

848

The Secure Business - Protect

Service Definition

Secure Business

Version 0.6 | September 2026

1. Service Overview

People need to work securely wherever they access the organisation's services. When access rules, device settings and information safeguards vary across the estate, ordinary changes can create exposure that is difficult to see. Protect establishes the selected safeguards and explains how customer teams should maintain them in daily operation.

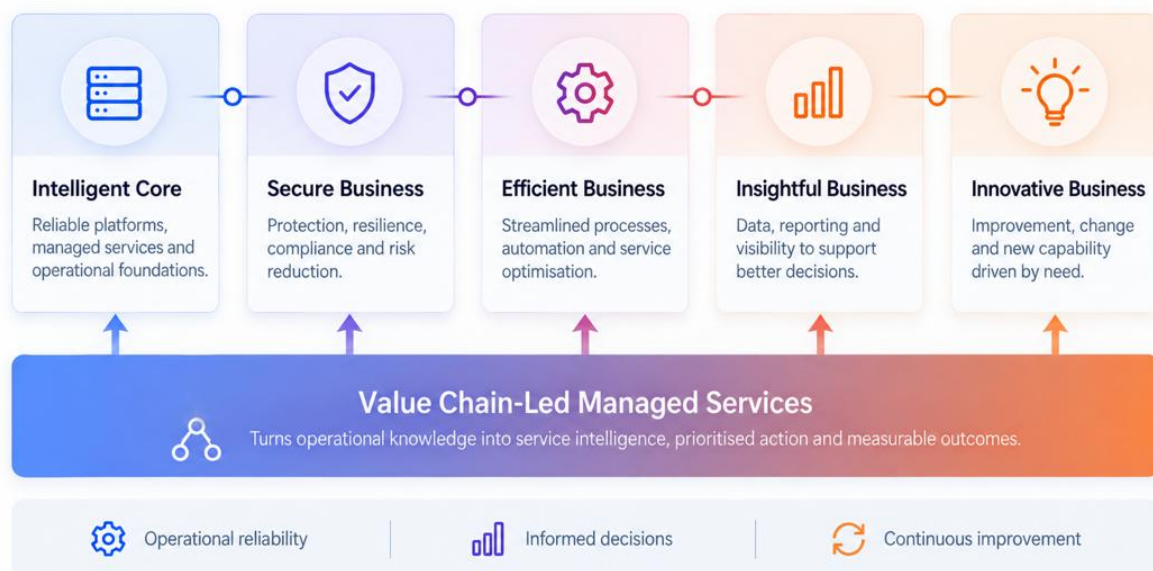
Protect sits within The Secure Business, part of 848's Intelligent Business Framework. The framework connects technology investment to the way the organisation operates, makes decisions and delivers services. Each engagement addresses the selected outcome while considering its place in the wider customer environment.



Powered by **Intelligence** | Driven by **People** | Focused on **Outcomes**

848 Intelligent Business Framework

A framework that aligns service delivery, security, insight and improvement to business outcomes.



From business need to usable capability

The service turns security requirements into practical configuration. Access decisions reflect the user's role and device condition; collaboration settings support safe sharing; information controls apply the agreed handling rules. The aim is a protection model that fits how the organisation works and can be sustained after implementation.

Identify can establish the risks and priorities that guide this work. Protect implements selected safeguards, while Detect and Respond address the visibility and action needed when suspicious activity occurs. The Intelligent Core provides the platform context, allowing security decisions to support wider productivity and data initiatives.

2. Scope and Service Boundaries

Customers select the elements that support their intended outcome. The scope identifies what 848 will deliver and the work retained by customer teams or suppliers.

