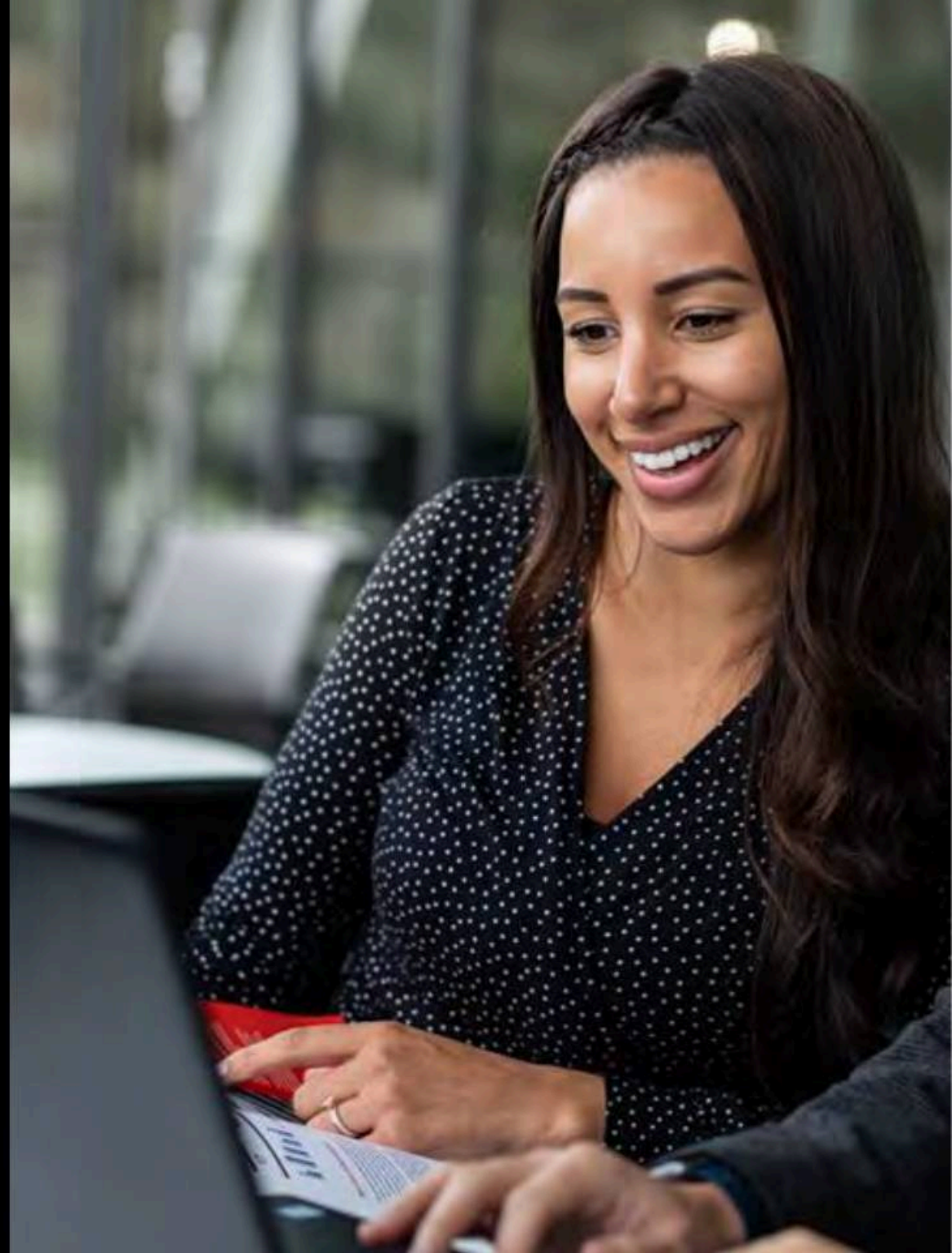


ROCK

Cynet Cybersecurity Platform

XDR & Threat Detection (SaaS)

Cynet



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 Cynet Cybersecurity Platform provides UK public-sector organisations with a natively automated XDR (Extended Detection and Response) capability.

We move beyond traditional reactive security to provide an all-in-one protection layer that covers your endpoints, users, networks, and cloud workloads through a single, intelligent agent.

In an era of sophisticated ransomware and state-sponsored threats, the detection to response window is the most critical metric for any CEO.

