Microsoft SOC service

Complete Microsoft security protection for your business

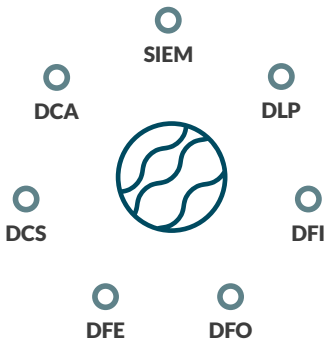
Technology advises, humans decide

Our Security Operations Centre (SOC) solutions deliver unbeatable protection for your business universe through a powerful combination of human and machine. Pairing Microsoft's Sentinel SIEM and Defender technologies with nearly two decades of cyber security experience, we draw upon information from state-of-the-art tools and enhance it with expert intelligence and analysis. Through this blend we deliver optimum results – identifying and solving security challenges with speed and efficiency.

The Microsoft SOC service is a premium-level SOC, offering you a bespoke service that delivers proactive cyber threat hunting, analysis, and remediation in real-time.

Microsoft SOC

7 protections



Included in this SOC

- Sentinel SIEM (Security Information and Event Management)
- Purview (DLP)
- Defender for Cloud (DCS)
- Defender for Cloud Apps (DCA)
- Defender for Identity (DFI)
- Defender for Office 365 (DFO)
- Defender for Endpoints (DFE)
- Threat Intelligence (GTIN)
- i3 case management including SOAR

Experts on watch

Our managed services provide peace of mind, with a dedicated SOC team on watch 24 hours a day, 365 days a year.

A handpicked selection of security analysts, threat hunters and cyber security engineers combine their expertise to interpret technology insights and action defensive measures on your behalf.

Is the Microsoft SOC the right SOC for me?

The Microsoft SOC is the ultimate solution for Microsoft-invested businesses looking for complete, enterprise-level cyber security protection. Tailored to your specific needs, this SOC provides robust protection against cyber security breaches, whether they are caused by external attackers or insiders threats. Our suite of leading defensive technologies is configured to strengthen your defences in three important ways:

- **Proactive defence** – Prevention is better than cure. Our cyber threat intelligence system provides advanced warning of cyber threats targeting your organisation or sector. Coupled with vulnerability management, we stay one step ahead of attacks by hardening your organisational defences.

- **Reactive defence: automated** – The first wall of defence. Industry-leading security tools protect your users and systems in real-time by automatically blocking network and malware threats, and preventing data theft and exfiltration attempts.

- **Reactive defence: incident response playbooks** – Enhanced threat response. Going one step further than automated tools alone, our analysts interpret insight from threat hunting technology to seek out indicators of compromise in your networks and trigger best-practice incident response processes.

In depth: Microsoft SOC benefits

- Rapid remote deployment of monitoring and protection software through cloud management.
- Key Risk Indicator and security maturity improvements delivered within 4 weeks of SOC deployment.
- Protect key data, intellectual property and client data from theft and accidental leakage.
- Harden networks and systems to common network intrusion attacks and malware.
- Detect targeted and sophisticated network attacks.
- Help protect against zero-day malware.
- Reduce employee overhead and improve speed of response through automated defence and remediation.
- Protect data stores and keep business operations moving with real-time detection and prevention.
- Faster root-cause analysis via multiple security logs including network, firewall, server, active directory, database and cloud systems.
- Joined up overview of security incidents in the event of a breach – slashing the time it takes to respond.
- Flexibility to evolve your service using our 'Roll Out Roll In' SOC protections with non-Microsoft SOC services including anti-ransomware, vulnerability management and security assurance.

In depth: Microsoft protections

Technology

Technology plays a vital role in protecting your IT. Your Microsoft SOC service is underpinned by state-of-the-art security tools:

