wavenet

EBOOK

Microsoft Defender For Business Endpoint Protection

Prevent, detect, investigate, and respond to advanced threats before they impact your business.

Microsoft

Elevate your security

Security remains one of the biggest concerns and most challenging responsibilities facing businesses today. With a rise in cyberattacks targeting small and medium-sized businesses, threats are becoming increasingly automated and indiscriminate, and striking at a significantly higher rate. In the last year, the industry has seen a 300% increase in ransomware attacks with over 50% reaching small businesses.

Microsoft Defender for Business is specially built to bring enterprise-grade endpoint security to businesses with up to 300 employees, in a solution that is easy-to-use and cost-effective.

Many Windows users will already be familiar with the Microsoft Defender brand, where Microsoft Defender Antivirus (formerly Windows Defender) was preinstalled in all modern versions of the operating system. Microsoft Defender for Business belongs to the same family of apps but is designed to offer protection above and beyond traditional antivirus, such as automated protection and response for up to 300 users within your organisation.

Elevate your security with Microsoft Defender for Business

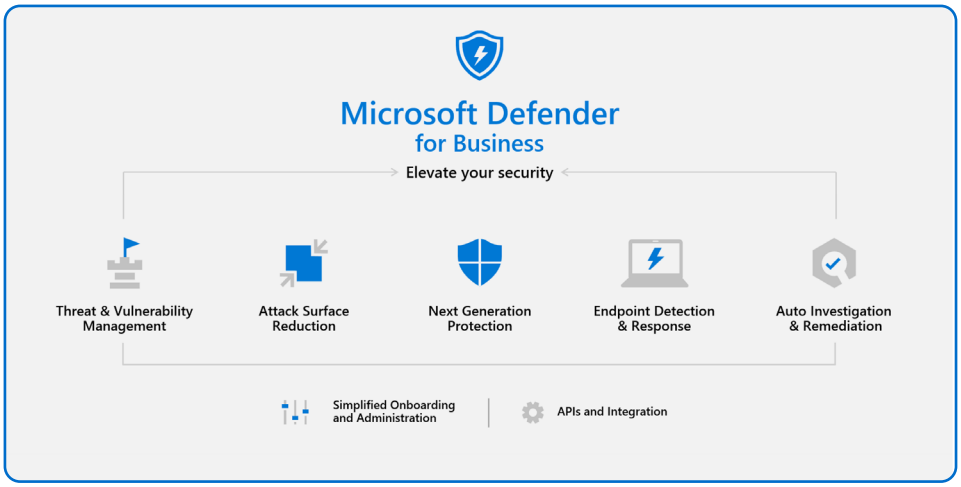
Today's top security threats are extortion or disruption from ransomware. Your business needs increased protection from these and other threats at an affordable price, so you can have peace of mind.

Defender for Business elevates security from traditional antivirus to next-generation protection, endpoint detection and response, threat, and vulnerability management, and more. It offers simplified configuration and management with intelligent, automated investigation and remediation.

Defender for Business helps you to protect against cybersecurity threats including malware and ransomware across Windows, macOS, iOS, and Android devices.

Enterprise-grade Endpoint Security

Microsoft have delivered the capabilities from Microsoft Defender for Endpoint solution and have optimised them for businesses with up to 300 employees.

