VIPRE EMAIL SECURITY
With Microsoft 365

VIPRE®

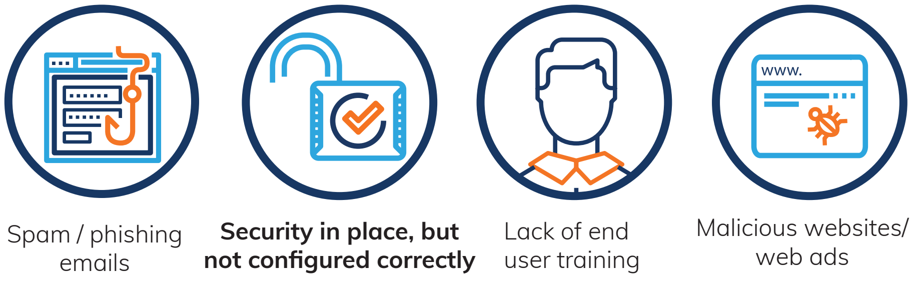
MOVING TO MICROSOFT 365?

Don't Settle For Security 'As Part of Your Package'...

With more companies moving to cloud services and embracing a hybrid workforce, this has become a global trend. Moving to the cloud for critical business functions makes sense, particularly with worldwide events forcing more businesses than ever before to adopt an agile working approach. However, with the move to cloud applications and services, it is essential that businesses invest in *defence in depth*, and that those defences are easy to manage, set up for their business and built by security experts.

Lock Down Your Most Vulnerable Areas

Email is the single biggest entry point for cyber-attacks and so it is critical that organisations do not limit protection in their most vulnerable area, and more importantly don't settle for pre-set security settings. In fact, in a recent study by VIPRE* it was found that one of the four biggest causes of ransomware infections is 'security in place, but not configured correctly'.

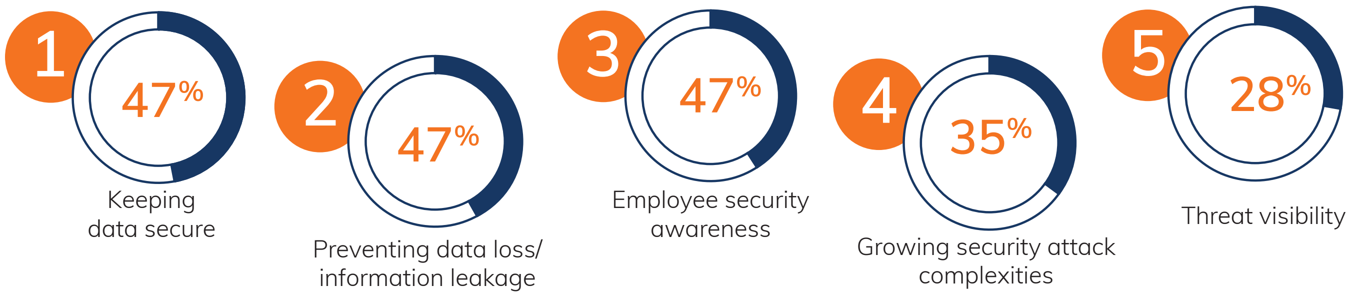

Spam / phishing emails
Security in place, but not configured correctly
Lack of end user training
Malicious websites/ web ads
www.

*Cause of Most Ransomware Infections, VIPRE 2020

> *"... some of our customers use Microsoft 365 and we find that VIPRE has much better reporting and configuration options when compared to Exchange Online Protection. We therefore recommend that our customers layer their email security with VIPRE Email Security. In addition to this, email replay functionality is critical for many businesses in the event of either error or disaster, and VIPRE offers 14 days of Email Replay as standard. Obviously when customers upgrade to Email Security Cloud, they then get 90 days of Email Replay and email continuity and so can access their email system in the event of any server problems."*
>
> **VIPRE UKI Gold Partner**

This highlights the need to partner with a security expert dedicated to ensuring your network is protected and who gives you security solutions that are already configured for top-tier protection from day one. This is where the use of cutting edge technology to power layers of defence really helps keep businesses secure with advanced capabilities such as behavioural analysis and threat intelligence playing an important role. At VIPRE, not only do we invest in these critical technology layers, we set you up for success by offering 1:1 on-boarding, administration portal walkthroughs and access to free training.

Our study received responses from over 1,000 SMB IT Admins and we asked them for the five biggest security challenges they face today**. The responses focussed on the below areas:



**Biggest IT Security Challenges, VIPRE 2020

Growing Security Attack Complexities

With attack complexity growth, IT Admins need to ensure they are protecting their networks from ever more sophisticated threats such as spear phishing emails, malware hidden in attachments and links that become weaponised after an email has already been delivered and scanned. Zero-day threats are always a concern and choosing a security vendor with enough experience and knowledge in behavioural analysis and machine learning should become standard for all organisations. The costs of layering security pale in comparison to the costs of cleaning up after a data breach, ransomware attack or phishing scandal.

Looking at those five focus areas for IT Admins in terms of cyber security, a key takeaway here is that organisations cannot afford to segment their security. They need to work with dedicated security vendors with experience in protecting all vulnerable areas. Here a security specialist can bring experience, depth of knowledge and service breadth to help businesses with protection against all threat vectors.

VIPRE has solutions to help businesses across all five areas of concern from standalone services to our Advanced Threat Protection package and on up to our Email Security Advanced Data Protection (ADP) Package.