- **Microsoft Defender for Identity**
  - Detect compromised user accounts and insider threats facing your organisation.
  - Protect user identities and credentials stored in Active Directory.
  - Identify and investigate suspicious user activities and advanced attacks throughout the kill chain.
  - Clearly understand the attack timeline to rapidly respond to network intrusions.
- **Microsoft Purview**
  - Stops data exfiltration through policy and risk-based protection.
  - Enables real-time tracking of on premise and mobile users.
  - Scan data at rest on premise file servers, detect, classify and protect (encrypt) sensitive data.
  - Protect against file uploads to cloud storage, and together with Defender for Cloud Apps, gain visibility of sensitive data exported to cloud shares.
- **Microsoft Defender for Endpoint**
  - Protects against advanced malware and network threats through risk-based alerting.
  - Reveals threat actors who already have a foothold on your network.
  - Detects zero-day risks and advanced persistent threats.
- **Microsoft Defender for Office 365**
  - AI to detect malicious and suspicious content and correlate attack patterns to identify campaigns specifically designed to evade protection.
  - Detect and prevent a wide variety of volume-based and targeted attacks including business email compromise, credential phishing, ransomware, and advanced malware.
  - Extended protection beyond email to SharePoint, OneDrive, Office applications and Microsoft Teams.
- **Microsoft Defender for Cloud**
  - Proactive threat prevention, enhanced visibility and automated protection across cloud infrastructures.
  - Protects virtual servers, containers, databases, key vault and app services.
  - Detects misconfigurations, ensures compliance with standards, assesses cloud assets and automates remediation of risks.
- **Microsoft Defender for Cloud Apps**
  - Cloud Access Security Broker (CASB) solution that helps secure your cloud applications and services.
  - Gives visibility and protection for SaaS apps and other cloud resources across multiple environments.
  - Provides shadow IT discovery, SaaS security posture management and app governance.

- **Microsoft Sentinel SIEM**
  - Monitors all your network and cloud systems to provide a unified view of your security posture.
  - Enhances the capabilities of all your security tools by joining up data to provide a comprehensive picture.
  - Speeds up root-cause analysis and enhances key risk indicator reporting.
- **i3 Security Incident Management Portal**
  - Tracks security alerts and incidents through a centralised portal.
  - Contains security run books tailored to your needs.
  - Shows you the 'metrics that matter' through live security posture and risk indicator dashboards.
- **Global Threat Intelligence Network (GTIN)**
  - Uses a database of current threats, campaigns, botnets and malicious websites to seek out indicators of compromise.

People

Humans are critical to interpreting and acting on technology's advice, which is why they're a huge part of what we do for you. Your Microsoft SOC team includes:

- **Security Engineer:** Ensures your systems seamlessly integrate with ours so everything works as it should.
- **Security Analyst:** Your eyes and ears. Monitors, analyses and investigates your IT estate 24x7.
- **Security Delivery Manager:** Oversees every element of your service from internal response process to coordination of different teams.
- **Security Assurance Consultant:** Answers the difficult questions and provides valuable guidance that supports your decisions.
- **Threat Intelligence Specialist:** Looks beyond your perimeter to seek and stop cyber threats before they cause harm.
- **Threat Hunter:** Harnesses endpoint data response technologies to hunt down and quarantine suspicious internal threats.

Process

We dot the I's and cross the T's by ensuring best-practice processes are meticulously followed during the deployment of our managed security services:

- **On-going tuning of alert and defensive rule sets:**
  Ensures your security stays matched to your organisation as it evolves.
- **Early warning threat intelligence:**
  Shows you how to best-protect your business before an attack strikes.
- **Active threat hunting:**
  Detects sophisticated attackers and advanced persistent threats.
- **Monthly Key Risk Indicator reporting:**
  Summarises the risks we've uncovered and prevented, benchmarked against key performance indicators.
- **Incident orchestration:**
  Resolves and remediates incidents through collaboration with your in-house teams.

Protection overview: SIEM

What is it?

SIEM (Security Information and Event Management) brings together all your security technologies into a single pane of glass. Logs are correlated from operating systems, cloud systems and bespoke applications, providing you with a holistic overview of your security estate.

