daisy.

ENDPOINT DETECTION & RESPONSE (EDR)

Cyber Security

PREVENT, DETECT AND RESPOND TO ADVANCED THREATS WITH ENDPOINT DETECTION & RESPONSE

The endpoint is the last line of defence and the most commonly exploited device in your network. With more people working from home than ever before, endpoint security is now far more critical and challenging, with a sharp increase in threats targeting end-users.

In addition, the threats facing cloud deployments are complex and require advanced Endpoint Detection & Response (EDR) solutions which utilise machine learning and behavioural analysis to identify and prevent zero-day attacks.

By partnering with leading EDR providers, Daisy can deliver the most appropriate protection to meet your business requirements including proactive management by the experts within our Security Operations Centre (SOC).

What is EDR?

According to Gartner, EDR solutions record and store endpoint-system-level behaviours, use various data analytics techniques to detect suspicious system behaviour, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems. They deliver four primary capabilities:

- Detect security incidents
- Contain the incident at the endpoint
- Investigate security incidents
- Provide remediation guidance

Four great reasons to deploy EDR

1. **Detect threats quicker and more accurately**
2. **Gain greater visibility**
3. **Reduce alert fatigue**
4. **Decrease incident response costs**

daisy.

Microsoft Partner
Microsoft

Gold Security
Gold Cloud Platform
Gold Windows and Devices
Gold Cloud Productivity
Gold Enterprise Mobility Management

ENDPOINT DETECTION & RESPONSE (EDR)

Find out more about Endpoint Detection & Response (EDR), speak to one of our sales specialists today:

enquiry@daisyuk.tech

0344 863 3000

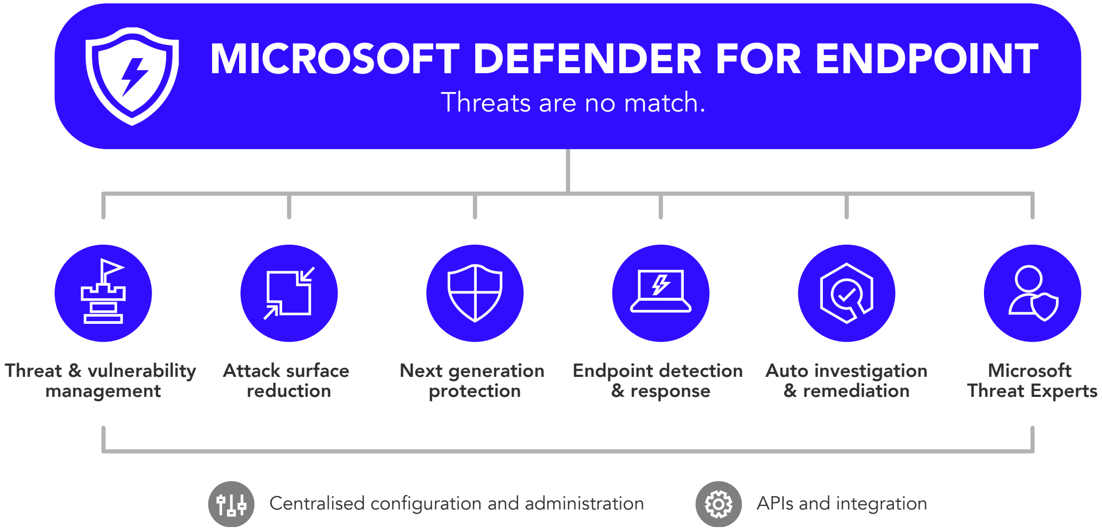
Microsoft Defender for Endpoint

Daisy have partnered with Microsoft to offer their Defender for Endpoint EDR solution. Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprises prevent, detect, investigate, and respond to advanced threats. Defender for Endpoint provides advanced threat protection that includes antivirus, antimalware, ransomware mitigation, and more, together with centralised management and reporting.

Daisy Managed Service

Daisy can provide a range of management options, from co-managed to fully managed to suit our customers. Our fully managed solutions include:

- Antivirus Compliance Management - Ensure devices are protected with the latest update signatures and configuration with a weekly review to check updates have been successfully deployed to the estate
- Vulnerability Management - Report on device compliance and vulnerable devices and react to detected vulnerabilities with a Critical or High CVSS score and propose resolutions
- Security Incident Management - Actively respond to security incidents in an automated and manual fashion to prevent, isolate, mitigate and remediate cyber attacks
- Reactive technical support, review meetings, configuration audits, and monthly reporting



MICROSOFT DEFENDER FOR ENDPOINT

Threats are no match.

Threat & vulnerability management

Attack surface reduction

Next generation protection

Endpoint detection & response

Auto investigation & remediation

Microsoft Threat Experts

Centralised configuration and administration

APIs and integration

Why Daisy?

- Daisy has a 25-year track record of delivering managed security services
- End-to-end expertise: securing data centre to device across cloud, connectivity and communications
- Skills and expertise: from our UK-based 24x7 Security Operations Centre (SOC)

Have you thought about…?

Cyber Security

Vulnerability Management – identify, categorise and prioritise the remediation or mitigation of vulnerabilities across your entire infrastructure

Modern Workplace

Microsoft 365 Management – support, optimise and secure your Microsoft 365 environment