

# CyberENTERPRISE

CyberENTERPRISE gives businesses a holistic and fully featured protection against many types of Cybercrime. We leverage intelligent behaviour analytics, next generation security monitoring and external vulnerability scanning to protect your organisation from cyber threats, both inside and outside the IT estate.



## What is CyberENTERPRISE?

**Our fully managed service works in harmony with your existing infrastructure to deliver unparalleled visibility across all environments, whether it is on-premises or in the cloud.**

By using the latest threat intelligence your organisation has the advantage to react to emerging threats efficiently and with ease, helping to keep even the most complex IT estates protected from cyber criminals.

Proactive services such as patch management, email and web monitoring, vulnerability assessments, phishing services and AI based behavioural analytics all help to keep your business protected while reducing the attack surface, making it even more difficult for cyber criminals to get the advantage.

## What does it do?

1. Protects all laptop and desktop devices against viruses, including many next generation viruses.
2. Ensures network and infrastructure devices are secure with the latest security patches.
3. Protects the corporate network from many malicious emails with automated learning.
4. Prevents users from being able to access harmful material online through the adoption of an appropriate web filtering policy.
5. Delivers monthly campaigns to test your employees against phishing attacks and educates them if they potentially expose your organisation to cybercrime.
6. Provides your business with Next-Generation Antivirus & EDR (Endpoint Detection and Response) enabling the detection and isolation of many suspicious endpoint activities.
7. Scans the external network based on IP addresses to determine any known vulnerabilities.
8. Scans the Dark Web for compromised corporate assets, such as passwords and personal user details.
9. Utilises next generation SIEM technology to provide real time analysis of security alerts, enabling organisations to discover trends and detect threats.
10. Utilises AI Behaviour Analytics technology to monitor suspicious or unusual user activity on your IT estate.

## INCLUDED IN THE PACKAGE

**Patch Management** - Our advanced patching fixes security vulnerabilities with Microsoft technologies including Windows, Exchange and SQL Servers.

**Email protection** - Intelligent email protection protects against known, and unknown, security threats in real time, including many commonly known phishing attacks, impersonation and spear-phishing attempts.

**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 use of public Wi-Fi and Social Media.

**Next-Gen Antivirus and EDR** - Our Next-Generation Antivirus and EDR uses behavioural data to determine if a user device on your network is a threat and then takes 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 give businesses a powerful real-time analysis of security alerts, enabling organisations to discover trends, and detect multiple types of threats.

**Behaviour Analytics (UEBA)** - Analyse user and machine activity to generate a baseline of activity so that alerts can be generated when usage is outside of the baseline, such as unusual logging in hours or locations.

**External vulnerability scan** - External risk assessment on all internet facing assets to identify if any external system has missing patches, thus exposing vulnerabilities.

**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.

**Access to the TMT SOC** - TMT's cyber experts who deliver the service are available to your organisation to handle any incidents that arise.