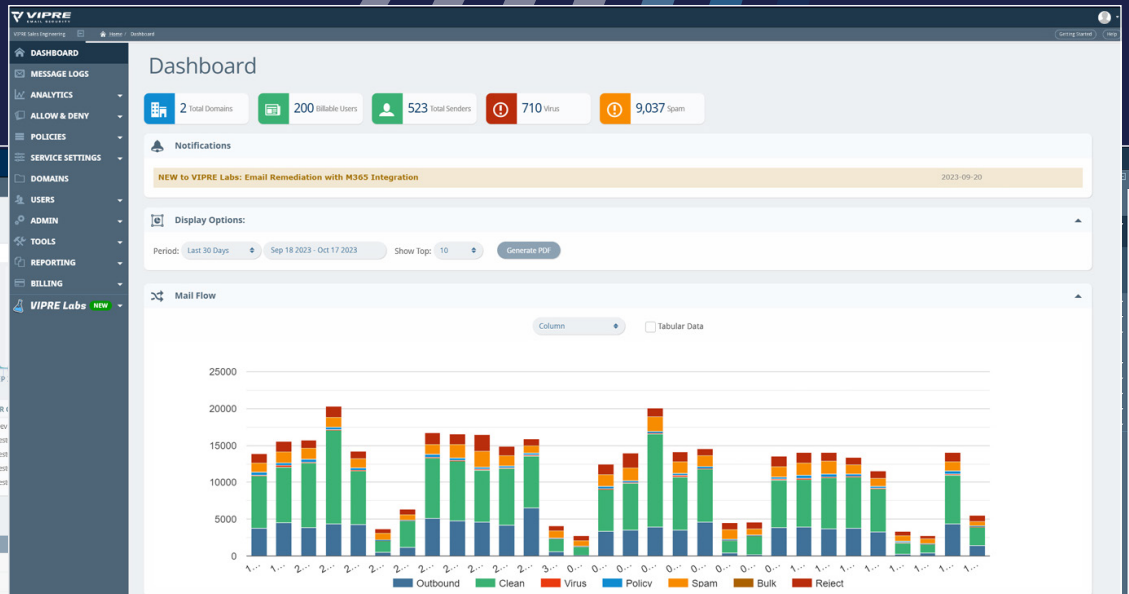
Protection for the Future, present and past.

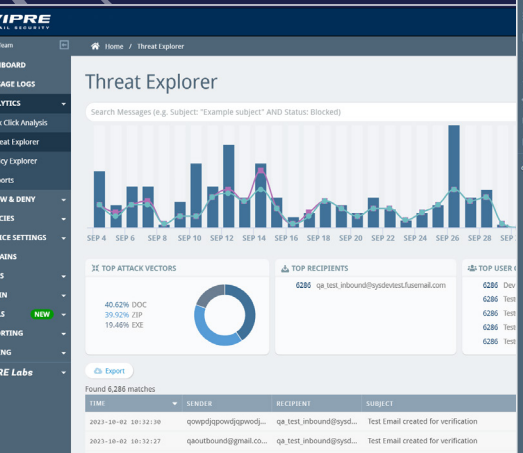
VIPRE Email Security Advanced Threat Protection

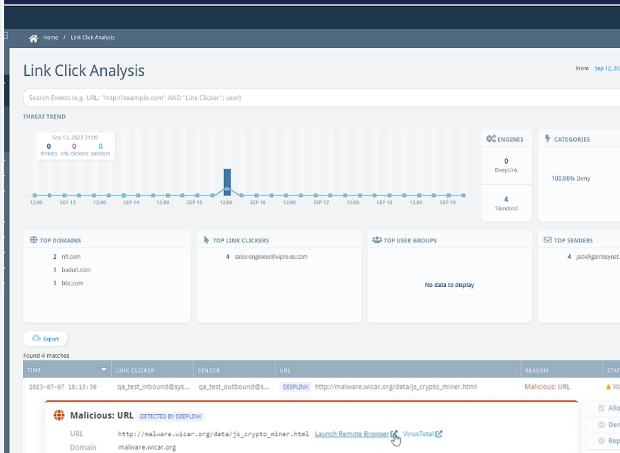
VIPRE SECURITY GROUP

VIPRE EMAIL SECURITY ADVANCED THREAT PROTECTION

Advanced email security for the future, present and past.







Content

VIPRE SECURITY GROUP

Solution at a Glance

Email Analytics

Comprehensive visibility into email threats and high value security information - enabling you to swiftly drill down an investigative path to relevant data and detail.

Remote Browser Isolation

Advanced tools and intuative UI to quickly and easily investigate any suspicious URL - in a real time, isolated sandbox.

ThreatAnalyzer

Perform a deep analysis of any discovered files/ URLs safely in a 'Sandbox' – a virtual machine in the cloud - and understand if they are malicious or not.

Threat Explorer

Investigate suspicious attachments, spot patterns, and drill down into each threat.

Email Remediation

Enables administrators to remove a malicious, or otherwise suspect email from a user's inbox even after it has been delivered.

