Solution Brief

Security Services

Powered by Reliance ACSN

Mitigate risk and protect your organisation. With rapid growth in endpoints, data volumes, cloud, and the overall complexity of the data centre, security isn't easy. Organisations have to evaluate the amount of protection they need based on their environment, budget, and the level of risk they can safely assume. Simply wanting as much security as possible is understandable - but unrealistic.

Business challenge

Cyber criminals and threat actors are taking advantage of crisis situations.

In a bid to maintain a level of productivity, companies are quickly advising their employees to work remotely, but to minimise delays and loss of productivity, they are not necessarily enforcing security protocols to avoid a potential flood of support tickets. Remote working can take many different forms, RDP, VPN or straight to SaaS cloud working, which are some of the 'most used' attack vectors by cyber criminals and threat actors.

An advanced approach

When you design your security programme, you begin with policy. Various policies address the cloud, the data centre, endpoints, mobile use, and the network. Point products are acquired to support each area.

The result, however, is often an unintegrated patchwork without a holistic and encompassing strategy. Insight has a robust security practice and the pulse on the IT security landscape. We have helped organisations secure their data and networks for more than 30 years. As a group of advisors, solution providers, and technical specialists, we maintain certification and immersion in the latest security technologies and best practices. Our Security Services consultants can help you consider the security implications of your business activities, and adopt solutions that are aligned with your needs and objectives. We begin by assessing your current environment, challenges, and requirements.

Meaningful solutions driving business outcomes

We help our clients modernise and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated.

Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.

Services portfolio

Remote user/device verification

Deliverables:

- Verifying and safeguarding the identity of users through multi-factor authentication.
- A simple, easy deployment, delivered as a managed service with minimum impact to security/IT resources.
- A highly usable, flexible solution that is easy to use, and integrates with multiple devices, application and methods of authenticates.

Remote endpoint assessment

Deliverables:

- Visibility of all end-points connected to your network.
- Identification of what vulnerabilitie.s
- Recommendations – for quarantining and remediation.

Remote security assessment

Challenges addressed:

- Ensure end-points are defended. With the majority of employees working remotely, identifying unmanaged end-points, connectivity issues, vulnerabilities and patching requirements becomes increasingly difficult, while quarantining endpoints, deploying fixes and updates that mitigate risk adds further complexities.
- Control the identification of a user relative to a device, preventing both accidental misuse through endpoints being in a home environment, and criminals taking advantage of the collapsed perimeter.
- Educate the remote user community and testing and evidencing their resilience – enabling security to identify and support users that potentially need additional help.
- Ensure regulatory and compliance requirements continue to be supported during challenging or crisis events.

Remote advisory

Deliverables:

- Education and training that is tailored to remote working, and drives engagement through connecting personal and business security.
- Testing of the remote workforce to establish resilience, promote continuous improvement, and identify users where additional support is beneficial.
- Scenario based crisis testing, which is designed and executed remotely – testing an organisation's crisis response.

Remote cyber-incident simulation activity

Deliverables:	Benefits
• Assigned expert resources. • A review of client's existing policies and procedures. • A choice of at least three scenarios that relate to the policy review. • Full remote GM of the incident session including content, media, role play and supporting resources/material.	• Testing and evidence of policies, procedures, decision making and key systems and resources availability. • Testing and evidence of readiness to respond to a major incident during a crisis. • Compliance or regulatory independent evidence that this is in place. • Structured and prioritised improvement planning for crisis management.

Insight

Find out more about our security services, contact your Insight Account Manager

08444 723 800 | contactus@insight.com | uk.insight.com