HORNETSECURITY

Stringent defence against the most sophisticated cyber-attacks

Hornetsecurity Advanced Threat Protection

As attackers create new cyber-attack methods, they are frequently using intelligent, blended attacks to heighten the chances of malicious code being able to infiltrate a targeted company's network. Hornetsecurity gives you tangible evidence that these Advanced Threats are being blocked.

Hornetsecurity's extensive threat intelligence database is vital in identifying and blocking new advanced threats and offers protection from:

- Ransomware
- Blended attacks
- Targeted attacks
- Business email compromise

The Advanced Threat Protection (ATP) service will protect clients' networks against a range of sophisticated attacks. The service has:

- Highly innovative forensic analysis engines
- A unique ability to minimise the risk of a data breach
- The tools to see tangible data to understand the depth and type of attacks on an organisation

ATP has 3 main elements to it:

- **Sandboxing with detailed reports** – The sandbox engine is a secure environment of virtual systems where suspicious emails can be opened and executed, including attachments or links. Behavioural and network-based analysis will be performed. The results are summarised in a detailed report, which can be used for IT forensic evidence protection.
- **URL Malware Control** – any links arriving on the mailserver will be scanned and opened within a secure proxy environment so the user can browse safely.
- **Targeted Fraud Forensic Analysis** – uses innovative detection mechanisms such as spy-out detection, fraud attempt analysis and intention spoofing recognition to detect and prevent social engineering attacks.

Key Benefits of ATP

- **Realtime notifications** – As soon as Hornetsecurity ATP detects an attack, an alert is sent immediately. This notification is detailed in nature and provides information on why the email has been intercepted.
- **URL scanning** – The URL rewriting engine secures all Internet calls from emails via the Hornetsecurity web filter. As standard, the sandbox engine will automatically scan all downloads.
- **Targeted Fraud Forensics** – Protects users from personalised attacks.
- **Sandbox engine** – Attachments are executed in a variety of system environments and their behaviour is analysed. An evidence log is created of all attacks attempted.
- **Ex Post Alert** – If it becomes apparent, at a later time, that an email is in fact malicious administrators are notified so they can take swift action across their environment.

Contact Brigantia

Suite 2.1, Hurstwood Business Centre, York Road, Thirsk, YO7 3BX

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com