ARC-IT Business Solutions Ltd
12 Gleneagles Court
Brighton Road
CRAWLEY
West Sussex
RH10 6AD

01444 817506
enquiries@aibs.co.uk
www.arcitbusinesssolutions.com

Arc Managed Endpoint Total Security Service Definition

1. Service Overview

Arc Managed Endpoint Total Security is a fully managed detection and advisory service providing continuous 24×7 monitoring across endpoints, Azure, Microsoft 365, network and firewalls. We identify threats such as ransomware, zero-day attacks, polymorphic malware and malicious network activity. Arc provides clear, actionable guidance. Remediation, containment and recovery are excluded.

2. Service Features (What's included)

1.1. Core Threat Detection and Analytics

- Behaviour-based ransomware detection.
- AI-driven next-generation malware protection and Anti-Virus.
- Managed Detection and Response (MDR) with threat intelligence to identify zero-day and polymorphic malware, aiming to stop threats before they harm your business.
- MITRE ATT&CK mapping of EDR/MDR/SOC alerts for clear context and faster triage.
- NIST Cybersecurity Framework–aligned operating model (Identify, Protect, Detect, Respond, Recover).

2.4. Endpoint Monitoring

- Event log monitoring for Windows and macOS.
- Malicious process and behaviour detection.
- Threat hunting and intrusion detection.
- Integration with third-party AV (Bitdefender, Cylance, Deep Instinct, SentinelOne, Sophos, Webroot, Windows Defender).
- You remain responsible for licensing any 3rd-party integrated tools.

2.5. Network and Firewall coverage

- Real-time firewall log analysis.
- DNS reputation and malicious connection alerts.
- Detection of C2 traffic, unauthorised services, lateral movement and privilege escalation.

2.6. Cloud Coverage

- Microsoft 365 security event monitoring and malicious login.
- Azure AD monitoring (sign-ins, risky users, conditional access policy drift).
- Integration with Azure logging services.

2.7. Security Operations Centre (SOC)

- 24x 7 continuous monitoring advanced threat detection.

- Real-time malicious activity detection.
- Early detection of indicators of compromise.
- EU-based SOC with UK service management.

2.8. Email and DNS Monitoring

- Monitoring of Microsoft 365, Barracuda, IRONSCALES, DNSFilter.
- Detection of phishing, spoofing and malicious resolution attempts

2.9. Service Management

- Structured onboarding.
- Quarterly service reviews.
- Optional access to customer portal.

2.10. Data handling and Retention

- Security events retained for 12 months.

2.11. Service Hours

- Monitoring is continuous 24×7.
- Arc service desk contact and standard communications and notifications are provided during Business Hours, defined as Mon–Fri, 09:00–17:30, excluding UK Bank Holidays

You may contact us by telephone during Business Hours on: -

+44 (0)1444 817506

or you may report an issue or make a request by emailing: -

SecurityDesk@aibs.co.uk

Optionally, you may request access to your own Arc-IT Web Support page, where you can submit and track the progress of your incident and request tickets.

3. Service Implementation (How we onboard you)

3.1. Initiation and Access

- Assign Arc Implementation Lead
- Confirm stakeholders and communications.
- Establish secure remote access, data sharing and permissions.

3.2. Design and Readiness

- Agree ingestion plan (endpoints, firewalls, Microsoft 365/Azure).

3.3. Deploy and Integrate

- Deploy agents and/or connect your existing EDR/AV tools.
- Connect log sources.

3.4. Tuning and Validation

- Suppression of false positives
- Stakeholder sign-off.

3.5. Go-live and Transition

- Switch to 24×7 monitoring.
- SLA metrics commence.

- Agree quarterly review cadence and KPI pack.

4. Customer Responsibilities and Dependencies

- Administrative access to endpoints, firewalls, Azure/M365 tenants and relevant security tools.
- Agreement to deploy required agents.
- If required, provide access to your existing AV/EDR platform.
- Syslog/API connectivity for network and firewall devices.
- Provide named contacts.
- Timely action and execution on Arc's advisory recommendations (we do not make changes on your behalf).
- Confirmation of accepted risk where our recommendations are declined by you.
- Maintain licensing for your chosen AV/EDR if our solution is not utilised.
- Maintain internet egress on TCP 443 for agent and log forwarding.
- Provide and maintain syslog/API connectivity for firewalls, networks and cloud services.
- Authorise any change window needed to enable data flows.

5. Exclusions

- The service does not include remediation, containment or recovery activities. You retain change control; we provide expert advice so you can act safely and quickly.
- User account, identity and access management security which is covered by Arc Managed User Total Security.
- Firewall rule changes, EDR policy changes, email security configuration changes. We advise, and you are responsible for the implementation.
- Vulnerability scanning, penetration testing, red teaming.
- On-site services, the service is delivered remotely.

6. Operational Service Levels and Targets

6.1. Service Levels

Severity	Impact	Description	Response Target	SLA KPI
Severity 1	Critical	Active compromise, ransomware, major breach indicators	2 hours	95% of all events/incidents responded to within target (measured on a quarterly basis)
Severity 2	Major	High-confidence malware, privilege escalation, lateral movement	4 hours	
Severity 3	Minor	Suspicious behaviour, isolated detections	1 business day	
Severity 4	Info	Low-risk or informational alerts	As scheduled	

Response = time from when Arc receives or generates an alert to when **initial advice** is provided to you.

6.2. Escalation

- The Customer may request that the severity of their event or incident be expedited by contacting the Customer Service Manager using the contact details in section 2.

6.3. Service Availability

- 99.9% availability for all SaaS components of the service

6.4. Reporting

The following KPI's will be reported to you on a quarterly basis:

- SLA response performance
- Mean Time to Detect
- Mean Time to Respond
- False positives
- Total monitored endpoint count

7. Technical Standards and Compliance

- Frameworks: NIST CSF operating model; MITRE ATT&CK mapping for detections and reporting.
- Data protection: UK GDPR compliant. We ingest security telemetry and metadata; we do not ingest business content.
- Locations: UK service management; SOC operations EU-based (Ireland and Poland).
- Retention: 12 months standard event retention
- Security of service delivery: MFA enforced for all Arc staff; least-privilege access; activities logged and auditable.