INTERMEDIA®
CLOUD COMMUNICATIONS

DATASHEET

AI Guardian for Microsoft 365 Exchange

Keep your business safe from known and emerging email threats.

- Protects email communications using natural language understanding, artificial intelligence and advanced data science techniques
- Analyzes thousands of signals across identity, behavior, language, and global threat data to catch attacks missed by traditional solutions
- Detects and stops targeted attacks such as VIP impersonation, payroll fraud, invoice fraud, and zero-day credential phishing
- Classifies threats under predefined detection categories and automatically remediates based on configurable actions
- Provides dashboard for reviewing and managing threats and data loss incidents, and customizing remediation policies

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.

AI Guardian builds on traditional email security solutions 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 offers small and medium-sized businesses enterprise-level security that is affordable, reliable, easy to deploy, use and configure, and specifically stops targeted attacks designed to evade traditional detection.

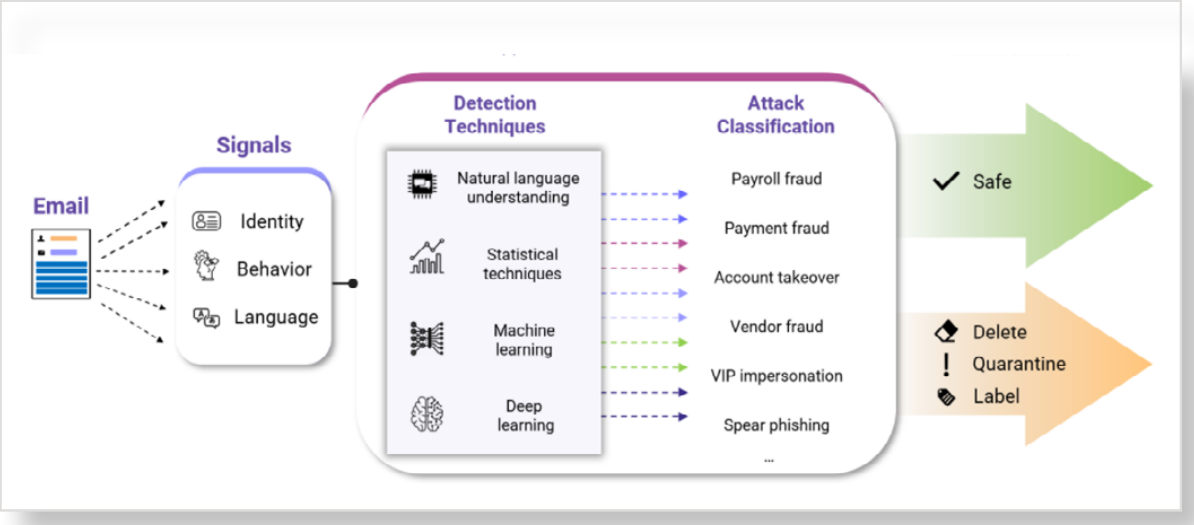
AI GUARDIAN FOR ANTI-PHISHING AND PROTECTION AGAINST TARGETED EMAIL ATTACKS

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. AI Guardian 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.

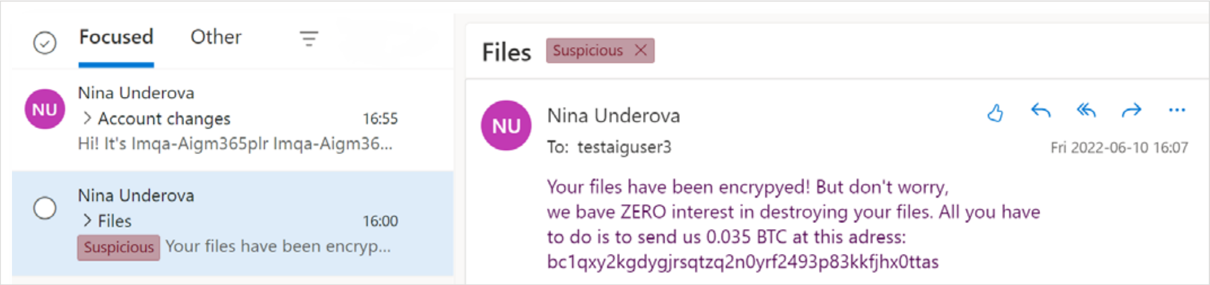
EXPANDED THREAT MODELS WITH AI GUARDIAN

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.



Nina Underova
> Account changes 16:55
Hi! It's Imqa-Aigm365plr Imqa-Aigm36...

Nina Underova
> Files 16:00
Suspicious Your files have been encryp...

Files Suspicious ✕

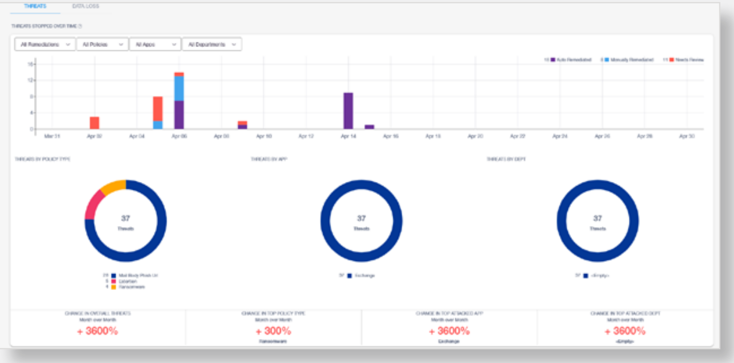
Nina Underova
To: testaiguser3
Fri 2022-06-10 16:07

