INTERGENCE

Service Description

Managed Backup-as-a-Service (BaaS)

Powered by N-able Cove Data Protection

Document classification: Commercial – Customer Facing
Version 1.0

Date: 27 July 2026

1. Service Overview

Intergence's Managed Backup-as-a-Service (BaaS) provides customers with a fully managed, enterprise-grade data protection service built on N-able Cove Data Protection — a cloud-native backup and disaster recovery platform purpose-built for business continuity and cyber-resilience.

Rather than customers having to design, deploy, monitor and maintain backup infrastructure themselves, Intergence takes end-to-end ownership of the service: configuration, daily monitoring, incident response, restore support, and ongoing reporting. The result is predictable, verifiable protection of business-critical data, backed by clearly defined service levels and 24/7 support.

This document describes the scope, technology, service levels, reporting and support model for the Intergence Managed BaaS offering.

2. The Technology – N-able Cove Data Protection

Cove Data Protection is a cloud-first backup and disaster recovery platform that unifies backup, data security, and recovery for servers, workstations and SaaS data (including Microsoft 365) in a single, multi-tenant console. Intergence uses this platform as the technical foundation of its Managed BaaS service.

Key architectural strengths that underpin the Intergence service include:

- Highly efficient, block-level incremental backup technology that dramatically reduces bandwidth and storage requirements, enabling more frequent backups and more restore points.
- Backups transmitted directly to resilient, geographically distributed private cloud data centres, isolated from customer and Intergence networks.
- Immutable “Fortified Copy” snapshots, created automatically every hour and retained for 30 days, which cannot be modified or deleted through the management console, API or CLI — providing a clean recovery point even if an attacker compromises administrative credentials.
- Built-in anomaly detection that raises real-time alerts on suspicious changes to backup jobs or policies, helping to detect credential-based attacks targeting the backup environment itself.
- AES 256-bit encryption of data in transit and at rest.

Intergence configures, monitors and manages this platform on the customer's behalf as part of the Managed BaaS service.

3. Service Scope – What Is Protected

The Managed BaaS service can be scoped to protect any combination of the following workloads, as agreed with the customer during onboarding:

Workload	Protection Provided via N-able Cove Data Protection
Physical Servers (Windows)	Image-based, agent-based backup of full server volumes and system state, with bare-metal and granular file/folder recovery.
Virtual Machines	Agentless and agent-based protection for VMware and Hyper-V guests, including application-consistent snapshots.
Workstations / Laptops	File-level and image-based backup of end-user devices, including roaming/remote devices connected via the internet.

Workload	Protection Provided via N-able Cove Data Protection
Microsoft 365	Exchange Online mailboxes, OneDrive for Business, SharePoint Online sites, and Teams data, backed up multiple times daily independent of Microsoft's native retention.
Databases	Application-aware backup of Microsoft SQL Server (and supported database platforms) with transaction log support for point-in-time recovery.
Cloud & Local Storage	Backups are encrypted and replicated to N-able's private cloud data centres; a local speed vault / local cache option is available for faster restores where required.

4. Service Features & Capabilities

Capability	Description
Backup frequency	Configurable per workload, as frequently as every 15 minutes for critical systems; typically daily for standard workloads.
Retention	Flexible retention schedules (daily, weekly, monthly, yearly grandfather-father-son) tailored to the customer's regulatory and business requirements, typically up to 12 months as standard, longer on request.
Encryption	AES 256-bit encryption in transit and at rest, with a customer-controlled private encryption key option available.
Ransomware resilience	Backups are stored off-site and are isolated and immutable by default. Fortified Copies create automatic, tamper-proof hourly snapshots retained for 30 days that cannot be altered, encrypted, or deleted via the console, API, or CLI — even with compromised credentials.
Anomaly & threat detection	Continuous anomaly detection flags suspicious or unauthorised changes to backup jobs and policies, providing early warning of credential-based attacks targeting backup infrastructure.
Backup verification	Automated backup integrity checks and recoverability testing confirm that backup images are viable and restorable, with alerting on failed or missed jobs.
Efficiency	Block-level, incremental-forever backup technology minimises bandwidth and storage consumption, enabling more frequent backups and shorter recovery windows.
Disaster recovery	Optional Cove Disaster Recovery as a Service (DRaaS) enables rapid virtualisation of protected servers in the cloud, minimising downtime in the event of a major incident.

5. Service Delivery Model – Roles & Responsibilities

The Managed BaaS service is delivered under a shared responsibility model. Intergence owns the day-to-day operation, monitoring and support of the backup environment; the customer is responsible for providing accurate information and timely notification of changes that affect the protected environment.

Responsibility	Intergence	Customer
Design and configuration of backup jobs, schedules and retention policies	✓	
Deployment and licensing of N-able Cove backup agents	✓	
Daily monitoring of backup job success/failure	✓	
Investigation and remediation of backup failures	✓	
24/7 service desk for incidents and restore requests	✓	
Monthly service and compliance reporting	✓	
Provision of accurate asset and workload inventory		✓
Timely notification of infrastructure, user or licensing changes		✓
Sufficient internet bandwidth at protected sites		✓
Nomination of an authorised contact for restore approvals		✓
Periodic participation in restore/DR test exercises	✓	✓

6. Onboarding & Implementation

- Discovery workshop to confirm in-scope devices, workloads and retention requirements.
- Deployment of N-able Cove backup agents and configuration of backup jobs, schedules and retention policies.
- Baseline (initial) backup and validation that all in-scope workloads are protected and reporting correctly.
- Test restore performed and evidenced before the service formally transitions into business-as-usual support.
- Handover to the Intergence 24/7 service desk and provisioning of customer portal access.

