



Endpoint as a Service

Microsoft Intune

G-Cloud 15

Service Description



Service Description

Endpoint as a Service | Assure 365

This Schedule forms part of Schedule 3 to the Agreement between Customer and Provider and sets out a description of the Services, Service Levels and Service Credits in relation to the Endpoint as a Service module from Assure 365 as given on a Service Order.

1. Additional Definitions

The following definitions apply in this Schedule:

Assure 365: Assure 365, or A365, is a collection of modular managed services designed to enable Customers to outsource their cybersecurity and IT operations. Each module taken be taken as a standalone service or packaged within in a bundle of services. Some examples of modules include SOC as a Service, Identity as a Service, Data Security as a Service.

Microsoft Intune: Microsoft Intune is a cloud-based endpoint management solution able to manage user access to devices and applications, including laptops, mobile devices, tablets, and virtual endpoints.

BAU: Business as usual is the normal operation of typical and routine tasks or functions within an organisation, for example in relation to ensuring the smooth daily operation of an Identity and Access Management (IAM) platform.

2. Additional Commercial Terms Relating to Endpoint as a Service

N/A

3. Additional Commercial Obligations Relating to Endpoint as a Service

3.1 The Customer will retain an active Microsoft Intune tenant alongside Intune for the duration of the Service.

3.2 The Customer will retain valid Intune licenses such as M365 Business Premium, Intune P1, or Intune P2.

3.3 The Customer will be responsible for any costs relating to the acquisition and ongoing subscription of M365, or other, Microsoft licenses required to enable the Provider to provide the Service.

3.4 The Customer will provide the Provider with the appropriate level of access to enable the provision of the full breadth and depth of the service, including onboarding and ongoing management, the expected level of access required is the 'Global Administrator' Entra ID role.

4. Endpoint as a Service

4.1 The Endpoint as a Service module from Assure 365 leverages the Microsoft Intune endpoint management solution to provide a fully outsourced Endpoint-led security and operations managed service to configure and maintain the Customers Intune environment in a secure manner.

4.2 Onboarding - Endpoint as a Service:

4.2.1 The Provider will issue a project plan outlining the high-level technical steps necessary to complete the onboarding of the service.

4.2.2 The Customer will review and agree to the issued project plan.

4.2.3 The Customer will grant appropriate access to the Provider.

4.2.4 The Provider will deliver a standardised onboarding in which security policies and configuration of Microsoft Intune will be assessed, and if appropriate, hardened to align with best practice configuration. Including device-based conditional access integration and maintenance.

4.2.5 The Provider will deploy necessary line-of-business applications supported by Microsoft Intune, for example Microsoft 365 and Teams.

4.3 Ongoing - Endpoint as a Service:

4.3.1 Maintenance of security policies and configuration, and continued alignment to established best practice. Any requests by the Customer to deviate from a recommended best practice will require business justification from the Customer and may be challenged by the Provider

4.3.2 24 x 7 x 365 operation of device lifecycle inclusive of provisioning and deprovisioning devices or external parties such as contractors and vendors.

4.3.3 24 x 7 x 365 auditing of Microsoft Intune audit logs to monitor for unusual user or administrative behaviour such as the enrollment of a new device or the modification of an Intune policy.

4.3.4 24 x 7 x 365 operation of BAU endpoint tasks such as remotely wiping data, provisioning and deprovisioning, and blocking or unblocking of at-risk devices.

4.3.5 Creation, ongoing maintenance, and deployment of device builds for all user stories.

4.3.6 Quarterly review of device security policy configuration to ensure alignment to Zero Trust principles. The Provider will review this configuration four times yearly.

4.3.7 Weekly scheduled patch management of Windows updates, including testing patches via pilot devices before wider deployment.

4.3.8 Retirement or forced-upgrade of devices that have reached end of life (EOL) or end of support (EOS). The provider will adhere to Microsoft's published EOL and EOS and will inform the Customer of any applicable dates once yearly. It should be noted that EOL and EOS are dictated by Microsoft and must be adhered to.

4.3.9 Ongoing security-first management of at-risk device types such as bring your own device ("BYOD") or shared devices. The Provider anticipates that non-typical devices such as BYOD or shared devices may require a modified set of security policies to appropriately secure the devices and that these devices may be temporarily required by the Customer.

4.3.10 Advice provided to Customer to harden their systems to prevent Security Incidents where potential vulnerabilities or lack of best practice by Customer have been identified by the Provider during operation of Microsoft Intune.

4.3.11 Mobile Application Management (MAM) for all applications supported by Microsoft Intune.

4.3.12 Where applicable, the Provider will implement appropriate security policies, within agreed technology stacks, where the Provider deems it beneficial to the ongoing success of the Endpoint as a Service module.