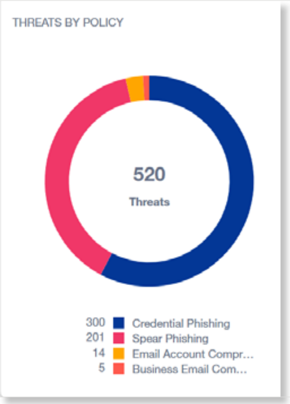
Your files have been encrypyed! But don't worry, we bave ZERO interest in destroying your files. All you have to do is to send us 0.035 BTC at this adress: bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0ttas

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

AI GUARDIAN DASHBOARD, REPORTING AND ANALYTICS

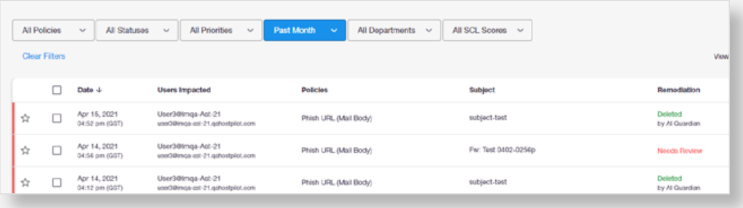
The AI Guardian dashboard provides a high level view of the types of threat your organization is encountering over days, weeks or months.



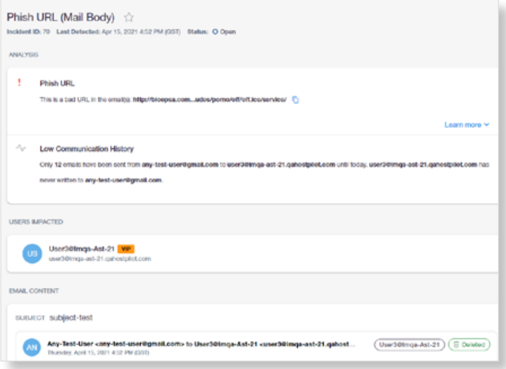


Threats are summarized by type and also by user or subgroup.

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



	□	Date ↓	Users Impacted	Policies	Subject	Remediation
☆	□	Apr 15, 2021 04:52 pm (GST)	User3@Imqa-Ast-21 user3@imqa-ast-21.qahostpilot.com	Phish URL (Mail Body)	subject-test	Deleted by AI Guardian
☆	□	Apr 14, 2021 04:56 pm (GST)	User3@Imqa-Ast-21 user3@imqa-ast-21.qahostpilot.com	Phish URL (Mail Body)	Fw: Test 0402-0256p	Needs Review
☆	□	Apr 14, 2021 04:12 pm (GST)	User3@Imqa-Ast-21 user3@imqa-ast-21.qahostpilot.com	Phish URL (Mail Body)	subject-test	Deleted by AI Guardian



Phish URL (Mail Body) ☆

Incident ID: 70 **Last Detected:** Apr 15, 2021 4:52 PM (GST) **Status:** ○ Open

ANALYSIS

! **Phish URL**

This is a bad URL in the email(s): **http://bloepsa.com...udos/pomo/off/oft.ico/service/**

Learn more

Low Communication History

Only **12** emails have been sent from **any-test-user@gmail.com** to **user3@imqa-ast-21.qahostpilot.com** until today. **user3@imqa-ast-21.qahostpilot.com** has never written to **any-test-user@gmail.com**.

USERS IMPACTED

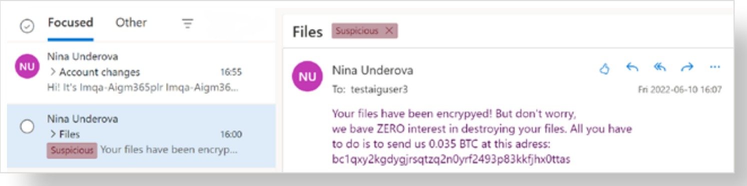
US User3@Imqa-Ast-21 VIP
user3@imqa-ast-21.qahostpilot.com

EMAIL CONTENT

SUBJECT subject-test

AN **Any-Test-User <any-test-user@gmail.com>** to **User3@Imqa-Ast-21 <user3@imqa-ast-21.qahost...** User3@Imqa-Ast-21 Deleted
Thursday, April 15, 2021 4:52 PM (GST)

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



NU Nina Underova
> Account changes 16:55
Hi! It's Imqa-Aigm365plr Imqa-Aigm36...

NU Nina Underova
> Files 16:00
Suspicious Your files have been encryp...

NU Nina Underova
To: testaiguser3
Fri 2022-06-10 16:07

Your files have been encrypyed! But don't worry,
we bave ZERO interest in destroying your files. All you have
to do is to send us 0.035 BTC at this adress:
bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0ttas

AI Guardian provides an additional layer of protection to emails that make it to users’ mailbox and builds on traditional email protection solutions 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.

Intermedia has been recognized by J.D. Power for providing “An Outstanding Customer Service Experience” for its Assisted Technical Support. J.D. Power 2021 Certified Assisted Technical Program, developed in conjunction with TSIA. Based on successful completion of an audit and exceeding a customer satisfaction benchmark for assisted support operations. For more information, visit **www.jdpower.com** or **www.tsia.com**.

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