

Executive Summary

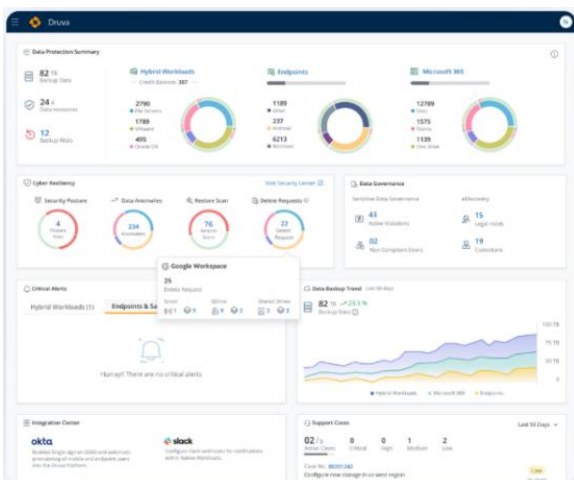
Qnetix delivers a managed Backup and Cyber Recovery Service that protects your organisation from ransomware, data loss, and recovery failures. Built on Druva Data Security Cloud, the service combines cloud native, air gapped, immutable storage with expert UK based management. You get comprehensive protection across SaaS, endpoints, cloud workloads, and on premises systems, plus tested recovery runbooks, minimum viable company hosting for disaster scenarios, and specialist add ons for databases and business applications. The result is faster recovery, lower costs, and confidence that your data is secure and retrievable when it matters most.

Problems Solved

- ✓ Legacy backup tools that are complex, slow to recover, and hard to scale
- ✓ Ransomware and insider threats that target backup systems
- ✓ Limited visibility across SaaS, cloud, and endpoint data sources
- ✓ Fragmented point solutions that increase risk and management effort
- ✓ Compliance gaps due to inconsistent retention, reporting, and audit trails

Business Benefits

- ✓ Reduce operational effort through a fully managed SaaS based solution
- ✓ Improve cyber resilience with air gapped, immutable backups and clean recovery
- ✓ Speed up recovery to minimise downtime and business disruption
- ✓ Strengthen compliance with policy based governance and audit readiness
- ✓ Optimise costs by removing backup infrastructure and simplifying operations



Data Protection → Modernize data protection to reduce costs and complexity	Public Cloud Backup → Hybrid Cloud Backup → End User Protection →
Cyber Response & Recovery → Bounce back from cyber attacks with data that is always safe and ready.	Accelerated Ransomware Recovery → Security Posture & Observability → Managed Data Detection & Response →
eDiscovery & Compliance → Secure, protect, and streamline data governance.	Sensitive Data Governance → eDiscovery & Legal Hold → Cloud Archive & Retention →
Meet Dru - Your Copilot for Data Security →	

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

Technical Leader Summary

Qnetix delivers a unified data protection solution using Druva SaaS, covering cloud, SaaS, endpoints, and virtualised platforms with centralised management and security automation. Qnetix adds automation, tested backup and recovery runbooks, hosting of recovery systems and minimum viable companies, expert integrations, add ons for database protection, CI CD protection and business applications, and an expert UK based service desk. The service includes air gapped and immutable backup storage, threat detection, fast recovery workflows, and integrations with leading security platforms. It supports policy driven RPO and RTO targets, global deduplication, and multi region resilience without infrastructure management.

ROI Benefits Typically Observed

- ✓ 40+ percent reduction in backup infrastructure costs
- ✓ 60+ percent reduction in administration effort
- ✓ 55+ percent improvement in recovery time objectives
- ✓ Elimination of capital expenditure for backup hardware and software licensing

Druva is a Gartner Magic Quadrant Leader

Figure 1: Magic Quadrant for Backup and Data Protection Platforms



Druva is a Leader in this Magic Quadrant. Its primary backup and data protection offering is Druva Data Security Cloud. Druva's operations are geographically diversified and most of its clients are in the enterprise and midmarket segments. During the evaluation period, Druva added cross-cloud backup with Azure Storage, integration with Microsoft Sentinel and Microsoft Security Copilot, and Managed Data Detection and Response (MDDR) services. Druva also introduced the AI-powered tool Dru Investigate, which accelerates threat analysis and response, as well as AI-powered anomaly detection for Microsoft 365 and VMware, and Druva Microsoft 365 Backup Express, leveraging Microsoft 365 Backup Storage.