Advanced Policies

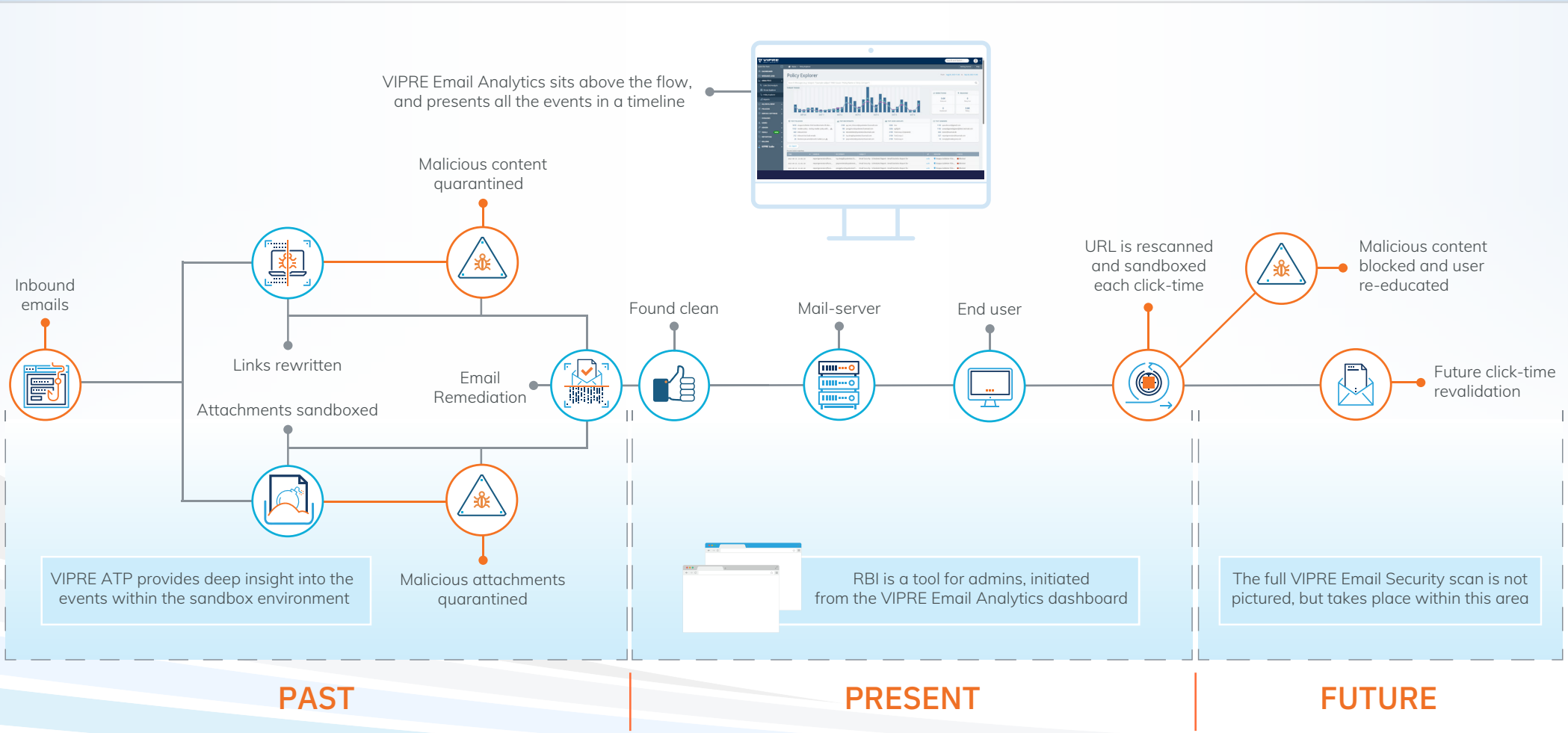
An extremely flexible, preventative tool, enabling administrators to customize almost every aspect of the VIPRE ATP service to the organization's requirements.

Continuity

If email services are disrupted, users have access to a rolling 90 days of their personal email traffic and can use the VIPRE ATP Continuity Portal as a webmail service to send and receive emails.

VIPRE SECURITY GROUP

VIPRE ATP Process



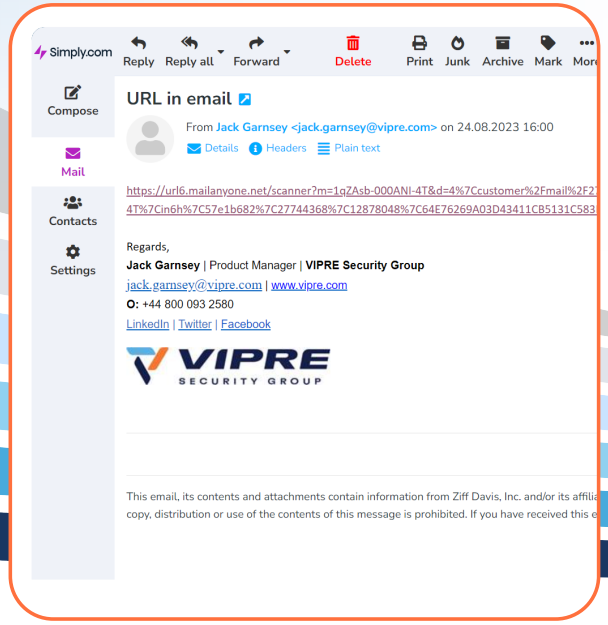
Link Isolation (End-User Experience)

Link Isolation is a powerful solution that protects users by neutralizing malicious URLs in emails and their destination web pages.
It utilizes advanced sandboxing technology, while simultaneously educating users about the dangers of clicking links in emails.

End-users no longer receive malicious URLs in emails. Instead, VIPRE ATP replaces the URL with a safe link, protecting the user.

When the safe link is clicked, the user is presented with a Link Isolation progress page as the content is dynamically scanned (see next page: 'Link Isolation Process')

The user is either safely redirected to the original website or is presented with a block / warning. Specific reasons for the caution are displayed, and the user is issued an educational video on cybersecurity.

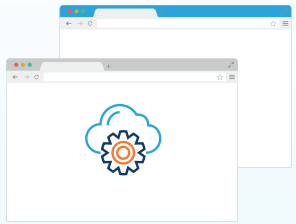


VIPRE SECURITY GROUP

Link Isolation (Process)

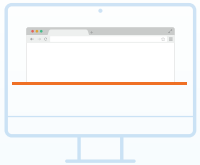
The process behind Link Isolation embodies VIPRE's efforts to interconnect the various components of the software seamlessly and comprehensively. The following infographic illustrates the extent of our security inspection on emails even after delivery.

REMOTE BROWSER



URL is opened in a remote browser in the cloud, 'crawled' and analyzed.

ANALYSIS



As the page is rendered, the following happens in real time:

Network requests and responses are monitored

All web page objects are effectively extracted and downloaded for analysis

Actions taken by JavaScript code are monitored

- HEURISTIC ANALYSIS
- STATIC ANALYSIS
- ZERO HOUR THREAT OUTBREAK DETECTION

EXTRACTIONS

Features extracted for analysis

JavaScript flow manipulation (Cross-site scripting etc. Code can be scanned and executed when isolated)

Navigation flow manipulation (Presence of redirections or deviations from normal navigation patterns)

Location hints (Does geolocation information match context?)

Visual heuristics (Visual spoofing of other companies, pop-ups, suspect ads, etc.)

Form and type extraction (How is data collected and processed?)

Form submission heuristics (Identify vulnerabilities, security issues/risks)

Online document recognition (Scan docs for known viruses, embedded links. Checking metadata for authenticity)

Title, page, document heuristics (Keywords, urgency, etc.)