Cynet's AutoXDR™ technology is designed to close this window by autonomously investigating and remediating 90% of threats in under a second, ensuring that a single infected device never escalates into a catastrophic organisational outage.

The Executive Pillars of Cynet XDR:

All-in-One Consolidation

We eliminate the complexity tax. Cynet integrates Next-Gen Antivirus (NGAV), Endpoint Detection (EDR), Network Analytics (NDR), and User Behavior (UBA) into one platform, reducing your licensing overhead and operational friction.

Autonomous Remediation

Most platforms only alert; Cynet acts. The platform's "AutoXDR" engine automatically isolates infected hosts, kills malicious processes, and roll-backs ransomware changes before your team even receives the notification.

24/7 "CyOps" Strategic Support

Included at no extra cost, Cynet's elite CyOps MDR team acts as a permanent extension of your leadership. They provide human-led threat hunting and expert incident response guidance around the clock, protecting you 365 days a year.

Low-Impact Continuity

The platform uses a single, ultra-lightweight agent (consuming <1% CPU) that protects your staff's productivity while delivering enterprise-grade resilience.



“Threat detection and response are strengthened significantly, reducing exposure while improving security confidence across the organisation.”

Ian Elsbury, COO at ROCK

Our Approach

We move beyond traditional reactive security by providing an all-in-one autonomous breach protection platform. Our approach ensures that your endpoints, users, networks, and cloud workloads are protected by a single agent that prioritises prevention and automated resolution over manual analysis.

Phase 1: Rapid Deployment & Visibility

Goal: Eliminate blind spots and establish enterprise-grade protection in hours, not months.

Single-Agent Architecture

We deploy an ultra-lightweight agent (<1% CPU) across your entire estate. The approach is designed for zero disruption to staff productivity.

Immediate Visibility

Upon activation, Cynet begins sensor fusion correlating data from endpoints, user behaviour, and network traffic to create a baseline of your organisational normal.

Phase 2: Autonomous Prevention & Deception

Goal: Neutralise threats at machine speed before they can escalate into a breach.

AutoXDR™ Remediation

We use Cynet's autonomous engine to investigate and remediate 90% of threats in under a second. The platform doesn't just alert, it kills malicious processes and isolates infected hosts automatically.

Deception Technology

We deploy traps, decoy files, servers, and credentials, across your network. These lure attackers into a safe, isolated environment, exposing their tactics without risking your real assets.

Phase 3: 24/7 Expert-Backed Assurance

Goal: Provide human-led stress testing and expert support to augment your leadership.

Included MDR (CyOps)

Every Cynet deployment is backed by the 24/7 CyOps team elite threat hunters who monitor your environment around the clock. They act as a permanent, zero-cost extension of your security team.

Continuous threat hunting

While the AI manages the 90%, the CyOps team proactively hunts for the sophisticated hidden 10% of threats, ensuring absolute protection.

Key Features

The Cynet platform provides a natively unified suite of capabilities designed to protect your organisation's capital, data, and reputation through automation first security.

Natively Unified XDR

Cynet removes complexity by consolidating multiple security disciplines into a single platform.

Endpoint Protection (NGAV & EDR)

Advanced prevention of ransomware and malware, combined with deep-forensic visibility into every device on your network.

Network Detection & Response (NDR)

Monitoring of internal traffic to identify lateral movement (where an attacker moves from one compromised machine to your critical servers).

User & Entity Behaviour Analytics (UEBA)

AI-driven monitoring of user accounts to detect compromised credentials or insider threats (e.g., an employee accessing sensitive data at 3 AM).

Deception Technology

Strategically placed decoys (files, credentials, servers) that lure attackers into a safe trap, providing an early warning of a sophisticated breach before it touches real assets.

AutoXDR™: Autonomous Remediation Playbooks

Most platforms only generate alerts; Cynet acts. The platform's autonomous engine reduces manual handling by 90%.

Machine-Speed Response

Investigates and remediates threats in under a second. The system automatically isolates infected hosts, kills malicious processes, and disables compromised accounts.

Root Cause Analysis

Automatically maps the entire lifecycle of an attack, telling you exactly how it started, what it tried to do, and how it was stopped.

Remediation Playbooks

Pre-configured workflows that execute complex multi-step responses (e.g., isolate host, block IP and reset user password) without human intervention.