Strengths (from Gartner)

- ✓ Strong product strategy execution: Building upon its enhanced SaaS-based platform architecture hosted on AWS, Druva has accelerated the delivery of new critical offerings and integrations. They include the introduction of an Azure Cloud storage tenant option for backing up AWS EC2 and Azure VMs, support for Microsoft Entra ID, Microsoft Dynamics 365 and agentless backup for Microsoft Azure SQL. Additionally, it has introduced optimized protection capabilities for Amazon S3, Amazon RDS and network-attached storage (NAS).
- ✓ AI-powered operational assistance and security insights: Dru Assist improves user experience through interactive reporting, guided workflows and smart troubleshooting. It features Dru Investigate for security, detecting insider threats, analysing anomalies and speeding up incident response.

- ✓ Proactive ransomware defence: Druva provides a free managed service as a native capability within its data protection platform, delivering proactive cyber resilience for customer backups. This service offers 24/7 monitoring, advanced threat detection and incident response using tailored playbooks, emphasizing early threat neutralization and ensuring reliable data recovery.

Solutions

Overview

The Qnetix Backup and Cyber Recovery Service is a fully managed service run by Qnetix using Druva technologies and platforms, combining cloud native backup, cyber recovery workflows, and security integrations into a single, managed solution. It protects data across major platforms and provides clean recovery paths, governance, and operational simplicity.

Features

- ✓ 100 percent SaaS delivery with no backup infrastructure to manage
- ✓ Air gapped, immutable storage and tamper resistant retention
- ✓ Fully managed service using Druva technologies and platforms
- ✓ Policy based backup, retention, and recovery controls
- ✓ Threat detection, quarantine, and curated recovery workflows
- ✓ Centralised visibility and reporting across all protected systems
- ✓ Automation and tested backup and recovery runbooks
- ✓ Hosted recovery systems and minimum viable company environment
- ✓ Expert integrations with security and monitoring tools
- ✓ Unlimited restores (no cloud egress charges)
- ✓ CI/CD and business application protection add-ons
- ✓ Self service recovery for end users
- ✓ UK based expert service desk

Benefits

- ✓ Faster recovery from cyber incidents and operational failures
- ✓ Reduced cost and complexity compared with legacy backup estates
- ✓ Improved audit readiness and compliance assurance
- ✓ Consistent protection for cloud, SaaS, and endpoint data
- ✓ Better security posture with integrated monitoring and alerting
- ✓ Reduced operational overhead and infrastructure costs
- ✓ Lower risk of data loss and reinfection
- ✓ Consistent protection across diverse data sources
- ✓ Clear accountability with a single managed provider
- ✓ Better visibility for security and IT teams
- ✓ Rapid onboarding with tested recovery procedures
- ✓ Resilient recovery environments for critical operations
- ✓ Less disruption through automation and runbook execution

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

Platform Solutions

Accelerated Ransomware Recovery Solution

- ✓ Automated ransomware recovery workflows and curated clean recovery points
- ✓ Threat intelligence, IOC scanning, and quarantine for suspicious backups
- ✓ Security command centre for posture visibility and response alignment
- ✓ Recovery scans and IOC checks to identify infected data
- ✓ Sandbox recovery to validate clean restores before production