Domain heuristics (Reputation, who is information, age of domain, SSL certificate etc)

REPORTING

Reporting and data analytics

- LIVE THREAT MONITOR
- SECURITY ALERTS
- VIPRE ATP REPORTS
- FORENSIC INFORMATION

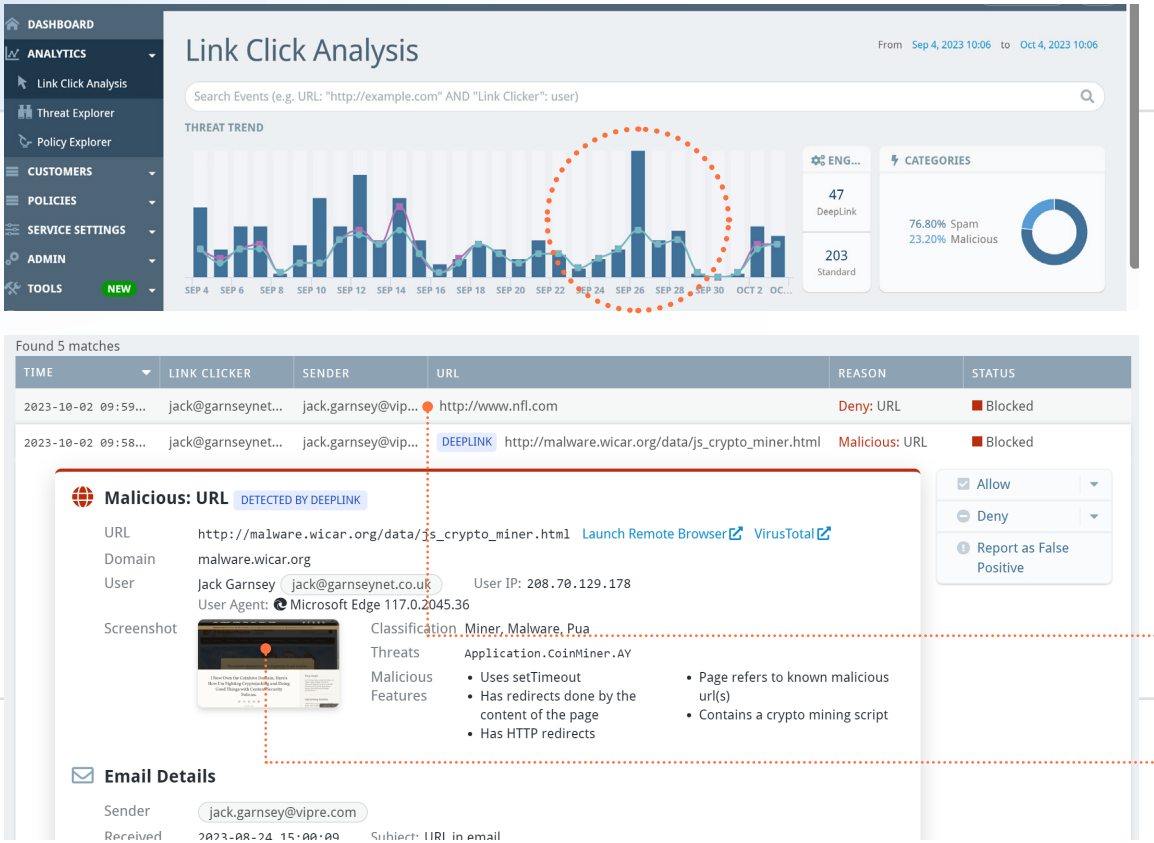
Link Click Analysis

With VIPRE ATP, links that have been clicked by end-users can be analyzed in an easy to use, interactive dashboard.

See how many suspicious links are being clicked by your organization, what threats you are subjected to and who your most vulnerable users are.

Identify patterns, including repeat offenders, common links and senders.

Dive deeper and drill down into a specific link - details of the email and the reason for the block can be quickly accessed.



Links that are clicked are categorized in one of the following ways:

Malicious - Items categorized as malicious are known malicious sites.

Suspect - Items that have been identified as suspicious sites, possibly unknown threats.

Spam - Items that have been identified as spam based on your configured policies.

URL

URLs can also be reviewed via the safety of VIPRE's Remote Browser Isolation

Safe Preview

- Quickly see & review a static image of the site

Remote Browser Isolation (RBI)

Remote Browser Isolation renders website content in virtual browsers sealed in cloud-based containers.
This enables administrators to quickly and easily investigate any suspicious URL - in a real time, isolated sandbox.

RBI is fully integrated within VIPRE Email Analytics and a log is created of all events.

When investigating suspicious links, the remote browser can be accessed in the following ways:

Within Link Click Analysis (Analytics > Link Click Analysis)

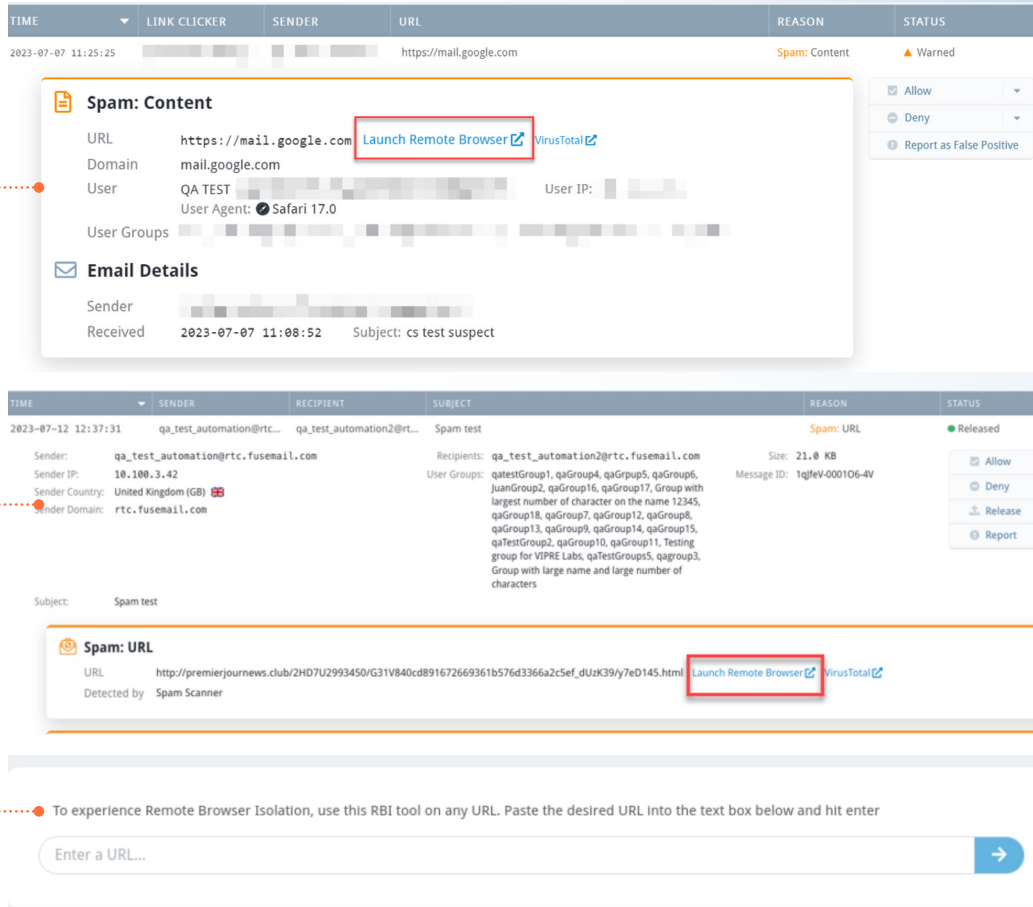
Scenario: You're already working in the Link Click Analysis dashboard to determine which email address sends your organization the highest number of malicious links. You see one URL you aren't sure about and would like to review it without risking the safety of the computer you're using.