Our Email Security ADP Package works to:

- keep data secure from both malicious and accidental data loss
- provide you with multiple ways to prevent data loss and leakage
- deliver smart, affordable security awareness training programmes
- cover the most vulnerable security areas with services that use machine learning and behavioural analysis
- report on threats as they come into your network, allowing IT Admins to manage all email quarantine reasons from one area

However, you don't have to go with a full data protection package to reap the benefits of a dedicated security provider. Our Email Security Advanced Threat Protection service keeps your number one threat vector locked down with traditional virus and spam checks working in tandem with behavioural analysis engines and real-time click scanning. When layered on top of the native Microsoft 365 security offering, this gives your organisation the powerful protection it needs to stay safe from the ever increasing sophistication of modern-day threats.

Please see page four of this document for more information on our email security solutions and do not hesitate to reach out to us on +44 (0) 800 093 2580 for information on our full portfolio of protection.

VIPRE Email Security 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**	add-on
Attachment Sandboxing**	add-on
Email Encryption	add-on
ImageAnalyzer	add-on
Email Archiving	add-on

*Email Security Cloud & Above
**Included in Email Security Advanced Threat Protection & Above

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

14 REASONS TO LAYER YOUR EMAIL SECURITY WITH VIPRE

Moving your business to Microsoft 365 makes sense in today's work environment, but to keep your network secure and protected make sure you invest in dedicated security across your attack vectors.

Here are 14 reasons we believe layering Microsoft 365 with VIPRE Email Security is a great security decision:

1. Layered security is stronger security, giving you multiple opportunities to catch threats before they hit your network.
2. Our cloud-based email security service performs multiple spam and virus scans using traditional anti-spam, anti-malware and antivirus checks, but also utilises our artificial intelligence and behavioural analysis engines to protect against more modern and sophisticated threats.
3. VIPRE are security specialists with over 25 years in the email security space dedicated to developing services which keep our customers' networks protected.
4. All crucial security settings are in place from day ONE, but you can work with our support team to tailor your protection to your organisation with our customisable advanced policies.
5. We include always-on email continuity with 90 days of email replay as part of our Email Security Cloud, Advanced Threat Protection and Advanced Data Protection packages.
6. You can easily build your own DLP rules in the management portal using advanced policies to pick up on keywords, key phrases and data strings.
7. We include DMARC, DKIM, Impersonation Protection and much more as standard.
8. With our attachment sandboxing and real-time click analysis we protect your network from zero day threats.
9. With VIPRE you have easy access to 24/7 Customer Support from one phone number and one email address.
10. Our customer SLA locks in your service levels so you can feel more in control of your protection.
11. Our spam capture rates are high! Keep the noise out of your users' inboxes and reduce the potential for problems.
12. VIPRE is an experienced IT Security vendor. We have been in IT Security for over 25 years and can offer you award-winning Email Security, Endpoint Security and Web Security. Our complete IT Security Portfolio also includes important modern-day protection for your users and data with services such as security awareness training, phishing simulations and protection from autocomplete mistakes as well as smart human-controlled DLP.
13. Our email security service works with Microsoft 365, meaning you keep all the benefits of Microsoft 365 and cloud business without losing out on specialist security.
14. Our service's modular design allows for additional protection such as email encryption, email archiving and protection from inappropriate imagery if the need arises.

VIPRE Email Security - Your Options

VIPRE offer multiple options for organisations to invest in advanced email protection. The unique modular design of our email security means that if you cannot find the perfect pre-built package for your needs, you can choose the elements that most reflect your security challenges - we offer the best of both worlds.

Email Security Cloud

Our award-winning, cloud-based email security service protects networks from viruses, spam, advanced email threats and data leakage via email.

It offers your organisation a secure solution for protecting your users no matter where they are - in the office, working from home or out on the road. Included in this service is always-on email continuity with 90 days of email replay, ensuring your business continues in the event of outages - planned and unexpected.

Email Security Advanced Threat Protection (ATP)

New and emerging threats require a layered email security approach including multiple levels of malware detection and behavioural analysis for zero-day threat prevention.

Our Email Security ATP package offers you a cloud-based, layered, email security solution incorporating the best in email anti-spam, anti-malware, antivirus and behavioural analysis as well as attachment sandboxing and protection against malicious URLs. ATP also includes a risk mitigating 90 days of email continuity.

Email Security Advanced Data Protection (ADP)

With our Email Security ADP bundle we have created the ideal solution to help organisations of all shapes and sizes keep their data safe from both human and technology vulnerabilities.

One of the most valuable resources a cyber criminal can get their hands on is an organisation's data - keeping it safe should be your no.1 priority. Safe data comes from a strong IT security infrastructure backed up by an educated workforce armed with data protection tools and knowledge. Our ADP package covers all key data loss vectors using advanced security, machine learning and behavioural analysis, coupled with user education and tools that enable your workforce to stay alert to simple mistakes with big consequences.

SafeSend

VIPRE SafeSend is an Outlook plugin which helps protect your organisation from accidental data leakage arising from autocomplete mistakes.

Sending an email to the wrong person is considered an embarrassing mistake until it turns into a serious data breach. What if that email held confidential information or had an attachment containing sensitive employee, product or financial details? SafeSend works to remove that potential for error by prompting email senders to confirm their recipient list and any attachments before enabling them to send an email. SafeSend's DLP module also supports further data protection by performing a deeper data protection scan, informing the user of any potential breaches or data loss.

Anti-Spam & Antivirus

Always-On Email Continuity

Post-Delivery Weaponised Link Protection

Attachment Sandboxing

Email Archiving

Email Encryption

Image Analysis

Protection From Misaddressed Emails & DLP

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