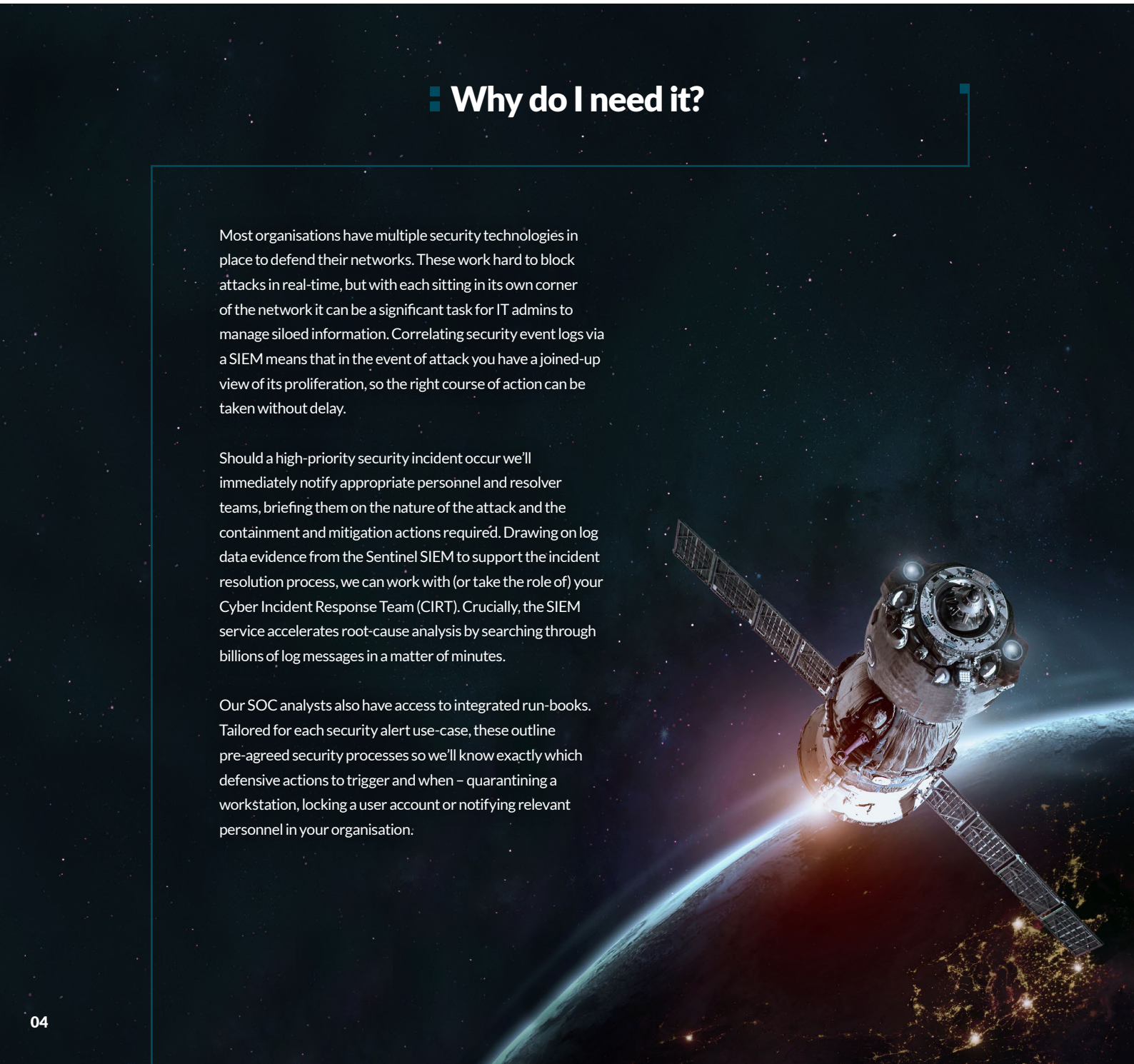
Alerts generated by the SIEM are sent to the i3 security incident management and response platform which is monitored by our expert SOC team in real-time. This enables them to quickly and effectively respond to alerts from multiple systems, all from one control centre.

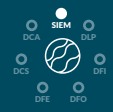
Why do I need it?

Most organisations have multiple security technologies in place to defend their networks. These work hard to block attacks in real-time, but with each sitting in its own corner of the network it can be a significant task for IT admins to manage siloed information. Correlating security event logs via a SIEM means that in the event of attack you have a joined-up view of its proliferation, so the right course of action can be taken without delay.

Should a high-priority security incident occur we'll immediately notify appropriate personnel and resolver teams, briefing them on the nature of the attack and the containment and mitigation actions required. Drawing on log data evidence from the Sentinel SIEM to support the incident resolution process, we can work with (or take the role of) your Cyber Incident Response Team (CIRT). Crucially, the SIEM service accelerates root-cause analysis by searching through billions of log messages in a matter of minutes.

Our SOC analysts also have access to integrated run-books. Tailored for each security alert use-case, these outline pre-agreed security processes so we'll know exactly which defensive actions to trigger and when – quarantining a workstation, locking a user account or notifying relevant personnel in your organisation.