Cloud Based Backup Solution

- ✓ SaaS based backup replacing on premises infrastructure and manual upkeep
- ✓ Global deduplication and efficient storage to reduce costs
- ✓ Policy driven retention and recovery for business critical data
- ✓ Rapid deployment without backup appliances
- ✓ Incremental, policy led backups with efficient storage use

Data Security Cloud Platform Solution

- ✓ Unified control plane for SaaS, endpoints, cloud, and hybrid data
- ✓ Air gapped, immutable backups with anomaly detection and threat hunting
- ✓ Built in governance, legal hold, and audit trail capabilities
- ✓ Common metadata view for cross workload insight
- ✓ Built in governance, legal hold, and audit trails

RPO and RTO Optimisation Solution

- ✓ Policy led recovery objectives aligned to business priorities
- ✓ Automated backup scheduling and rapid restore paths
- ✓ Reporting for recovery performance and resilience readiness
- ✓ Minute level recovery points for critical workloads
- ✓ RPO and RTO reporting to highlight gaps

CloudCache Performance Solution

- ✓ Local cache for faster restores and reduced latency
- ✓ Optimised bandwidth usage through deduplication and compression
- ✓ Reliable recovery at scale for distributed and remote environments

Posture Observability Solution

- ✓ Security posture visibility with scorecards and risk dashboards
- ✓ Continuous monitoring to detect gaps and misconfigurations
- ✓ Actionable recommendations to strengthen cyber resilience

Scalable Storage Solution

- ✓ Elastic storage that grows from terabytes to petabytes
- ✓ Auto tiering between hot and cold storage to balance performance with cost
- ✓ Long term retention without infrastructure expansion or new hardware

Sensitive Data Governance Solution

- ✓ Discovery, classification, and monitoring of sensitive data across workloads

- ✓ Policy based controls to reduce exposure and compliance risk
- ✓ Centralised reporting for audit and governance teams

Cloud and Infrastructure Solutions

Air Gapped EC2 Backup Solution

- ✓ Agentless protection with automatic discovery across accounts and regions
- ✓ Cross account and cross region recovery for resilience
- ✓ Malware scanning on recovery with file level and full instance restore options

Amazon RDS Backup Solution

- ✓ Application consistent backup with point in time recovery
- ✓ Granular restore options for database workloads
- ✓ Centralised policy management across multiple RDS instances

Amazon S3 Backup Solution

- ✓ Version aware protection and recovery for S3 buckets
- ✓ Lifecycle retention policies aligned to governance requirements
- ✓ Visibility across object storage usage and risk

AWS Protection Solution

- ✓ Unified, agentless protection across key AWS services from a single console
- ✓ Air gapped and immutable backups with automated recovery workflows
- ✓ Cross account and cross region recovery options

Microsoft Azure Backup Solution

- ✓ Agentless onboarding with SaaS simplicity for Azure workloads
- ✓ Centralised policy management and reporting
- ✓ Multi region recovery support with alternate region failover

Azure Blob Backup Solution

- ✓ Granular recovery for containers and objects with flexible restore locations
- ✓ Compliance driven retention controls aligned to governance needs

Azure Files Backup Solution

- ✓ File level recovery for shared file services
- ✓ Policy based backup scheduling and retention for Azure Files estates

Azure Protection Solution

- ✓ Unified protection for Azure compute and storage
- ✓ Air gapped, immutable backups with rapid recovery
- ✓ Centralised reporting and compliance visibility across Azure estates

VMware Backup and DR Solution

- ✓ Agentless backup with change block tracking for vSphere and VMware Cloud
- ✓ One click failover with automated recovery and failback runbooks
- ✓ Immutable backups with threat detection for cyber resilience

Nutanix AHV Backup Solution

- ✓ Agentless, application aware protection with change block tracking
- ✓ Global deduplication and automated tiering to reduce cost
- ✓ Centralised management and fast recovery across Nutanix environments

Phoenix Backup Solution

- ✓ Unified backup, DR, and archive for on premises workloads with cloud based management
- ✓ Incremental forever backups with global deduplication
- ✓ Policy based recovery aligned to business needs

