zero Day malware

Graymail Protection

Super spam filter for newsletters and alike

Email Signatures

Update and control Email Signatures for compliance and branding purposes



INKY PRO

Everything in Advanced Plus:

Generative AI

Understand language and intent to stop email threats with precision

Outbound Mail Protection (OMP)

Detect and prevent data loss with interactive safeguards for outgoing emails

Email Encryption

Easy-to-use encourages organizations to keep their data secure

DMARC Monitoring

Monitor domain usage to improve email delivery

MODERN EMAIL SECURITY PLATFORM



"INKY's platform covers all the email security and compliance solutions our customers need. The ability to partner with one vendor for multiple products boosts efficiency and improves our bottom line."

Ivan Burkett

Director of Information Technology
GB Tech



"Email is almost always the first avenue a threat actor will take. That is why we partner with INKY. They do an excellent job protecting against phishing attacks, which is vector #1."

Matt Panizari

Sales Engineer

Arete Incident Response



"INKY makes it so easy to install with their auto- onboarding on Microsoft 365. 6 minutes and I'm done."

Matthew Galimi

Founder & CEO
Divergent IT

Key Capabilities

Phishing is still the number one cause of data breaches for companies and the hooks are getting sharper. Most people don't realize how far the problem has advanced. Today's criminals employ a variety of incredibly sophisticated techniques that elude even the most skeptical and well-trained eyes. This is where INKY excels. Through GenAI, AI, and machine learning INKY catches what others miss.



Conversation Analysis

INKY GenAI can "read" each email and fully understand its intent. This allows INKY to identify scams that simple pattern matching cannot.



Computer Vision

INKY renders every email and applies computer vision algorithms to "see" each email as the human recipient will. This helps identify brand impersonation attempts.



QR Code Detection

INKY AI scans and decodes QR codes to determine if the encoded URL is safe.



Approximate Matching Engine

INKY's proprietary approximate matching engine finds brand indicative and scam indicative text, despite attacker cloak attempts like zero font and other tricks.

Block impersonations and coach users to make safe decisions easily with Standard Email Protection.

Shut down impersonators by detecting unusual behavior.

Over two dozen computer-vision and text analysis models see an email much like a person does — only better. Our AI spots fakes, checks if senders are legitimate, and flags suspicious emails like brand impersonation and phishing before you ever click.

85%

Of data breaches are caused by human error.

Source: Verizon

\$125,612

Is the average cost of a Business Email Compromise (BEC) attack.

Source: FBI

38%

Of all cybercrimes involve reported phishing attacks.

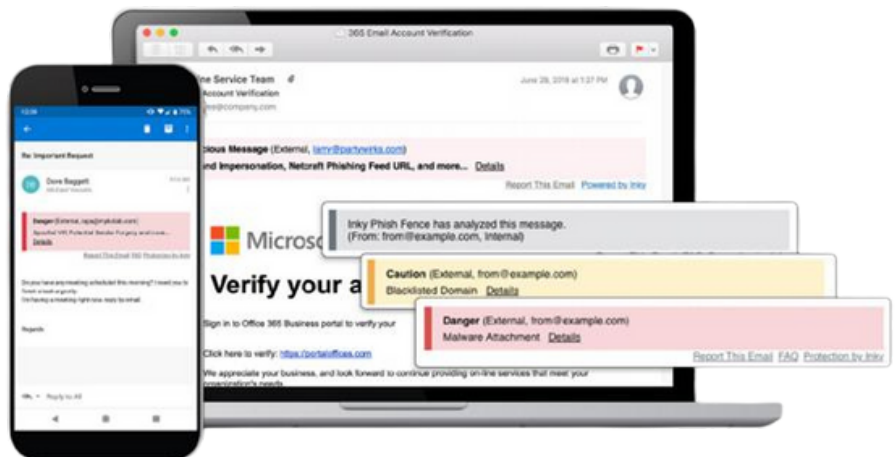
Source: FBI

Compromised email accounts let the bad guys in.

When successful, online imposters acting as company managers or executives can do more financial harm to a business than any other type of cybercrime. Once they have control of a high-profile email account and act as a company authority, these imposters direct wire transfers, facilitate fictitious vendor payments, and more.

Coach users to make smart decisions in real time.