SOC management

- **Alert use-cases** – Starting with a baseline security alerting ruleset, we evolve this over time to implement new alerts as required.
- **Fully managed service** – Our SOC analysts monitor your security alerts 24/7 and can supply ad-hoc reporting upon request.
- **Evolving service** – We continually adapt our monitoring and alerting methods to match the ever-changing threat landscape. Our SOC team are up-to-date with the latest threat trends and keep watch for new techniques, tactics and procedures being deployed by cyber attackers.
- **Bespoke Integrations** – We work with your custom business applications, rather than relying on pre-existing modules to integrate data feeds.

Reporting

- **Key Risk Indicator reports (KRI)** – Weekly or monthly KRI reports provide a full picture of your security monitoring service. These highlight the most important risks, whilst providing insight into recent threats and the steps taken to defend against them.
- **Key Performance Indicators (KPI)** – We benchmark our performance by tracking incident response and resolution times.
- **i3 access** – All customers have access to our i3 incident management portal, granting real-time visibility into how our analysts are investigating and responding to security incidents.
- **Flexible alert notifications** – When our analysts identify a threat, they'll notify you via your chosen method – through email, in the i3 portal, by telephone or through integrations with other incident management platforms.

Protection overview: Purview

What is it?

Microsoft Purview inspects and analyses all the data that is being accessed or transferred within your network. This could be between devices in your organisation, or externally.

Purview policies can be configured to trigger alerts or preventative actions based on:

- The type of information being transferred (e.g. credit card numbers, personal information, data classification markings).
- The source of the information (e.g. sensitive systems, specific end user devices).
- Who is performing the activity (e.g. members of the finance department, Active Directory groups, users who are soon to leave the organisation).
- The destination of the data (e.g. unauthorised email services, file sharing services, instant messenger services).

Why do I need it?

Purview provides protection against data leaks and data theft while offering the ability to classify and protect data.

With a client-server architecture, the agent software runs on user devices no matter their location whilst policies are managed centrally by the SOC. This means that both office-based and remote users are always protected with up-to-date policies, which are synchronised within seconds.

SOC management

- **Policy control** – Quickly and easily apply changes to your Purview policies via request to our SOC team – giving you full control without the need to train in-house teams in the technology.
- **Fully managed service** – Our SOC analysts monitor your security alerts 24/7 and can supply ad-hoc reporting upon request.
- **Custom policy building** – We work with you to build a set of policies that matches your organisation's needs and covers industry best practice.

Additional DLP features

- **Content aware protection** – Monitor and control data in motion, deciding which confidential files are permitted to leave the company. Filters can be set by file type, application, content, Regex and more.
- **Enforced encryption** – Automatically secure data by encrypting files and emails.
- **eDiscovery** – Scan data at rest on premise file servers, detect, classify and protect (encrypt) sensitive data.
- **Detect upload to cloud shares** – Protect against file uploads to cloud storage, and together with Defender for Cloud Apps, gain visibility of sensitive data exported to cloud shares.

Protection overview: Defender for Identity

What is it?

Our Microsoft Defender for Identity service supports the detection of advanced attacks on your networks. Defender for Identity leverages your on-premises Active Directory signals to identify, detect and investigate advanced threats, compromised identities, and malicious insider actions directed at your organisation.

Defender for Identity monitors and analyses user activities and information across your network, such as permissions and group membership, creating a behavioural baseline for each user. Defender for Identity then identifies anomalies with adaptive built-in intelligence, giving you insights into suspicious activities and events, revealing the advanced threats, compromised users and insider threats facing your organisation. Defender for Identity's proprietary sensors monitor organisational domain controllers, providing a comprehensive view for all user activities from every device.

Why do I need it?

Using Defender for Identity we are able to:

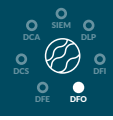
- Detect compromised user accounts and insider threats facing your organisation.
- Protect user identities and credentials stored in Active Directory.
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain.
- Clearly understand the attack timeline to rapidly respond to network intrusions.

SOC management

- **Real-time monitoring and investigation** – Real-time investigation of detected threats, closing out false positives and ensuring appropriate automated defensive actions are taken including triggering manual host quarantine when needed.
- **Advanced incident analytics** – Includes malware sandboxing and analysis of zero-day malware threats.
- **Cyber threat intelligence** – Correlate with indicators of compromise stored in our threat intelligence system (GTIN).