4.3.13 Business Hours support for general Customer enquiries relevant to Microsoft Intune.

4.3.14 Intune maintenance such cleanup of unnecessary devices or similar redundant objects.

4.4 Unless otherwise expressly agreed, the following are not included in Endpoint as a Service:

4.4.1 Configuration and management of endpoint XDR or anti-virus platform or similar.

4.4.2 Configuration and management of non-Microsoft Intune endpoint management platforms.

4.4.3 Incident response actions for device-based attacks or threats.

4.4.4 Remedial/recovery work following a Security Incident.

5. Exclusions

5.1 Only the activities, deliverables, and responsibilities expressly detailed within this Service Description are included. Any service elements not specifically stated are excluded from the scope unless agreed in writing by both parties.

6. Service Levels

The Provider will respond according to the following Service Levels on Ticket Open and the priority levels assigned by the Provider.

Response Time (contractual)

	Priority Level	Target SLA	Expected Performance
Enhanced Hours 24x7x365	P1 – High	15 Mins	95%
	P2 – Medium	30 Mins	95%
Standard Business Hours	P3 – Moderate	1 Hour	95%
	P4 – Minor	2 Hours	95%

Triage Time (non-contractual)

	Priority Level	Target SLA	Expected Performance
Enhanced Hours 24x7x365	P1 – High	1 Hour	90%
	P2 – Medium	2 Hours	90%
Standard Business Hours	P3 – Moderate	8 Hours	90%
	P4 – Minor	24 Hours	90%

Monthly Response Time performance is calculated as follows:

For each Priority Level the performance for Response Time (“Actual Performance”) is calculated as:

Actual Performance = Number of incidents recorded for each Priority Level within SLA Target in any month / number of Incidents recorded for the Priority Level in total in any month * 100

This is then compared to the Expected Performance for each Priority Level given in the Response Time table above.

7. Service Credits

If the Actual Performance is less than the Expected Performance in any month for either of the P1 or P2 Priority Levels, Service Credits equivalent to (1) week's Charges for the Service shall be due to Customer such that maximum Service Credits of two weeks Charges for the Service may be payable in any month.

Service Credits cannot be obtained in relation to:

- Triage Time;
- In connection with P3 or P4 Priority Levels; and,
- During the first 3 months of the Service being live.

Endpoint as a Service

Device & App Deployment, Configuration and Management.
Strengthen Security and Enhance Compliance Across Your Organisation.

Powered by Microsoft Intune. Realised by CyberOne.

CyberOne's Managed Endpoint Service delivers comprehensive protection for devices and applications across your digital landscape. Built on Zero Trust principles and powered by Microsoft Intune, it provides a scalable approach to endpoint security, offering secure, resilient management with minimal overhead.

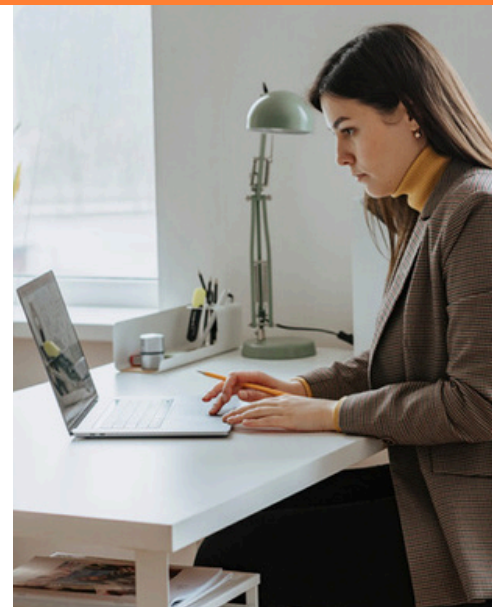
Part of CyberOne's Assure 365 suite, our fully outsourced Managed Microsoft Security solution offers modular cyber security services tailored to your needs. It delivers comprehensive, scalable protection to strengthen resilience and empower you to focus on your core business objectives.

What is Microsoft Intune?

Microsoft Intune is a leading endpoint management solution that protects devices, apps and data across diverse environments. Supporting both corporate and BYOD devices, Intune enforces essential security features like encryption, password protection and remote wipe, integrating with Microsoft Entra ID to align with Zero Trust principles.

Intune simplifies app management, enabling secure deployment, configuration and updates. Its Mobile Application Management (MAM) secures corporate data on personal devices through app-specific policies without full device enrollment.

CyberOne's Endpoint as a Service, powered by Intune, delivers a comprehensive solution for endpoint security, compliance and control. This enables organisations to support secure remote work, optimise device performance and maintain compliance with minimal overhead.



Key Features of CyberOne's Endpoint as a Service

CyberOne's comprehensive Managed Endpoint Service secures devices and applications, streamlines management and enforces security policies—reducing your organisation's risk and ensuring compliance across all endpoints.



Device & Mobile Management

Full lifecycle management for corporate and BYOD devices inc. enrollment and configuration.



Mobile Application Management (MAM)

App deployment, configuration and policy control for corporate and personal devices.



Security Policy Enforcement

Enforce device security policies and routinely review for compliance.



Device Compliance

Monitoring and enforcement of security standards to restrict non-compliant devices.



Conditional Access Integration

Apply and manage Zero Trust security policies to limit unauthorised device access.



Patch Management

Schedule automatic updates, test patches and monitor device update status.



Remote Wipe & Device Retirement

Remotely wipe compromised, lost or stolen devices.



