Total Endpoint Security and Compliance

With flexible working becoming the norm within many organisations, you need to ensure a high level of cyber security protection and monitoring across all your endpoints. With Total Endpoint Security and Compliance from Complete I.T., you have peace of mind that your endpoints are monitored and secure no matter where your teams are working.

Cyber threats are evolving rapidly with cyber criminals adapting to the new ways we are working. From Phishing emails to Malware, we are seeing criminals take advantage of the fact we are not all in the office and cannot turn to our colleague or IT team for advice or to confirm an email or link is safe.

Cyber-attacks are not limited to large enterprises, the same methods are used to attack SME's where business downtime, fines and reputational damage can, at worst, lead to business closure.

With Total Endpoint Security and Compliance your business devices are protected and monitored 24/7 with malicious activity detected before malware is deployed.

cit Complete I.T.

The Components and Benefits

Threat Detection and Remediation

Our EDR (Endpoint, Detect & Response) works by using AI to monitor endpoint and network events, reviewing behaviours and recording the information in a central database so further analysis, detection, investigation, reporting, and alerting can take place.

Many thousands of virus and malware attack variants including zero day and cryptomining attacks recognised quickly as well as the root causes of these malicious behaviours by quickly identifying and diagnosing corrupt source processes and system settings.

In addition, the EDR can provide both Network and Device control allowing your business to restrict defined applications from running, restricting the use of removable storage ensuring you're further improving your data security.

Security Operations Centre (SOC)

Monitoring is a key component and needs a human element to analyse threats when they're identified. With a Security Operations Center (SOC) monitoring your endpoint alerts 24/7, you can focus on your core business knowing your systems are safe and action will be taken should any suspicious activity be detected.

Malicious behaviour is detected, stopped and quarantined to protect your systems. A member of the SOC will then investigate the threat and take the appropriate action.

Threat Coverage

Using the latest behavioural and AI based technology, any suspicious activity is picked up in real time, regardless of where your endpoints are (office, home, airport, café, hotel, etc.).

Terms Explained

How does an EDR differ to anti-virus?

Traditional Anti-virus, scans, detects and removes, where EDR tracks, monitors, and analyses data on endpoints to enhance the fortification of your environment.

What is a SOC?

A SOC (Security Operations Centre) is a team of information security specialists who are responsible for monitoring and analysing security posture and security information.

What is a Zero Day Attack?

A zero day attack is an unknown security vulnerability that cyber criminals will leverage to gain access to systems and data these attacks will not be picked up by anti-virus alone.