Additional DFI features

- **Reconnaissance** – Identify rogue users and attackers' attempts to gain information about user names, group membership, IP addresses assigned to devices, resources and more, using a variety of methods.
- **Compromised credentials** – Identify attempts to compromise user credentials using brute force attacks, failed authentications, user group membership changes and other methods.
- **Lateral movements** – Detect attempts to move laterally inside the network to gain further control of sensitive users, utilising methods such as Pass the Ticket, Pass the Hash, Overpass the Hash and more.
- **Domain dominance** – Highlighting attacker behaviour if domain dominance is achieved, through remote code execution on the domain controller, and methods such as DC Shadow, malicious domain controller replication, Golden Ticket activities and more.
- **Investigate alerts and user activities** – Defender for Identity attack timeline allows us to leverage the intelligence of smart analytics and quickly investigate threats, and gain insights across the organization for users, devices, and network resources. Seamless integration with Microsoft Defender for Endpoint provides another layer of enhanced security by additional detection and protection against advanced persistent threats on the operating system.



Protection overview: Defender for Office 365

What is it?

Our Defender for Office 365 service uses industry-leading AI to detect malicious and suspicious content and correlate attack patterns to identify campaigns specifically designed to evade protection. Detecting and preventing a wide variety of volume-based and targeted attacks including business email compromise, credential phishing, ransomware and advanced malware.

Defender for Office 365 uses a layered defence-in-depth approach that analyses and protects against threats from the point at which an email is received by Office 365 to when it is delivered.

Why do I need it?

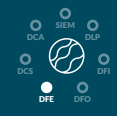
While email remains the primary attack vector, it is no longer the only way individuals collaborate at work. Beyond email, it is important to ensure protections extend to malware infected content and suspicious links across the digital estate. Defender for Office 365 uniquely extends protections beyond email to SharePoint, OneDrive, Office applications and Microsoft Teams. If malicious files or links are uploaded or shared, our protection layers will detect it, block it, and contain the threat by preventing the file from being opened or shared in the future.

SOC management

- **Real-time monitoring and investigation** – Real-time investigation of detected email threats, closing out false positives and ensuring appropriate defensive actions are taken such as locking compromised email accounts and deleting phishing email.
- **Advanced incident analytics** – Includes malware sandboxing and analysis of zero-day malware threats.
- **Cyber threat intelligence** – Correlate with indicators of compromise stored in our threat intelligence system (GTIN).
- **Annual phishing simulations testing** – Perform both non targeted and targeted phishing simulations to your user base and key stakeholders (finance team, HR team, C-Level) to test their ability to detect and report phishing emails. Report on findings to enable training to be directed to the users most in need.

Additional DFO features

- **Edge protection** – Detect and block malicious emails at the network edge through network throttling, domain reputation checks, backscatter detection, directory based edge filtering.
- **Sender intelligence** – Detect sender account compromise, DMARC/DKIM/SPF/ARC checks, domain impersonation, cross domain intelligence spoofing, mailbox and user intelligence spoofing.
- **Content filtering** – Review message contents in real time using heuristics, machine learning, AV engine, linked content and URL detonation.
- **Post delivery protection** – Includes replacing malicious links with safe links, end user reporting, malware and phishing zero-hour auto purge.



Protection overview: Defender for Endpoint - MDR

What is it?

Our Microsoft Defender for Endpoint - MDR (Managed Detection and Response) service delivers real-time detection and prevention of advanced network threats and malware. Using a combination of machine learning, signature detection and threat intelligence, MDR will identify anomalous activity on endpoint systems and will automatically block and quarantine high risk events. Low risk events are also flagged to the SOC team for further investigation.

Why do I need it?