Periodic security training often falls short with distracted, busy users. INKY's Email Assistant provides continuous coaching, helping users make safe choices on any device.



Phishing is still the number one cause of data breaches for companies and the hooks are getting sharper. Most people don't realize how far the problem has advanced. Today's criminals employ a variety of incredibly sophisticated techniques that elude even the most skeptical and well-trained eyes. This is where INKY excels. Through AI, and machine learning INKY catches what others miss.

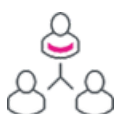
Stay secure with INKY in your corner.

Outsmarting malicious actors takes nothing less than agility and ceaseless innovation. Through GenAI, AI, and machine learning, INKY catches what others miss.



Computer Vision

INKY renders every email and applies computer vision algorithms to "see" each email as the human recipient will. This helps identify brand impersonation attempts.



Text Understanding & Conversation Analysis

INKY incorporates language understanding so it can "read" each email and understand its intent. This allows INKY to identify scams that simple pattern matching cannot.



QR Code Detection

INKY AI-driven QR code detection technology scans emails for QR code imagery and decodes these images to determine if the encoded URL is safe.



Approximate Matching Engine

INKY's proprietary approximate matching engine finds brand indicative and scam indicative text, despite attacker cloak attempts like zero font and other tricks.

STANDARD FEATURES

Inbound Email Protection

Internal Email Protection

NextGen AI Detection

Advanced Computer Vision

QR Code Defense

Anomaly Detection

Standard Attachment Analysis

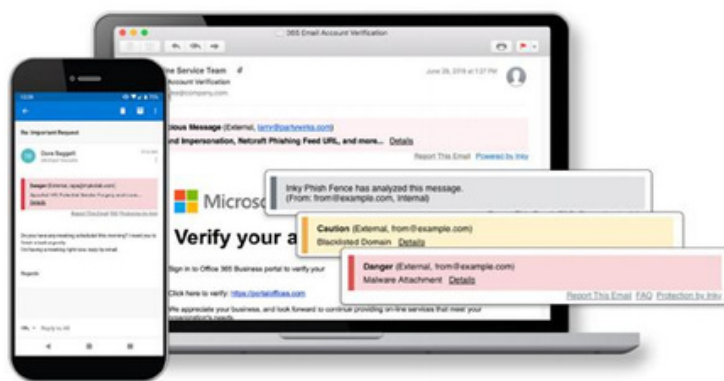
URL Time-of-Click Protection

Geo-Blocking Spam Filtering

Block threats, prevent data leaks, and ensure compliance with the only GenAI-powered email security platform.

INKY Advanced scans it all—outbound & inbound—for smarter, trusted email security.

GenAI and AI models assess every message, checking for spoofing, phishing, and threats hiding in attachments. INKY flags distractions like graymail, keeps your domains in check, prevents data leaks from outbound email, and makes encrypting sensitive messages as easy as adding a subject line tag—all in one solution.



Coach users to make smart decisions in real time.

Periodic security training often falls short with distracted, busy users. INKY's Email Assistant provides continuous coaching, helping users make safe choices on any device.

Stay secure with INKY in your corner.

Outsmarting malicious actors takes nothing less than agility and ceaseless innovation. Through GenAI, AI, and machine learning, INKY catches what others miss.



Computer Vision

INKY renders every email and applies computer vision algorithms to "see" each email as the human recipient will. This helps identify brand impersonation attempts.



Text Understanding & Conversation Analysis

INKY incorporates language understanding so it can "read" each email and understand its intent. This allows INKY to identify scams that simple pattern matching cannot.



QR Code Detection

INKY AI-driven QR code detection technology scans emails for QR code imagery and decodes these images to determine if the encoded URL is safe.

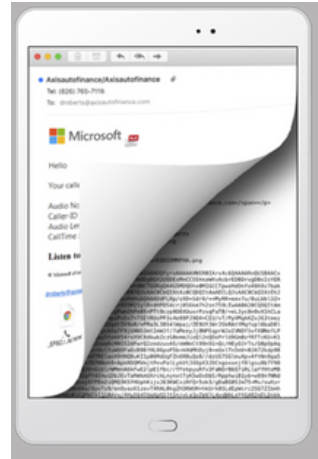


Approximate Matching Engine

INKY's proprietary approximate matching engine finds brand indicative and scam indicative text, despite attacker cloak attempts like zero font and other tricks.