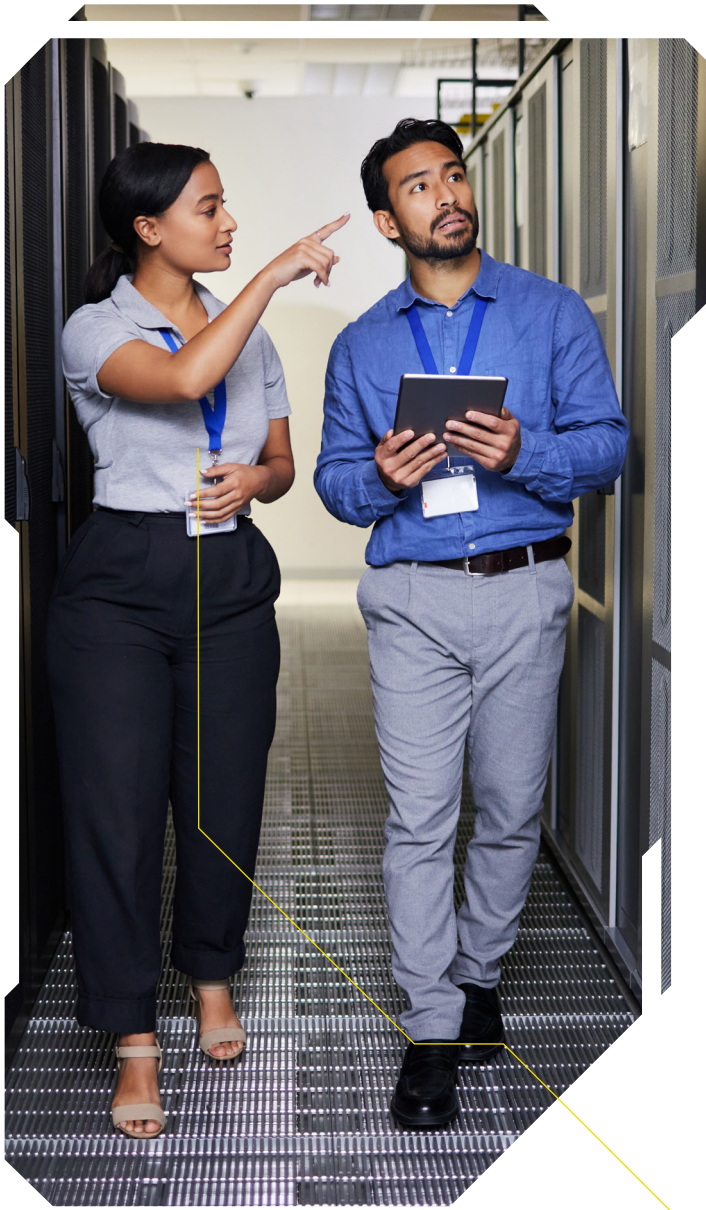


Defender for Business includes the following capabilities:

- **Threat and vulnerability management:** Helps you to prioritise and focus on the weaknesses that pose the most urgent and the highest risk to your business. By discovering, prioritising, and remediating software vulnerabilities and misconfigurations you can proactively build a secure foundation for your environment.
- **Attack surface reduction:** Reduces your attack surface (places that your company is vulnerable to a cyberattacks) across your devices and applications using capabilities such as ransomware mitigation, application control, web protection, network protection, network firewall, and attack surface reduction rules.
- **Next-generation protection:** Helps to prevent and protect against threats at your front door with antimalware and antivirus protection, on your devices and in the cloud.
- **Endpoint detection and response (EDR):** Provides behavioral-based detection and response alerts allowing you to identify persistent threats and remove them from your environment. Manual response actions within Defender for Business will allow you to act on processes and files, while live response will put you in direct control of a device to help ensure it's remediated, secured, and ready to go.
- **Automated investigation and remediation:** Helps to scale your security operations by examining alerts and taking immediate action to resolve attacks for you. By reducing alert volume and remediating threats, Defender for Business allows you to prioritize tasks and focus on more sophisticated threats.
- **APIs and integration:** Enables you to automate workflows and integrate security data into your existing security platforms and reporting tools. For example, you can pull detections from Defender for Business into your security information and event management tool.

Servers

Defender for Business Servers is an add on that provides security for Windows and Linux Servers within Microsoft Defender for Business, delivering the same level of protection for both endpoints and servers within a single admin experience inside of Defender for Business, helping you to protect all your endpoints in one location.



Microsoft Windows Servers

Manage Windows clients and servers with the same simplified security administration experience when using Windows Server 2012R2 and later. Recommended security settings are activated out-of-the-box, and wizard-driven antivirus and firewall policies are available. You can onboard servers using local scripts, Group Policy, or with Configuration Manager.

Linux servers

Linux servers use deployment scripts allowing you to manually onboard or integrate into an existing management platform such as Chef, Puppet, and Ansible, to onboard your servers.

Wavenet Managed Service

Operating from Wavenet's CyberGuard Security Operations Centre (SOC), our highly skilled team of security experts take responsibility for the implementation, configuration, and monitoring of our customers' environments, detecting, and investigating incidents and alerts in line with our priority-based SLA system.

The following is included in the service:

- Triage and Investigation of alerts from the supported technologies and platforms.
- Carry out response actions based on alert investigation findings i.e., isolation of devices, removal of malicious files etc.
- Continual development and maintenance of the supported technologies to provide the highest level of protection against the latest and emerging threats whilst considering the requirements of the business.
- Ongoing development and implementation of detection analytics across the technologies used, to defend against threats appropriate to the organisations threat landscape.
- All alerts investigated and followed up within our defined priority-based SLAs.

Priority	Time to first response	Time to resolution
Critical	15 minutes	1 hour
High	15 minutes	2 hours
Medium	1 hour	4 hours
Low	4 hours	24 hours

Licensing

Microsoft Defender for Business is available as part of the Microsoft 365 Business Premium Plan or as a standalone product.

There's an upper limit of 300 users but each user can have up to 5 devices. Therefore, you can install protection on up to 1500 appliances.

To protect servers, you will need a separate license, Microsoft Defender for Business Servers, which is an add-on to the main plan. A license will be required for each server instance and is available for both Microsoft Windows Server and Linux.

WAVENET.CO.UK

0333 234 0011

Wavenet Limited
One Central Boulevard
Blythe Valley Park
Solihull, West Midlands
B90 8BG

cyberguard@wavenet.co.uk

wavenet

Networking & Connectivity

Unified Communications & Voice

Contact Centres

Mobile Solutions & IoT

IT, Cloud & Technology

Network Intelligence

Cyberguard