24/7 CyOps: Elite Managed Detection & Response (MDR)

Every deployment is backed by Cynet's global team of security experts, included at no additional cost.

Continuous Threat Hunting

Human experts proactively search your environment for hidden threats that bypass automated controls.

Incident Response Guidance

In the event of a high-severity alert, the CyOps team provides immediate, expert guidance to your leadership on containment and recovery.

Zero Salary Overhead

You gain the capability of a global Security Operations Centre (SOC) without the six-figure costs of hiring and retaining specialist cyber talent.

Key Benefits

Our Cynet 360 AutoXDR service provides a measurable return on investment by shifting your security from a manual, reactive cost centre to a high-speed, automated management control.

Radical Cost Consolidation (High ROI)

Elimination of the complexity

We replace multiple standalone security tools with a single, unified platform. The outcome is a 40-45% reduction in security buying costs and a significant decrease in vendor overhead.

Elite Talent at Zero Cost

Every deployment includes 24/7 CyOps MDR support. This provides you with a global team of threat hunters and incident responders without the six-figure salary costs of building an in-house SOC.

Absolute Risk Containment

Sub-Second Response

Human-led security is too slow for modern ransomware. Our autonomous engine investigates and remediates threats in under one second, isolating infected devices and killing malicious processes before they can move laterally through your network.

Minimised Dwell Time

By reducing the time an attacker spends in your environment, we drastically lower the potential cost of a breach. Every day saved in dwell time protects your organisation from the millions of pounds in damages typical of a prolonged incident.

Operational Simplicity & Productivity

Autopilot Security Operations

We free your IT team from the alert fatigue of thousands of false positives. Cynet's AI filters the noise, allowing your staff to focus on managing security strategy rather than operating technical tools.

Ultra-Lightweight Continuity

Our single-agent architecture consumes less than 1% CPU, ensuring that your staff's productivity is never compromised by the security software designed to protect them.

Defensible Governance & Trust

Board level transparency

We translate millions of technical data points into a single, intuitive dashboard. You gain a decision ready view of your security posture, showing exactly how threats were neutralised.

Sustained public trust

By ensuring continuous availability and data integrity, the outcome is the safeguarding of your organisation's reputation and its license to operate in the public eye.

Management & Governance

Our governance model for Cynet is designed for Operational Autonomy. We provide the platform, the onboarding, and the expert baseline, while the platform's native AI and Cynet's global SOC (CyOps) manage the high-frequency threat landscape.

Product Delivery Model

ROCK provides the license and launch capability, ensuring the platform is correctly integrated into your estate, but the ongoing eyes on screen monitoring is handled by the platform's autonomous logic and the included CyOps team.

Onboarding & Configuration

ROCK ensures the initial deployment is aligned with Cyber Essentials Plus and your organisational risk profile.

Platform Health Support

ROCK acts as your Tier-1 support for licensing, billing, and general platform availability queries.

Autopilot Operation

Once deployed, the platform operates independently. Your internal IT team remains the primary owner of the console, supported directly by Cynet's 24/7 experts.

The 24/7 CyOps Overlay

Even as a product-only purchase, you are never on your own. The service includes Cynet CyOps, a global Managed Detection and Response (MDR) team that acts as a native extension of the product.

Autonomous Escalation

If the platform detects a critical threat that requires human intervention, the CyOps team proactively contacts your designated leads with remediation instructions.

Incident Response Assistance

You have single click access to global security experts from within the dashboard for guided response during a crisis.

Continuous Governance

As your supplier, ROCK provides the admin guardrails to ensure the product remains a high-value asset.

Quarterly Account Reviews

We meet with your leadership to review license utilisation and ensure you are gaining maximum value from the platform's feature set.

Subscription Lifecycle Management

We manage the renewal and scaling process, ensuring your protection grows in line with your organisational expansion.

Outcome Documentation

We ensure you have access to the automated compliance reports (ISO 27001, NIST) generated by the platform for your annual audits.

Security & Data Protection

We manage your security data under a Secure by Design philosophy. Since this is a Product-Only Provision, the data is protected by Cynet's native, multi-layered security framework, hosted on high-availability AWS infrastructure.

Data Sovereignty & Encryption

All telemetry, including process executions, file modifications, and network connections, is encrypted at rest using AES-256 and in transit via TLS 1.2+.

Cynet production workloads run across multi-region AWS environments. For UK public-sector clients, the outcome is the ability to align data storage with protected jurisdictions, supporting UK GDPR and Data Protection Act requirements.

