

SOC

SECURITY OPERATIONS CENTRE

Comprehensive Threat Management
for Complete Security

reflectiveit.com/SOC



Microsoft Partner
Silver Cloud Productivity
Silver Small and Midmarket Cloud Solutions

What is a Security Operations Centre (SOC)?

A SOC is your most important defence against cyber-attacks.



A qualified team of cyber security experts who proactively **monitor and protect** your business from cyber-attack around the clock.

Who Needs a SOC?

1 Startups

Growing startups need to protect their expanding digital footprint. Our SOC offers scalable security that grows with you and as your threats grow.

2 Small Businesses

70% of cyber attacks are targeted at small and medium businesses. Our SOC protects you without you needing in-house resources.

3 Medium-Sized Enterprises

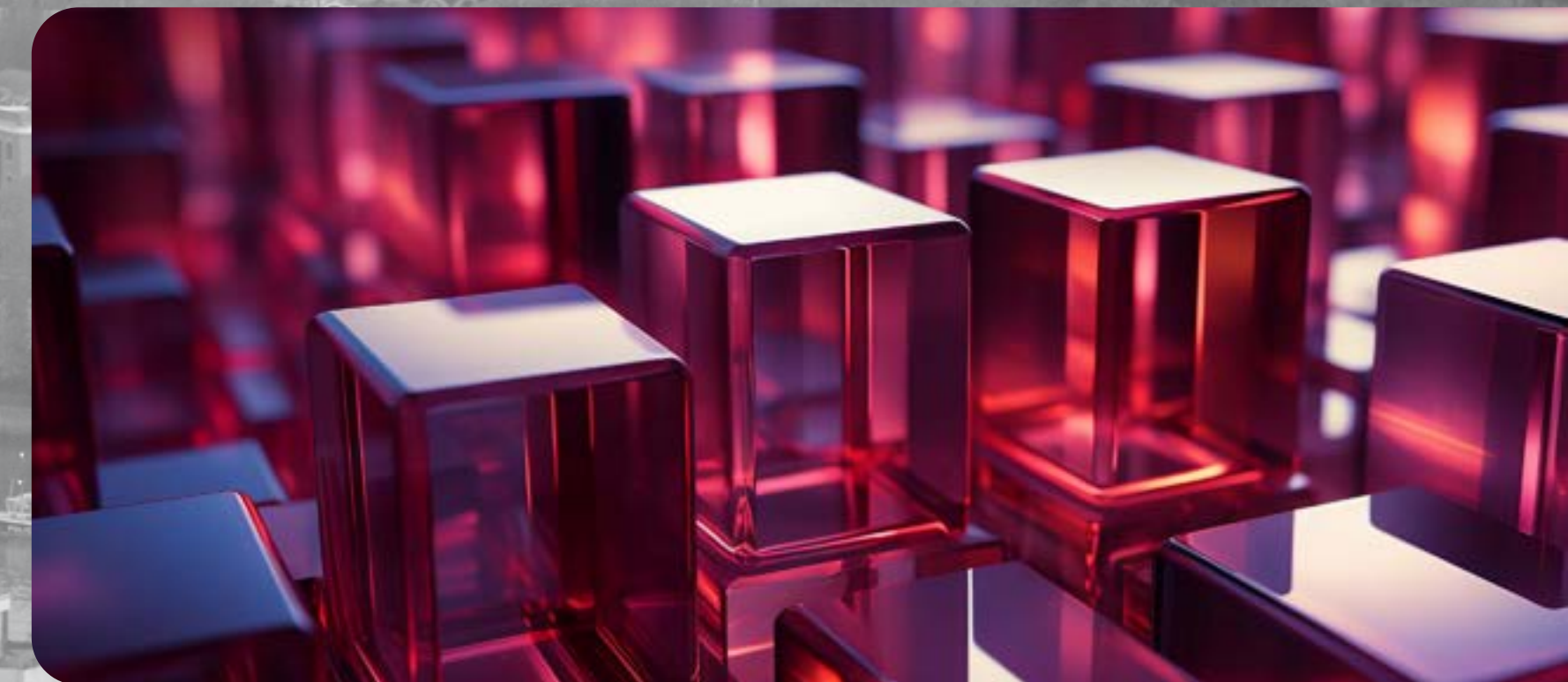
As your business grows, so do the risks. Our SOC ensures comprehensive protection for mid-sized companies.