End-of-Life Management

Safe retirement of devices including full decommissioning and wiping data securely.



Endpoint DLP

Restrict access to removal media such as USBs to mitigate data exfiltration.



Enhanced Visibility & Reporting

Insights into security, compliance and device health to identify risks and enhance protection.

Unlock Business Value with CyberOne

Enhanced Endpoint Security

24x7 protection with proactive threat detection, remote wipe and device compliance enforcement to reduce risks.

Scalable Compliance

Automate and maintain consistent policies across all devices, ensuring adherence to regulatory standards.

Simplified Device Control

Apply security controls to limit unauthorised access, enforcing policies for corporate and personal devices.

Secure Data Access

Enable controlled data access for remote users, ensuring secure collaboration without compromising security.

Actionable Insights

Gain insights into device health, compliance status and security posture to make informed, proactive decisions.

Operational Efficiency

Streamline device provisioning, updates and patching, reducing workloads through automated management.

Enhanced User Experience

Provide seamless, secure access to apps and resources, supporting remote and hybrid work without friction.

Reduced Risk

Align device security policies with organisational risk levels to prevent unauthorised access and data breaches.

Business Continuity

Ensure uninterrupted access to critical resources, supporting resilience and rapid recovery from disruptions.

Cost Savings

Minimise in-house security demands and reduce expenses associated with endpoint management and compliance.

Why Choose CyberOne's Endpoint as a Service?

Choosing CyberOne's Managed Endpoint Service gives your organisation the expertise, resilience and efficiency needed to secure devices, keep apps updated, protect data and ensure compliance with ease.

1. Expertise You Can Trust

CyberOne's certified Microsoft specialists optimise Intune for robust endpoint security, proactively addressing evolving threats and industry best practices.

2. Guaranteed Security Outcomes

An NCSC Assured Service Provider, CyberOne upholds high standards in security and compliance, ensuring sensitive data is safeguarded organisation-wide.

3. Proactive Threat Detection

With NCSC Cyber Incident Response Level 2 accreditation, CyberOne provides real-time 24x7 monitoring and rapid response to help your organisation adapt to emerging threats, ensuring endpoint resilience.

4. Streamlined Device Management

CyberOne simplifies device provisioning, updates and deprovisioning, enhancing productivity while reducing IT overhead.

5. Maximised Microsoft ROI

Fully leverage your Microsoft investment with CyberOne's certified expertise across Intune, Microsoft 365 and the wider Security suite.

6. Ongoing Monitoring & Reporting

Supported by our CREST-accredited SOC, CyberOne delivers comprehensive reporting for full visibility into device health, compliance, and security posture, empowering informed decision-making.

General Pricing Information

No sector-specific pricing applies. The quoted pricing information for this service applies equally across all client sectors.

All pricing information is quoted in pounds sterling (GBP) and prices are exclusive of VAT at the applicable rate (unless otherwise stated)

Resource-Based Pricing (Time & Materials)

Resource-based pricing is defined in the SFIA Rate Card for this service.

The SFIA Rate Card (available as a separate attachment, downloadable from the service web page) lists the options of day rates applicable to this service, for each SFIA grade, with the bold figure showing a typical average for a London based service delivery before any discounts are applied.

Buyers and suppliers will explore the relevant rates in clarification questions permitted as part of the buying process and agree as part of a Call-Off Contract.

Education Discounts

Additional discounts may apply to educational institutions across all charging models and will be negotiated during the purchasing stage.

Fixed Price Service Charge

Where applicable, services can be provided on a fixed price basis. For example, using an assumed number of resources at the agreed SFIA rate, with an agreed set of deliverables.

This approach enables accurate spend control and forecasting for customers and can be negotiated during the purchasing stage.

Volume / Combination Discounts

All prices are quoted without volume or combination discounts. Discounts may apply where the volume or work combination is appropriate, but will be subject to negotiation and agreement during the purchasing stage.

Pricing for Combined Services

If a client wishes to purchase several discrete G-Cloud 15 services as a single package, the total price will be the combination of the individual service line prices.

About CyberOne

CyberOne is a Microsoft Security Solution Partner and member of the Microsoft Intelligent Security Association (MISA). We deliver one of the UK's most advanced AI-augmented Managed eXtended Detection & Response (MXDR) services, recognised with Microsoft-verified Managed XDR solution status, enabling organisations to move with confidence from risk to resilience. Powered by Microsoft's market-leading security technologies and realised by CyberOne's accredited experts, we help businesses anticipate and contain modern threats so they can thrive.

With 24x7x365 Global SOC coverage, NCSC accredited Cyber Incident Response, CREST SOC and Penetration Testing accreditations and guaranteed SLAs, CyberOne combines Microsoft Security with expert consulting, professional and managed services to protect operations, achieve compliance and build lasting resilience.

Accreditations & Certifications

CyberOne's services are backed by the world's leading standards bodies including NCSC, CREST and ISO as well as our key technology partners, whilst our experts are backed by industry-leading certifications, cementing our role as leaders in cyber security.



✉ hello@cyberone.security

☎ +44 (0) 3452 757575

🌐 cyberone.security