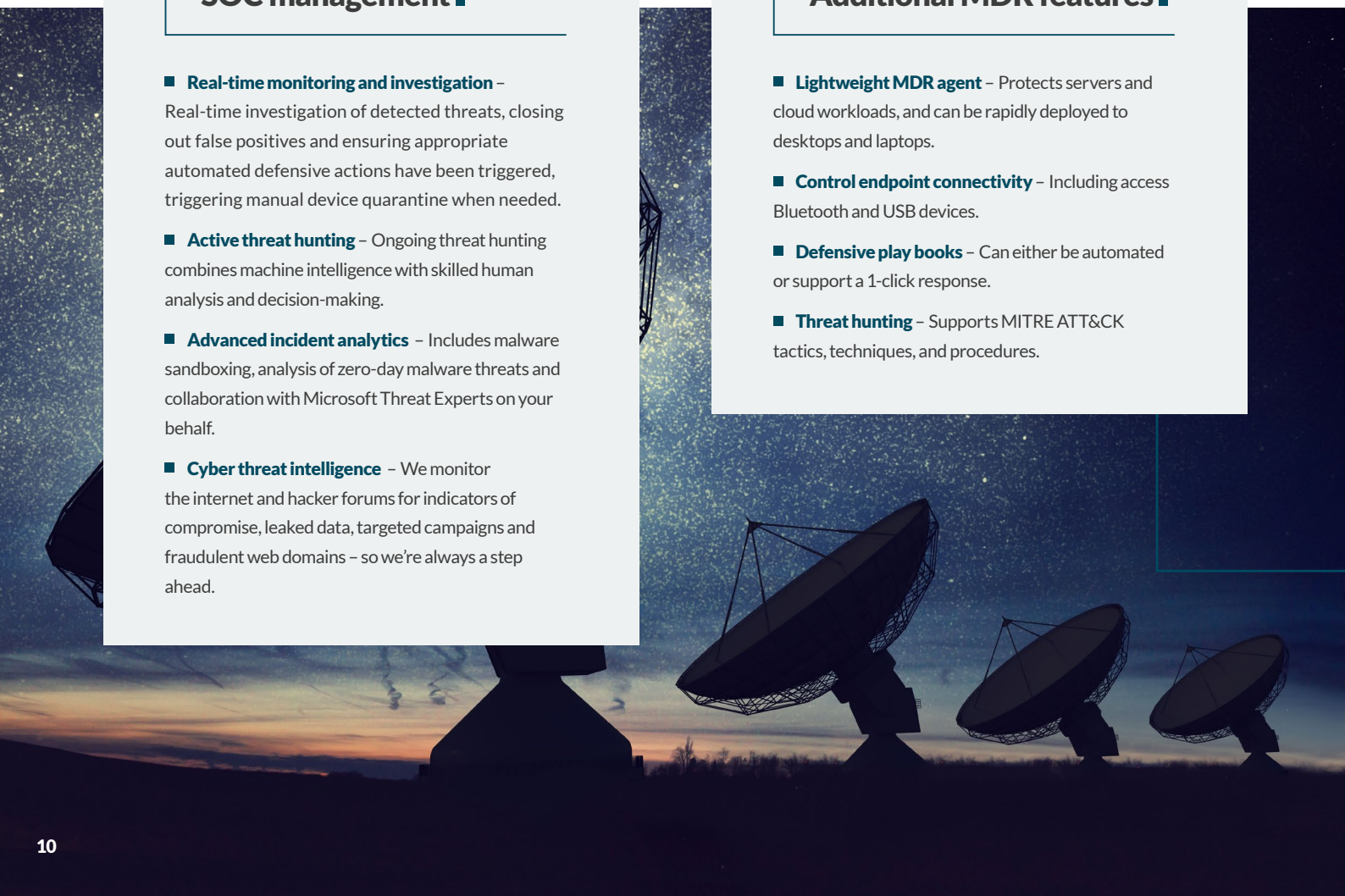
MDR goes beyond even the best of anti-virus products. Rather than defending only against known threats, MDR allows a SOC team to actively hunt for zero-day cyber attacks and Advanced Persistent Threats. MDR is the ideal technology for organisations who are concerned about advanced threats and malware - it ensures that attackers can't gain a foothold on your networks.

SOC management

- **Real-time monitoring and investigation** – Real-time investigation of detected threats, closing out false positives and ensuring appropriate automated defensive actions have been triggered, triggering manual device quarantine when needed.
- **Active threat hunting** – Ongoing threat hunting combines machine intelligence with skilled human analysis and decision-making.
- **Advanced incident analytics** – Includes malware sandboxing, analysis of zero-day malware threats and collaboration with Microsoft Threat Experts on your behalf.
- **Cyber threat intelligence** – We monitor the internet and hacker forums for indicators of compromise, leaked data, targeted campaigns and fraudulent web domains – so we're always a step ahead.

Additional MDR features

- **Lightweight MDR agent** – Protects servers and cloud workloads, and can be rapidly deployed to desktops and laptops.
- **Control endpoint connectivity** – Including access Bluetooth and USB devices.
- **Defensive play books** – Can either be automated or support a 1-click response.
- **Threat hunting** – Supports MITRE ATT&CK tactics, techniques, and procedures.



Protection overview: Defender for Cloud

What is it?

Our Defender for Cloud service continuously assesses your cloud resources for misconfigurations, compliance gaps and emerging threats. By combining security posture management and cloud workload protection, it allows you to prevent, detect and respond to risks in real time.

Why do I need it?