Within Threat Explorer (Analytics > Threat Explorer)

Scenario: You're already working within the Threat Explorer tool to determine which user groups receive the most spam emails and want to investigate one email a little closer.

Email Security Cloud Tools

Scenario: You have a list of URLs that you obtained outside of VIPRE Email Security Cloud and would like to review them in the safe environment of a remote browser.



Suspicious Attachment (VIPRE ThreatAnalyzer Sandbox)

Any attachments extracted from the original email can be analyzed via integration to another VIPRE service, ThreatAnalyzer.

VIPRE ThreatAnalyzer enables you to perform a deep analysis of any discovered files/URLs safely in a 'Sandbox' – a virtual machine in the cloud – and tells you if they are malicious or not.

- Investigate potential threats and understand their attack patterns.
- Gain deep insight into any attack: every file or key touched by the attack, every process started, every network connection made, and understand exactly what the attack is trying to do.
- All threat data is checked against a vast database of known threats embodied in our VIPRE ThreatIQ intelligence service.

FILE TYPES

Supports wide variety of file types

Executables, PDF Documents,
Office Documents, Powershell Scripts, etc...

ThreatAnalyzer records lots of activity triggered leaving multiple layers of data for analysis:

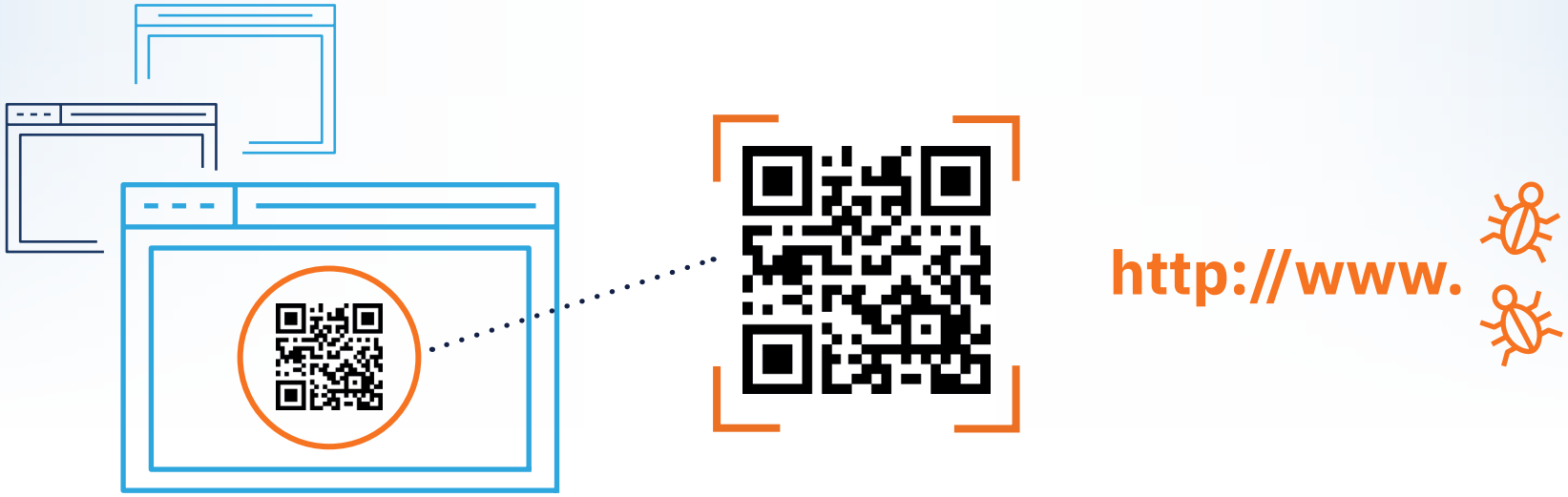
FILE ANALYSIS

- Processes launched
- Files created / accessed / changed / deleted. Copies of each file saved
- Registry keys created / accessed / changed / deleted
- Network data transferred in / out
- Mutexes, Named Pipes, etc...
- DNS lookups, IP addresses contacted, etc...
- Reverted to clean state after each sandbox run i.e. disposed of
- All files containing images undergo scanning for QR codes, which are then converted into URLs and inspected for potential malicious activity

Suspicious Attachment (VIPRE ThreatAnalyzer Sandbox)

VIPRE ThreatAnalyzer also has an inline QR code detection engine.

This feature enables deeper analysis by scanning and parsing QR codes found in attached PDFs, Word documents, and images within messages.



VIPRE Threat Explorer

VIPRE Threat Explorer enables administrators to investigate suspicious attachments.