Service	Outcome
Identity and access management	Design and configuration in Entra ID establish authentication and Conditional Access. Selected privileged access, single sign-on and joiner–mover–leaver processes support the agreed identity lifecycle.
Endpoint and device protection	Intune and Defender for Endpoint apply device compliance and protection baselines. Patch governance and operational guidance explain how customer teams sustain the configuration; routine patch deployment is separately scoped.
Secure remote access	Conditional Access and Azure VPN establish the agreed remote access pattern. Device compliance and identity integrations connect access decisions to the existing environment.
Email and collaboration security	Defender for Office 365 policies address phishing and harmful content. Selected safeguards across Microsoft 365 collaboration workloads support the agreed sharing and communication model.
Information protection	Purview configuration applies selected sensitivity labels and data loss prevention policies. Agreed retention and encryption settings support the customer's information handling requirements.
Cloud application access security	Defender for Cloud Apps connections and policies provide visibility of application use and control selected sessions. The implementation is handed over for ongoing administration.
Zero Trust architecture design	A design defines trust boundaries and control relationships across the selected environment. Proof-of-concept configuration can validate the design; full rollout requires its own implementation scope.
Secure configuration and cloud security	Agreed Microsoft environment baselines and Defender for Cloud configuration expose deviations. Remediation within the selected baseline is included; wider workload or network redesign is separate.
Phishing simulation and awareness	Selected campaigns measure user responses and provide targeted awareness activity. Campaign findings guide reinforcement; a wider organisational training programme is separate.

Dependencies and exclusions

The selected tenants and control families define the implementation boundary. Existing platform defects, incident investigation and continuous security operations require separate arrangements. Control configuration does not confer regulatory certification. Zero Trust design and cloud monitoring configuration do not automatically include full deployment or an ongoing managed monitoring service.

3. How 848 Delivers the Service

Delivery follows the selected scope, using the customer's operating context to guide the work. The sequence below explains how evidence and decisions progress towards the agreed outputs. Customer review and knowledge transfer form part of that progression.

Understand the protection requirement

848 reviews the current configuration with security and platform owners. Access patterns and information handling requirements establish what safeguards need to achieve. The customer confirms the selected users and workloads, including exceptions that must be considered in design.

Design safeguards that fit the environment

848 defines the relevant control model and configuration decisions. Customer owners review the effect on access and working practices before implementation. Dependencies on licensing, existing identity services and device compliance are resolved or recorded as constraints.

Implement and validate the controls

848 configures the agreed Microsoft capabilities and tests representative users or devices. Results show whether the selected policies behave as intended. Baseline deviations within scope are addressed, while wider issues are recorded for customer action.

Prepare the operational owner

848 explains configuration decisions and the tasks needed to maintain them. The receiving team reviews the documentation and test findings. Knowledge transfer supports handover of control ownership, including how exceptions and subsequent changes should be considered.

4. Service Delivery and Management

4.1. Deliverables and Outcomes

The outputs give the customer a usable record of the work and the information needed to act on it. The selected elements determine which deliverables apply; findings and limitations remain visible alongside the results.

Deliverable	Use for the customer
Control design and configuration	Records the access boundaries, settings and selected safeguards implemented for the engagement.
Validation and campaign findings	Shows representative test results or campaign observations, with limitations and follow-up actions.
Operational guidance	Explains routine control ownership and the configuration knowledge needed by the receiving team.

4.2. Working with 848

Security owners approve control requirements and exceptions. Platform administrators provide access and coordinate customer changes. Information owners confirm classification and retention needs where those controls are selected.

Participant	Responsibility
848 delivery team	Performs the selected work, explains findings and documents the relevant outputs. Coordinates review and knowledge transfer with the customer.
Customer service owner	Confirms the intended outcome and scope. Makes customer decisions and identifies who can resolve dependencies or approve changes.
Customer specialists and suppliers	Provide relevant information and agreed access. Complete retained activity and participate in review or validation where their systems or processes are involved.
Receiving team	Reviews the relevant outputs and takes ownership of the activities that continue after handover.

4.3. Service Assurance

Acceptance considers the approved design, implemented settings and representative validation results. Campaign acceptance covers the agreed execution and reporting. The customer reviews outstanding exceptions with the operational owner.