7. Service Levels & Key Performance Indicators (SLA/KPI)

The following service levels apply to the Managed BaaS service. Targets are indicative of Intergence's standard managed service commitment and will be confirmed and formally agreed within the customer's signed Service Level Agreement / Schedule.

KPI / SLA Metric	Target	Measured & Reported
Backup job success rate	≥ 99.5% of scheduled jobs completed successfully per month	Monthly service report
Backup failure alerting	Failed/missed jobs identified and actioned within 1 business hour of detection	Continuous monitoring log
Recovery Point Objective (RPO)	As low as 15 minutes for critical workloads; 24 hours standard, per agreed backup schedule	Backup schedule configuration
Recovery Time Objective (RTO)	File/folder restore: within 4 hours of approved request. Full server/image restore: within 8–24	Restore ticket records

KPI / SLA Metric	Target	Measured & Reported
	hours depending on data volume. DRaaS virtualisation (where subscribed): within 2 hours	
Service desk availability	24 hours a day, 7 days a week, 365 days a year	Telephony/ticketing system logs
Incident response times	Per severity level – see Section 7	Ticketing system (time-to-first-response)
Monthly report delivery	Issued within 5 business days of month-end	Report distribution log
Data durability	Backup data replicated across resilient, geographically redundant cloud data centres	N-able Cove platform architecture
Ransomware-resilient copy	Immutable hourly "Fortified Copy" retained for a minimum of 30 days on all protected devices	Platform configuration – always on

7.1 Incident & Restore Request Severity Levels

Severity	Definition	Target Response	Target Resolution / Restore Initiation
P1 – Critical	Total backup failure across an environment, or an active/urgent restore required to recover from data loss or a security incident.	15 minutes	1 hour (restore initiation)
P2 – High	Repeated or persistent failure of a single job/workload; standard restore request affecting business operations.	1 hour	4 business hours
P3 – Medium	Isolated backup failure with no immediate business impact; configuration change request.	4 business hours	1 business day
P4 – Low	General queries, reporting requests, or minor configuration assistance.	1 business day	3 business days

8. 24/7 Service Support Desk

All incidents, restore requests, and service queries relating to the Managed BaaS service are handled through the Intergence Service Desk, which operates 24 hours a day, 7 days a week, 365 days a year.

- Multi-channel access: telephone, email and the Intergence customer portal.
- All requests are logged, tracked and prioritised in the Intergence service management (ITSM) platform against the severity levels defined in Section 7.1.
- Named service delivery contact for escalation management and service review coordination.
- Emergency restore and ransomware-recovery support available out of hours for P1 incidents.

9. Customer Portal Access

Customers are provided with dedicated portal access to maintain visibility and control over their backup estate, including:

- Real-time dashboard of backup job status across every protected device and workload
- Self-service visibility of backup history, retention points and storage usage
- Ability to raise restore and support requests directly to the Intergence service desk
- Access to historic monthly service reports and SLA performance data
- Role-based access so customer administrators can view status without vendor-level configuration access
- Audit trail of configuration changes and administrative actions

10. Monthly Service Reporting

A formal service report is issued every month, providing transparent evidence of service performance and data protection posture. Each report includes:

- Executive summary of backup health across all protected devices and workloads
- Job success/failure statistics and trends, with root-cause commentary on repeat failures
- Storage consumption and retention compliance by device/workload
- Restore requests actioned during the period, with turnaround times against SLA
- Security-relevant events, including anomaly detection alerts and any Fortified Copy activity
- Capacity and licensing summary, including any devices requiring onboarding or decommissioning
- SLA/KPI performance summary against the targets in Section 7
- Recommendations for service improvement (e.g. retention changes, DR test scheduling)

Reports are reviewed with the customer at an agreed cadence (e.g. monthly or quarterly service review) and form the basis of continual service improvement discussions.

11. Governance & Continual Service Improvement

- Scheduled service reviews to assess SLA/KPI performance, capacity trends, and emerging risks.
- Periodic restore and disaster recovery test exercises, with results documented and shared with the customer.
- Annual review of retention policies and scope against the customer's regulatory and business continuity requirements.
- Proactive recommendations where backup configuration, licensing, or protection levels should evolve alongside the customer's IT environment.

12. Exclusions & Assumptions

- The service protects data within the agreed scope only; newly provisioned devices or workloads must be notified to Intergence for onboarding and are not automatically covered.
- Restore time objectives assume the customer has approved the restore request and provided any required authorisation without delay.
- The service does not include remediation of underlying infrastructure faults, malware removal from live systems, or forensic investigation, which may be available under separate Intergence security services.
- Sufficient internet bandwidth at the customer's site(s) is required to meet backup and restore windows; Intergence will advise if bandwidth is assessed as insufficient.

- Third-party platform availability (e.g. Microsoft 365, N-able Cove infrastructure) is subject to the relevant vendor's own service levels.

13. Contact & Next Steps

Contact: David Poulton, **Email:** dpoulton@intergence.com, **Mobile:** +44 (0)7990736095