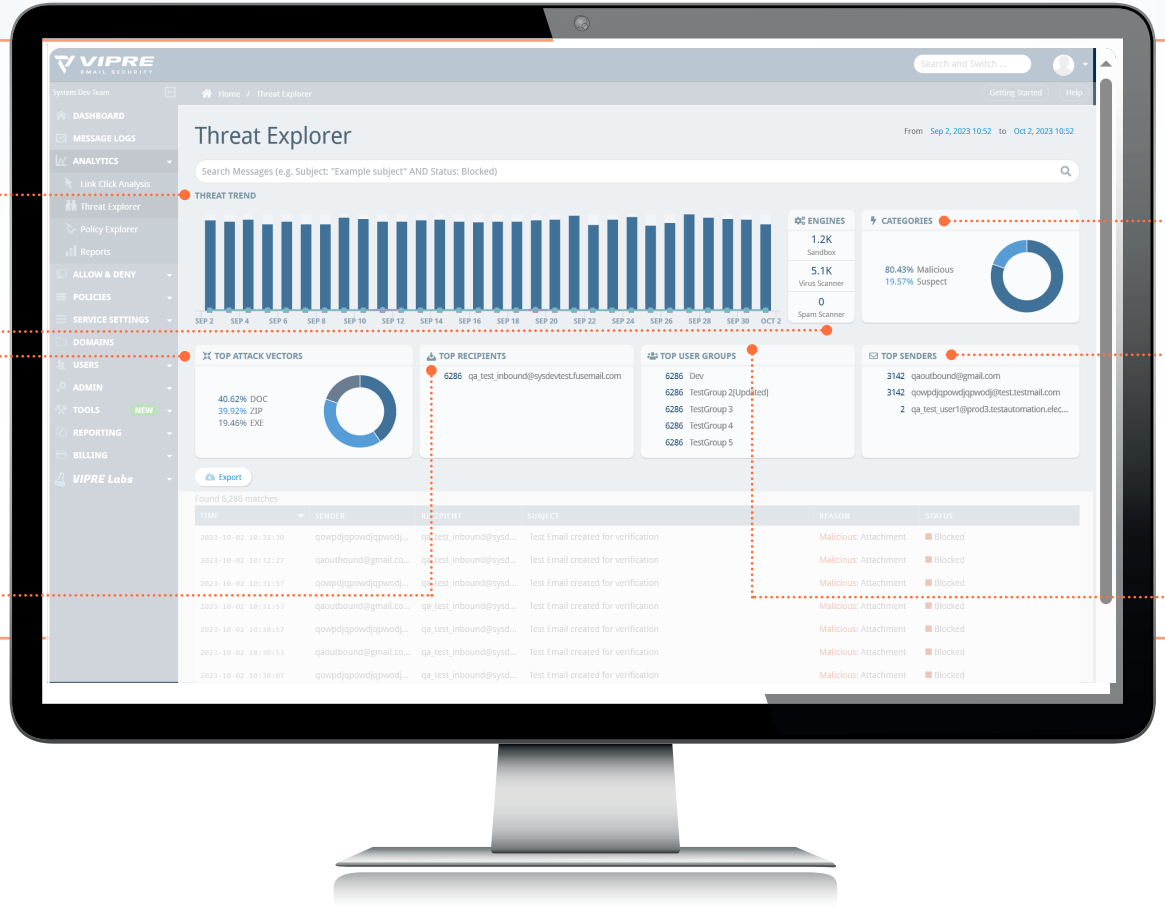
All sandbox blocks and warnings are presented in the Threat Explorer area of the admin portal.
From here it's possible to see patterns, including targeted recipients, common file types and senders.

Threat Trend
Shows emails received by your organization that potentially contain threats

Engines
Number of threats caught by our various Threat Detection Engines

Top Attack Vectors
Top 5 types of attack sent via email

Top Recipients
Top 5 user email adresses in your organization that received suspicious or known malicious messages



Categories
Different categories of threat

Top Senders
Top 5 email address that send suspicious or known malicious messages to your organization

Top User Groups
Top 5 user groups in your organization that received suspicious or known malicious messages

VIPRE SECURITY GROUP

VIPRE Threat Explorer (Example)

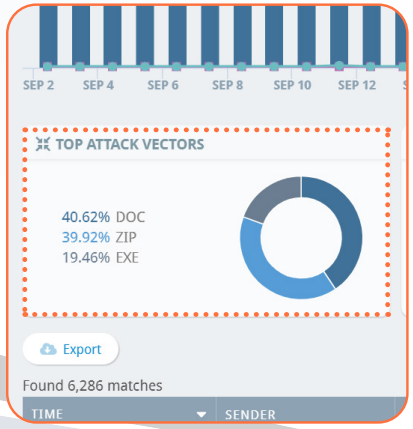
VIPRE Threat Explorer enables administrators to quickly drill down and investigate threats - details of the email and the reason for the block can be quickly retrieved.

VIPRE Threat Explorer presents all the relevant data to the administrator including the specific behaviors that have led to the suspicious classification.

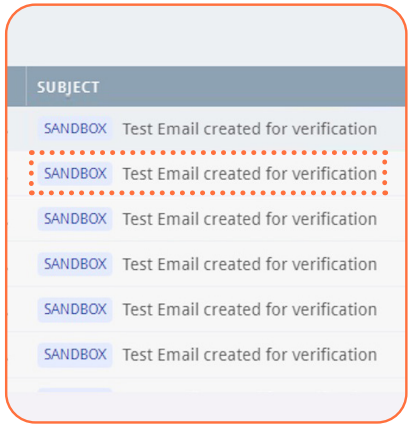
At the end of the investigation, the administrator can Report, Release, Allow or Deny the attachment from the same dialogue.

Click on Threat Explorer.

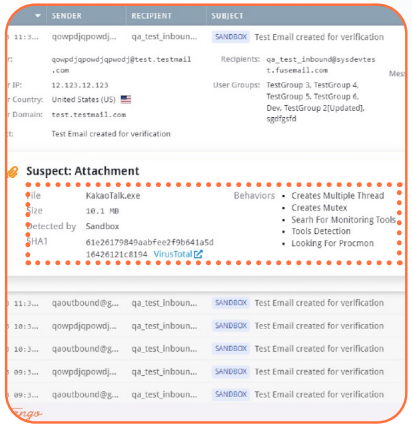
Drill down into Executable files from the interactive chart.



