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 User Total Security Service Definition

1. Service Overview

Arc Managed User Total Security provides user-focused protection across Microsoft 365 combining anti-phishing, user security training, dark web monitoring, SaaS threat detection and SaaS backup into a single service. Automated response actions are available but only enabled with explicit customer approval during onboarding.

2. Service Features (What's included)

2.1 Prevent - Email Threat Protection

- Anti-phishing. AI-powered phishing defence blocks malicious emails in Microsoft 365 before they reach your end users, reducing exposure to potential threats. Blocks impersonation & ransomware along with intuitive user coaching to identify and block social engineering attacks.
- Internal Mail Protection. Account takeover protection with sender profiling & social graphing anomaly detection.
- Computer Vision. Renders every email and applies computer vision algorithms to see each email as the human recipient would. This helps identify brand impersonation attempts.
- QR Code Detection. AI scans and decodes QR codes to determine if the encoded URL is safe.
- Employee Shield creates a customer banner in emails where user can mark message as safe or not.

2.2 Prevent - User awareness and Training

- User awareness training delivered annually with quizzes, tracking and automated directory sync.
- User susceptibility testing including phishing simulations and automatic training for failures.

2.3 Prevent – Dark web monitoring

- Dark web monitoring for compromised credentials. Detects compromised credentials early, allowing for immediate action to prevent unauthorized access to sensitive data.

2.2 Respond (Cloud Detection and Response)

- SaaS event alerting for:
    - Suspicious logins.
    - Abnormal device activity.
    - Account compromise indicators.

    - OAuth app activity monitoring
    - Privileged account changes
    - MFA disable alerts
    - Mailbox rule manipulation
    - Shared file exposure
    - Insecure SaaS configuration detection
- Automated account lockdown, login blocking and threat response workflows, only after prior explicit customer agreement. These are disabled by default.
- Prevent logins from unusual work locations and unknown devices.
- User identity validation. Reconcile device data with SaaS data to ensure only authorized users on authorized devices can gain access to critical company SaaS applications
- 24×7 monitoring and detection.
- Notifications are sent to you during Business Hours, defined as Mon–Fri, 09:00–17:30, excluding UK Bank Holidays.

2.3 Recover (SaaS Backup)

- Automated point-in-time backups for Microsoft 365 up to 3× daily.
- Protection against accidental deletions, misconfigurations and cyberthreats.
- Independent backup storage outside of Microsoft 365/Azure.
- Flexible restore options including granular, point-in-time and non-destructive recovery.
- Recovery and protection of Microsoft Exchange, SharePoint, OneDrive, Personal Files and Documents in Teams.
- Backup for Microsoft Entra ID with 6 automated backups per day and 8-hour RPO.
- Unlimited retention by default while the user subscription remains active.

2.4 Optional Supported SaaS (Available on Request)

- Salesforce
- Slack
- Duo
- Okta
- Dropbox.

2.5 Additional Features

- Graymail protection. Filter our bulk or low priority marketing messages that do not pose any threat and generic spam filters often let through. Users will get a cleaner inbox allowing them to focus on legitimate business messages.
- DMARC monitoring**.** Protects your domain from spoofing to maintain reputation.
- GenAI intent analysis. Uses generative AI to look at the intent of messages, picking up on patterns of fraud, urgency, credential harvesting and other scam signals that simple filtering might miss. It labels and scores emails based on the likely intent behind the content

2.6 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 plan to securely connect the service to your Microsoft 365 tenant and SaaS data sources.

3.3. Deploy and Integrate

- Complete integration to monitored SaaS 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 monitored resource. Including Microsoft Global Admin consent.
- Reviewing and approving automation workflows.
- Agreement to deploy required agents and complete required integrations.
- 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 internet egress on TCP 443 for agent and log forwarding.
- 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.
- Endpoint security which is covered by Arc Managed Endpoint Total 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 indicators of account takeover, impossible travel, etc	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.

- Recovery Point Objective (RPO) 8 hours.
- Recovery Time Objective (RTO) 4 hours.

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

- SLA response performance.

- User security score. Provides a comprehensive and timely view of the current state of security, including recommendations. Security score will summarise:
    - User behaviour risk
    - Phishing test performance
    - Dark web exposure
    - SaaS Alerts weighting
    - Policy compliance

7. Technical Standards and Compliance

- Frameworks: NIST CSF operating model; MITRE ATT&CK mapping for detections and reporting.
- Data protection: UK GDPR compliant. Security telemetry ingests metadata only, for backup full SaaS content is stored in encrypted form.
- Retention: Unlimited retention by default while the user subscription remains active.
- Security of service delivery: MFA enforced for all Arc staff; least-privilege access; activities logged and auditable.