Roc

roctechnologies.com

Roc Cyber Security

Evolving business resilience to enable secure transformation and growth

Protecting your organisation against cyber threats is a moving target. Cyber threats are not just relentless, they are continually evolving, exploiting new and unconsidered vulnerabilities, be they technology or human. But the tools we use to protect against these threats are also advancing rapidly – leaving IT teams struggling to ensure they have the right skills and experience. And with the exploitation of AI making the technology that enables these crimes more accessible, more affordable and more scalable than ever before, it's clear why cyber security remains the top priority for IT leaders.

Knowing how and where to focus your efforts and resources is vital.

At Roc, we work in partnership with you, to understand what's critical, and what outcomes you need to keep your people and data safe. We offer a wide breadth of services - from cyber readiness to full critical incident support – and align our solutions to your needs, whether that is enhancing or extending existing capabilities or using our vast experience and knowledge to support in the areas you need. The result is a continually evolving, high impact, strategic solution to cyber security that offers your business support and protection where it matters most.

Cyber protection: more than just business resilience

The risks are real. Cybercrime continues to be a significant threat to organisations, costing the UK approximately £27bn annually.

But it's not just financial loss: it's about data loss and the compromise of critical IP; reputational damage and the loss of customer trust; and about service disruptions and loss of revenue generation functions, which ultimately impact an organisation's bottom line and ambitions for longer term growth.

That's why cyber security shouldn't be deemed as an additional layer to an IT strategy, but regarded as a strategic driver - and an indicator of a business's success. With the pace of technological change accelerating, and with technology driving competitive advantage, a comprehensive cyber security strategy is essential. Why? Because it doesn't just protect your business from threats, it provides a resilient digital foundation from which you can accelerate digital transformation, pre-empt risks and ultimately protect your bottom line.

At Roc, we work to understand your specific, long term business objectives and build our services by use-case. We remove technical complexity and accelerate implementation - getting you protected faster, by:

- Identifying technology, services and compliance gaps within an end user environment
- Providing strategic insights and tailored recommendations, delivering unparalleled value.
- Identifying potential vulnerabilities within systems and networks, ensuring these are proactively addressed and any potential risks are mitigated before exploitation by malicious actors.
- Providing organisations with the insight and intelligence you need to make informed decisions around cybersecurity investments, helping to prioritise risk mitigation efforts and allocate resources effectively.

By doing this, we help you to establish a cyber security foundation as a fundamental, fully integrated part of your business risk and investment strategy.

"Our customer success is underpinned by technical excellence and our expertise in delivering within secure and governed environments – where the protection and integrity of data is critical."

Chelsea Chamberlin, CTO, Roc

Supporting your cyber security journey

We have designed and structured a portfolio to answer your strategic challenges at all stages of your cyber security journey.

Readiness

Our readiness portfolio offers a series of assessment tools that deliver actionable insight into your organisations current and future risks and vulnerabilities, helping you understand and meet compliance requirements and prepare for the adoption and integration of new technologies.

Prevention

Bringing together best of breed technologies from Tier 1 global vendors, as well as bespoke, subject matter experts, we deliver comprehensive, solution based, protection across your infrastructure against internal and external threat actors.

Managed detection and response

Highly scalable services designed to extend and enhance your internal cyber security capabilities according to your needs, delivered through Roc's in-house 24/7/365 Security Operations Centre, including rapid detection and response to the management and mitigation of active or potential security incidents.