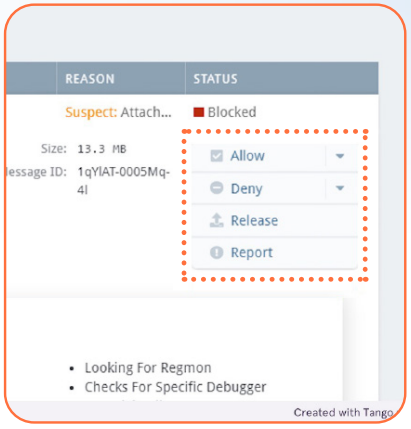
Click on a specific email.



Review details on the file that was stopped.



Review actions.



VIPRE SECURITY GROUP

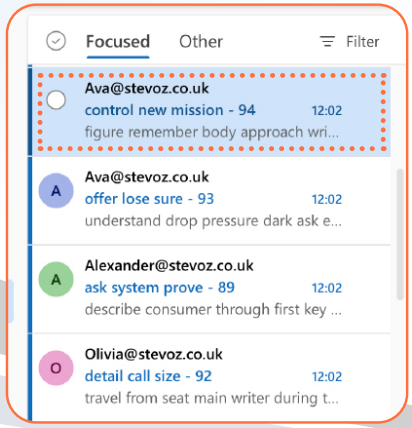
Email Remediation

VIPRE ATP Email Remediation enables administrators to remove a malicious or suspicious email from a user's inbox even after it has been delivered.

Administrators can search for, locate and remove email from a users inbox, or from the inboxes of multiple users.

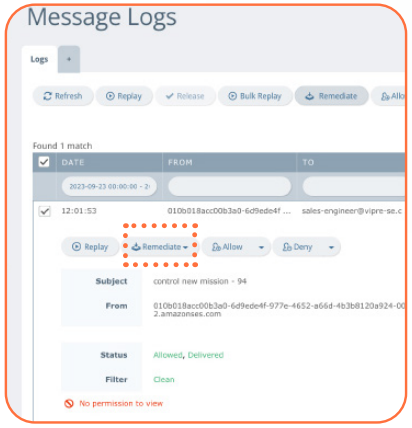
This is achieved through a simple integration with Microsoft 365, and the following workflow:

In an end user mailbox, see email that needs to be remediated.

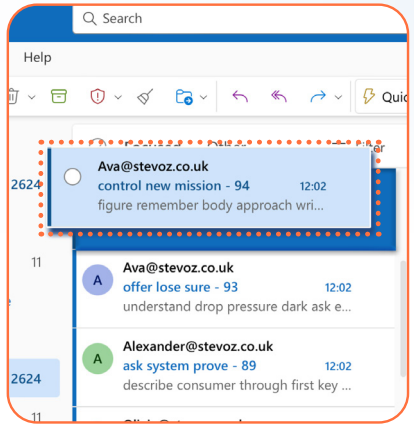


Search for and locate the email that needs to be remediated.

Click remediate on the selected email.



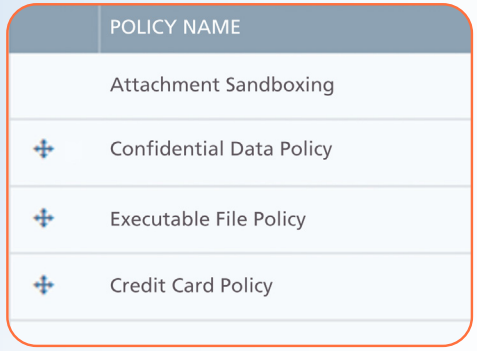
The email in question is no longer in the users inbox.



VIPRE SECURITY GROUP

Advanced Policies

Advanced policies are an extremely flexible, preventative tool, enabling administrators to customize almost every aspect of the VIPRE ATP service to the organization's requirements. These policies augment your email security, preventing known scenarios and can be tailored to your organization's business policies. Examples include:

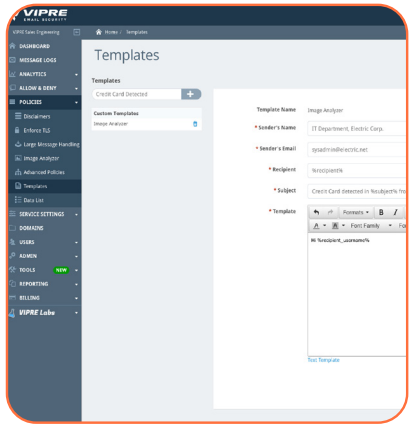


Confidential Data Policy – Quarantining outbound emails containing confidential project data such as project names, financial documents, etc.

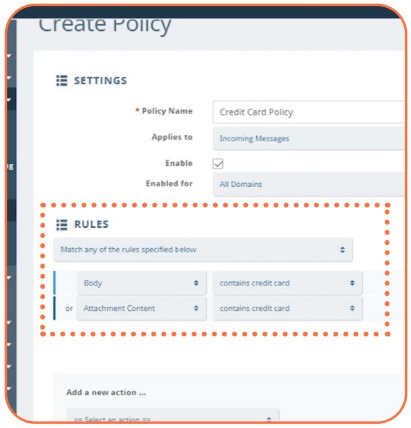
Executable File Policy – Quarantine any inbound or outbound email with .exe file(s) attached.

Credit Card Policy – Quarantining any inbound or outbound email that contains credit card information.

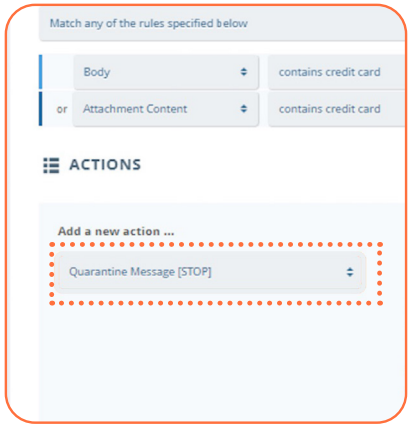
Create and customize your template, including the content of the email notification.



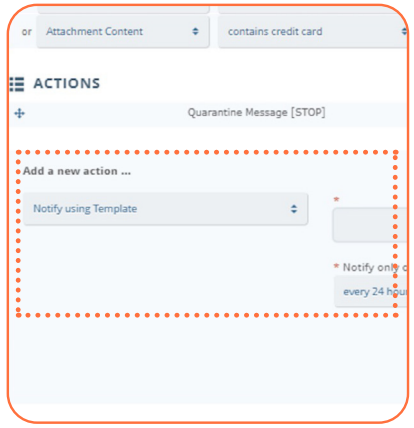
Create a 'Match Any' rule, for both the body of the email and the attachment content.



