VIPRE EMAIL SECURITY

Solution Brief

ADVANCED THREAT PROTECTION (ATP)

Layered Security with Sandboxing and Phishing Protection

Cybersecurity threats continue to evolve as attackers employ advanced techniques like zero-hour exploits and customised malware to stay a step ahead. Traditional signature-based solutions are necessary but may lack the modern analytics to prevent all zero-hour and targeted attacks. A more powerful protection is needed. New and emerging threats require a layered email security approach that includes multiple levels of malware detection, and must cover common attack vectors such as malicious attachments and URLs simultaneously.

SMBs Under Attack, Email Attachments Widely Targeted

Often seen as easy targets, criminals prey on small and medium-sized businesses while leveraging advanced techniques to bypass traditional security. Typically, smaller organisations do not have the resources that larger enterprises have, so they need a solution that will provide them with a similar level of advanced protection in a cost-effective, easy to manage package. VIPRE ATP is perfect for SMBs challenged with limited IT resources.

- "The average company received over 94% of their detected malware through email while over 45% of malware was delivered by email attachments containing common Microsoft Office documents"
  – Verizon 2019

VIPRE Email Security Advanced Threat Protection (ATP) offers enterprise-grade email protection in an easy to use, out of the box package. VIPRE ATP defends end users against the newest most sophisticated strains of malware, weaponised attachments and phishing techniques that evade traditional detection.

Comprehensive Solution from a Single Vendor

VIPRE is the single source from ordering and provisioning to award-winning support. Get more for less with a single trusted vendor.

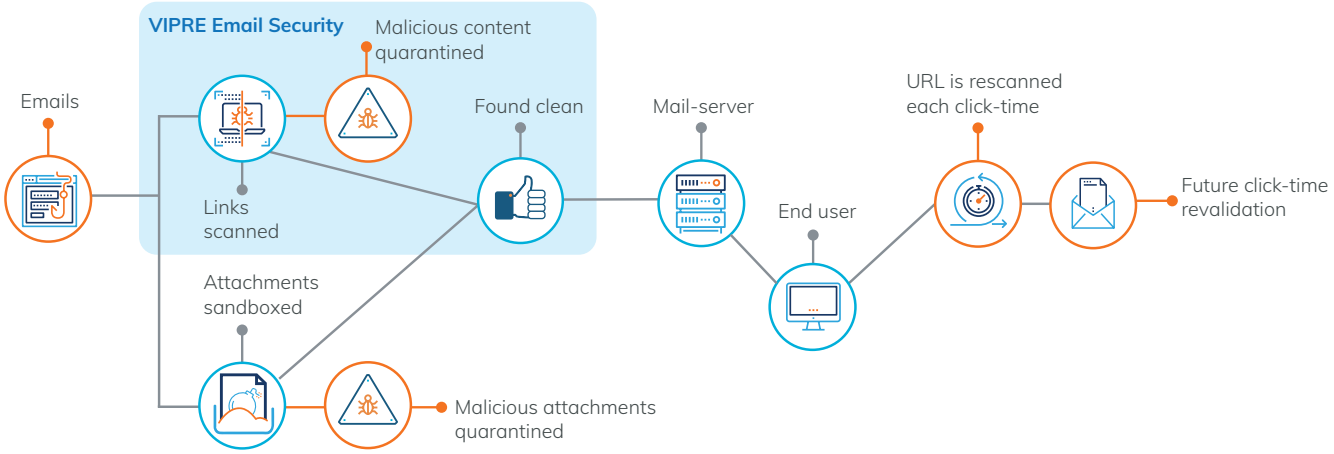
Single Solution for Multiple Attack Types

Powerful email security incorporating protection against malicious attachments and URLs simultaneously.

Zero-hour Protection

Signature-based bulk malware detection, combined with sandboxing and machine learning behavioural analysis, deliver powerful defence against zero-hour malware.

VIPRE Email Security Cloud: Journey Leveraging ATP



Powerful Protection with Layered Defence

At the core of VIPRE ATP is VIPRE Email Security Cloud, the platform that provides a solid foundation for email reception, handling, and bulk protection. This base platform includes core anti-spam, anti-malware, and anti-phishing technology, continuity protection against email server downtime, and highly customisable filtering and routing rules.

- Core email reception and routing engine
- Provides tough anti-spam, anti-malware, and anti-phishing protection against bulk malware
- Sophisticated custom routing/filtering rules to meet any business need
- 90-day continuity protection to guard against email server outages

Attachment Sandboxing goes a step further than traditional anti-malware by executing extracted attachments in a protected cloud sandbox environment. The behaviour of the executed content is observed and compared against our database of millions of malware samples using sophisticated machine learning to determine if the content could be malicious.

- Powerful sandboxing technology
- Protects against evasive and sandbox-aware malware
- Dynamic, isolated cloud virtual machine environment that scales easily to handle the load from all clients
- Detailed behavioural analysis output that explains exactly what the attachment tried to do upon execution

Phishing Protection provides another layer of defence against embedded malicious URLs by closing the time gap, often exploited by attackers, between receipt-time scanning (performed by the core platform) and when an end user clicks on the URL. All an attacker has to do is to wait to set up a malicious domain until sometime after an email is sent, and users could be fooled into visiting a phishing site. Phishing Protection closes that gap by rewriting the URLs embedded in emails and re-scanning them at click-time, ensuring that users stay protected.

- Performs a deep scan of URLs and blocks links that can lead to malware infection
- Re-writes URLs in emails for click-time protection
- Schedule reports and statistics
- Create custom messaging

Email Security ATP Features

Anti-spam & Antivirus	✓
Outbound Email Scanning	✓
Email Replay	90 Days
Allow & Deny List	✓
Disclaimers (HTML & plain text)	✓
TLS Encryption	✓
Large Message Handling	✓
Advanced Policies	✓
Custom Policies	✓
DLP	✓
Spoofing Protection	✓
End-User Spam Reports	✓
LDAP Integration	✓
End-User Access	✓
VB-Checker	✓
Always-On Continuity	✓
Phishing Protection	✓
Attachment Sandboxing	✓
Email Encryption	add-on
ImageAnalyzer	add-on
Email Archiving	add-on

SLA

Known Virus Detection	100%
Spam Detection	99.9%
Service Availability	99.9%

Management

Dashboard	✓
Multi-Level Logins & Permissions	✓
Message Logs	90 Days
Spam & Quarantine	90 Day Retention