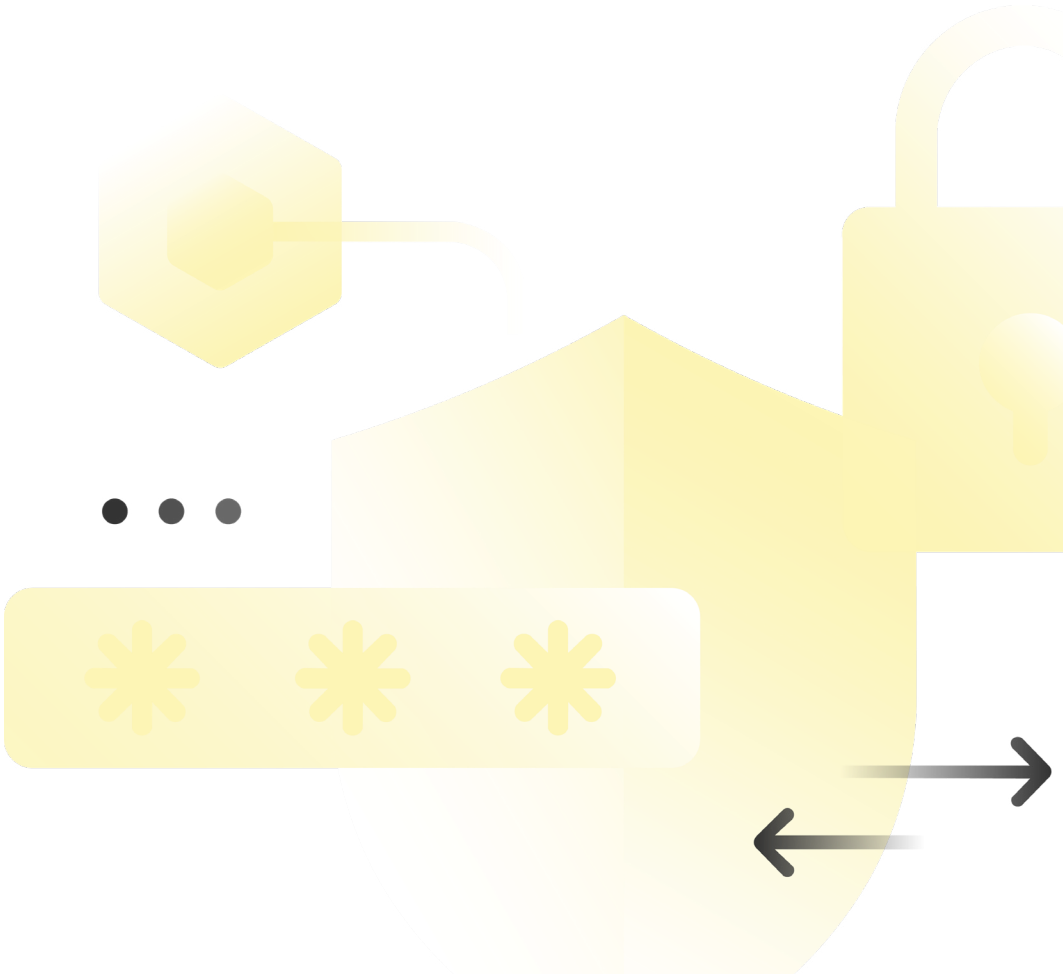
Critical incident support

Corporate response and specialist expertise to support your business when dealing with a serious breach, including crisis communications, ransomware negotiation and legal advice.

Readiness

Cyber readiness is the cornerstone of your cyber security strategy, helping you to identify the strengths and weaknesses in your approach and policies, as well as prepare for and assess the impact of major changes to your digital estate. Readiness also extends to your existing infrastructure, auditing and testing to identify specific vulnerabilities and finding opportunities to improve.

From a regulatory point of view, with a full audit trail delivered with all our services, you can demonstrate your readiness for cyber accreditations and offer evidence for insurance purposes.



Cyber Readiness Assessments

Our Cyber Readiness Assessment goes beyond questionnaires and check-boxes, employing multiple technical tools to monitor your applications and networks in real time. This allows us to create an holistic view of cyber risks, strengths, weaknesses and deliver a tailored, context-driven report with actionable intelligence that can be used as a basis for your cyber improvement plan.

Assess risks in realtime

We establish a detailed understanding of your organisation's cyber risk using our own comprehensive security assessment, alongside evaluation by our own experts, to gather strategic insights.

Then, we deploy on-premises read-only data collectors and scan in-scope assets to gather information from your systems in realtime and assess your external facing assets to identify and potential vulnerabilities. This identifies the potential for exploitation of your systems and networks by malicious actors. A full report is provided which can be used to support ISO 27001 and CES accreditation. This level of assessment is also a helpful reference point for cyber insurers.

Helping you prioritise risks

Utilising these insights, we work with you to identify where your cyber resources are best allocated for maximum effectiveness. We provide you with tailored recommendations that allow for proactive remediation and further risk mitigation.

Areas explored include but are not limited to:

- Asset Management
- Email security
- Privileged access
- Cloud application security
- External attack surface
- Brand and third party reputation
- Exposed credentials
- Compliance analysis

Vulnerability Management Planning

How prepared is your organisation to identify and respond to cyber threats?

Many organisations assume that conducting vulnerability scans is sufficient to understand how, when, and why attacks may occur; however, a scan is exactly that – an automated process to find common vulnerabilities.