Inbound Email Protection

Over two dozen computer-vision and text analysis models see an email much like a person does — only better. Our AI spots fakes, checks if senders are legitimate, and flags suspicious emails like brand impersonation and phishing before you ever click.

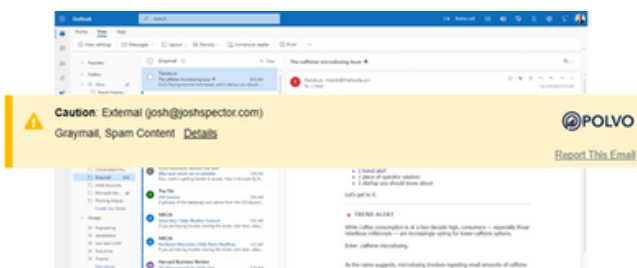
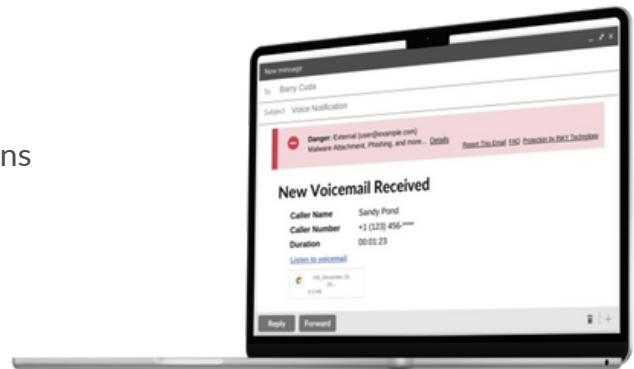


Internal Email Protection

Compromised email accounts let the bad guys in. INKY builds dynamic profiles or behavior models of originating senders with software modules using stylometry and social graphing. As the models grow, INKY uses anomaly detection to filter out and block impersonation attempts.

Advanced Attachment Analysis

Deep analysis in less than a second. Advanced Attachment Analysis transforms the way organizations protect themselves from malware. By analyzing the behavior of software components rather than their signatures, AAA can detect known malware threats and zero-day attacks.

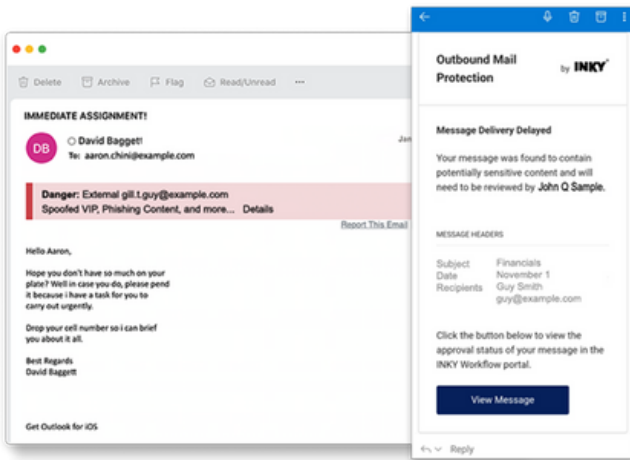


Graymail Detection

Graymail is bulk email you opted into but may no longer want. Our Generative AI-powered protection flags graymail, applies warning banners, and routes it to a custom folder for distraction-free review.

DMARC Monitoring

DMARC is now a vital security measure for protecting your clients' domains, reducing spam complaints, and ensuring all emails reach the intended inbox. INKY's DMARC Monitoring gives you full visibility across all your domains to defend against spoofing, phishing, and reputation issues.

