White paper

Effective protection in all phases of a cyber attack with Microsoft 365 Defender

www.globalknowledge.com
info@globalknowledge.co.uk
0118 912 1929

Introduction

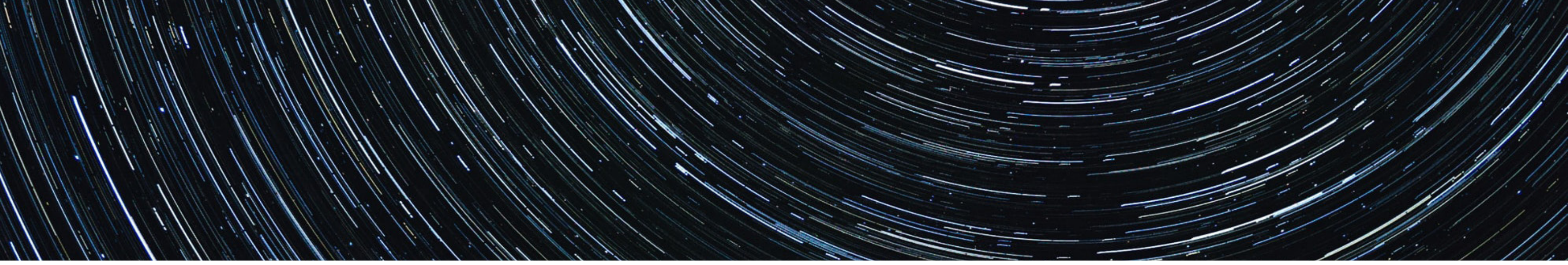
Change is a constant in the never-ending arms race between hackers and cybersecurity experts. Attacks have become more complex, common and creative, posing new challenges and requiring better tools to tackle familiar and newly emerging threats.

While the specifics of individual attacks can vary, it is possible to identify certain patterns and phases that apply to most cyber attacks. They generally follow the following stages:

- **The reconnaissance phase.** The attacker identifies a vulnerable target and figures out how to exploit it.
- **The weaponisation phase.** The hacker uses the previously gathered information to find and create ways that allow him/her to get into the target's network. Spear phishing mails or whaling attacks are prime examples.
- **The delivery phase.** Phishing mails are sent and/or 'watering hole' web pages are posted on the internet.
- In **the exploitation phase**, the attacker starts to reap the rewards of his/her attack by attaining passwords and usernames and infiltrating deeper into the network and IT infrastructure of the victim.
- In **the installation phase**, the attacker ensures continued access to the network. This phase is usually quickly followed by **the command and control phase**, in which the hacker gets unrestricted access to the entire network and administrator accounts.
- **The action on objectives phase** involves the theft of data or the targeting of a company's operations—for example, by blocking access to devices, applications and data through the instalment of ransomware.

Effectively protecting your IT infrastructure and operations during these phases, calls for security solutions that ensure you recognise each stage. Furthermore, the security solution should give you the opportunity to act upon these different threats. Microsoft 365 Defender does just that. Read on to find out more about 365 Defender and why you need it.

Table of contents



What is Microsoft 365 Defender, and why do you need it?

Microsoft 365 Defender is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate and respond to advanced threats. Microsoft 365 Defender, part of Microsoft's XDR solution, leverages the Microsoft 365 security portfolio to automatically analyse threat data across different domains, building a complete picture of each attack in a single dashboard.

365 Defender consists of four components that protect all the elements of your IT landscape.

1. **Identities.** Manage and secure hybrid identities and simplify employee, partner and customer access.
2. **Endpoints.** Microsoft Defender for Endpoints combines preventive and post-breach protection, automated response and response for endpoints to secure and safeguard all of your devices.
3. Microsoft Defender for **Cloud Apps** gives you full control over your data and allows you to detect threats across cloud services and apps. This gives you the opportunity to stop attackers from getting beyond the reconnaissance phase.
4. Secure your **email, documents and collaboration tools** with Microsoft Defender for Office 365.

Built-in AI functionalities allow 365 Defender to prevent attackers from accessing your organisation's IT infrastructure and stop attacks before they happen. This allows you to stop them from reaching the delivery and exploitation phases. By understanding the attacks and context across domains it eliminates lie-in-wait and persistent threats, but also protects your network and endpoints against current and future breaches.

Additionally, Microsoft 365 Defender allows you to view prioritised incidents in a single dashboard to reduce confusion, clutter and alert fatigue. The automated investigation capabilities of 365 Defender ensure you spend less time on detection and response and focus your efforts on triaging critical alerts, and responding to threats.

Other important features of Microsoft 365 Defender are:

- **Advanced hunting**. This feature provides a query-based threat-hunting tool that lets you proactively find breaches and create custom detections.
- Microsoft Secure Score for Devices. This functionality helps you dynamically assess the security state of your enterprise network and identify unprotected systems. It also recommends actions to improve the overall security of your organisation.

"Built-in AI functionalities prevent attackers from accessing your organisation's IT infrastructure."

What can Microsoft 365 Defender do for you?

Microsoft 365 Defender comes with a lot of security and business benefits. Have you ever found yourself frustrated by the plethora of consoles required to manage cloud security? Microsoft 365 Defender unites all your essential security functionalities and tools under one umbrella solution. This allows for effective protection in all phases of a cyber attack on one platform and in one single environment.