At Roc, we go further. Our analysis of your estate allows us to discover, prioritise, and remediate vulnerabilities and misconfigurations. This contributes to your internal risk management approach, provides cost effective patch management, protects you from OS vulnerabilities and provides valuable input into your corporate risk register.

Pen Testing

For additional depth, Roc also offers Pen Testing, also known as Ethical Hacking. The objective of a Pen Test is to simulate the actions of a malicious threat actor in order to identify vulnerabilities within applications and services. Put simply, a Pen Test is an authorised attack, simulating what a hacker would do by gaining access, reaching the point of simulating a malicious act and reporting to the business what was achieved and how the vulnerability was exploited.

Delivering both an executive summary and detailed technical report, you will gain a deep understanding of your cyber risk exposure, allowing you to prioritise cyber investment and understand the gaps that may need to be filled to meet regulatory requirements.

Roc's cyber consultancy team can work with you to plan a path to mitigating high, medium, and low risks, in order of priority and based on alignment to your cyber security strategy.

Types of Pen Test

Web App
Exploting weaknesses within your website

WiFi
Identifying weaknesses within your internal wifi networks

Internal
Assessing your internal infrastructure

External
Testing your perimeter and public facing networks

Vulnerability Management Planning

AI assurance and Readiness

Are your AI systems trustworthy? We provide you with testing for AI application security, data leakage via prompts, hallucination and model poisoning.

We also offer an AI Readiness assessment, which focuses on protecting, structuring, and managing your data in a way that means you can safely leverage the use of AI Technology (such as Microsoft Co-Pilot), while mitigating the threat of data leakage internally.

In order to achieve this, we conduct a thorough assessment, including stakeholder wokrshops, and technology audits, ensuring your are leveraging existing licenses and technology sufficiently to protect your data, examples include:

- Privileged Identity Management
- Data Tagging
- Data Storage, including locations and user access
- Use and access of Outlook, SharePoint, and Exchange Online

The outcome of this is a fully documented approach, with clear steps, to ensure your organisation is fully ready, and protected, at the point of deploying AI technology – which is becoming a necessity to achieve organisational growth and enhance productivity.

Cyber incident exercise

Boost your readiness and validate your Incident Response plan with a full scale Cyber Incident exercise. By simulating a breach, you can assess your team, your process and the effectiveness of your technology while keeping track of incremental improvements.

This will allow you to test and strengthen allowing identification, remediation and recovery processes.

Accreditation Support

Consider Roc your virtual Chief Information Security Officer (CISO). We will work in partnership with your team to build out your accreditation strategy.

Your organisation will receive gap analysis, remediation planning and audit support, in person. Our consultation will help you achieve and maintain your key accreditations, such as Cyber Essentials, Cyber Essentials Plus and ISO 27001 as well as to develop your corporate policies and help you put the necessary controls in place.

