GTMailPlus.ATP

Additional protection against malware

Cybercriminals have engineered malware that detects and evades "advanced" security tools, and up to **70% of malware in use today uses one or more evasion techniques** to avoid detection.

GTMailPlus' Advanced Threat Protection (ATP)

GTMailPlus' Advanced Threat Protection (ATP) adds an additional layer of protection providing advanced malware detection, utilising its global threat intelligence network. With its deep content inspection, the ATP solution works using behaviour based technology utilising its elastic sandbox environment to visualise and report on exactly what the malware interacts with compared to the typical signature based detection which relies upon previously known exploits.

> **The ATP which GTMailPlus uses scored a perfect detection rate of 100%** in all test categories with zero false positives. No other vendor or product has achieved this level of performance, in over 20 years of testing.
>
> **NSS Labs, 2017**

Why is ATP needed?

Cybercrime is projected to exceed $2 trillion by 2019 and malware is the primary culprit in many of these security breaches. Today's malware has become so sophisticated that it can detect and outsmart "next generation" security systems, including those with the latest sandbox appliances, firewalls, and IPS. Unlike those other technologies, **GTMailPlus.ATP** defeats the most advanced and evasive malware.

Sophisticated malware can determine whether it is on an actual user's device, or inside an environment like a sandbox, or a virtual machine instance. Once it detects these environments it alters its behaviour and avoids detection. Deep content inspection can remain hidden while determining which malicious objects are capable of evasion techniques and then provide the appropriate input to analyse the complete range of malicious behaviour.
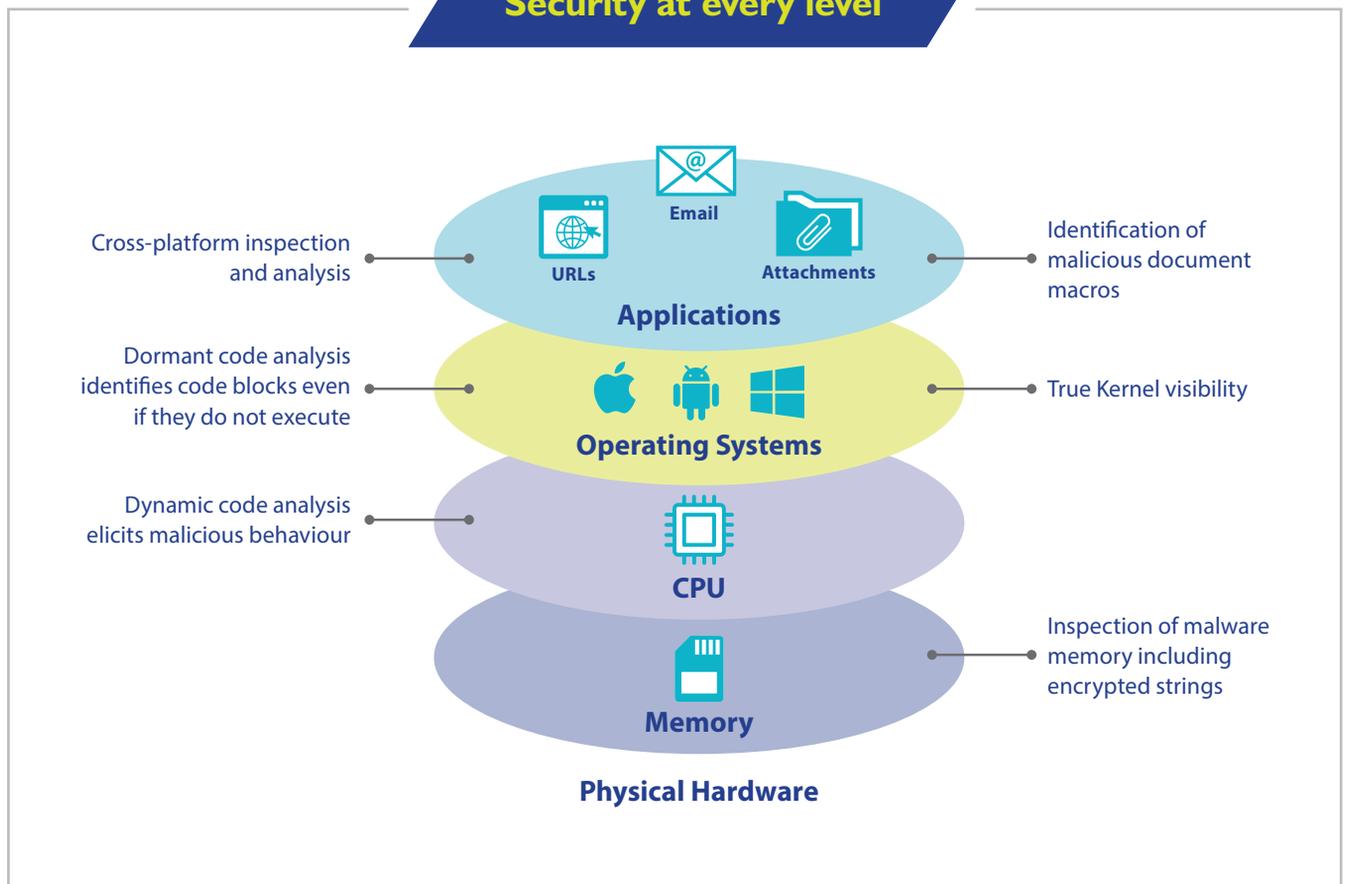
GTMARITIME
SECURING ESSENTIAL COMMUNICATIONS

**Learn more about ATP.
Speak to our sales team today.**

E: sales@gtmaritime.com T: +44 (0) 1925 818918

✔ **Deep content inspection** - designed to provide complete visibility into malware behaviour while remaining hidden

✔ **Zero download or administration** - a fully managed service controlled and operated by GTMaritime

✔ **Global threat intelligence network** - automatically shares with all ATP partners the malware behaviours and indicators of compromise of every malicious object that ATP has curated and analysed

✔ **Complete system emulation** - an all-encompassing intelligent environment

✔ **Unmatched accuracy** - delivered 100% threat detection in 2017 NSS Labs' Breach Detection Systems group test for the second year in a row, outperforming every other vendor

✔ **Behaviour based** - can observe 100% of the actions that a malicious object might take, even when those actions are delegated to the operating system or other programs

✔ **Detects zero day exploits** - unlike antivirus signature based tools which require testing and analysis after infection

Security at every level

Cross-platform inspection and analysis

Identification of malicious document macros

Email

URLs   **Attachments**

Applications

Dormant code analysis identifies code blocks even if they do not execute

True Kernel visibility

Operating Systems

Dynamic code analysis elicits malicious behaviour

CPU

Inspection of malware memory including encrypted strings

Memory

Physical Hardware

GTMARITIME
SECURING ESSENTIAL COMMUNICATIONS

**Learn more about ATP.
Speak to our sales team today.**

E: sales@gtmaritime.com **T:** +44 (0) 1925 818918