INTERMEDIA®
CLOUD COMMUNICATIONS

DATASHEET

Intermedia Email Protection with AI Guardian Threat Protection

Keep your business safe from known & emerging email threats.

Comprehensive, multi-layered protection against malware and unknown email threats	Protection against malicious links in emails and attachments	Data loss prevention and outbound email protection	Ultimate IT administrator control and visibility with flexible policies	Sophisticated AI Guardian protects against impersonation, zero-day (previously unknown) and targeted attacks

Traditional email security identifies incoming threats based on known signatures to protect against malware, viruses and threats distributed via spam. But today, many email attacks are laser focused and evade traditional detection by adopting advanced techniques and targeting human nature. Adversaries mask payloads by standing up zero-day domains, research their targets, and often impersonate trusted parties to steal money and data. Email security engines based solely on signatures or metadata are no longer enough to protect businesses from these advanced attacks.

Intermedia Email Protection for Intermedia Hosted Exchange is designed to protect your organization from sophisticated, real-time email threats that can cripple or even take down your business. It uses multiple industry-leading email scanning engines to prevent spam, viruses, malware and phishing from reaching your mailboxes. With Email Protection Premium, the AI Guardian Premium layer builds on that by analyzing thousands of signals – including the language of the email – to stop a wide range of targeted attacks that evade traditional detection. AI Guardian Premium also provides a threat dashboard for visibility into the types of attacks and targets within your organization, along with configurable remediation options. Intermedia Email Protection Premium with AI Guardian Premium provides Intermedia business email customers with industry-leading email protection, including AI-assisted protection, in a single easy-to-use service.

FEATURES

Multiple industry-leading email security engines for comprehensive protection against known, unknown and emerging threats	Protection against emerging email threats through URL live-scanning of emails and attachments	Marketing (graymail) management helps users prioritize important messages	Point-of-click protection against malicious links with Intermedia LinkSafe™
Simple, intuitive creation and management of email rules and policies in a single interface	User and admin quarantines or immediate delivery to the Junk Email folder through tight integration with the Intermedia mailbox	AI Guardian Premium protects against payroll and invoice fraud, impersonation, and other types of attacks	Worry-Free Experience™ with 99.999% availability service level agreement and 24x7 expert support (TSIA Rated Outstanding and J.D. Power Certified)

Comprehensive, multi-layered protection against malware, targeted attacks and unknown email threats: Intermedia Email Protection Standard and Premium are cloud-based email security solutions that use multiple engines to stop spam, phishing and all types of known, unknown and emerging malware. It benefits from threat intelligence collected from almost 1 billion mailboxes worldwide and is designed to deliver a detection rate of over 99% with very few false positives, as well as fast response to real-time threats.