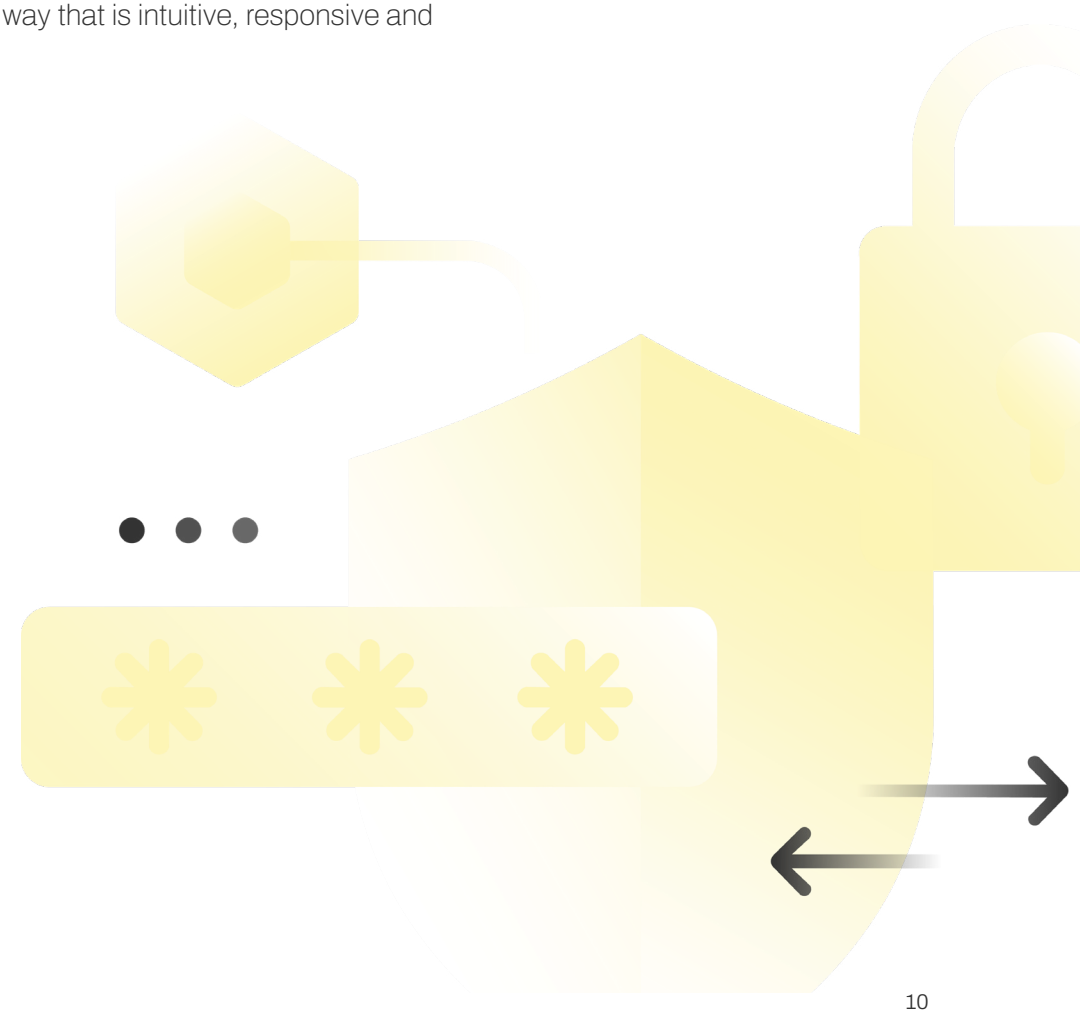
What's more, we can help with advice on changing laws and regulations, in the context of your business, so that you can ensure your cyber strategy is fully aligned and your business is fully compliant.

Prevention

Traditionally, perimeter protection against unauthorised actors – such as hackers, bots and other threats - has been handled by externally facing, on premise firewalls. However, the cyber security landscape has become more complex: cloud computing, IoT, integrated supply chains and hybrid work environments have blurred the boundary lines, making it almost impossible to define a perimeter.

An advanced, multi-faceted approach is needed.

At Roc we partner with best of breed, Tier 1 global security vendors, meaning we can deliver a range of firewall technologies, access control solutions and zero trust solutions, and AI-powered services to strengthen your network in a way that is intuitive, responsive and intelligent.



Perimeter Security

Protect your organisation from external network attacks, Denial of Service attacks, data leakage, DNS attacks, intrusion and attacks on your cloud environments. Roc designs and implements physical and logical controls in line with industry best practice, secure by design standards and our own experience working in highly governed and secure industries, to make sure you have the best protection possible at the demarcation between your digital assets, the internet and your third parties. As our customers move to cloud, SaaS and hybrid environments with a truly mobile user base, the network perimeter can be hard to define. Roc helps to establish digital demarcation points and implement appropriate controls to make sure you can exchange data and provide access to your networks securely and safely.

Technical Controls

Roc works alongside our industry-leading technology partners to design and implement security solutions which integrate with your environment and work together to give you the highest levels of protection from cyber risk and visibility of threats.

Our solutions include:

- Endpoint Protection
- XDR
- Cloud Security Posture Management (CSPM)
- User and Entity Behavioural Analysis (UEBA)
- Identity Protection
- Third Party Risk Management (TPRM)
- Network Security Management
- Intrusion Prevention
- Dark Web Monitoring

SASE (Secure Access Service Edge)

Our design and implementation of SASE solutions gives you Software Defined Networks (SDN), Virtual perimeter security, Self provisioning, Central management and Utilisation reporting. Working with a small number of carefully selected technology partners, we will deliver and manage all the benefits of a SASE solution for you. SASE from Roc removes the necessity to build complex, dynamically routed networks for failover and load balancing, and automates the process of enabling services or an entire new site so that changes can be made in minutes.

Roc work with you to design traffic flow models and make sure your data is delivered in the most efficient was possible no matter how many sites you have, and we ensure that the right security controls are effective, tested, and applied uniformly.

SASE for Roc means enabling any user, to work from any location, with any device in a completely secure and resilient way, enabling business continuity and maximising productivity.

