Email Threat Prevention (ETP) Service

Norm's Email Threat Prevention Service is a module from Norm's Cyber Security as a Service (CSaaS) offering.

Organisations face an ever-increasing number of email-based threats from junk and spam emails to malware and advanced threats. The majority of threats arrive by email in the form of URLs linked to credential-phishing sites, fraudulent bank transfer requests and weaponised file attachments. The highly targeted and customisable nature of email allows cybercriminals to successfully exploit it, making email the primary choice for cybercrime.

The Email Threat Prevention Service detects and blocks unwanted email, especially targeted advanced attacks. The service is built upon FireEye's Email Security Cloud platform providing cloud-based email security of your inbound and outbound email traffic which is scrutinised & analysed 24/7/365.

This service module focuses on the Technology element of Norm's holistic trinity of cybersecurity - People, Process and Technology. Its purpose is simple:

- Comprehensive inbound and outbound email security detecting and blocking malware and phishing URLs as well as impersonation techniques
- Provides in-depth knowledge about email threats with first-hand knowledge of attacks and attackers
- Display the results with monthly reports and real-time reporting

The Email Threat Prevention Service constantly monitors your corporate email traffic activity allowing for immediate response to respond, quarantine and isolate.

Service Features

You will gain access to Norm's managed service offering the following features:

- Powered by FireEye's Cloud Email Security platform which is a fully-featured secure email gateway providing a range of security protection from Anti-Virus, Anti-Spam, Anti-Phishing, Sandbox Analysis, Advance URL enabling protection from known and unknown (Zero Day) attacks. Features include:
    - Email threat monitoring for inbound and outbound email traffic for advanced threats, spam and viruses. The scanning of outgoing email traffic protects an organisation's domains from being blacklisted
    - Advanced URL Inspection to identify, isolate and immediately stop malicious URL, impersonation, and attachment-based attacks, before they enter an organisation's environment
    - Provides in-depth knowledge about attacks and attackers from frontline investigations and observations of adversaries
    - Sandboxing analysis validate threats by executing them in isolation – detonating samples and blocking them in real-time
    - Integrates seamlessly with cloud-based email systems such as Microsoft Office 365 with Exchange Online Protection and G Suite
    - Automated remediation for Office 365 - emails that become retroactively malicious after delivery to a user's inbox can be extracted

- Email Security draws on this real evidence and contextual intelligence about attacks and bad actors to prioritise alerts and block threats in real-time.
- Emails are analysed and quarantined (blocked) if unidentified (zero-day) and advanced threats are found hidden in:
    - All attachment types, including EXE, DLL, PDF, SWF, DOC/ DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 and ZIP/RAR/TNEF archives
    - URLs embedded in emails, PDFs and Microsoft Office documents
    - Credential-phishing and typosquatting URLs
    - Unknown OS, browser and application vulnerabilities
    - Malicious code embedded in spear-phishing emails
- Email Security enables analysts to use custom YARA rules to manage and enhance detections, stop the latest threats and identify ongoing campaigns
- In-depth and broad visibility and detection of email security activity throughout your organisation's corporate environment.
- Real-time reporting is available and accessible via Norm's Visualiser portal.

How the Email Threat Prevention Service works

The Email Threat Prevention Service is a cloud platform which monitors your corporate email traffic in each direction for threats from viruses, spam, malicious attachments, URLs, embedded code and traffic to/from known attackers/sources.

To protect against malicious and fraudulent emails, organisations simply route messages via norm's email security platform, which analyses the emails for spam, known malware/viruses and impersonation tactics first. It then uses the URL defence technology and sandboxing, to analyse every attachment and URL for threats and stop advanced attacks in real-time.

Email Security analyses every email attachment and URL to accurately identify today's advanced attacks. Realtime updates from the entire FireEye security ecosystem combined with attribution of alerts to known threat actors provide context for prioritising and acting on critical alerts and blocking advanced email attacks. Known, unknown and non-malware-based threats are identified with minimal noise and false positives so that resources are focused on real attacks to reduce operational expenses.

You will be provided access to the ETP control panel which will allow you to configure allow and block lists against email addresses, domains and IP addresses; as well as manage quarantined emails.

The service can be deployed in two modes:

- Active-Protection: This deployment method will analyse emails and quarantine threats for active protection. Organisations simply update their MX records to route messages to FireEye.
- Monitor-Only: For this deployment method organisations just need to set up a transparent BCC rule to send copies of emails to FireEye for threat analysis

Norm's online visualiser provides access to the monthly reports, but also the technical details of all the alarms and incidents in real-time.

On-Boarding Process

Once your order is received, a member of our customer experience team will take ownership of your order and contact you to introduce themselves as your project lead. They will arrange a Welcome call with you to guide you through the process, outlining who will be responsible for each element of the installation, and introduce you to your Norm technical lead. The onboarding process will include:

- Providing you with our service handbook detailing our service operational processes, SLA and contacts
- Assisting with installation and integration on to the platform including co-ordination with your IT/Network team(s) or provider(s)
- Enrolling you into Norm's email security platform
- Providing access to Norm's Visualiser platform

Once the service is fully deployed our customer experience team will provide you with access to the Norm visualiser. This visualiser will provide you with an overview of all the alerts detected in your environment, related technical details as well as access to reporting.

The SOC will also be on hand to provide technical advice and assistance on cyber-security queries or issues should this be required. They will support you throughout the on-boarding process, assisting with the required changes to your existing email platform and the initial configuration of the Email Security service.

Technical Requirements

The Email Threat Prevention Service can integrate seamlessly with cloud-based email systems such as Microsoft Office 365 with Exchange Online Protection and G Suite.

The Email Security platform can be deployed in two modes:

- Active-Protection: This deployment method will analyse emails and quarantine threats for active protection. Organisations simply update their MX records to route messages to FireEye.
- Monitor-Only: For this deployment method organisations just need to set up a transparent BCC rule to send copies of emails to FireEye for threat analysis

Service Availability

Upon subscription, to the service, the customer will be provided with access to Norm's Visualiser where all of the alert data, technical data/incidents and reports will be made available. The Norm Visualiser is available 24x7.

The service is managed within norm's UK based Security Operations Centre (SOC), 24hrs a day, every day of the year. The Customer Experience teams are available during UK business hours, Monday to Friday 9:00 to 17:30hrs, excluding public holidays.

Software updates for the email security platform will be automatically managed by the Norm platform.

The Customer Experience and SOC teams will be on hand to provide technical advice and assistance for any queries or issues should this be required.

Customer Responsibilities

- The Customer will be responsible for selecting the deployment mode and changing MX records as required.
- The customer will be responsible for updating allow and deny lists, the customisation of rules as required, and the release of mis-identified emails
- The Customer shall nominate an administrator internally for the Norm Visualiser and Email Security platforms.
- The Customer shall be responsible for user administration within the Norm Visualiser.