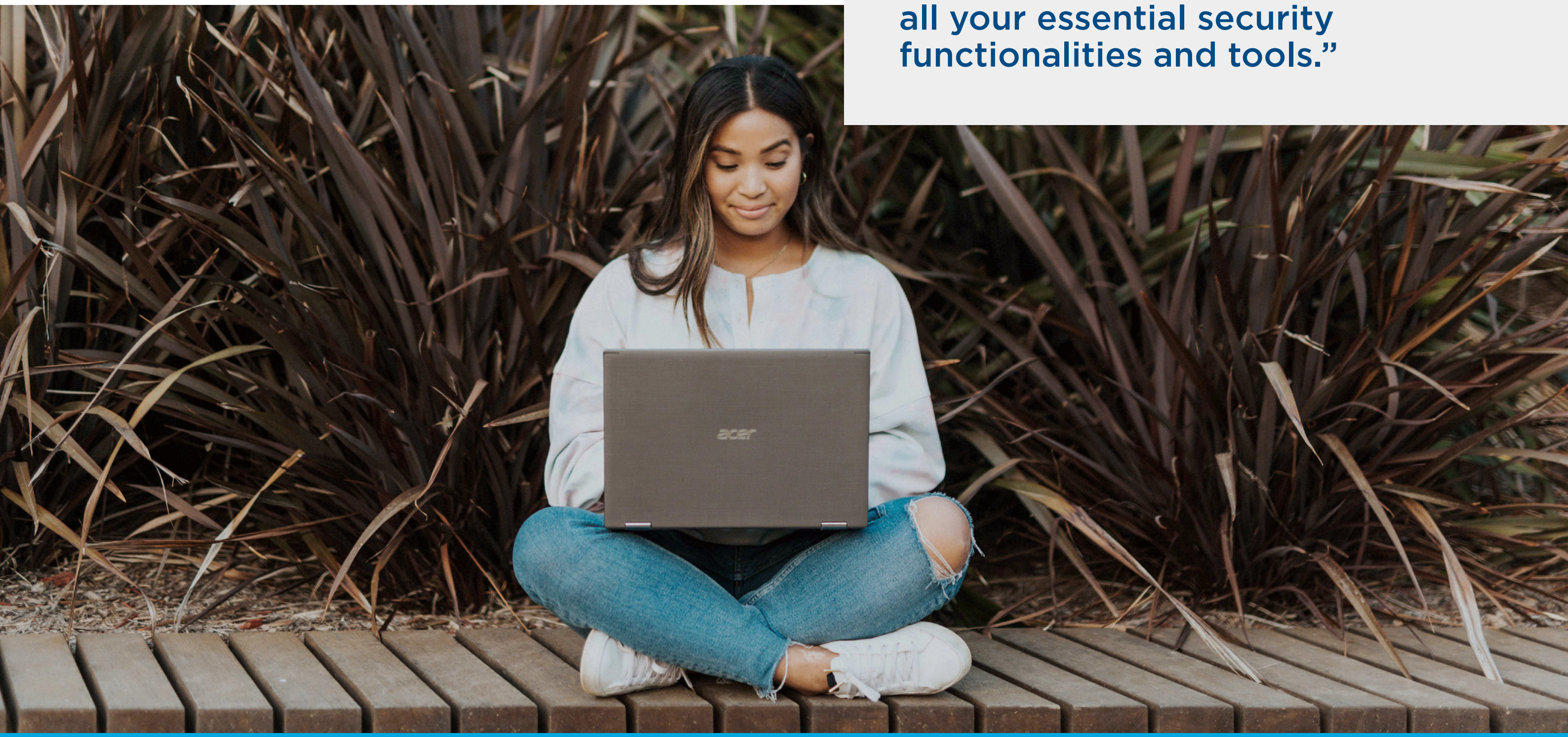
Such a unified view reduces the time analysts spend switching between various security products as part of an investigation; meaning your security experts can spend their time on active remediation and less time pulling information from multiple tools. Because 365 Defender also collects data from the individual apps and pieces them together into a combined incident queue, the analyst can get the full scope of an attack in real time.

Furthermore, 365 Defender is easy to integrate with Azure Sentinel, an advanced two-in-one SIEM and SOAR security solution. This gives you an even more comprehensive security overview without the need to develop any custom data connectors. If you integrate with Sentinel, 365 Defender can be a 'one-stop shop' for advanced security solutions.

Learn how to use Microsoft 365 Defender

The Global Knowledge course **Microsoft Security Operations Analyst** teaches you everything that you need to know about Microsoft 365 Defender and the broader Microsoft security ecosystem. In this course, you will learn how to mitigate threats in all phases of a cyber attack using Microsoft 365 Defender, Azure Sentinel and Azure Defender. The course is tailor-made for people who work in a security operations job role and helps participants prepare for the exam SC-200: Microsoft Security Operations Analyst.

> **"Microsoft 365 Defender unites all your essential security functionalities and tools."**



More information

Would you like to find out more about Microsoft 365 Defender and an all-encompassing security approach that effectively targets all the different phases of a cyber attack? Then be sure to **contact us** by sending an email to **info@globalknowledge.co.uk** or calling 0118 912 1929 for more information or book the course Microsoft Security Operations Analyst.

CONTACT US

www.globalknowledge.com
info@globalknowledge.co.uk
0118 912 1929