Email Threat Prevention Service

What is it?

The **norm.** Email Threat Prevention Service detects and blocks unwanted and malicious email traffic, including targeted and advanced attacks such as phishing and whaling. The service is powered by FireEye's Email Security Cloud platform, which provides cloud-based, 24/7/365 email security for both inbound and outbound email traffic.

The Email Threat Prevention Service constantly monitors corporate email traffic activity and quarantines and isolates suspicious emails.

The purpose of the **norm.** Email Threat Prevention Service is simple:

* To provide comprehensive inbound and outbound email security by detecting and blocking malware, phishing attempts and spoof emails
* To deliver in-depth knowledge of the latest email threats and first-hand knowledge of current attack techniques
* To present the results with monthly and real-time reporting via the **norm.** online Visualiser portal

Why now?

Organisations face an ever-increasing number of threats from email-based spam, malware and advanced threats. The majority of advanced threats arrive by email in the form of malicious attachments or URLs linked to credential-phishing sites and fraudulent wire transfer services. The highly targeted and customisable nature of email allows cybercriminals to successfully exploit it, making email the primary vehicle for many attacks.

The **norm.** Email Threat Prevention service constantly monitors corporate email traffic and uses this intelligence to prioritise alerts and block threats in real-time.

Can you afford to leave your business open to cyber-attacks?

What's included?

* Access to our Email Threat Prevention Service, powered by FireEye's Cloud Email Security platform – a feature-rich secure email gateway providing a range of security features including anti-virus, anti-spam, anti-phishing, sandbox analysis and advanced URL filtering to provide protection from known and unknown (Zero Day) attacks.
* Monitoring and analysis of inbound and outbound email traffic for advanced threats, spam and viruses. Scanning outgoing email traffic protects an organisation's domains from being blacklisted. Features include:
  * Advanced URL inspection to identify, isolate and immediately stop URL, impersonation, and attachment-based attacks, before they enter an organisation's environment
  * In-depth knowledge of attacks and attackers from frontline investigations and observations of adversaries
  * Sandboxing analysis to validate threats by executing them in isolation – detonating samples and blocking them in real-time
  * Analysis and quarantine (blocking) of unknown and advanced threats
  * Prioritisation of alerts and threat blocking through the accumulation of evidence and contextual intelligence concerning attacks and bad actors
  * In-depth visibility and detection of email security activities throughout an organisation's corporate environment
  * Real-time reporting via our online Visualiser portal

Want more detail?

For the full Service Description of our Email Threat Prevention Service <<ClickHere>>.
To register your interest and get one of the team to call you <<ClickHere>>
or just give us a call on **+44 (0)20 385 55242.**

norm.

In a nutshell…

The **norm.** Email Threat Prevention Service provides real-time, comprehensive protection against email-based cyber-attacks. It is simple to set up and gives subscribers real-time visibility into threats that have been identified and remediated. Whether it is deployed as part of our holistic CSaaS offering, or as a standalone module, the service delivers tangible results and ROI from day one.

How does it work?

The **norm.** Email Threat Prevention Service is a cloud platform which monitors corporate email traffic in both directions for threats from viruses, spam, malicious attachments, URLs, embedded code and traffic to/from known attackers/sources. To protect against malicious and fraudulent emails, messages are routed via the **norm.** email security platform, which analyses the emails for spam, known malware and viruses, and impersonation tactics first. It then uses URL defence technology and sandboxing to analyse every attachment and URL for potential threats and stop advanced attacks in real-time.

The **norm.** online Visualiser portal provides access to monthly reports and technical details of alarms and incidents in real-time.

FAQs…

I have an anti-spam, anti-virus and anti-malware email solution – isn't this the same?

Many email security solutions rely solely on commodity intelligence, anti-spam filters and anti-virus software. Advanced threats can easily bypass these signature-and reputation-based products. The **norm.** Email Threat Prevention Service protects businesses against advanced threats as well as providing the signature-and reputation-based protection seen in other platforms.
Our comprehensive secure email security service is comprised of a range of cyber security features including anti-virus, anti-spam, anti-phishing, sandbox analysis, and advanced URL filtering to defend against known and unknown (Zero Day) attacks.

I already have MS Office 365. Why do I need something else?

Microsoft Office 365 is great for managing email in the cloud, but it's not a cyber security solution. On the contrary, there are a growing number of cyber attacks that specifically target Office 365 applications. Only a dedicated, proven cybersecurity solution, which has been specifically designed to defend against advanced threats will protect your people, data and assets.

Will I need cyber security trained staff to understand the reports from this service?

We know how hard it is to recruit and retain good cyber security staff, that's why we give you access to our highly trained team of experts. They do all the complex work for you, and we provide visibility of the results via our clear and simple Visualiser portal. This gives you the information you need, at your fingertips, in a format that everyone can understand.

Will I be protected from phishing / whaling emails?

Yes – advanced threats including targeted phishing emails will be monitored, detected and blocked. Email Threat Prevention from **norm.** routinely identifies spear-phishing and whaling messages containing malicious links and attachments, often including those which have been missed by other email security solutions.

Does this mean I don't need to educate my users about email security threats?

Regardless of how effective an email security solution is, it is still important to educate your employees to be wary of these types of threats on an ongoing basis. For example, some emails do not contain malicious code or a suspicious URL, they will simply masquerade as a legitimate request for financial details or log in credentials – and they could have been sent from the compromised mailbox of a supplier or customer. Cyber awareness training therefore goes hand in hand with any technological solution.

How long does the service take to set up?

It is relatively straightforward to set up the **norm.** Email Threat Prevention Service and be protected within days. Once your corporate emails directed to the platform, you will start to see report information immediately.

Is there any benefit to the business beyond the direct security improvements?

The **norm.** Email Threat Prevention Service not only demonstrates that your business takes cyber security seriously, it also reduces your operational risk, helps to safeguard your reputation with customers, suppliers and regulatory bodies (such as the ICO), and ultimately improves the value of your business.