4 Large Enterprises

Big businesses face complex security challenges. Our SOC delivers advanced threat monitoring, detection and response for extensive IT infrastructures.

5 Organisations with Limited IT Resources

Companies without dedicated cyber security teams can outsource some or all of their requirements to us.



Benefits of an Outsourced SOC

Cost-Effectiveness

Avoid the upfront costs to recruit, train, manage and optimise a large team of cyber security engineers.

24 x 7 x 365 Protection

Enjoy peace of mind from around-the-clock AI protection and expert human monitoring.

Access Cyber Security Expertise

Gain access to the technical knowledge of our cyber security professionals.

Enhanced Threat Protection

Benefit from our experience in combatting threats across multiple organisations.

Scalability

Be able to easily adapt your security as your business grows and as threats grow.

You Are Free To Focus On Growth

Be free to concentrate on your business while we handle cyber security attacks for you.

Be Immediately Protected

We will have protections in place for you within hours.

Achieve real and meaningful business outcomes

01.

Minimise upfront costs

Avoid the large expenditure required to recruit, train and optimise a team of 24 x 7 x 365 cyber security engineers.

02.

Stakeholder assurance

Customer, shareholders, partners, employees and your supply chain can be confident that you detect and respond to cyber-attacks.

03.

Reputation management

We carefully help you manage your reputation with customers and stakeholders during a cyber attack.



04.

Operational continuity

Should an attack bypass your defences, we help you recover with the confidence that the attack is contained.

05.