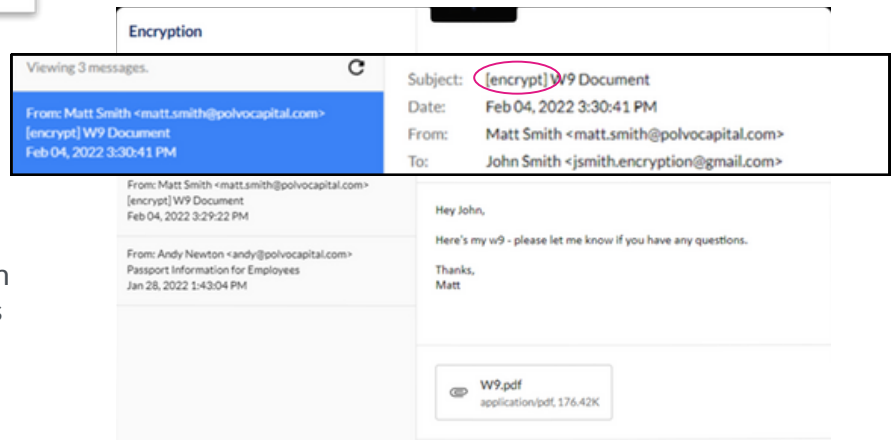


Outbound DLP Detection

Prevent High Risk Data Loss Before It Gets Out The Door. INKY scans outbound emails for sensitive data like credit card or bank info. If detected, it triggers your pre-set workflow—alerting the sender and approver, and enforcing a review before release.

Encryption Portal

Guard Sensitive Data and Prevent Breaches with Easy-To-Use Encryption - INKY leverages state-of-the-art 256-bit encryption to protect proprietary information sent to its intended recipient. Simply add "[encrypt]" to the subject line of an email and let the technology take care of the rest.



ADVANCED FEATURES

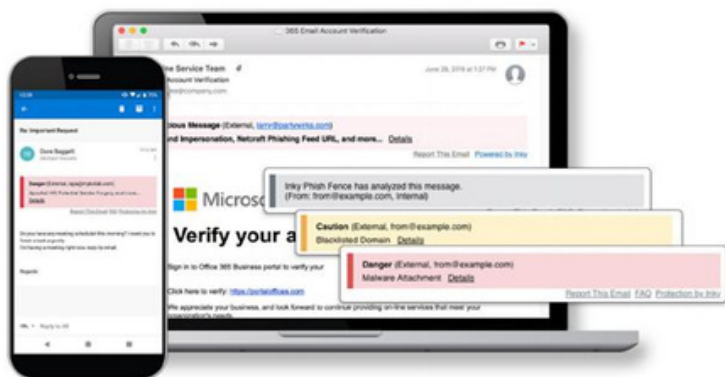
Inbound Email Protection
Internal Email Protection
Advanced Attachment Analysis
Advanced Graymail Detection
Customer Graymail Delivery Locations
End User-Managed Graymail
Outbound DLP Protection
Encryption Portal

GenAI Intent Analysis
NextGen AI Detection Capabilities
Advanced Computer Vision
QR Code Defense
Anomaly Detection
URL Time-of-Click Protection
DMARC Monitoring

Stop threats, cut the noise, and deliver GenAI-powered email protection with INKY Pro.

INKY instantly checks every message, link, and attachment for risk.

GenAI and AI models assess every message, checking for spoofing, phishing, and threats hiding in attachments. It flags distractions like graymail and keeps your domains in check—giving you smarter security without the extra effort.



Coach users to make smart decisions in real time.

Periodic security training often falls short with distracted, busy users. INKY's Email Assistant provides continuous coaching, helping users make safe choices on any device.

Stay secure with INKY in your corner.

Outsmarting malicious actors takes nothing less than agility and ceaseless innovation. Through GenAI, AI, and machine learning, INKY catches what others miss.



Computer Vision

INKY renders every email and applies computer vision algorithms to "see" each email as the human recipient will. This helps identify brand impersonation attempts.



Text Understanding & Conversation Analysis

INKY incorporates language understanding so it can "read" each email and understand its intent. This allows INKY to identify scams that simple pattern matching cannot.



QR Code Detection

INKY AI-driven QR code detection technology scans emails for QR code imagery and decodes these images to determine if the encoded URL is safe.

