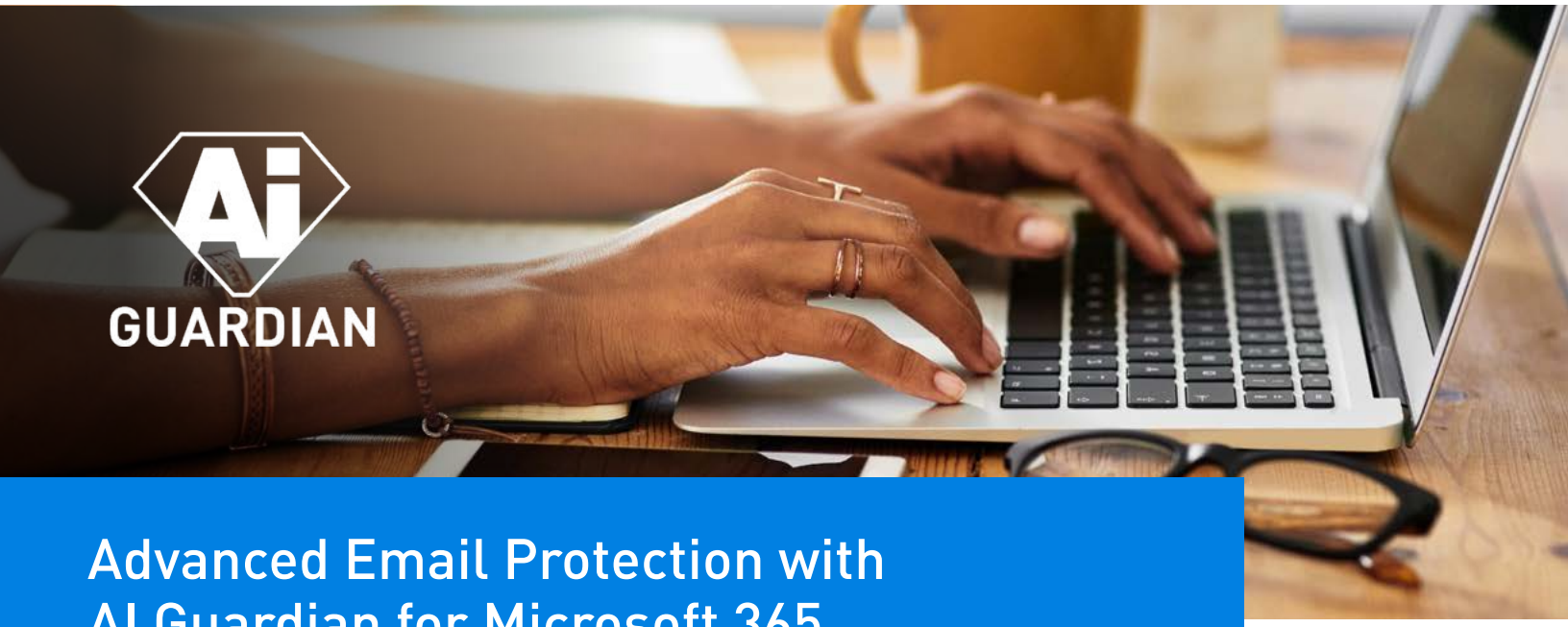
INTERMEDIA
CLOUD COMMUNICATIONS

DATASHEET



Advanced Email Protection with AI Guardian for Microsoft 365

Keep your business safe from known and emerging email threats.

Comprehensive, multi-layered protection against malware and unknown email threats.

Point-of-click protection against malicious links in emails.

Data Loss Prevention and outbound email protection.

Ultimate IT administrator control and visibility with flexible policies.

Sophisticated AI Guardian protection against impersonation, zero-day (previously unknown) and targeted attacks.

Traditionally, email security solutions focused on protection against malware, viruses and threats distributed via spam. Today, email threats have evolved, and fraudsters employ more sophisticated techniques, such as social engineering, impersonation and targeted spear-phishing attacks, to bypass traditional email security checks. Signature-based email protection engines are no longer enough on their own to protect businesses from these advanced attacks.

Advanced Email Protection for Microsoft 365 is an email security solution designed to protect your organization from sophisticated, real-time email threats that can cripple or even take down your business and provide visibility into the types of attacks and targets within your organization. It uses multiple industry-leading email scanning engines to prevent spam, viruses, malware and phishing from reaching your mailboxes.

AI Guardian builds on Advanced Email Protection by analyzing thousands of signals – including the language of the email in the inbox – to stop a wide range of targeted attacks that evade traditional detection with customizable user notifications and remediation options and a threat dashboard for targeted attacks.*

*AI Guardian is available as an add-on to Advanced Email Protection or standalone.