www.link.com

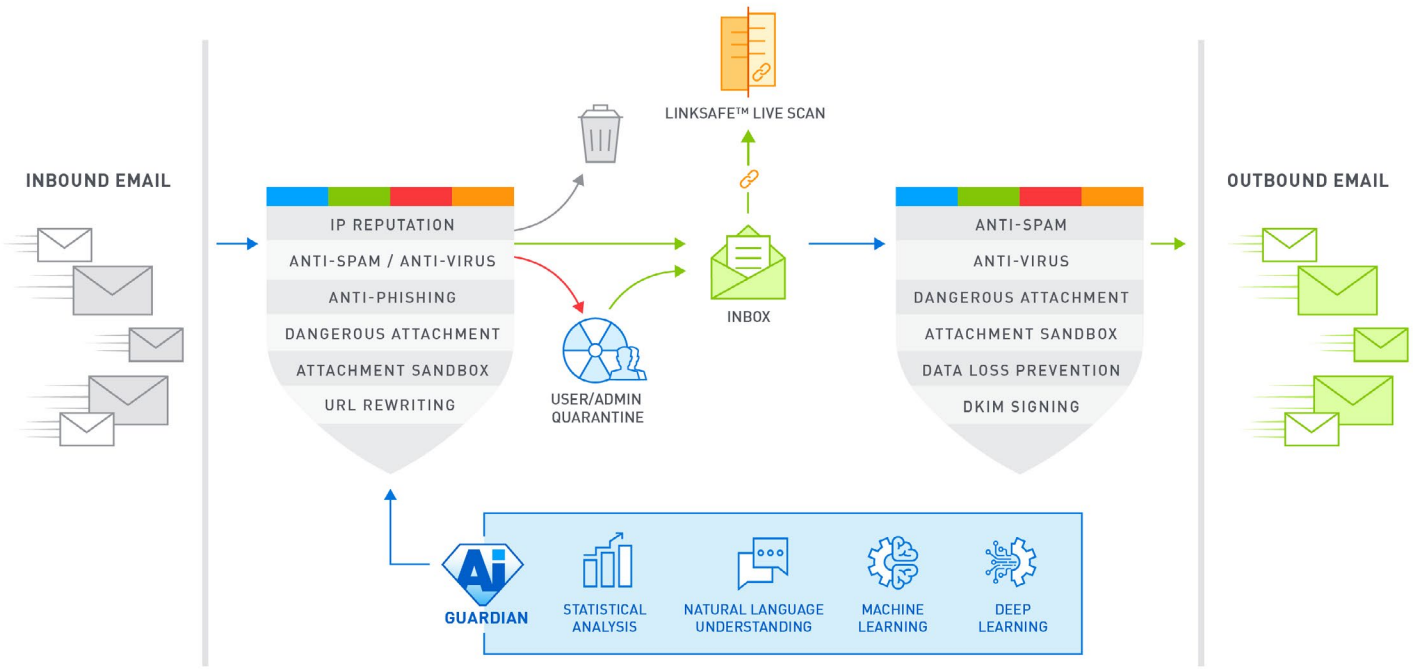
Point-of-click protection against malicious links in emails: Targeted and spear-phishing attacks often bypass existing security controls by embedding malicious links within email messages. Intermedia LinkSafe provides “zero hour” protection against known, unknown and emerging email threats. This technology rewrites all URLs within inbound mail and performs a real-time scan of the target site every time the link is clicked by the end-user to prevent users from accessing phishing sites or webpages containing malicious code.

Comprehensive IT administrator control and visibility with flexible policies: Many businesses are faced with a lack of resources and security expertise that leads to an inability to effectively deploy and manage email security solutions. That can leave the door open to attacks. Intermedia Email Protection provides an intuitive interface that makes this solution easy to use for businesses of all sizes. Administrators have broad control over how fraudulent or suspicious mail is being handled and are able to define company-wide, group and user level policies.

Data Loss Prevention and outbound email protection: Business-critical email communication often involves sensitive data. Therefore, businesses need visibility and control over email leaving their organization. Data Loss Prevention (DLP) offers outbound email protection for businesses from negligent or accidental leakage of sensitive or proprietary data.

AI Guardian for anti-phishing and protection against targeted email attacks: As phishing and Business Email Compromise (BEC) attacks continue to grow in sophistication, businesses need to ensure the adoption of email security controls that detect and respond to such social engineering attacks. Intermedia Email Protection Premium includes AI Guardian Premium capabilities to help organizations detect, analyze, and stop targeted threats including ransomware, credential phishing, extortion, payment and payroll fraud, social engineering attacks, VIP and employee impersonation. AI Guardian Premium is designed to flag suspicious mail into predefined attack categories, provide deep insights into threat signals (including in the email's language), and automatically remediate the threats based on preconfigured actions. AI Guardian Premium includes analytics, reporting, and configurable remediation so you can better understand your threat environment and provide better protection for your users.