Multi-Tenant Isolation & Integrity

Cynet utilises a dedicated schema per customer. This ensures that your organisational risk data is logically isolated from all other tenants, preventing any cross-talk or unauthorised access between environments.

Every action performed within your dashboard whether by your IT team or the 24/7 CyOps experts, is fully logged. You have real-time access to audit information, ensuring complete accountability for all security operations.

Access Control & Personnel Vetting

Access to the Cynet management console is governed by Role-Based Access Control (RBAC) and enforced with mandatory Multi-Factor Authentication (MFA) and SSO integration.

The 24/7 CyOps personnel who support your environment operate under strict Least Privilege protocols. They only access your environment for active investigations or support, and all such access is audited and logged.

Resilience & Continuous Testing

The platform is built on an EKS-based microservices architecture, providing a 99.9% SLA for system uptime. Your protection is always on backed by automated daily backups and multi-week retention.

Cynet undergoes external Penetration Testing at least every 6 months. The outcome is a platform that is continuously stress-tested against the same tactics it is designed to block.



Resilience & Availability

In the public sector, downtime is more than a technical failure, it is a disruption of essential services.

ROCK's Cynet provision is engineered for uninterrupted protection, ensuring that your defensive shield is as resilient as the infrastructure it protects.

Availability & Uptime Guarantee

Always on protection

The Cynet SaaS platform is hosted on a globally distributed, high-availability AWS architecture. With a target of 100% availability and a financially backed 99.9% SLA, the outcome is the assurance that your security monitoring never goes dark.

Machine-Speed Continuity

Resilience is defined by the speed of recovery. Cynet's AutoXDR™ engine is designed to isolate threats and roll back unauthorised changes (such as ransomware encryption) in under one second, ensuring your operations continue without manual intervention.

Human Resilience

Guaranteed Response Cadence.

Included in the product is 24/7 access to CyOps, Cynet's elite MDR team. They provide a documented 2-hour response commitment for critical incidents, ensuring you have expert guidance when you need it most.

Heartbeat Monitoring

The CyOps team continuously monitors the health of your Cynet deployment. If a server's security heartbeat is lost, the outcome is an immediate proactive outreach to your team to remediate connection issues before a gap in coverage occurs.

Data & Configuration Resilience

Immutable Security Intelligence

Your security configurations and incident logs are protected by automated daily backups and multi-region redundancy. The outcome is a permanent, ransomware-proof audit trail that remains available for forensic analysis or regulatory review.

Low-Impact Performance

The Cynet agent is designed for operational resilience, consuming less than 1% CPU. The outcome is a security layer that protects the organisation without degrading the performance of the critical applications your staff rely on.

Data Management, Portability & Exit

We manage your security data under the principle of "Metadata Sovereignty." Since this is a product only offering, the platform is engineered to store only the technical telemetry required for protection, ensuring your organisational privacy is maintained by design.

Data Governance & Sovereignty

Guaranteed Residency

Cynet 360 is a cloud-native SaaS platform hosted on AWS. For UK public-sector clients, the outcome is the ability to ensure that data storage and processing remain within UK/ EEA jurisdictions, satisfying all UK GDPR and Data Protection Act 2018 obligations.

Logical Isolation

Your data is stored in a dedicated schema per customer. This ensures absolute data isolation, preventing cross-talk between different organisations and providing a clean, auditable boundary for your risk intelligence.

Data Retention & Auditability

Transparent History

The platform maintains system logs and user audit data for a standard period (typically 6 to 12 months). The outcome is a permanent, defensible record of every security event and administrative action, ready for audit.

Granular Control

Your internal IT team has real-time access to these audit logs, ensuring that who, what, and when is always visible at the click of a button.

Data Portability & End-of-Contract Transition

We recognise that agility is a core requirement for public-sector leadership. Our approach ensures you maintain full control over your data lifecycle:

Frictionless Extraction

During the term of the contract, you can export your alert data, incident reports, and system logs via the Cynet console or API. This ensures you can integrate your security intelligence with other internal business systems or long-term archives.

Secure a Clean Exit

Upon contract termination, the outcome is a formal decommissioning process. The SaaS tenant is terminated, and all customer data is permanently deleted from the AWS production environment. This prevents "data residue" and ensures your risk blueprint does not exist beyond the life of the agreement.

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