Advanced Email Protection with AI Guardian offers small and medium-sized businesses enterprise-level security that is affordable, reliable, and easy to deploy, use and configure.

FEATURES

Multiple industry-leading email security engines for comprehensive protection against known, unknown and emerging threats	AI Guardian protects against payroll fraud, invoice fraud, impersonation, and other types of attacks	"Zero day" protection against emerging email threats through URL live-scanning	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 mail-box integration with Microsoft 365	Worry-Free Experience™ with 24x7 expert support (TSIA Rated Outstanding and J.D. Power Certified)

COMPREHENSIVE, MULTI-LAYERED PROTECTION AGAINST MALWARE, TARGETED ATTACKS AND UNKNOWN EMAIL THREATS

Advanced Email Protection is a cloud-based email security solution that uses 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.

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. LinkSafe™ URL Protection provides “zero day” 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.

DATA LOSS PREVENTION AND OUTBOUND EMAIL PROTECTION

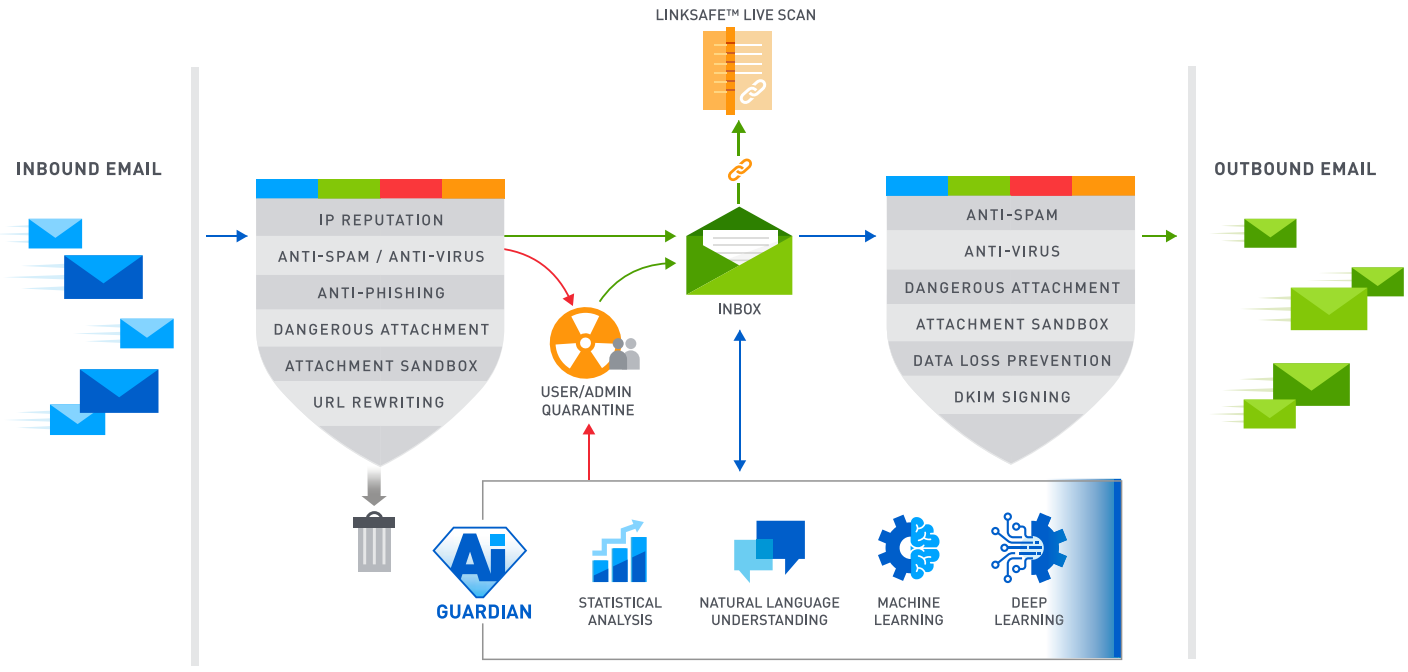
Business-critical email communication often involves sensitive data. Therefore, businesses need visibility and control over email leaving their organization. Data Loss Prevention (DLP) offers outbound email protection for businesses from negligent or accidental leakage of sensitive or proprietary data. Administrators can block outbound mail that violates pre-determined policies before it leaves your organization.

COMPREHENSIVE IT ADMINISTRATOR CONTROL AND FLEXIBILITY WITH VISIBLE POLICIES

Small and medium-sized businesses are often 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. Advanced 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.

