Managed Endpoint Security Microsoft

Discover how you can get complete endpoint protection.

Cyber-criminals are getting smarter.

With evolving methods to threaten networks and endpoint devices, businesses are becoming more concerned about staying safe.

Our managed endpoint security solution addresses the threats posed by cyber-attacks. We do this by constantly monitoring activity at the endpoint through our SOC and applying necessary security policies. You can trust us to keep your business safe. We've partnered with Microsoft, a leading provider of endpoint solutions to deliver our Managed Service.

This secures all of your connected devices with Defender for Endpoint installed – from laptops to servers – and the network they all work on against cyber-threats. And evolve as they do.

Get complete control and visibility of your endpoints, wherever they are. So you can block suspicious traffic and spot malware and cyberattacks before they threaten your network. And our dedicated experts have a wealth of security knowledge and experience to give you the support you need, 24/7.

As a cloud-based solution, Microsoft Defender for Endpoint requires no on-site infrastructure. This means we can deploy the service across thousands of endpoints within hours, wherever they are. It's also fully-scalable, without any costly upgrades.

Integrated Microsoft licensing

If you're already a Microsoft E5 license holder, then Defender for Endpoint access will already be included in your package, so you don't need to worry about extra licensing costs.

The technology

We'll protect your endpoints from cyber threats by detecting advanced attacks and data breaches, prioritising your security incidents, and improving your overall security system.

But what technology does it actually include?

Endpoint behavioural sensors

Embedded in Windows 10 and Microsoft Monitoring Agent (MMA). These sensors collect and process behavioural signals from the operating system and send data to your private, isolated, cloud instance of Microsoft Defender for Endpoint.

Cloud Security Analytics

Microsoft's big-data, device-learning technology – that spans cloud products and online assets – detects threats and recommends responses in advance. So you're always prepared.

Threat Intelligence

This lets your Managed Endpoint Security Microsoft solution identify attacker tools, techniques, and procedures and instantly send alerts.

As it's built into Windows 10 and up, and Windows Server 2019, no agents are needed to be installed.

These sensors collect and process behavioural signals from the operating system and send the data to your private cloud (on MS Azure).

Key Features

Next generation protection

Microsoft Defender Antivirus brings together machine learning, big-data analysis, in-depth threat resistance research, and the Microsoft cloud infrastructure to protect your devices to the highest standard.

Key features include:

- Behaviour monitoring
- Cloud-based protection
- Machine learning
- URL Protection
- Automated sandbox service.

Endpoint detection and response

Detect and react to threats in real-time. When a threat is detected, alerts are created in the system for one of our analysts to investigate. Alerts with the same attack techniques or attributed to the same attacker are aggregated into an entity called an 'incident'. This allows our analysts to collectively investigate and respond to your security threats.

Key features include:

- Alerts
- Historical endpoint data
- Response orchestration
- Forensic collection
- Threat intelligence
- Advanced detonation and analysis service
- Advanced hunting.

Automated investigation and remediation

Automatically investigates alerts and defends against complex threats to significantly reduce the volume of alerts that must be investigated by your IT team. Depending on how it's set up, the automated investigation will either need user approval or automatically fix threats.

Attack surface reduction

The first line of endpoint defence in the stack. By making sure settings are adjusted properly and applying these techniques to stop hackers from exploiting weaknesses in your system, you can resist cyberattacks.

Key features include:

- Hardware-based isolation
- Application control and device control
- Exploit protection
- Network protection, web protection
- Controlled folder access
- Network firewall
- Attack surface reduction rules.

Threat and vulnerability management

Built-in technology that uses sensors to find device vulnerabilities in real-time. You can also set whether it prioritises vulnerabilities based on the threat level, sensitive information on your devices and your business context.

Microsoft threat experts

Managed threat hunting provides proactive hunting, prioritization, and additional context and insights from experts to identify and respond to threats quickly and accurately. You get targeted attack notification and access to Microsoft experts on demand. Only available for MS3 customers.

Why work with us?

Protection of your endpoints has become ever-more more important with the increase in remote working and the BYOD to work methods. So it's crucial that you're not only protecting your endpoints, but that you're also prepared with the best technology, people, and skills to protect against the evolving threat landscape.

React fast to cyber security incidents

Because we own a large amount of the network, we have a ringside seat. Which means we see what security incidents are happening on the UK network, before they happen to you. We're a team of more than 3,000 security experts who can identify security risks, neutralise them in real-time and protect you against them. The same people who protect our business, can protect yours too.

Managed Endpoint Security

Our managed service is an unrivalled set of features that take care of securing your business, so you can focus on what you do best. With three tiers to select from, you can choose the service that's right for you.

What could Managed Endpoint Security do for you?

Visit bt.com/corporate-security

Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

May 2021