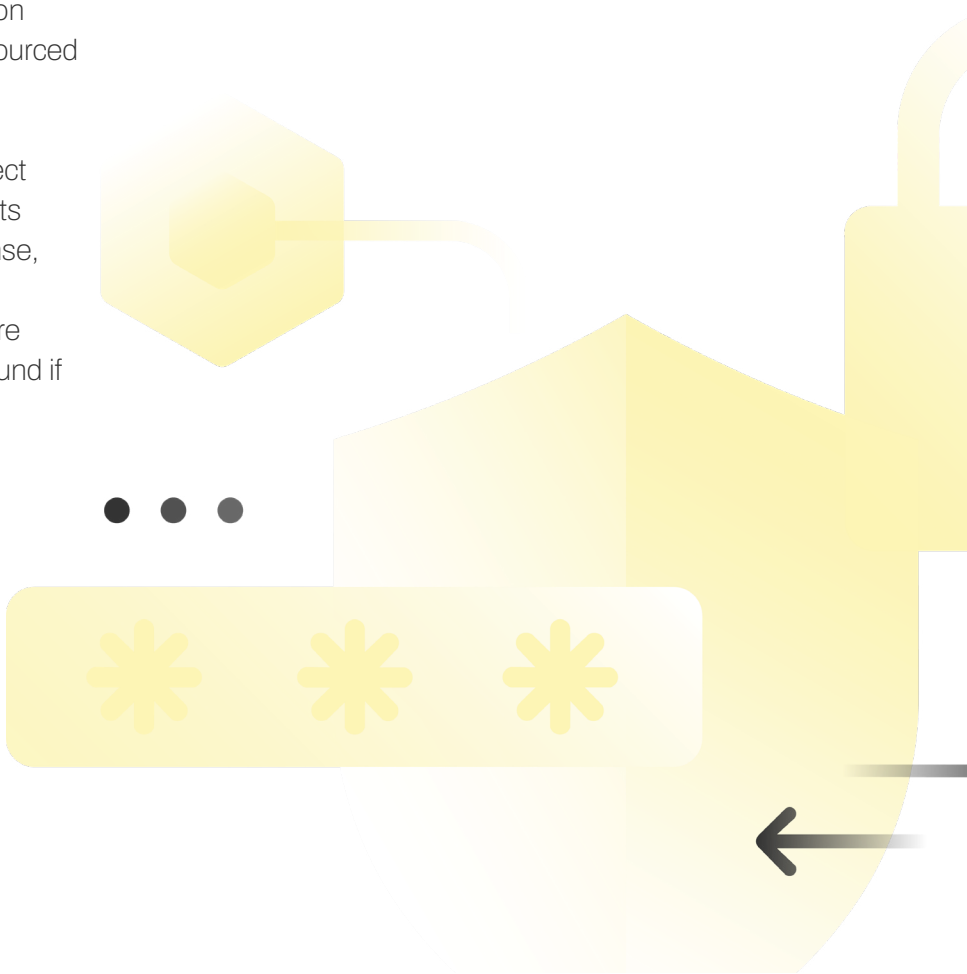
Managed Detection and Response

Knowing you have been hacked is often the first challenge to overcome. Whilst some attacks – notably ransomware – are public proclamations of a breach, most attacks are silent, pervasive. Today, it takes an average of 194 days to identify a data breach according to IBM, costing companies millions - and the longer an attack goes on, the greater the damage it inflicts.

That's why early detection is essential. Through our in-house SOC, Roc offers a variety of services to support with your organisation, expanding, extending and enhancing your existing detection and response capabilities according to the needs of your business.

We offer complete flexibility in our adoption models, with an entry level monitoring and notification service through to a fully outsourced Security Operations Centre. Through our scalable service model, Roc can help you detect any potential or active incidents and coordinate a rapid response, including technical support, monitoring critical infrastructure and provide teams on the ground if necessary.

- 24/7/365 in-house SOC
- All our SOC analysts are cleared to BPSS, SC or DV levels, for the most rigorous levels of security for your data and systems
- >60% engineers DV cleared
- Google SecOps and Microsoft Sentinel
- Multiple consumption models available:
  - Supply
  - Platform as a Service
  - SOC as a Service



SOC Foundation

SOC Foundation offer is an entry level service giving organisations access to 24/7/365 monitoring capability at an accessible price. The service makes maximum use of your existing tools, increasing your ROI, and includes the opportunity to add additional response services, should your organisation need them, at compelling rates.