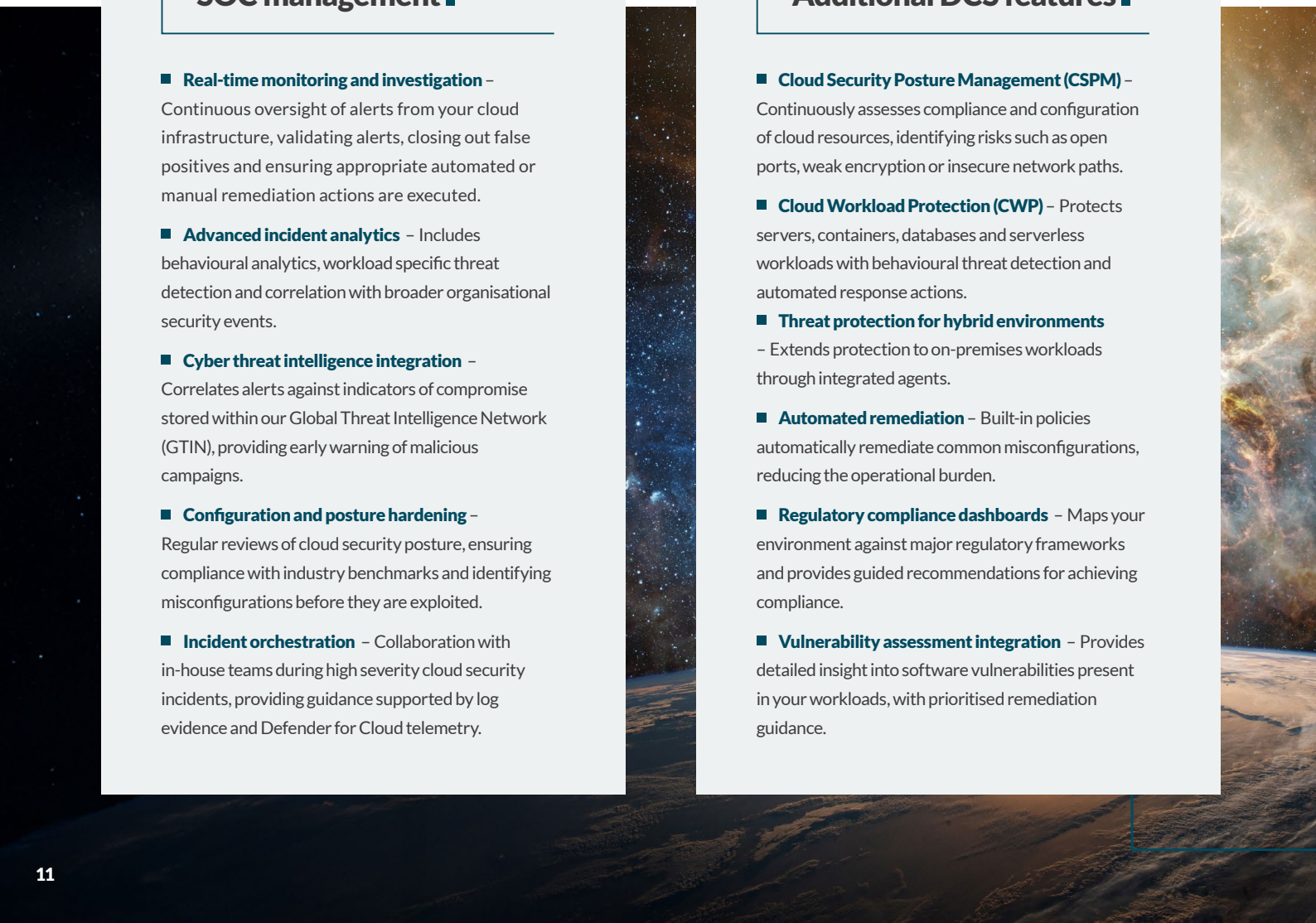
Defender for Cloud supports the defence of your cloud environment, ensuring your business is able to function in the cloud without additional risk. Integrated alerts and analytics ensure that advanced threats are identified early, while automated remediation accelerates containment and reduces the window of exposure.