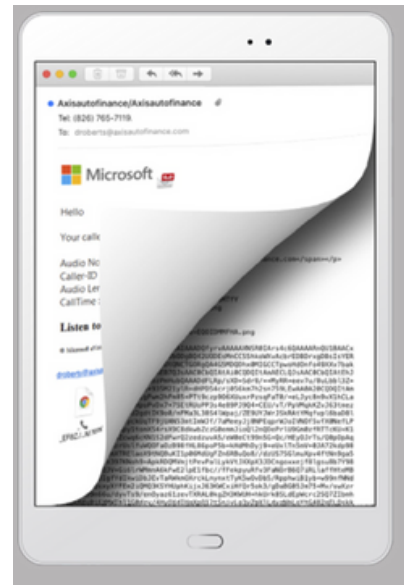


Approximate Matching Engine

INKY's proprietary approximate matching engine finds brand indicative and scam indicative text, despite attacker cloak attempts like zero font and other tricks.

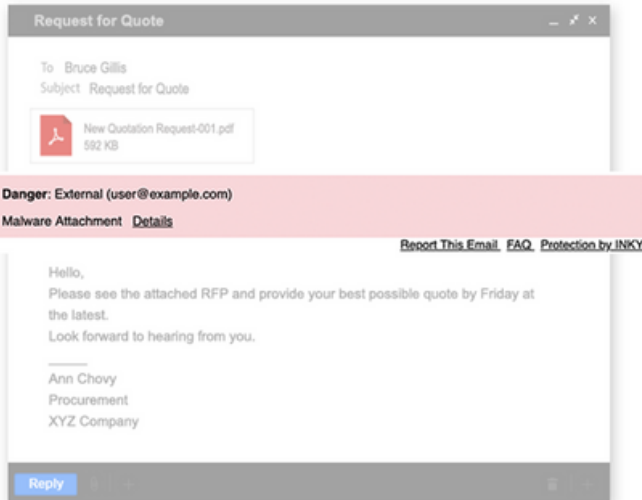
Inbound Email Protection

Over two dozen computer-vision and text analysis models see an email much like a person does — only better. Our AI spots fakes, checks if senders are legitimate, and flags suspicious emails like brand impersonation and phishing before you ever click.



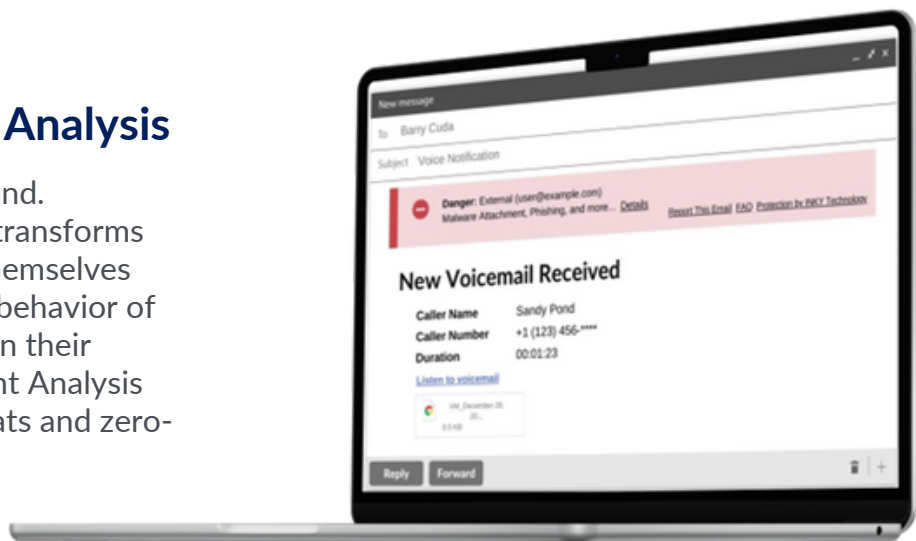
Internal Email Protection

Compromised email accounts let the bad guys in. INKY builds dynamic profiles or behavior models of originating senders with software modules using stylometry and social graphing. As the models grow, INKY uses anomaly detection to filter out and block impersonation attempts.