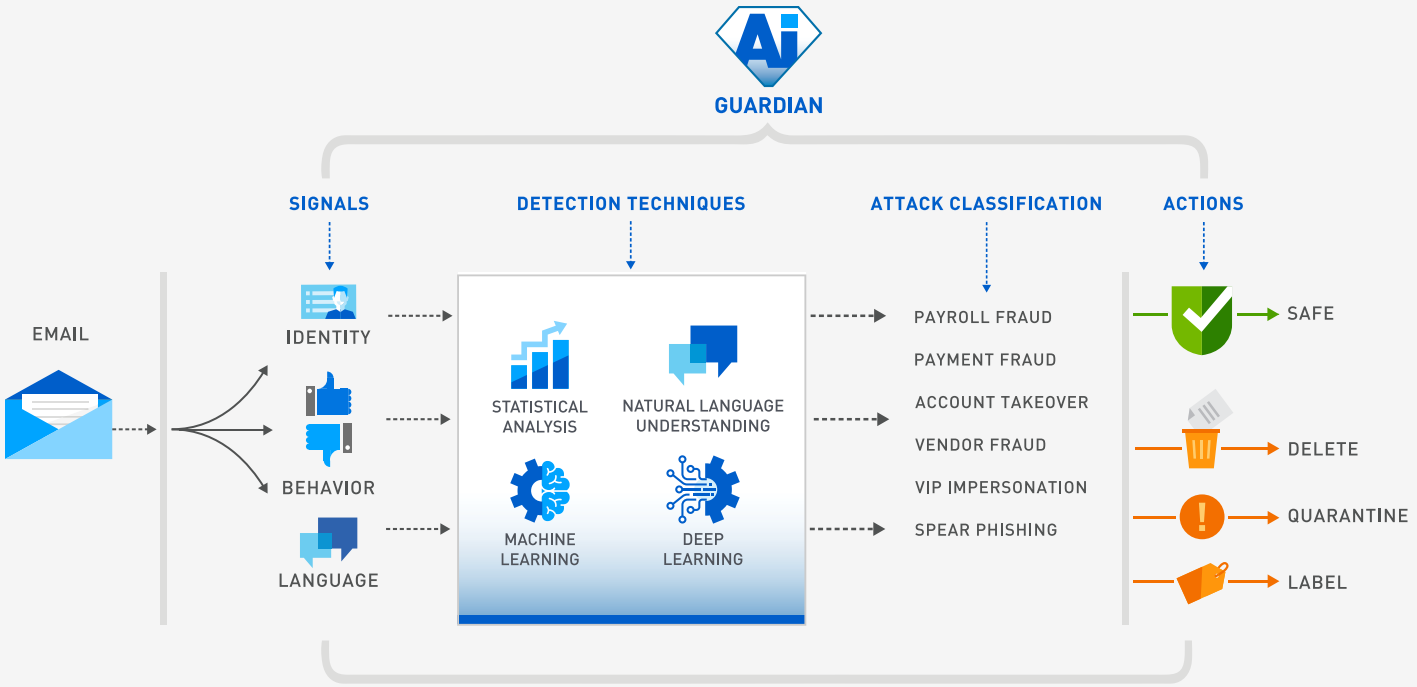
INTERMEDIA EMAIL PROTECTION MAIL FLOW



*AI Guardian available with Email Protection Premium

EXPANDED THREAT MODELS FOR EMAIL PROTECTION PREMIUM WITH AI GUARDIAN PREMIUM

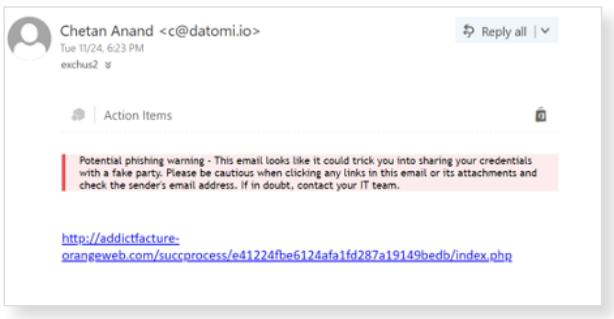
AI Guardian uses three types of models to protect you. A global threat model looks at targeted attacks encountered across customer environments so that learning from threats that are encountered anywhere are incorporated into threat protection across all organizations. A model is also built that is specific to your organization based on the regular legitimate communications associated with your organization so that unusual behavior can be identified.



