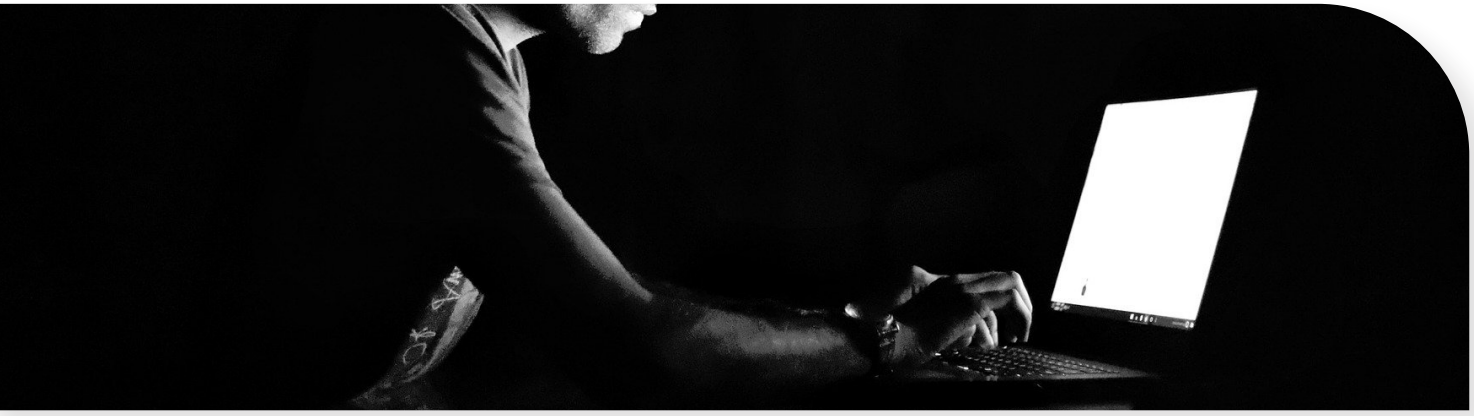
Tailor Made TECHNOLOGIES IT & Communications

Managed Cyber Security

TMT's range of managed cybersecurity packages provides organisations of all sizes 360-degree prevention and response against global cyberthreats and data breaches, providing peace of mind that your organisation is secure, and business assets are protected.



MANAGED SECURITY PACKAGES

CyberSTART - CyberSTART gives businesses a high level of protection against the most common cyber threats, to protect and identify security issues within the IT estate. CyberSTART is the entry package for SME customers.

CyberACTIVE - CyberACTIVE is a full defence in-depth cyber solution tailored for SME customers. CyberACTIVE utilises the latest industry-leading security technologies to deliver a high level of protection against cybercrime.

CyberCOVER - Designed as the entry package for mid-market organisations, CyberCOVER provides protection and response to cybercrime with sophisticated tools to both upskill employees and aid the prevention of cybercrime.

CyberPRO - Specially formed for mid-market organisations, CyberPRO helps enforce security policies to infrastructure with intelligent external threat awareness that utilises our industry-leading external vulnerability scanning technology.

CyberENTERPRISE - Our most comprehensive TMT package utilises state-of-the-art proactive security monitoring technology (SIEM), which is trusted by the world's leading companies and financial organisations. CyberENTERPRISE gives businesses a holistic, comprehensive protection against cybercrime by leveraging intelligent behaviour analytics, proactive SIEM monitoring, and external vulnerability scanning, to protect from both inside and outside the business.

FEATURES

Antivirus - Protects your user's computer or laptop against web viruses.

Patch Management - Our advanced patching fixes security vulnerabilities with Microsoft technologies including Windows, Exchange, and SQL Servers. Also, we extend this protection to critical network and infrastructure appliances and devices such as Routers, Switches, and WiFi Access points.

Email Protection - Intelligent email protection protects against known and many unknown security threats in real-time, including many commonly known phishing attacks, impersonation, and spear-phishing attempts. Users of the system share information about threats autonomously, blocking malicious material before it is known to be harmful.

Web Protection - Advanced Web Protection is installed on every desktop or laptop device owned by your organisation and prevents users from visiting known suspected websites and following links sent to them in phishing attacks.

Phishing & Cyber Awareness Training - TMT cyber experts trigger nonharmful real-world phishing campaigns against your employees every month to expose areas for training and improvement. We also deliver training on modules such as good password hygiene, Password Managers, Data Privacy and Data Protection, and the use of public Wi-Fi and Social Media.

Next-Gen Antivirus and EDR - Our Next-Generation Antivirus and EDR use behavioural data to determine if a user device on your network is a threat and then take action to block and contain it from causing harm.

Proactive Security Monitoring (SIEM) - Using corporate "blue chip" security for the SME Market Proactive Security Monitoring gives businesses a powerful real-time analysis of security alerts, enabling organisations to discover trends, and detect multiple types of threats.

Behaviour Analytics (UEBA) - Our SIEM platform leverages UEBA technology that enables us to detect and alert on suspicious user and device behaviour. Our machine learning UEBA solution baselines normal user behaviour that enables the detection of abnormal behaviour.

Internal Cyber Scan - Provides detail on possible insider threat by tagging high-risk servers and users by using internal network probes that alert if unauthorised logins occur on restricted machines or tagged user logs in outside of typical hours.

External Vulnerability Scan - External risk assessment on all internet-facing assets to identify if any external system has missing patches, thus exposing vulnerabilities. All issues are assigned a risk level as per industry standards (common vulnerabilities and exposures).

Dark Web Scanning - Dark Web scanning monitors the criminal underworld and retrieves information about the business, and its users, who have compromised credentials or personal information In a third-party data breach.