- Fixed cost of just £5000 per annum + £1500 onboarding for up to 1000 users**
- 24/7/365 monitoring and alerts delivered by our in-house team, meaning you can respond to an attack immediately
- If a breach happens you can access our incident responders on demand at a pre-agreed, fixed rate
- The service supports your accreditations and may help reduce the cost of your cyber-Insurance

Our Soc Foundation provides all organisations, no matter their size, with the opportunity to leverage their cyber tooling investment 24/7/365., mitigating the threat of an undetected breach without the cost of a full Security Operations Managed Service.

SOC Service Packages

Security Operations is not a 'one size fits all', and we believe organisations should be allowed flexibility in their Cyber Services portfolio. That's why, Roc has developed a SOC offering which allows organisations to tailor their package based on their business needs and strategic outcomes.

		Standard	Enhanced	Elite
Monitoring and Alerts	Delivered through the Roc in-house SOC team	0900 - 1700 Monday - Friday	24/7/365	34/7/365
Onboarding	Services included as part of your onboarding include:	✓	✓	✓
Ongoing rule and playbook creation	This service offers the development of analytics rules, automated responses and triggers to key incidents within your SOC	Optional	✓	✓
Continual tuning	Ongoing review and development of detection mechanisms and threat intelligence	Optional	✓	✓
Parser and ingestion support	Supporting the transfer of data from multiple sources across the network estate in the SOC	Optional	✓	✓
Platform support	Ongoing management and maintenance of your SOC platform	✓	✓	✓
Dashboard creation and support	Development of visual tools for at a glance analysis and reporting	✓	✓	✓
Threat research and hunting	Proactive identification of previously unknown, or ongoing non-remediated threats, within an organisation's network	✓	✓	✓
SecDevOps	Supporting your teams with bespoke integrations, automations and data extraction and transformation	Optional	Optional	✓
Incident Response	Technical response and remediation to incidents	Optional	Optional	✓
AI guardrails	Development of safeguards to put in place to prevent customer articificial intelligence (AI) models from causing harm to your organisation	Optional	Optional	Optional

Critical incident support

If a serious breach does take place, having a robust business continuity and disaster recovery plan is critical. Roc can help you manage and control the broader impact on your business, mitigating further risk, protecting your reputation and avoiding financial penalties.

In addition to on the ground technical experts to support your in-house teams, we can provide corporate specialists to cover all aspect of support, from crisis communications and reputation management to compliance and legal advice to asset tracing and investigations.

Our capabilities include:

Incident Management

Onsite technical specialists up to and including NCSC Level 2 responders working with your team to detect and remediate the threat, and recover your systems and data.

Threat analysis and removal

Establishing a definitive answer as to what caused the breach, and removing all infection or malicious presence from your digital estate, with remediation to prevent further attacks.

Impact assessment

A full and thorough tracking of activity, residency and data loss.

Law enforcement liaison

Reporting of criminal activity, ongoing updates and data handling to PACE requirements.

Specialist corporate support:

- Asset tracing and recovery – helping you to recover stolen data
- Cryptocurrency investigations – tracing and recovering stolen or ransomed crypto funds
- Threat intelligence – researching specific threats
- Digital evidence gathering and reporting – compilation of dossiers to support prosecution, offering forensic investigation to PACE standards
- Internal investigation support – offering discrete support for sensitive or internal user data leaks
- Legislation and regulation support – offering representation and liaison with legal bodies
- Reputation management – take-down handling and malicious content tracking, recovery from data breaches, addressing cyber squatting and misinformation

Roc: Delivering tangible outcomes

At Roc, security is at the forefront of everything we do. We have supported some of the UK's most secure and complex organisations for more than a decade, ensuring their long-term success and growth. We understand that the protection of your data, assets, processes and systems is critical.

Our people host a wealth of cross-industry experience, advising, monitoring, securing and building resilient digital infrastructures for our customers, as well as safeguarding their valuable assets.

We also understand that every organisation's infrastructure and system requirements are unique, which is why we tailor your solution to your organisation's specific requirements, employing best-of-breed technologies that deliver measurable, tangible outcomes along the way.

A diverse, global security foundation

Universal SC to DV clearance in technical teams

24/7/365

UK based Secure Operations Centre

Highly flexible and scalable security services portfolio

National in-house field services capability

Strategic partnerships with world leading cyber-focused technology partners

Find out more about how Roc can help secure your business.

Contact us today or visit our website at www.roctechnologies.com

Roc Technologies Limited
1 Lindenmuth Way, Greenham Business Park
Greenham, Thatcham, RG19 6AD

0845 647 6000
roctechnologies.com