Phoenix NAS Backup Solution

- ✓ Scalable NAS protection with file level recovery for large shares
- ✓ Long term retention with efficient storage tiering
- ✓ Centralised visibility for NAS estates

Applications and Endpoints Solutions

Microsoft 365 Backup Express Solution

- ✓ Rapid recovery optimised for large scale Microsoft 365 tenants
- ✓ Granular restore for mail, files, and collaboration data

Microsoft 365 Backup Solution

- ✓ Full coverage for Exchange, OneDrive, SharePoint, and Teams
- ✓ Long term retention beyond native platform limits
- ✓ Self service recovery to reduce support load

Dynamics 365 Backup Solution

- ✓ Protection for Dynamics 365 CRM data and configurations
- ✓ Consistent backups and restore options for business workflows
- ✓ Governance controls aligned to compliance needs

Entra ID Backup Solution

- ✓ Protection for directory objects, identity configurations, and access settings
- ✓ Support for recovery of critical access data
- ✓ Improved security posture through protected identity data

Google Workspace Backup Solution

- ✓ Coverage for Gmail, Drive, and collaborative documents
- ✓ Granular recovery for users and shared data
- ✓ Retention policies aligned to governance requirements

SaaS Apps and Endpoints Solution

- ✓ Discovery and protection of common SaaS services in use
- ✓ Unified policies and consistent recovery across SaaS and endpoint data
- ✓ Centralised reporting and policy enforcement

Salesforce Archive Solution

- ✓ Searchable archive to reduce platform storage costs and improve performance
- ✓ Policy driven retention and governance controls for long term compliance
- ✓ Data lifecycle management for cost optimization

Salesforce Sandbox Seeding Solution

- ✓ Automated sandbox refreshes with relationship integrity and reliable seed data
- ✓ Data masking options for sensitive data in test environments
- ✓ Faster development cycles with consistent test data

Endpoint Data Protection Solution

- ✓ Incremental backups for Windows, macOS, and Linux endpoints
- ✓ Self service, user initiated restores to reduce helpdesk load
- ✓ Centralised management and policy enforcement

Security Integrations Solutions

CrowdStrike Integration Solution

- ✓ Correlation of endpoint detections with backup events through shared telemetry
- ✓ Improved ransomware detection and compromise indicators
- ✓ Faster investigation timelines and response coordination

Microsoft Sentinel Integration Solution

- ✓ SIEM correlation of backup telemetry ingested into Sentinel with security events
- ✓ Automated alerts and investigation workflows
- ✓ Improved visibility across security operations

Palo Alto Integration Solution

- ✓ SOAR workflows for quarantine and recovery actions
- ✓ Automated response for suspicious activity aligned to security playbooks
- ✓ Integrated security orchestration for incident response

Splunk Integration Solution

- ✓ Real time ingestion of backup events into Splunk for centralised monitoring
- ✓ Correlation of backup telemetry with wider security data
- ✓ Audit and compliance reporting for incident response

Sumo Logic Integration Solution

- ✓ Cloud native SIEM integration with real time analytics for backup telemetry
- ✓ Faster anomaly detection through event correlation
- ✓ Improved investigation with correlated security insights

Service Delivery

The sections below describe the typical onboarding and support journey for Qnetix services. Each service is tailored to your scope, change windows, and operational priorities.

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

Onboarding and Setup

Onboarding is designed to be fast, low risk, and fully managed by Qnetix. You provide authorised contacts and access requirements, and we handle provisioning, configuration, validation, and documentation handover. Training is included where required. Standard onboarding and offboarding are included at no cost, with additional onboarding support available at a pre agreed rate.

Typical onboarding phases include:

- ✓ Discovery and requirements validation
- ✓ Access provisioning and security alignment
- ✓ Service configuration and integration
- ✓ Testing, validation, and acceptance
- ✓ Go live and handover into steady state

The timeline is agreed with each customer and aligned to change windows and delivery priorities.