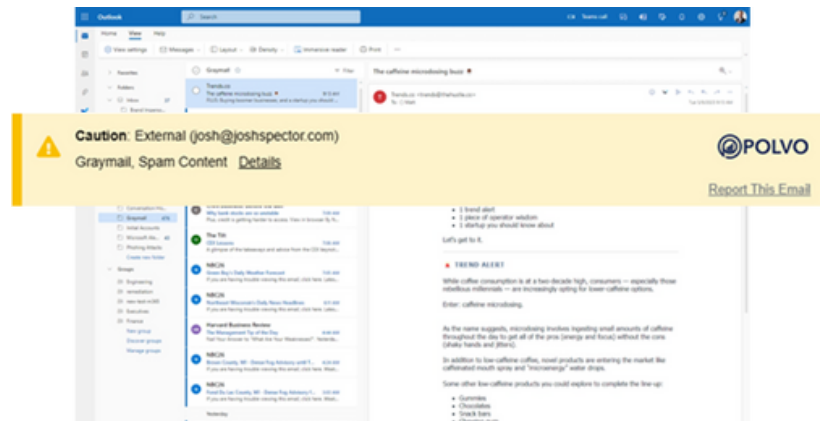
Advanced Attachment Analysis

Deep analysis in less than a second. Advanced Attachment Analysis transforms the way organizations protect themselves from malware. By analyzing the behavior of software components rather than their signatures, Advanced Attachment Analysis can detect known malware threats and zero-day attacks.



Graymail Detection

Graymail is bulk email you opted into but may no longer want. Our Generative AI-powered protection flags graymail, applies warning banners, and routes it to a custom folder for distraction-free review.



DMARC Monitoring

DMARC is now a vital security measure for protecting your clients' domains, reducing spam complaints, and ensuring all emails reach the intended inbox. INKY's DMARC Monitoring gives you full visibility across all your domains to defend against spoofing, phishing, and reputation issues.

PRO FEATURES

Inbound Email Protection
Internal Email Protection
Advanced Attachment Analysis
Advanced Graymail Detection
Customer Graymail Delivery Locations
End User-Managed Graymail
DMARC Monitoring

GenAI Intent Analysis
NextGen AI Detection Capabilities
Advanced Computer Vision
QR Code Defense
Anomaly Detection
URL Time-of-Click Protection

✦ Intelligent Defense Powered by INKY

INKY sees, reads, and stops email threats with unprecedented precision.

GenAI is redefining the future of email security. With billions of dollars lost each year to phishing attacks and data breaches, email security continues to be a critical concern for Managed Service Providers (MSPs) and their clients. Traditional methods of threat detection, which rely on pattern-based detection, often fall short in keeping up with the ever-evolving tactics of cybercriminals.

However, with the integration of Generative AI, INKY can now understand the meaning and intent behind every email, regardless of how cleverly it is worded or disguised. This revolutionary new capability takes email security to a whole new level.

INKY's GenAI detects an "unsubscribe" option, triggering further threat investigation.

Subject: Michel York | William Goodsell ✦
From: William Goodsell <wgoodsell@internetwebintel.com> ✦
To: <michel@polvocapital.com>

January 20th, 2025 8:40:54 AM

Caution! This message is potentially suspicious.
Graymail, First-Time Sender

Hi Michel,

I just was reviewing your company website and was impressed with your portfolio of services. How do you protect your clients' sensitive data?

We recently helped a SAAS company implement a new security framework, which galvanized their security posture and boosted client confidence.

Would you be interested in a quick chat to explore how we can strengthen your security practices?