Set rules for quarantining.



Create a notification for when the rule triggers.



Policy Explorer

Once you have defined your organization's policies, Policy Explorer provides the visibility across all blocked emails sent or recieved by users within your organization.

Threat Trend
Shows the threats for a given time frame

Top Policies
Top 5 policies blocking the messages

Top Recipients
Top 5 recipients in your organization that receive blocked messages

Directions
Number of incoming/outgoing blocked messages

Reasons
The reason for the block

Top Senders
Top 5 senders who send messages that are blocked by your organization

Top User Groups
Top 5 user groups in your organization that received or sent blocked messages

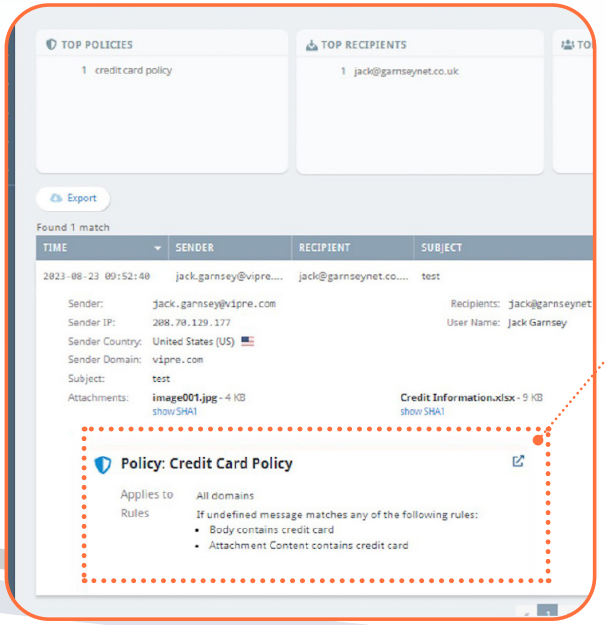
Using Policy Explorer to Locate Policy Triggers

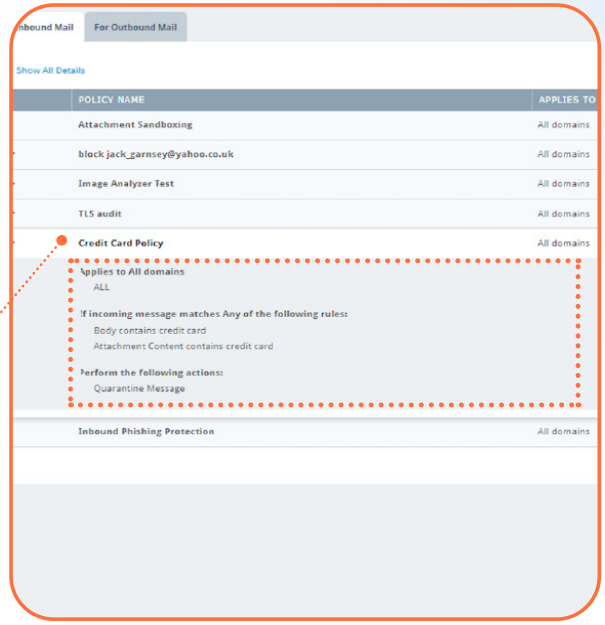
Using the previous credit card example, the administrator can find instances of the policy triggering within the Policy Explorer dashboard:

Drill down from any of the data points (widgets) or to a point in time on the histogram.

View detailed information on the reason for the block.

View or edit the policy responsible for the trigger.





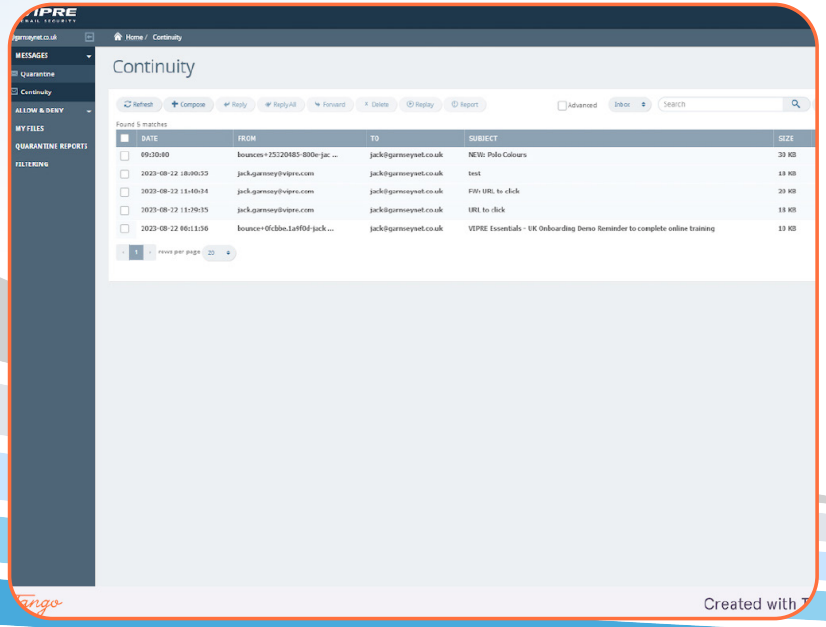
VIPRE SECURITY GROUP

Continuity

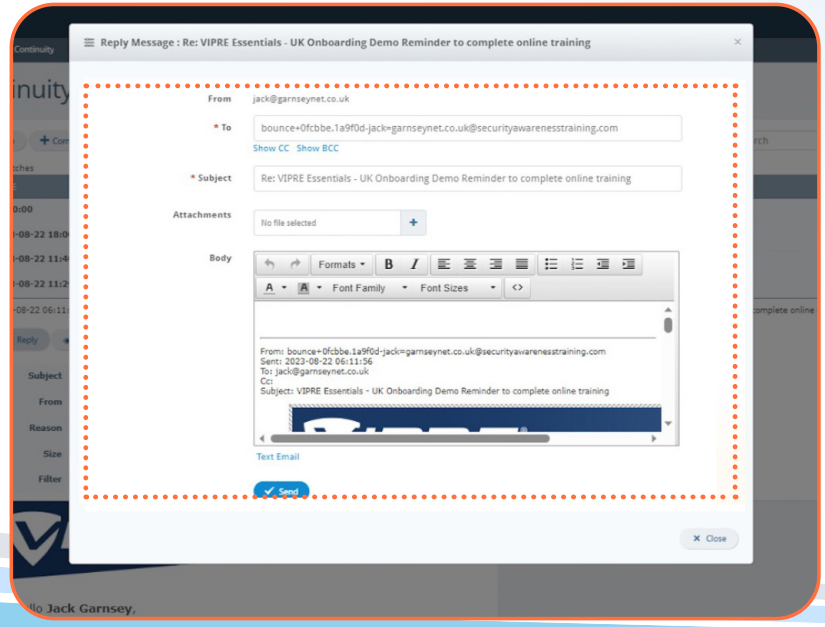
The VIPRE ATP portal also provides user level access to business continuity tools.