Ongoing Delivery and Support

Support is provided through email and online ticketing with clear priority-based response times:

- ✓ P1 (Critical - Service down or severely impacted): Within 4 hours
- ✓ P2 (High - Significant functionality impaired): Within 8 hours
- ✓ P3 (Medium - Minor functionality issue): Within 2 business days
- ✓ P4 (Low - General inquiry or enhancement request): Within 3 business days

Customers can set and adjust ticket priority and track status through the full lifecycle.

Proactive service management includes monitoring, patching, planned maintenance, and continuous improvement. We operate ITIL aligned practices for incident, problem, request, change, and capacity management to keep services secure, stable, and optimised.

Reporting and Reviews

Quarterly reporting and service reviews provide visibility and accountability. Reports cover:

- ✓ SLA performance and uptime
- ✓ Incident and change summaries
- ✓ Usage and capacity trends
- ✓ Risk, compliance, and improvement actions

Reviews focus on performance, planned improvements, and roadmap alignment with agreed action tracking and follow ups.

Account Management

Each customer is assigned:

- ✓ A Technical Account Manager for service oversight, escalation, and governance
- ✓ A Principal Engineer for technical assurance, troubleshooting, and optimisation

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

Formal service reviews are quarterly, with ad-hoc check ins available as required. Governance aligns to ITIL principles, including service level management, change enablement, and capacity planning.

Security and Compliance

Security and compliance are delivered through a structured governance model with a dedicated security team responsible for operations, certifications, and internal audit. The Qnetix security team report directly to the Qnetix Managing Director. Documented policies include Access Control, Audit and Accountability, Configuration Management, Contingency Planning, Identification and Authentication, Information Security, Information Technology, Personnel Security, Physical and Environmental Security, Risk Assessment, System and Information Integrity, Vendor Management, and Business Continuity.

Services are designed for resilience using a multi data centre architecture. Customer systems can be replicated across separate data centres or cloud locations to remove single points of failure, enabling automatic failover and continued availability in the event of hardware, network, or site incidents. Additional architectural and resilience details are available on request.

Security and compliance activities are agreed on a case-by-case basis to align with customer requirements and sector obligations.

About Qnetix

Qnetix is an outcome driven IT managed service provider supporting startups, growing businesses and the UK public sector. We operate as an extension of leadership and technical teams, delivering measurable outcomes through technology innovation, structured runbooks, governance, and accountable service delivery.

Our mission is to improve customer operations with reliable, secure, and cost efficient services backed by UK based support. Our values are trusted, expert, and outcome driven.

We provide end to end IT services that scale with your business, including hosting, multi cloud and private cloud services, security and compliance, DevOps and DevSecOps, Kubernetes, observability and monitoring, end user support, SaaS applications, and AI systems management. We use AI to supplement engineering delivery and operate management systems that oversee service quality and risk.

Customers choose Qnetix for predictable delivery and clear governance, with a dedicated UK lead architect on every engagement and flexible commercial models, including outcome based contracts. We provide a 24x7 command centre, ISO aligned governance, and a global talent pool backed by strong vendor relationships. Rapid onboarding and continuous optimisation help customers move quickly while staying secure and compliant.

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

Case Studies

The following case studies include the products referenced in this service description.

UK Public Sector Customer Case Study

Qnetix Backup Service: Backup and Cyber Recovery for 4,000 Users

Overview

A UK public sector organisation required a modern, resilient backup and cyber recovery service for 4,000 users across core business lines. The customer needed to strengthen cyber resilience, reduce operational overhead, and ensure predictable governance without disrupting critical services. Qnetix delivered the Qnetix Backup Service using our backup and cyber recovery managed platform, providing secure, scalable protection with clear service accountability.

