Secure your #1 threat vector

Email is now the leading attack vector for cybercriminals intent on network infiltration—so implementing the right security solution is critical to preventing costly breaches.

VIPRE Email Security Cloud delivers unparalleled protection from advanced email threats and accidental or malicious data leakage via email—in the office or on the road, no matter the device.

Featuring a multi-layered security platform leveraging powerful machine learning technology, VIPRE Email Security Cloud delivers six levels of scanning to keep users safe from known and emerging email-based threats, including viruses, malware, spam, bulk mail, phishing, and spoofing. The solution also meets the needs of today's modern businesses with easy cloud-based deployment and a convenient browser-based portal.

Multiple layers of security, enable VIPRE Email Security Cloud to deliver:

Ransomware Prevention

VIPRE helps you bolster your defense against phishing attacks, the #1 attack vector for ransomware.

Real-time Monitoring

VIPRE's reporting system monitors the status of inbound and outbound email messages and provides quarantine summaries on an hourly, daily or weekly basis.

Simple, Secure Administration

VIPRE Email Security Cloud is entirely web-based with no software to install.
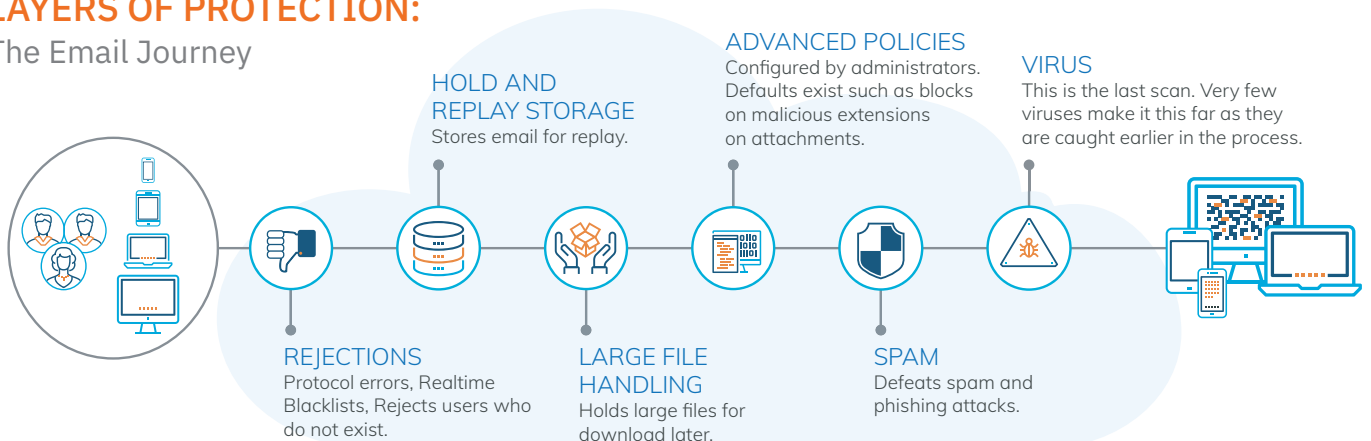
Robust User Management

The solution offers both user- and group-based policies, with advanced options for more sophisticated rule management.

VIPRE Email Security Cloud provides:

- Rich dashboard visibility through the VIPRE console into all types of email threats, including spam, viruses, and quarantined messages
- Powerful anti-spam, antivirus and anti-phishing technology that crushes unwanted or malicious messages while increasing operational efficiency
- Always-on email continuity, so users can still access emails from a web browser on any device even when the email server, like Office 365, is unavailable
- End-user spam reports and robust email logs
- Platform independence plus support for any email client or server (Microsoft Outlook, Lotus Notes, Office 365 and Google Apps)

LAYERS OF PROTECTION:
The Email Journey

HOLD AND REPLAY STORAGE
Stores email for replay.

ADVANCED POLICIES
Configured by administrators. Defaults exist such as blocks on malicious extensions on attachments.

VIRUS
This is the last scan. Very few viruses make it this far as they are caught earlier in the process.

REJECTIONS
Protocol errors, Realtime Blacklists, Rejects users who do not exist.

LARGE FILE HANDLING
Holds large files for download later.

SPAM
Defeats spam and phishing attacks.

Robust and Efficient Email Defence

With VIPRE Email Security Cloud, you can easily:

- Reduce the amount of time spent on email-related tasks for both staff and IT administrators
- Enjoy a user-friendly interface and effective spam filtering
- Protect the most-targeted attack vector from accidental or malicious acts, at any time, on any device, from anywhere

Take Charge of Email Security

VIPRE Email Security Cloud gives you the tools you need to better defend networks and users from data-breaching malware and sophisticated phishing scams.

- **Comprehensive Email Defence:** All inbound messages are scanned for viruses, malware and other suspicious content. Outbound filtering can be enabled for an additional layer of protection. VIPRE SLA guarantees 100% virus protection and at least 99.9% spam prevention, with less than 0.01% false positives.

- **Easy Management:** Easy to install, configure and manage from a single console, with robust default settings that can be customised for unique requirements, such as internal policies or regulatory compliance.

- **Attachment Defence:** Users can easily manage message disposition depending on type, size, or number of attachments, including the option to delete virus-infected attachments while keeping the related email message.

- **Message Quarantine:** Quarantine digests can be sent daily or multiple times a day, and quarantine retention can be set for any number up to 90 days. Certain types of messages, such as those from blocked senders, can be excluded from digest emails.

- **Robust Reporting:** Pre-configured reports are available to view within the administration console, and reports can be sent on a set schedule. Administrative-level reports show total/percentage caught by domain, top senders and recipients.

- **Logs:** Email logs can be viewed per user or group. Logs can be filtered by inbound/outbound, date/time received, status, sender, recipient, and subject.

- **User Permissions:** Users can be given the ability to manage their own settings - including aliases, spam sensitivity, and quarantine digest schedule - as well as edit sender lists and create custom filters and disclaimers. Users can also be designated as an Organisation Admin with some or all admin privileges.

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	90 Days
Email Link Isolation	add-on
Attachment Sandboxing	add-on
Email Encryption	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

VIPRE
SECURITY GROUP

FOR MORE INFORMATION visit **www.VIPRE.com**
call **+44 (0) 800 093 2580** or email **uksales@VIPRE.com**