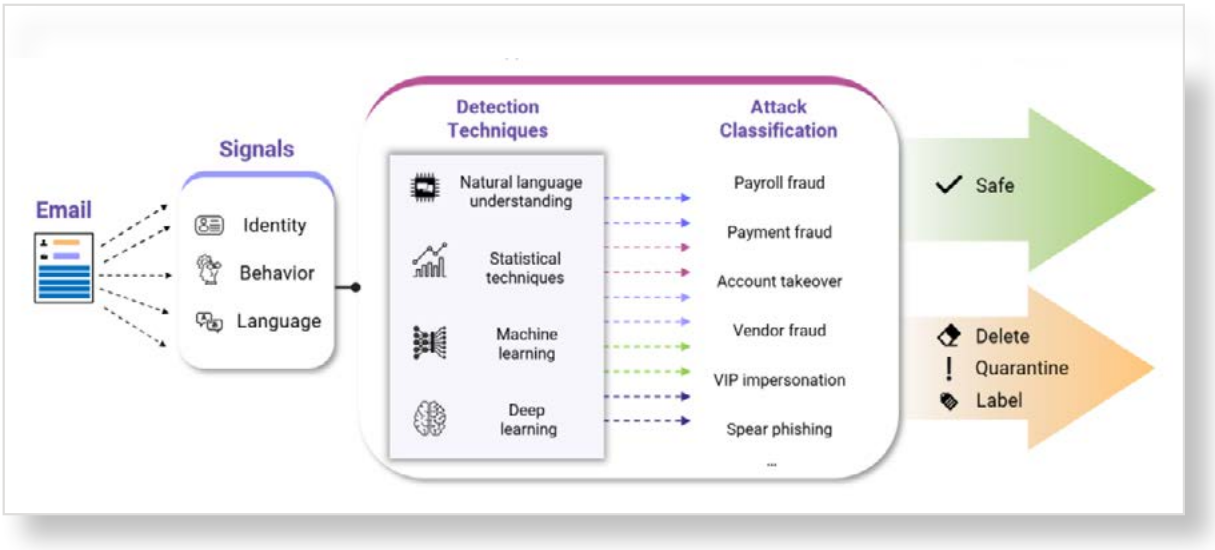
AI GUARDIAN FOR ANTI-PHISHING AND PROTECTION AGAINST TARGETED EMAIL ATTACKS

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 Advanced Email Protection with AI Guardian capabilities helps 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 acts on emails in a user's inbox and 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 includes analytics and reporting and customizable remediation so you can better understand your threat environment and provide better protection for your users.



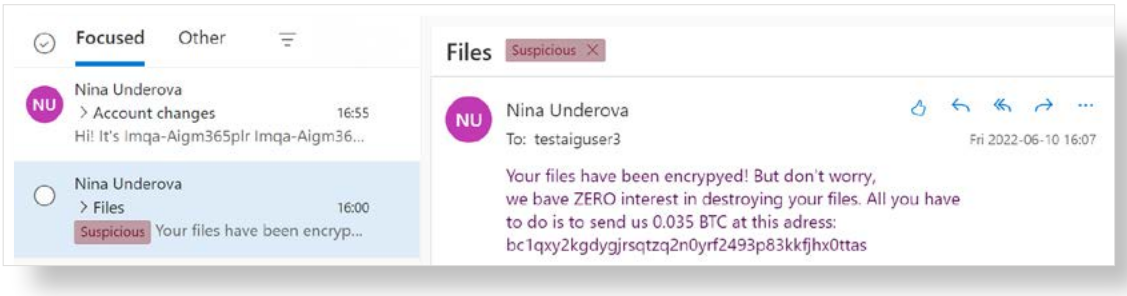
EXPANDED THREAT MODELS WITH AI GUARDIAN

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.

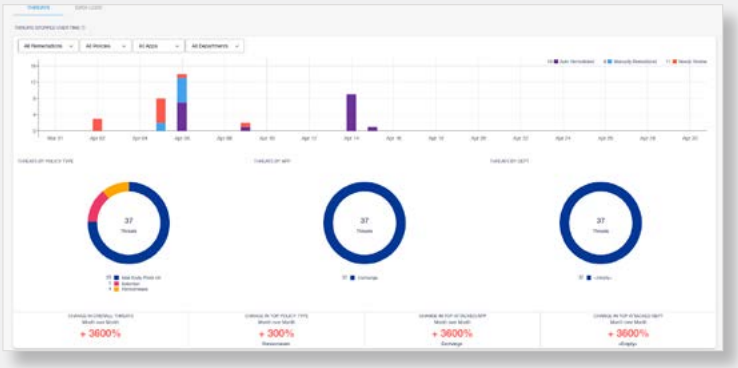
AI Guardian applies natural language techniques to look for language within emails that imply urgency and actions associated with targeted attacks, and flag these for the user and report them to administrators.