Customer Context

The customer operates essential public services, supporting front line operations and internal teams with a mix of cloud and on premises systems. Existing backup arrangements were fragmented and required significant manual effort to manage. The organisation wanted improved recovery confidence, a consistent operating model, and assurance that security and compliance could be maintained at public sector standards.

Objectives

- ✓ Establish consistent backup and cyber recovery coverage across 4,000 users and core business services
- ✓ Improve recovery confidence and reduce the risk of data loss following cyber incidents
- ✓ Reduce day to day administration burden through managed service operations
- ✓ Provide transparent reporting, governance, and predictable costs
- ✓ Align with public sector requirements for resilience and assurance

Solution

Qnetix implemented the Qnetix Backup Service, a fully managed backup and cyber recovery solution delivered through our platform. This approach provided an enterprise grade solution while keeping service operations centralised and consistent. The customer benefited from a single, managed service model with Qnetix accountable for implementation, ongoing operations, and continuous improvement.

Key elements of the solution included:

- ✓ Managed backup and recovery platform, owned and operated by Qnetix on behalf of the customer
- ✓ Comprehensive backup coverage for user data and core business systems
- ✓ Cyber recovery workflows designed to improve resilience and restoration confidence
- ✓ Centralised monitoring and management to reduce administrative burden
- ✓ Security and compliance controls aligned to public sector expectations

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

Implementation and Transition

Transition was delivered using our ITIL standards based delivery model. Qnetix worked directly with authorised customer contacts to gather requirements, confirm access, and align service configuration with existing policies. Backup configurations and policies were established as part of onboarding, with no additional cost.

The transition plan focused on continuity of service and minimal disruption. Key steps included: 1. Discovery and validation of systems, data priorities, and recovery objectives 2. Access provisioning and security alignment 3. Service configuration and policy setup 4. Initial protection, testing, and validation 5. Steady state operations and reporting handover

Service Management

Qnetix provided an end-to-end service management as part of the delivery model. The customer received a fully managed service with clear governance and a structured operational rhythm, aligned to ITIL practices for incident, problem, change, and capacity management.

Service management included:

- ✓ Quarterly governance and roadmap reviews
- ✓ Monthly reporting on service status, changes, and improvements
- ✓ Proactive monitoring and management of backups
- ✓ Proactive issue identification and resolution
- ✓ Collaborative change and deployment support
- ✓ Continuous optimisation based on service data and customer priorities

Outcomes and Benefits

The customer achieved a more robust backup and cyber recovery capability, with improved operational control and governance. The managed service model reduced internal effort, and reporting created clear visibility for leadership and assurance teams.

Key outcomes included:

- ✓ Achieved 99.9 percent backup success rate with 100 percent recovery confidence
- ✓ Reduced administration burden by 34 percent through fully managed service
- ✓ Recovery time objectives improved from 24 hours to under 4 hours for critical systems
- ✓ Greater compliance confidence via consistent policies and reporting
- ✓ Clearer accountability with a single managed service provider
- ✓ Cost savings of approximately 40 percent compared to previous fragmented solutions

Operational Impact

The Qnetix Backup Service allowed the organisation to focus on core public services while maintaining a strong security posture and recovery readiness. Proactive service management reduced risk, and the transition delivered fast time to value without disruption.

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

Why Qnetix

Qnetix brought proven delivery across backup, cloud, security, and managed services, supported by direct partnerships and a mature operating model. Our approach ensured the customer received the benefits of an enterprise grade platform with completed vendor service accountability, structured governance, and continuous improvement. Customer is still supported by Qnetix today.

UK Industrial Manufacturer Customer Case Study

Full Back Office IT Outsource

Overview

A UK industrial manufacturer required a fully managed backoffice IT service to stabilise operations, improve security, and reduce the burden on internal teams. The customer wanted a single partner to manage cloud and on premises infrastructure, development platforms, security controls, and user support, while keeping services available across multiple regions and business units. Qnetix delivered a full outsource model with clear governance, proactive management, and measurable service outcomes.