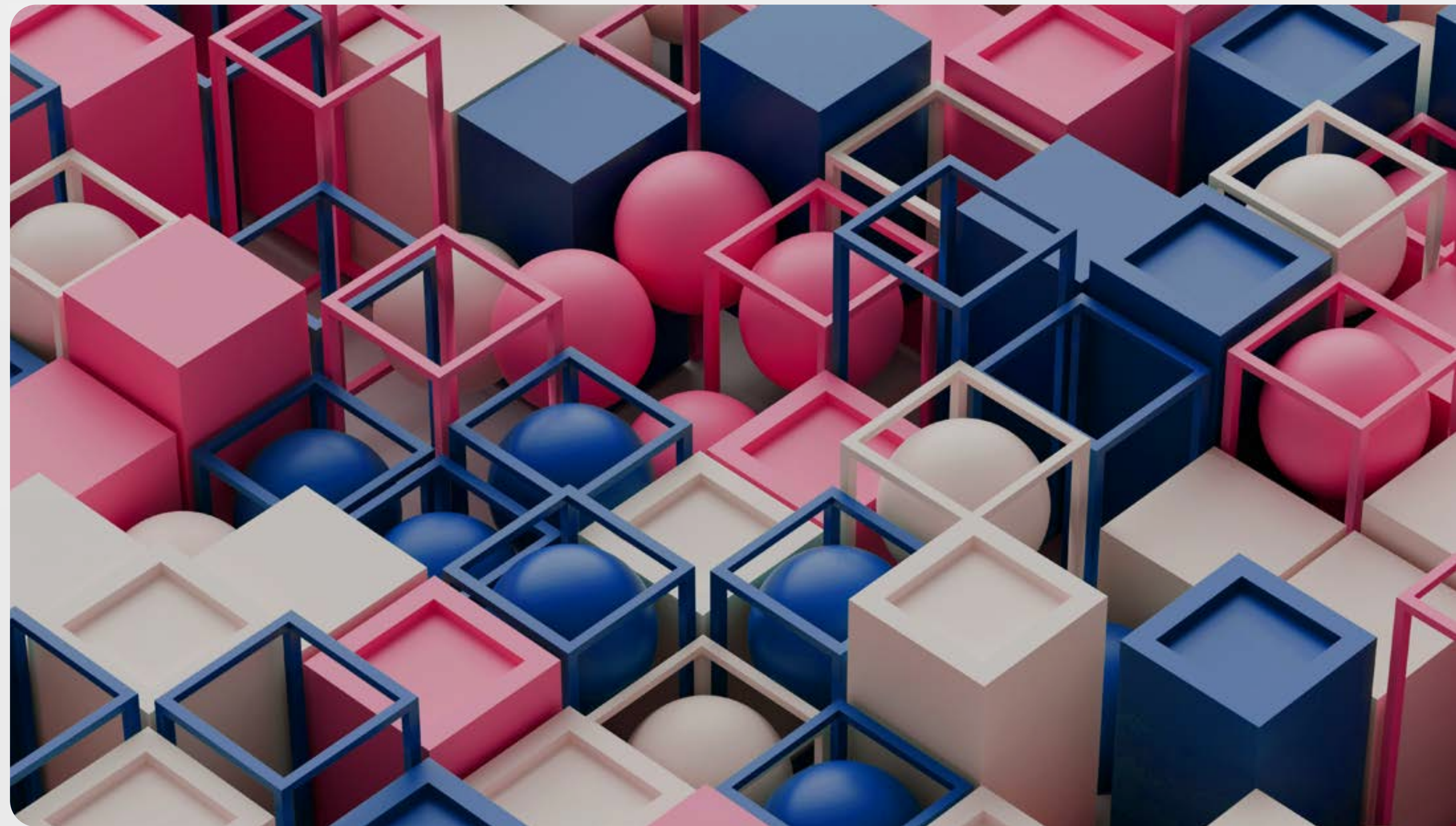
Reduced cyber insurance

Incident detection & response is increasingly a requirement of cyber insurance providers.

How we can protect you from cyber-attack

✓ CORE SOC SERVICES

- Managed incident detection & response (MDR)
- SOC as a Service (SOCaaS)
- XDR, SIEM and SOAR
- Proactive threat hunting
- Threat management
- Vulnerability management
- Attack surface reduction
- Penetration testing / red teaming
- Ransomware protection
- Malware analysis





Comprehensive Managed Incident Detection & Response for Complete Security

Our SOC doesn't just respond to threats,
it proactively prevents them.

We ensure the security of your IT environments through
continuous monitoring, proactive threat hunting and real- time
vulnerability assessments.

Managed Detection & Response

Our SOC delivers for you all the way through the cyber incident lifecycle:

From detection to recovery

03

Threat Containment

When a threat is detected, immediate action is taken to neutralise it, reducing the risk of prolonged system outages and safeguarding your business's reputation.

01

24x7x365 Always-On Monitoring

The majority of attacks are observed to be outside of business hours, so it is vital your IT environments are protected around the clock.

02

Rapid Threat Identification

Potential threats are quickly identified and addressed before they can disrupt your operations, minimising downtime and preventing data loss.

04

In-Depth Incident Analysis

Gain a clear understanding of each security incident with a detailed analysis that identifies any underlying issue so you can strengthen your defences against future attacks.

05

Clear and Actionable Reporting

Stay informed with transparent reports that provide actionable insights. These enable you to make risk-assessed decisions to continuously improve your cybersecurity posture.

Advanced cyber security protection you can rely on

You need more than just security tools. Our SOC provides a complete solution that redefines how your business approaches cyber security, ensuring you are always protected.

How we protect you:

1 Complete Incident Management

Our experts handle every aspect of your security end to end, from 24 x 7 monitoring to resolution.

2 Integrated Solutions

We seamlessly integrate with your existing Microsoft environment, which reduces risk and cost.

3 Beyond Endpoint Security

Protect all your network components, including servers, IoT devices, and firewalls.

4 Proactive Threat Prevention

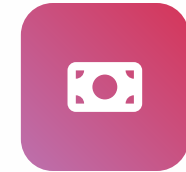
Stay ahead of emerging threats with advanced intelligence, data and analytics.



Seamless integration with your existing Microsoft environment

Our Security Operations Centre (SOC) integrates with your existing Microsoft infrastructure, allowing you to enhance your cybersecurity posture without additional software purchases. This ensures your business can leverage its current investments in Microsoft technologies while benefiting from comprehensive security coverage.

Why This Matters:



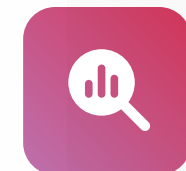
Cost-Efficiency

By utilising your existing Microsoft licenses, you avoid the expense and complexity of acquiring and managing additional security software. This makes our SOC an economical choice for businesses already using Microsoft products.



Unified Security Environment

Integration with your Microsoft infrastructure centralises all security operations, providing seamless monitoring and management across your entire digital ecosystem.



Optimised Performance

Our SOC is optimised to work within the Microsoft environment, ensuring that security measures do not hinder the performance of your IT systems but instead enhance their efficiency and reliability.