SOC management

- **Real-time monitoring and investigation** – Continuous oversight of alerts from your cloud infrastructure, validating alerts, closing out false positives and ensuring appropriate automated or manual remediation actions are executed.
- **Advanced incident analytics** – Includes behavioural analytics, workload specific threat detection and correlation with broader organisational security events.
- **Cyber threat intelligence integration** – Correlates alerts against indicators of compromise stored within our Global Threat Intelligence Network (GTIN), providing early warning of malicious campaigns.
- **Configuration and posture hardening** – Regular reviews of cloud security posture, ensuring compliance with industry benchmarks and identifying misconfigurations before they are exploited.
- **Incident orchestration** – Collaboration with in-house teams during high severity cloud security incidents, providing guidance supported by log evidence and Defender for Cloud telemetry.

Additional DCS features

- **Cloud Security Posture Management (CSPM)** – Continuously assesses compliance and configuration of cloud resources, identifying risks such as open ports, weak encryption or insecure network paths.
- **Cloud Workload Protection (CWP)** – Protects servers, containers, databases and serverless workloads with behavioural threat detection and automated response actions.
- **Threat protection for hybrid environments** – Extends protection to on-premises workloads through integrated agents.
- **Automated remediation** – Built-in policies automatically remediate common misconfigurations, reducing the operational burden.
- **Regulatory compliance dashboards** – Maps your environment against major regulatory frameworks and provides guided recommendations for achieving compliance.
- **Vulnerability assessment integration** – Provides detailed insight into software vulnerabilities present in your workloads, with prioritised remediation guidance.



Protection overview: Defender for Cloud Apps

What is it?

Our Defender for Cloud Apps service enables organisations to detect the risky usage of SaaS applications, enforce governance policies and identify anomalous behaviour in real time, helping to identify shadow IT and reduce the associated risks.

Why do I need it?

By integrating directly with Microsoft 365, third party SaaS platforms and underlying cloud services, Defender for Cloud Apps provides deep insight into how your cloud resources are used. It also ensures that your sensitive data remains protected wherever it travels, especially when used in third-party SaaS applications outside of your Microsoft estate.

SOC management

- **Real-time monitoring and investigation** – Continuous analysis of cloud app activity, validating alerts and ensuring appropriate governance actions are executed.
- **Anomaly detection and incident analysis** – Identifies suspicious behaviour such as impossible travel, unusual download patterns, mass file deletions or risky OAuth app permissions.
- **Shadow IT discovery** – Identifies the unsanctioned cloud apps used across your organisation and evaluates their risk profile using integrated threat intelligence.
- **Cyber threat intelligence correlation** – Alerts are cross referenced with GTIN indicators to detect malicious cloud-based behaviours or compromised applications.
- **Policy governance support** – Our SOC team helps define and tune access, session and data governance policies to reflect your operational and compliance needs.

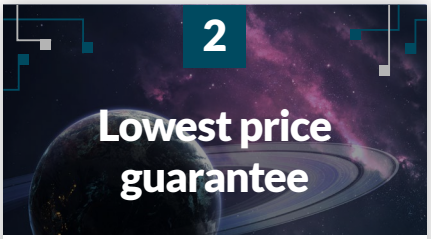
Additional DCA features

- **SaaS Security Posture Management (SSPM)** – Evaluates and improves the security posture of your connected SaaS applications.
- **App Governance** – Detects risky or malicious behaviour from OAuth based apps with elevated permissions.
- **Conditional access app control** – Enforces real time session controls, such as blocking downloads, restricting uploads or monitoring sessions for sensitive content.
- **Data protection policies** – Protects against data leakage by enforcing DLP policies across cloud applications.
- **Risk based access control** – Automatically adjusts access policies for users exhibiting unusual or high-risk behaviour.
- **Comprehensive cloud usage analytics** – Provides visibility into user activity, failed logins, API usage and connected apps across your cloud estate.

Our customer pledge

We want you to be completely satisfied with your SOC service – our promise to you:

Put us to the test and let us run your 24x7 Security Operations for free for the first 3 months. You can benchmark our performance against pre-agreed success criteria – and if you're not convinced after the pilot, it won't cost you a penny.



Our mission is to make high-quality, tailored managed security services affordable to the mid-market – and we stand by our word. If you find another provider who can offer a like-for-like SOC service for lower cost, we will refund the difference.

When you take part in our pilot you can expect the full Zepko service, not a trimmed down version. We'll run a full 24x7 SOC operation, providing access to our specialist SOC team, process models and procedures, at the same level as our existing customers.

Take the next step

Found the right SOC for you? Get in touch with us to start your 3-month pilot or for more information about our services.

+44 (0) 845 074 0790 | **info@zepko.com**

Get in touch

zepko