Customer Context

The customer operated mixed environments across multiple regions, with separate non-production, production, and shared service zones. The estate included cloud infrastructure, firewalls, monitoring tools, developer platforms, and Kubernetes clusters, alongside core operating systems and storage services. Previous support arrangements were fragmented, with limited operational visibility and inconsistent processes.

Objectives

- ✓ Consolidate backoffice IT operations under a single managed service
- ✓ Improve service availability, security, and operational consistency
- ✓ Establish clear governance, reporting, and escalation routes
- ✓ Provide reliable support for infrastructure, platforms, and end users
- ✓ Enable predictable service delivery across regions and environments

Solution

Qnetix delivered a full backoffice IT outsource service, providing day to day operational management, security oversight, cloud platform support, and developer enablement. The service focused on resilient cloud operations, secure access and monitoring, and reliable CI and CD pipelines to keep development teams productive.

Key elements of the solution included:

- ✓ Managed cloud infrastructure across production and non-production regions
- ✓ Security monitoring, alerting, and remediation processes across network and platform layers
- ✓ Centralised monitoring and log management for infrastructure and application platforms
- ✓ Managed CI and CD toolchains, including source control, build pipelines, and code quality systems
- ✓ Developer platform support to keep teams productive and releases reliable
- ✓ Managed storage, DNS, and connectivity services
- ✓ Structured governance, reporting, and service optimisation

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

- ✓ Hosting services for non-public cloud systems

Systems in Scope

The service covered an estate across shared, non-production, and production zones, including:

- ✓ Firewalls, security monitoring appliances, and network policy controls
- ✓ Monitoring systems for infrastructure and application health
- ✓ Development platforms and toolchains for build, release, and artifact management
- ✓ Kubernetes clusters supporting core business applications
- ✓ Cloud infrastructure services including compute, networking, identity, storage, and monitoring
- ✓ Shared storage services and connectivity components
- ✓ DNS, load balancing, and secure connectivity services

Service Management

Qnetix delivered a fully managed service across UK business hours with 24x7 coverage for critical incidents. The service included proactive management, structured reporting, and continual improvement, with a strong emphasis on cloud operations, security, developer enablement, and ITIL aligned incident, problem, change, and capacity management.

Service management included:

- ✓ Proactive monitoring, alerting, and incident response
- ✓ Patch management and configuration control to an agreed monthly schedule
- ✓ Capacity planning and performance management
- ✓ Cloud operations management across infrastructure, network, and identity services
- ✓ Security management including vulnerability handling, access review, and policy enforcement
- ✓ CI and CD platform management to maintain reliable developer workflows
- ✓ Backup configuration, monitoring, and restore support
- ✓ Documentation management and best practice guidance

Support and Response

Support was delivered through a 24x7 helpdesk with clear escalation pathways and priority based response. The model included Level 2 support for systems in scope, with escalation to customer technical teams where required.

Outcomes and Benefits

The customer achieved consistent operational control, improved service availability, and reduced internal effort. The outsource model created predictable delivery, clear accountability, and a stable platform for ongoing growth.

Key outcomes included:

- ✓ Achieved 99.7 percent service availability across production and non-production environments
- ✓ Mean time to resolution improved by 42 percent through proactive monitoring and clear escalation
- ✓ Security posture strengthened with full patch compliance and zero critical vulnerabilities
- ✓ Reduced operational load on internal teams by 41 percent

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

- ✓ Greater visibility through structured reporting and governance
- ✓ Infrastructure costs reduced by 32.7 percent through optimised cloud operations

Summary

Qnetix delivered a full backoffice IT outsource service for a UK industrial manufacturer, covering infrastructure, platforms, security, and support across a complex multi region estate. The result was a more resilient, well governed service with predictable outcomes and a clear operational model. Customer is still supported by Qnetix today.

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise