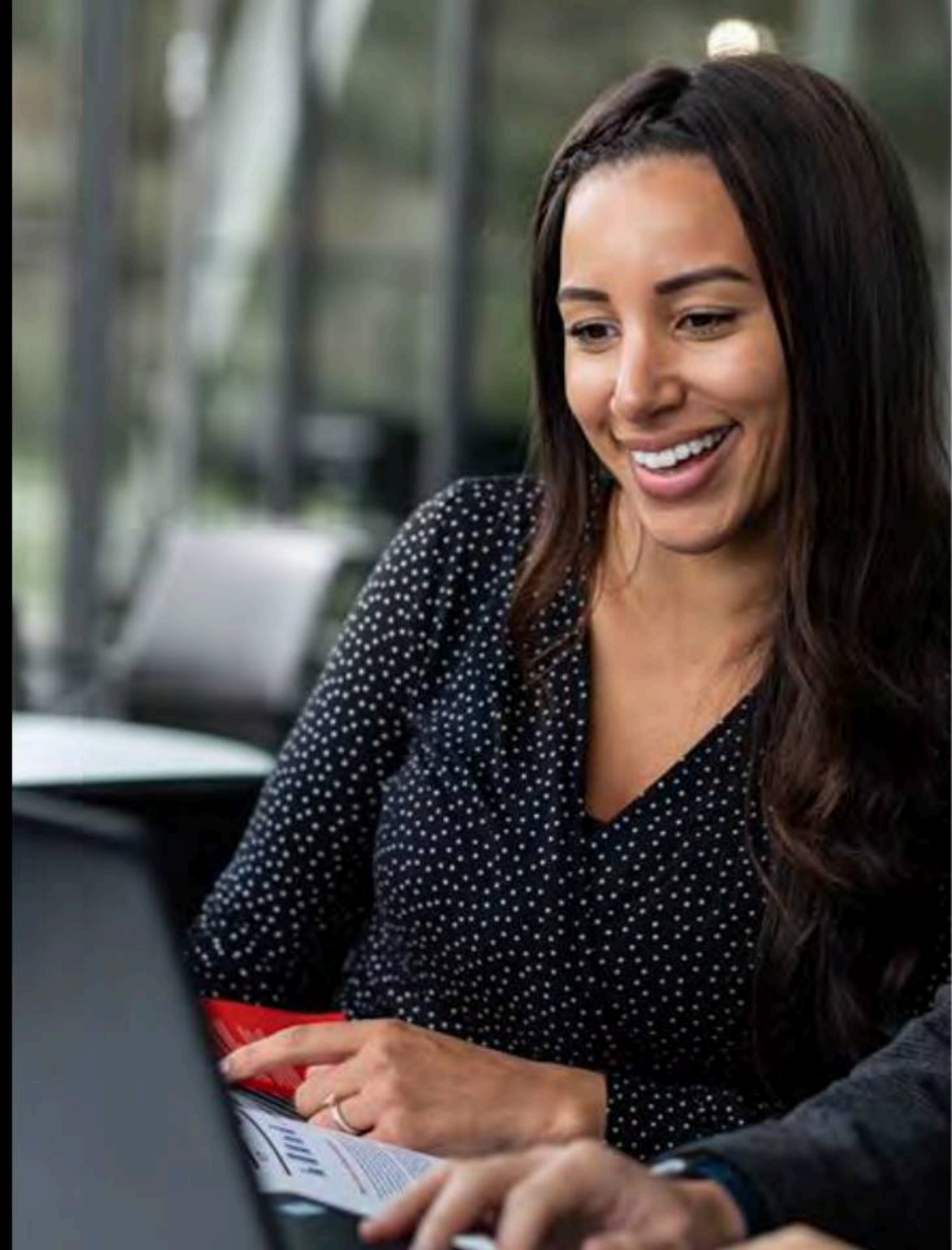




Cybersecurity Services

[Service guide](#)



About ROCK

ROCK is a technology services group delivering cloud, cybersecurity and managed IT services to public sector, healthcare, education, housing and regulated organisations.

Headquartered in the UK, the ROCK Group supports clients globally across and beyond Europe and North America.

The group is structured for scale and resilience, combining disciplined delivery with deep regulatory understanding. This enables ROCK to operate as a trusted partner in complex, high-assurance environments where reliability and security are critical.

The group operates through two focused service disciplines:

- As a Managed Service Provider (MSP), ROCK runs and optimises cloud platforms, infrastructure and modern workplace environments.
- As a Managed Security Service Provider (MSSP), ROCK delivers continuous cyber defence, risk management and compliance-led security operations.

These services can be consumed independently or combined into a unified operating model.

Clients partner with ROCK for clarity and confidence. From a client standpoint, every partnership is shaped by three principles.

Commitment – Through clear ownership and long-term partnership.

Proof – Through measurable outcomes, service metrics and transparent reporting.

Certainty – Through predictable delivery, resilient design and controlled change.

ROCK supports organisations to modernise securely and operate more effectively. We pair technical depth with practical guidance to support informed decisions and keep technology aligned to business priorities.

The group operates within a mature governance framework aligned to ISO 27001:2022, ISO 9001:2015 and Cyber Essentials Plus.

Engineering and service practices are consistent, repeatable and auditable, enabling scale while managing risk.

Ongoing investment in people, platforms and innovation strengthens capability and keeps services responsive to evolving needs. As a strategic partner, ROCK helps clients improve today while building the foundations for long-term change.

Responsible & Sustainable Delivery

ROCK is committed to delivering Social Value alongside high-quality technology services. Our approach is aligned to the UK Government Social Value Model and focuses on creating good jobs, developing skills, supporting inclusive employment, strengthening supply chains, protecting the environment, and promoting workforce wellbeing.

Social Value is embedded into how we operate as an organisation and how we deliver services, including through fair working practices, skills development and training, responsible supply chain management, environmental sustainability, and community engagement.

For each contract, commitments are tailored to customer needs and local context, and agreed during mobilisation and contract governance.



Our Services

ROCK's Cybersecurity Services deliver a Managed Security Operations Centre (SOC) integrated with senior Technology Leadership. We provide public-sector organisations with a turnkey solution for continuous threat detection, incident response, and strategic security governance.

The service combines an AI-driven XDR platform with Virtual CTO (vCTO) leadership, ensuring that sophisticated threat detection is always paired with strategic business context.

This allows organisations to maintain high-velocity digital transformation while ensuring that security operations are well-governed, resilient, and audit-ready.

The Operational Pillars of ROCK XDR:

Cross-Domain Protection

We provide continuous, automated detection and response across Microsoft Defender, Sentinel, AWS, and hybrid infrastructures, eliminating blind spots in complex multi-supplier environments.

Strategic Governance (vCTO)

Senior-level oversight that translates XDR telemetry into "decision-ready" risk insights, enabling boards to make informed technology investments based on evidenced risk.

Proactive Resilience

Continuous vulnerability assessments and posture governance ensure that environments remain aligned to best-practice baselines, such as the Microsoft Cloud Adoption Framework.



“A complete cybersecurity capability that reduces organisational risk while strengthening resilience across cloud and users.”

Ian Elsbury, COO at ROCK

Our Approach

Our approach is built on the principle that security is only as strong as its weakest link. We apply a structured methodology that integrates technical integrity with board-level governance to ensure total exposure management.

Phase 1: Total Exposure Discovery

We begin by establishing a definitive baseline of your current cybersecurity posture.

Asset & Shadow IT Discovery

Identifying all workloads across the estate to eliminate "blind spots" that introduce unmanaged risk.

Control Validation

Assessing existing security configurations against the Microsoft Cloud Adoption Framework and ISO standards to ensure a secure foundation.

Phase 2: Proactive Managed Defence

We operate a secure-by-default model that prioritises prevention and rapid response.

Unified Threat Detection

Continuous monitoring of identities, endpoints, and cloud workloads to identify suspicious activity before it impacts service delivery.

Vulnerability Prioritisation

Identifying and managing technical debt through structured risk registers, ensuring remediation effort is focused on the areas of greatest material impact.

Phase 3: Strategic Governance & Continuous Improvement

We translate operational data into long-term strategic value.

Executive Security Leadership

Providing senior-level guidance (vCTO) to support informed, risk-based technology investment and resource allocation.

Compliance & Audit Assurance

Maintaining "always-ready" documentation for UK GDPR and Cyber Essentials Plus, ensuring the organisation remains resilient to regulatory pressure.

Key Features

Our cybersecurity service combines intelligent detection, expert analysis and structured governance to give organisations dependable, real-time protection.

Each feature is designed to strengthen resilience, reduce risk and support confident decision-making.

24/7 Continuous Monitoring

Real-time visibility across the entire digital estate, ensuring threats are triaged and contained promptly.

Prioritised Risk & Vulnerability Register

A live, structured view of your security exposure, aligned to business impact for clear remediation planning.

Strategic Security Roadmap

Development and oversight of a technology strategy that ensures security investment is traceable to organisational objectives.

Incident Response & Recovery Guidance

Structured protocols and expert support to help the organisation respond rapidly and confidently to high-pressure security events.

Identity & Access Governance

Continuous oversight of user privileges and policy compliance to reduce credential-led attack paths.

Executive Insight & Assurance Reporting

Board-level summaries that provide clear visibility of delivery progress, risks, and required decisions.

Key Benefits

Our cybersecurity services deliver measurable improvements to risk management, operational efficiency and organisational confidence.

Each benefit supports safer, more resilient operations without adding complexity or burden to internal teams.

Reduced Organisational Risk

Identify and remediate vulnerabilities early, preventing the unmanaged technical debt that leads to service outages.

Accelerated Delivery Velocity

Benefit from secure guardrails that allow your teams to adopt new cloud and digital services safely and efficiently.

Improved Value for Money

Avoid duplicated or poorly directed security spend through informed prioritisation and strategic leadership.

Board & Stakeholder Confidence

Provide senior responsible owners (SROs) with the documented evidence and decision-ready insights needed to satisfy governance obligations.

Management & Governance

Our cybersecurity service is delivered through a structured, transparent and ITIL-aligned service management model.

We focus on clarity, predictable processes and ongoing communication, ensuring organisations understand their security posture and the actions required to enhance it.

Service Desk & Analyst Support

All alerts, incidents and requests are handled through ROCK's Service Desk, where specialist analysts triage security events, provide guidance, and escalate complex cases to senior security engineers. Every interaction is logged and tracked for full visibility and auditability.

Security Monitoring & Operational Oversight

We continuously monitor identity, endpoint and cloud telemetry, reviewing alerts for severity, context and potential impact. Analysts provide actionable recommendations, supported by clear communication and rapid escalation where necessary.

Governance & Review Sessions

A dedicated Service Delivery Manager leads structured governance reviews, typically monthly or quarterly, covering:

- Threat trends and incident summaries
- Vulnerability and configuration findings
- Compliance and policy alignment
- Progress against previous actions
- Recommended improvements and emerging risks.

This ensures decision-makers have the information needed to manage risk effectively.

Documentation & Audit Trail

We provide structured support during security incidents, including investigation, containment guidance and coordination with third-party vendors such as Microsoft or AWS when platform-level escalation is required. Clear escalation paths ensure critical events are addressed quickly.

Reporting & Insight

Comprehensive monthly security reports summarise:

- Alerts and investigations
- Identified vulnerabilities
- Identity-related risks
- Policy or baseline deviations
- Recommended actions and prioritisation

Reports are designed for both technical and non-technical audiences, supporting strategic decision-making.

Security & Data Protection

Security is at the core of our service delivery. ROCK applies robust, ISO-certified controls and cloud-native protections to safeguard customer environments, ensuring that threats are identified quickly, risks are managed effectively and sensitive data remains secure.

ISO-Certified Governance

Our service operates within ROCK's ISO 27001:2022 certified Information Security Management System.

This ensures consistent controls for access management, incident response, logging, audit trails, data handling and supplier assurance.

Data Handling & Privacy

ROCK does not store or process customer production data outside of logged alerts or operational metadata required for service delivery. Any information handled is protected under UK GDPR, Cyber Essentials Plus and our internal data governance framework.

All customer data remains within the client's own cloud or on-premise environment unless otherwise agreed.

Identity & Access Controls

All ROCK engineers access client systems through tightly governed, least-privilege accounts protected by multi-factor authentication. Activities are logged, monitored and reviewed regularly to maintain accountability and protect tenant integrity.

Secure Monitoring & Telemetry

We collect and analyse security alerts from Microsoft Defender, Sentinel, AWS GuardDuty and other authorised sources. Data is transmitted securely via encrypted channels and handled only by vetted personnel.

Incident Response Assurance

ROCK follows documented incident response processes aligned to NCSC guidance and ISO 27035. Critical events are escalated rapidly, with clear communication and timelines for containment recommendations.

Data Retention & Secure Disposal

Operational security data is retained only for as long as required for service delivery and contractual obligations. At contract end, all retained metadata is securely deleted using ISO-aligned sanitisation practices.



Values & Outcomes

Our Cybersecurity Services deliver meaningful improvements to risk management, operational efficiency and organisational confidence.

We help clients build stronger defences, respond faster to emerging threats and make informed decisions grounded in real evidence.

Operational Value

Reduced internal workload, as ROCK manages continuous monitoring, alert investigation and day-to-day security operations.

Greater service stability, with early detection of risks and rapid communication of containment or remediation actions.

Improved coordination, supported by clear escalation pathways and structured incident handling processes.

Financial Value

Avoided costs from security incidents, enabled by proactive detection and faster response.

Better use of existing technology investments, ensuring security tools like Defender, Sentinel or GuardDuty operate effectively and efficiently.

Predictable budgeting, with transparent pricing and no unexpected charges.

Security & Compliance Value

Stronger security posture, built on continuous monitoring, vulnerability assessment and governance alignment.

Improved audit readiness, supported by clear reporting and evidence-based insights.

Reduced risk exposure, as identity misuse, misconfigurations and emerging threats are highlighted early.

Strategic & Organisational Value

Better leadership visibility, with clear summaries of risks, incidents and recommended priorities.

More informed decision-making, underpinned by accessible, high-quality security intelligence.

An adaptable security model, capable of scaling and evolving as organisational needs change.

Accreditations & Certifications

ROCK maintains a proven, independently assessed way of working that underpins every service, helping us provide the best IT solutions to our clients. Our certifications and partnerships show that we take security, governance and quality seriously, strengthening our credibility through best-practice services, recognised standards, and ongoing accreditation.

Security Clearances

BS7858:2019 Screening

All staff undergo background screening aligned to BS7858:2019 for roles with access to client systems or sensitive information.

Security Check

Staff can hold UK Government Security Check clearance where required by the service scope, buyer requirements or contractual obligations.

Enhanced DBS Checks

Enhanced DBS checks are performed for staff supporting regulated or sensitive environments where required by client contracts or service scope.

Strategic Partnerships

ROCK works with a range of leading cloud and technology providers to deliver secure, resilient and well-governed services.



Microsoft Partner

Cloud, identity, security and productivity services across Azure, Microsoft 365, Microsoft Entra ID and Microsoft Defender.



AWS Partner

Infrastructure and platform services including compute, storage, networking and security.



Cisco and Meraki

Cloud-managed networking, SD-WAN and secure connectivity solutions.



Cloud Security & SASE

Secure access, firewalling, SD-WAN and ZTNA capabilities, including cloud security.



Backup & Recovery | N-Able & Cove

Cloud-based backup, replication and disaster recovery solutions supporting cloud, hybrid and endpoint environments.



Endpoint & Device Management

Endpoint security, configuration, monitoring and lifecycle management tooling across user devices and servers.



SonicWall

Network security, firewalling, secure remote access and SD-WAN capabilities for on-premise and cloud-connected environments.

Certifications & Compliance



ISO 27001:2022

Certified information security management system demonstrating effective controls for data protection, access management and operational security.



ISO 9001:2015

Certified quality management system supporting consistent service delivery, continuous improvement and effective governance.



Cyber Essentials Plus

Independently verified assurance of strong baseline cybersecurity controls across all operational systems.



ICO registration

Fully registered with the Information Commissioner's Office for data processing compliance.

How To Buy

This service can be procured quickly and compliantly through the Crown Commercial Service (CCS) G-Cloud 15 Framework under the Cloud Support lot.

This provides a streamlined route for public-sector organisations to access high-quality managed support without needing to run a full tender.

What Buyers Can Expect

- Fast mobilisation, with service commencement scheduled quickly after award.
- No contract negotiation, as all terms follow the standard G-Cloud framework.
- Transparent pricing, published and fixed in accordance with the G-Cloud catalogue.
- Clear onboarding processes, including asset discovery, documentation intake and communication setup.

Purchasing Steps

1. Search for ROCK on the Digital Marketplace under: Managed IT Services - Cloud Support
2. Review the Service Definition, pricing document and terms.
3. Shortlist ROCK based on your technical, operational and commercial criteria.
4. Evaluate shortlisted suppliers following CCS guidance.
5. Award a Call-Off Contract directly to ROCK through G-Cloud 15.
6. Agree service scope and onboarding timelines with our mobilisation team.

Support with Procurement

ROCK can support buyers with:

- Responding to clarification questions
- Helping shape scope within the boundaries of G-Cloud
- Providing guidance on service levels, onboarding and shared responsibilities
- Supporting internal approvals or business case preparation

We remain fully compliant with CCS rules - no pre-award customisation of terms.





Your cybersecurity partner to reduce risk,
strengthen resilience and build trust.

rock.co.uk