Take your cyber security strategy to the next level

Reflective IT has helped businesses like yours stay protected from cyber threats for over two decades.

Our Security Operations Centre (SOC) aligns to the best security and quality frameworks available globally



ISO 27001: This standard ensures that your business implements best practices for protecting sensitive information and enhancing trust and security through a systematic approach.



ISO 9001: Focused on quality management, ISO 9001 supports continuously improving your security processes, ensuring they evolve to meet new threats.



NIST CSF: This framework provides structured guidelines for managing cybersecurity risks, helping your business adopt best practices to enhance resilience against attacks.



MITRE: Leveraging the MITRE ATT&CK framework helps your business anticipate and defend against cyber threats by understanding and countering real-world adversarial tactics.

Why we leverage the MITRE ATT&CK framework for you

The MITRE ATT&CK framework is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies across all industries globally



Leveraging Community Knowledge

Proactively prevent breaches by addressing common attack patterns shared by the security community.



Real-Time Response and Recovery

Ensure faster recovery and reduce financial impact with rapid threat neutralisation.



Industry Specific Security Posture

You get industry specific knowledge and expertise to ensure common industry weaknesses and attacks are mitigated.



Enhanced Analysis

The framework helps us identify patterns and behaviours associated with advanced threats, leading to more accurate and timely identification.

Designed for peace of mind

Our clients choose us because they have trust in what we do.

We address industry-specific challenges and as a partner handle your cyber security, enabling you to focus on innovation and growth.



Our total defence approach, future-ready technologies, and long-term cost benefits ensure that your organisation is well-equipped to face cyber security challenges.

Seamless Integration and Ongoing Optimisation

Starting with Reflective IT's SOC service is easy:



Initial Assessment

Comprehensive evaluation of your current security infrastructure.



Integration

We'll integrate into your existing environment and immediately get to work.



Continuous Monitoring

We conduct in-depth investigations to understand the impact of incidents.



Regular Reporting

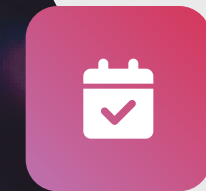
We'll provide detailed recommendations and full transparency.



Ongoing Optimisation

Continuous improvements based on the latest threat intelligence.

How we will welcome you to our Security Operations Centre



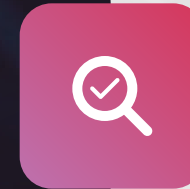
Step 1: Initial Consultation and Assessment



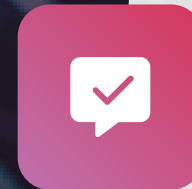
Step 2: Customised Security Plan Development



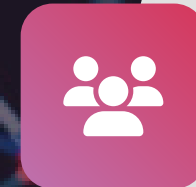
Step 3: Implementation and Integration



Step 4: Continuous Monitoring and Proactive Threat Hunting



Step 5: Ongoing Support and Optimisation



Step 6: Training and Knowledge Transfer



Step 7: Long-Term Partnership

Meet the Team



David Hartup
Founder and Managing Director

IT professional with over 20 years' experience in IT strategy, IT management and services delivery.



Stephen Holmes
Head of Cyber Security

Over 20 years' experience leading cyber security strategy and building cyber security operations teams.

- ✓ Established in 2003, based in London with global coverage
- ✓ Cyber security operations and managed IT services provider
- ✓ Microsoft Cloud Partner - access to the latest tools and technologies as they are released
- ✓ ISO 27001:2022 and ISO 9001 Certified
- ✓ Deep security expertise across a wide range of technologies



Get in touch

With a **98% client retention rate** and a strong reputation for excellence working to globally recognised frameworks, we are a safe choice to help manage your cyber threats and reduce your risk.

Protect your business today

Reach out to us at:

0207 317 4535

sales@reflectiveit.com

And take the first step towards
a secure digital future.

Disclaimer. This document is for informational purposes only and does not form part of any official recommendations by Reflective IT. While every effort has been made to ensure the accuracy and reliability of the information provided, Reflective IT does not accept any responsibility or liability for any errors or omissions, or for any loss or damage that may arise from reliance on this information. Should the receiving organisation fall victim to a phishing attack or any other cyber security breach, Reflective IT is indemnified from any claims, damages, or legal actions. For specific advice or assistance, please contact Reflective IT directly.