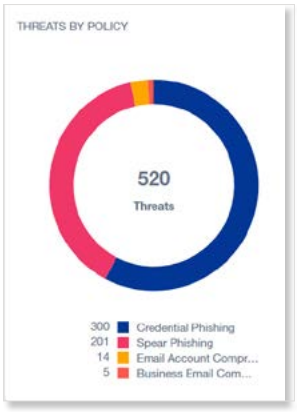


Administrators can also set policies to quarantine or delete these messages.

AI GUARDIAN DASHBOARD, REPORTING AND ANALYTICS

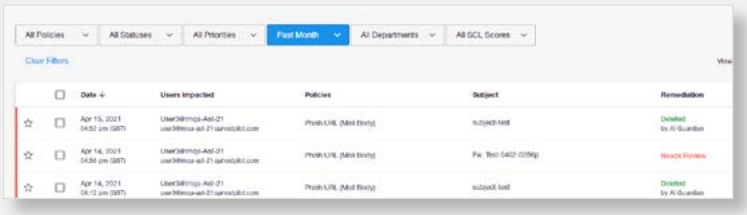
The AI Guardian dashboard provides a high level view of the types of threat your organization is encountering over days, weeks or months.

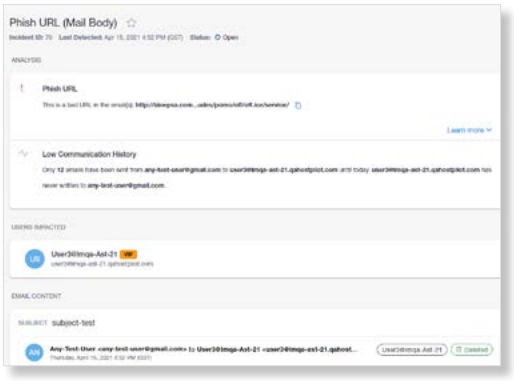




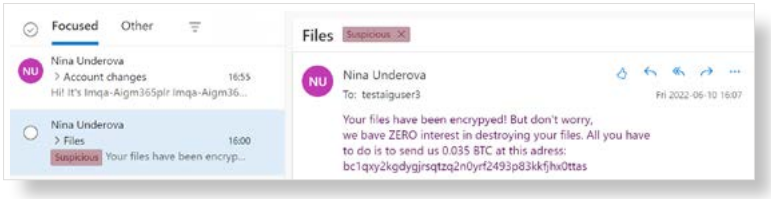
Threats are summarized by type and also by user or subgroup.

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.



Advanced Email Protection uses multiple industry-leading email scanning engines to prevent spam, viruses, malware and phishing from reaching your mailboxes.

FEATURES	DESCRIPTION
Multiple industry-leading security engines	Combines and compares assessments of multiple industry-leading email security engines for comprehensive protection against known, unknown, and emerging threats.
Inbound Malware and Threat protection	Blocks emails that contain known malware signatures
Phishing Protection	Designed to protect against phishing and spoofing attacks. Configurable policies determine actions taken on emails containing such attacks. Unlike traditional attachment-based attacks, many phishing attacks do not deploy their payload/malware within a file attachment. Instead, they attempt to coerce a user into taking an action such as: • Visiting a webpage (that contains malware, or is designed to capture login credentials) • Executing a financial transaction
Inbound Spam filtering	Blocks emails with known spam signatures
Safe & Blocked Senders lists	Restricts or allows senders by email address, domain or IP address
Attachment Sandboxing	Potentially dangerous attachments are checked in a safe sandboxing environment and unsafe attachments are handled based on configurable policies.
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™
Impersonation protection	Specific protection against impersonation attacks by comparing the actual sender to the purported sender.
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.
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.

AI Guardian provides an additional layer of protection to emails that make it to users' mailbox and builds on Advanced Email Protection by analyzing thousands of signals – including the language of the email – to stop a wide range of socially engineered targeted attacks that evade traditional detection.

FEATURES	DESCRIPTION
Ransomware protection	Detects emails trying to get users to download and install Ransomware by directing them to access links or to open attachments.
Credential phishing protection	Detects emails containing links or redirects to fake login pages attempting to get users to disclose their credentials.
Extortion protection	Detects emails that threaten users with bad consequences unless they take a specific action.
Payment fraud protection	Detects emails impersonating an external entity to defraud the organization e.g. with fraudulent invoices.
Payroll fraud protection	Detects emails impersonating an employee to steal money or payroll-related information with fraudulent W-2 or direct deposit requests.
Social engineering protection	Detects emails that try to trick you into handing over sensitive information.
VIP and employee impersonation protection	Specific protection against impersonation attacks on VIPs and other key internal staff.
Attachment scanning	Scans attachments for malicious and zero-day links.
AI Guardian Dashboard	SSO access to the AI Guardian dashboard to review threats and DLP incidents, and one-click threat remediation.

Questions? Contact Us Today.
800.379.7729 sales@intermedia.com
intermedia.com