Finally, each mailbox and user have their own standard communication analyzed so that emails that don't fit the expected pattern can be flagged.

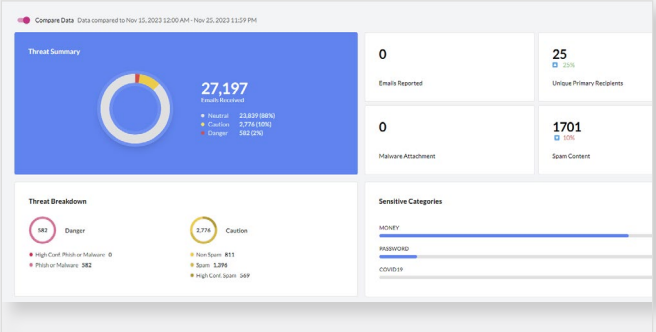
AI Guardian applies natural language techniques to look for language within emails that imply urgency and actions associated with targeted attacks, and flag these emails with banners for the user and report them to administrators.

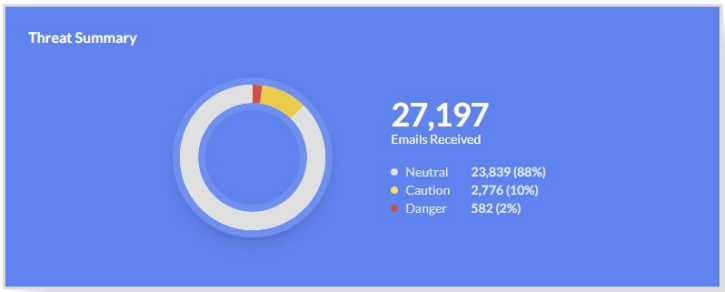
AI Guardian then applies educational banners to the message, based on the identified threat type, to alert the user. Administrators can also set policies to quarantine or delete these messages.



EMAIL PROTECTION PREMIUM AI GUARDIAN DASHBOARD, REPORTING AND ANALYTICS

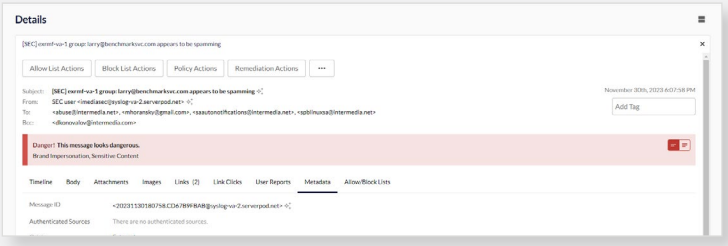
The AI Guardian Premium dashboard provides a high level view of the types of threat your organization is encountering over days, weeks or months.



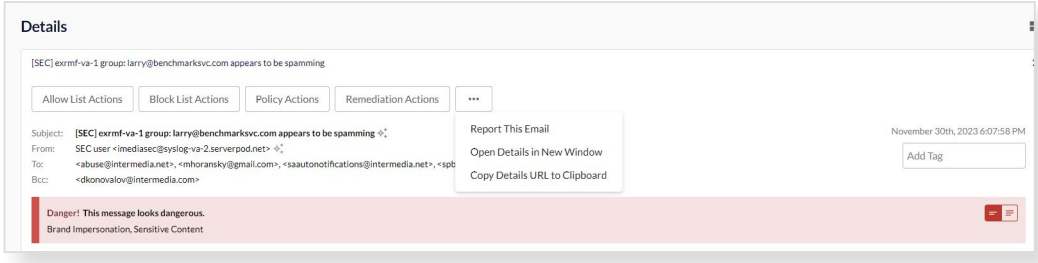


Threats are summarized by type and also by user or subgroup.

An administrator can click into threat types for more detail to review individual threats and actions taken.



AI Guardian displays the reasons why an email has been flagged.



Intermedia Email Protection Features

FEATURE	DESCRIPTION	EMAIL PROTECTION STANDARD	EMAIL PROTECTION PREMIUM
Multiple Best-Of-Breed Security Engines	Multiple industry-leading email security engines for comprehensive protection against known, unknown, and emerging threats.	✓	✓
Inbound Malware Protection	Blocks emails that contain known malware signatures.	✓	✓
Inbound Spam Filtering	Blocks emails with known spam signatures.	✓	✓
Safe & Blocked Senders Lists	Restricts or allows senders by email address, domain or IP address.	✓	✓
Basic Attachments Defense	Certain file types could be considered to be dangerous, such as executables. These settings control how messages with files attached are handled.	✓	✓
Email Tracking	Track individual inbound emails with delivery status, detailed explanation of how an email has been processed and quarantine status.	✓	✓
Email Reporting (Reports)	Visibility of detected email threats.	✓	✓
Group-Based Email Protection Policies	Policies can be assigned to domains, distribution lists, or mailboxes.	✓	✓
Advanced Attachments Defense	Controls how messages with potentially dangerous file types attached, such as executables, are handled.	✓	✓
URL Protection With Intermedia Linksafe™	Point-of-click protection against links to potentially harmful, dangerous websites with Intermedia LinkSafe.™	✓	✓
Phishing Protection	A set of features designed to protect against phishing and spoofing attacks. Actions on emails contain such attacks depend on set up in Inbound policies. Unlike traditional attachment-based attacks, these types of attacks don't typically contain their payload/malware within a file attachment. Instead, they attempt to coerce a user into taking an action such as: • Visiting a web-page (that contains malware, or is designed to capture login credentials). • Executing a financial transaction.	✓	✓
Graymail Management	Helps users prioritize important messages from bulk email that comes from a legitimate external source.	✓	✓
Outbound Malware Protection	Protects others against malware emails sent from customer's mailboxes in case those had been compromised.	✓	✓
Outbound Spam Filtering	Protects others against spam emails sent from customer's mailboxes in case those had been compromised.	✓	✓
DKIM Outbound Signing	Protects email senders and recipients from spam, spoofing, and phishing. DKIM is a form of email authentication that allows an organization to claim responsibility for a message in a way that recipients can validate.	✓	✓

FEATURE	DESCRIPTION	EMAIL PROTECTION STANDARD	EMAIL PROTECTION PREMIUM
Outbound Content Filtering (DLP)	Data Loss Prevention (DLP) offers outbound email protection for businesses from negligent or accidental leakage of sensitive or proprietary data. Administrators can block outbound mail that violates pre-determined policies before it leaves your organization.	✓	✓
Attachment Sandboxing	Potentially dangerous attachments checked in a safe sandboxing environment and action set in policy will be applied to unsafe attachments.		✓
AI Guardian Premium			
Dashboards and Reporting	Understand the threats targeting your organization each day.		✓
Global Mailbox Search	Perform forensic searches of all messages delivered to mailboxes.		✓
User Coaching	Train users on potential threats through email banners for interactive learning.		✓
Spear Phishing Protection	Detect threats attempting to impersonate a trusted person.		✓
VIP Spoofing Protection	Detect threats attempting to spoof your executives and VIP's.		✓
Business Email Compromise (BEC) Protection	Detect threats without traditional payloads, such as URL's and attachments.		✓
Account Takeover Protection	Detect and prevent account takeover attempts.		✓
Brand Forgery Detection	Determine the apparent brand using color palette, layout features and prominent text.		✓
Sensitive Content Detection	Detect sensitive or harmful content in emails such as passwords and financial content.		✓
Content Disarm and Reconstruction (CDR)	Automatically remove potentially harmful executable content in emails.		✓

Intermedia has been recognized by J.D. Power for providing "An Outstanding Customer Service Experience" for its Assisted Technical Support. J.D. Power 2023 Certified Assistance and Technical Support ProgramSM recognition is based on successful completion of an evaluation and exceeding a customer satisfaction benchmark through a survey of recent servicing interactions for its technology service and support operations. For more information, visit www.jdpower.com

Questions? Contact Us Today.