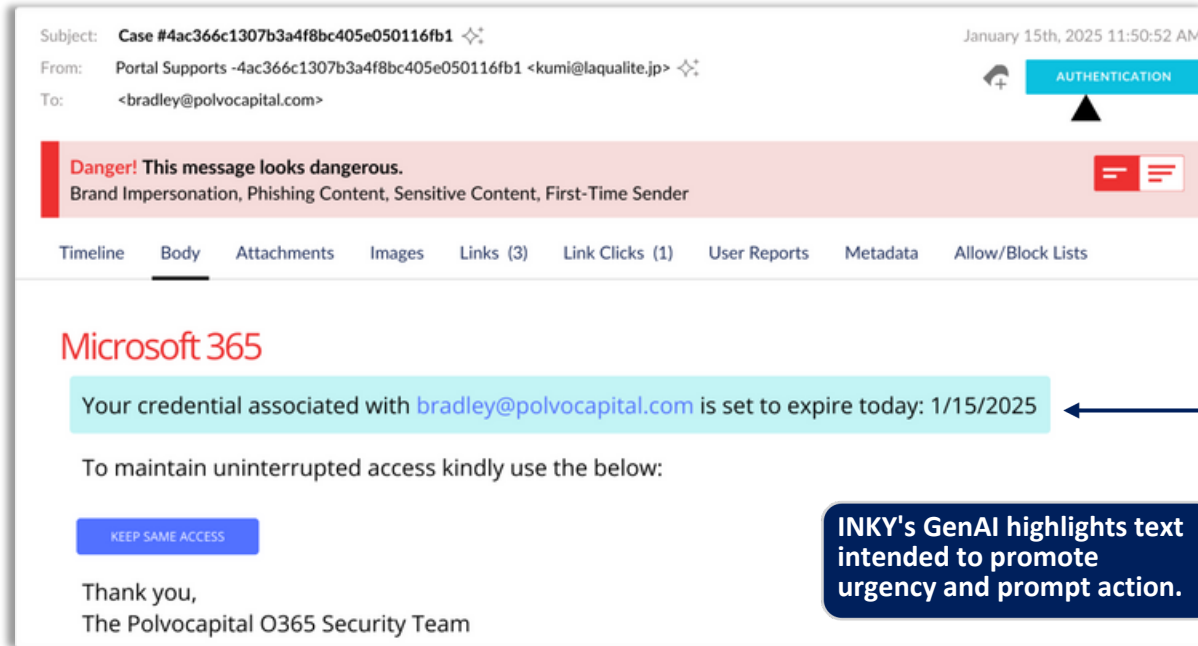
Best Regards,
William Goodsell

P.S. If you're not into this chat, reply with 'beans' and I'll gracefully exit!

Cleverly disguised unsubscribe message is highlighted.

INKY understands language like a human.

INKY's Computer Vision AI has been able to review email and understand its visual meaning for many years. Now, with Generative AI, INKY can read and understand the text of each email. INKY's deep understanding of language anticipates every way a request, threat, or scam could be worded. This capability ensures proactive, zero-day protection against phishing attacks.



Key Benefits of INKY Generative AI



Human-Level Language Understanding

INKY GenAI processes email content much like advanced chatbots, interpreting meaning and intent regardless of phrasing. This enables superior detection of zero-day attacks, thwarting even the most cleverly worded attempts to evade pattern-based detection systems.



Integrated Obfuscation Countermeasures

Combining GenerativeAI with INKY's existing countermeasures for cloaked text (e.g., zero font, Unicode, and homograph techniques), the platform transforms obfuscated email content into clean text for precise analysis.



Explainable Results

The INKY Dashboard highlights specific sections of an email that contribute to its assessment, giving administrators actionable insights and confidence in the AI's decision- making process.



Enhanced Graymail Detection

INKY's popular graymail filter is now even more accurate and effective, providing greater productivity and inbox organization for users.



Broad System Integration

Generative AI is infused into all aspects of INKY's platform, including the analysis of website content linked in emails and third-party cloud services.



Privacy-First Approach

INKY's Generative AI operates entirely within the company's infrastructure, ensuring that no company data or personally identifiable information (PII) is exposed to third parties.

Seeing is believing.

GenAI optimizes the INKY Email Assistant by providing end users with specific, actionable advice. For administrators, the INKY dashboard offers a visual breakdown of what INKY GenAI detected, making it simple to track and understand email threats.

“Generative AI represents a major leap forward in email security. We think it fundamentally changes the game, making things harder for attackers, and enables us to provide our partners with the best information security protection on the market.”



Dave Baggett
CEO and Founder

INKY's GenAI scans every email without exception.

Generative AI is seamlessly integrated into every step of our email analysis pipeline. When enabled, it analyzes 100% of incoming emails that pass initial reputational and spam checks. This is in stark contrast to the practices of other email security vendors who only analyze a fraction of the emails entrusted to their care. INKY's thorough approach ensures that no threat goes undetected. Additionally, our system can convert obfuscated email content into clean text, making it easier to analyze and understand the true intent of the sender.

INKY EMAIL SECURITY PLATFORM



Advanced

Inbound Mail Protection (PF)
Internal Mail
Protection (IMP)
Advanced Attachment
Analysis (AAA)
Graymail Protection
Email Signatures



Pro

Everything in
Advanced Plus:
Generative AI
Outbound Mail
Protection (OMP)
Email Encryption
DMARC Monitoring