If email services are disrupted, users have access to a rolling 90 days of their personal email traffic and can use the Continuity Portal as a webmail service to send and receive emails. As VIPRE receives external emails ahead of customer's core email services / email servers, if these services are disrupted, VIPRE provides the continuity.

End users log into webmail to view 90 days of email and manage their settings.



Compose, reply, forward, etc., as with any webmail client.



Why Choose VIPRE ATP?

- ✓ Powerful, multi-layered protection for your organization's most vulnerable attack vector - email
- ✓ Comprehensive visibility into email threats
- ✓ Intuitive portal presents high value security information enabling you to swiftly drill down and take action
- ✓ Next-generation sandboxing of email attachments and URLs
- ✓ Interactive tools to empower, educate, and enable your users
- ✓ Technology designed to neutralize zero-day attacks
- ✓ Easy deployment with intuitive management interface
- ✓ Seamless integration with Microsoft 365
- ✓ Technical support always on-hand for advice and assistance

VIPRE SECURITY GROUP

North America
sales@vipre.com
+1 855 885 5566

UK and other regions
uksales@vipre.com
+44 (0)800 093 2580

DACH Sales
dach.sales@vipre.com
+49 30 2295 7786

Nordics Sales
nordic.sales@vipre.com
+45 7025 2223

VIPRE SECURITY GROUP

VIPRE Advanced Email Threat Protection (ATP)

SOLUTION BRIEF

Insights

Email is one of the most common forms of communication today, and this is particularly true for business purposes.

A recent study projects that there will be 4.73 billion email users worldwide by 2026. This is due in large part to the fact that a good portion of the workforce relies on email for the majority of their work communications, especially remote and hybrid workers. Email is also a significant medium for communicating with current and prospective customers, used for advertising and conveying important information. As email continues to rise steadily in popularity, cybercriminals are developing and advancing tactics to take advantage of email users.

4.73 BILLION email users worldwide by 2026

Evolving Email Threats

While bad actors are constantly looking for new and innovative ways to launch their attacks, they also often fall back on tried-and-true methods.

Phishing is one of the oldest and most reliable tricks in the cybercriminal handbook: one estimate states that more than 90% of successful cyberattacks begin with phishing emails. There is a broad range of potential consequences of falling for a phishing email, and attackers use phishing as a gateway into an organization.

74%

of data breaches in 2022 involved the human element.

There are two main techniques that cybercriminals use in phishing emails:

1. Deceptive links—Bad actors use social engineering and deceptive tactics to lure users into clicking a link that directs the target to whatever page the attacker wants. One common example is a spoofed login page where attackers harvest login credentials.

2. Identity deception—Attackers disguise themselves as a legitimate organization or individual in order to trick their targets into action. Business email compromise (BEC) is a prominent example of this type of threat.

Phishing opens the door for cybercriminals to launch all manner of attacks. They can use phishing to obtain access to an organization's systems without exploits or hacking, by simply deceiving users into providing them authorized login credentials. They can also use attachments in combination with social engineering in order to infiltrate a company with malware, including ransomware. Malicious attachments have lately been growing in proportion when compared with malicious deceptive links used by bad actors.

Artificial intelligence (AI) is a tool that cybercriminals have adopted into their arsenal, using it to optimize their attacks for success. It can be used to make the tone and diction of phishing emails sound more natural, even imitating the writing style of certain individuals, thus eliminating many of the "red flags" that individuals are taught to look out for. AI can also automate the process of sending phishing emails, saving cybercriminals time and effort.

How to Protect Your Inbox

There are many measures that organizations and individuals can take in order to protect against email threats. These tactics represent a variety of angles from which to approach email threats, accounting for gaps in security with technology, policy, and user awareness altogether. It is important to layer these strategies to create a robust strategy for preventing email threats. VIPRE Security Group suggests some comprehensive strategies for defending your inbox against phishing and other types of threats.

According to Verizon's Data Breach Investigations Report, 74% of data breaches in 2022 involved the human element. Successful phishing attacks are particularly likely to be the result of human error. This is why employee training and awareness is a vital part of any security strategy. Users should be educated on how to identify and respond to threats such as phishing emails, thus decreasing the chance that an employee will be fooled by a phishing attack.

Besides security training, there are technological solutions that organizations can implement in order to defend against email threats. Automated features such as advanced email filtering and scanning, email authentication protocols, URL inspection and link isolation, attachment analysis, and continual monitoring are all crucial tools in an email defense strategy. These steps can be achieved with properly implemented and configured software tools, often with multiple features combined into one solution, such as VIPRE's Advanced Threat Protection.

There are many measures that organizations and individuals can take in order to protect against email threats.

With the above solutions in place, the chances of an attack or a mistake occurring are lower, but not zero. This is why it is necessary to employ email encryption and email remediation. Encryption is a way to ensure that cybercriminals do not have access to sensitive data, even if an email does fall into the wrong hands. Email remediation is a mechanism that can retract suspicious emails that manage to get around security measures.

Conclusion

Protecting against email threats should be a top priority for organizations, as a wide variety of attacks can be launched via email and have the potential to cause significant damage.

Phishing is a major danger, and cybercriminals have recently adapted their tactics to use AI to their advantage, making their attacks even more insidious. Implementing a robust and layered email security strategy requires a number of different measures and policies, from employee security training to software solutions.

For a more in-depth view of the most pressing current email threats and how to protect against them, you can download the full whitepaper here.

VIPRE SECURITY GROUP

North America
sales@vipre.com
+1 855 885 5566

UK and other regions
uksales@vipre.com
+44 (0)800 093 2580

DACH Sales
dach.sales@vipre.com
+49 30 2295 7786

Nordics Sales
nordic.sales@vipre.com
+45 7025 2223