Review focus	What is checked
Scope alignment	The delivered work and outputs address the agreed requirements and selected service elements.
Evidence and validation	Findings or test results show the basis for conclusions, including known limitations and unresolved dependencies.

Review focus	What is checked
Customer acceptance	Relevant owners review the outputs and understand any open actions before accepting the commissioned work.

4.4. Onboarding

Onboarding establishes the conditions needed for useful delivery. The customer and 848 confirm what the engagement should achieve and check that the people and information needed for the selected work will be available.

Preparation	What needs to be established
Outcome and scope	Confirm the selected elements, boundaries and expected outputs, together with the customer's priorities.
Information and access	Relevant Microsoft licences, tenant access and an accurate user or device inventory are required. Customer teams provide existing policies and confirm the representative test population.
Participants and decisions	Identify the service owner, relevant specialists and receiving team. Confirm review participants and escalation routes.
Delivery readiness	Agree the applicable schedule and customer prerequisites. Confirm any operational constraints affecting access, validation or handover.

4.5. Operating and Improving

Customer teams maintain the controls after handover. Changes in user behaviour or the platform estate can justify further review. A separate Detect or managed service engagement can provide continuing operational visibility where commissioned.

4.6. Handover and Exit

The handover explains control dependencies and any exceptions left open. Customer administrators take responsibility for ongoing policy administration unless a managed arrangement expressly includes it.

Handover item	Purpose
Agreed outputs	Provide the final documents or configuration material relevant to the selected service.
Findings and open actions	Preserve the evidence, limitations and remaining work for the customer or receiving provider.
Knowledge and ownership	Explain how the outputs should be used and confirm who owns the next operational or improvement activity.

5. Why 848

848 helps organisations improve how technology supports the way they operate, make decisions and deliver services. Our focus is not on deploying technology for its own sake, but on connecting technology investment to measurable business outcomes.

Our services are aligned through The Intelligent Business Framework, which brings together five outcome areas: The Intelligent Core, The Secure Business, The Efficient Business, The Insightful Business and The Innovative Business. This provides a consistent way to move from technology foundations and security through to operational efficiency, data-led decision-making and innovation, without treating each requirement as an isolated project.

848 combines consulting, engineering and managed service capability within one UK-based team. That matters because the people who design and implement change understand how technology must operate once it enters live service. Architecture, cloud, security, data, Power Platform, Dynamics 365, Microsoft 365 and managed services can therefore be considered as connected parts of the customer environment rather than separate technical towers.

Our Microsoft capability is supported by established partner credentials and practical delivery experience across Microsoft Azure, Microsoft 365, Power Platform, Dynamics 365, Fabric, Sentinel, Defender, Intune, Entra ID and Purview. 848 is a Microsoft Solutions Partner for Security and a Microsoft Direct CSP, giving our teams direct access to Microsoft technologies, programmes and commercial capability.

Service quality and security are supported by recognised organisational standards. 848 holds ISO/IEC 27001, ISO 9001, Cyber Essentials and Cyber Essentials Plus, with security-cleared capability available where required. These controls sit behind the way we manage information, quality, access, risk and service delivery across customer engagements.

What differentiates 848 is the connection between delivery and improvement. Through Value Chain-Led Managed Services, service information is converted into practical intelligence about how technology and services perform across users, teams, suppliers, systems and hand-offs. Service Flow Analysis extends that view by identifying friction, delay, rework, unclear ownership and recurring service issues across end-to-end journeys. The result is a clear improvement backlog based on real operational evidence rather than assumption.

We also place a strong emphasis on internal capability. Knowledge transfer, clear ownership and practical handover are built into our services so that customers understand what has been delivered, how it works and how it should evolve. Where 848 remains involved, improvement continues through review, prioritisation and measurable service outcomes rather than static support.

For customers, the result is a partner able to move from strategy through design, implementation, validation, operation and improvement while maintaining a consistent view of the wider business outcome. 848 brings together the people, Microsoft capability and service intelligence needed to make technology easier to operate, easier to improve and more valuable over time.