CWSI.

CWSI Cloud Security Services

Where is the weakest link in your cloud strategy?

Adoption of cloud services continues to grow at a rapid rate as organisations migrate workloads to achieve scale and agility, whilst driving costs down. With the implementation of cloud services, organisations enter a shared responsibility model with their cloud service provider for their cloud security.

CWSI Azure Security Review

CWSI have created an evaluation service that will provide comprehensive insights into your existing Azure presence and the potential risks linked to it. We will gauge your organisation against industry standards to construct a clear roadmap towards the utmost secure environment.

Azure Security Review is a comprehensive review of your organisations Azure environment.

CWSI's Microsoft Certified Engineers will review the environment checking over 200 configurations before producing a comprehensive report scoring your environment in each area against industry best practices. We will provide you with a view and recommendations on:

- The risks you are currently exposed to.
- Future potential risk exposure.
- Areas of recommendations for remediation.

Customer Technical Workshop	Access Set Up	Data Gathering	Report Creation	Security Presentation & Security Recommendations

In the most recent Digital Defence Report, Microsoft shared some insights into customers who had been compromised.

The three main contributing factors were:

Weak identity controls:
Credential theft attacks remains one of the top contributing factors. 88% of impacted customers did not employ AD and Azure AD security best practices. This has become a common attack vector as attackers exploit misconfigurations and weaker security postures in critical identity systems to gain broader access and impact to businesses.

Ineffective security operations:
These processes do not just present a window of opportunity for attackers, but significantly impact the time to recover. 93% of Microsoft investigations during ransomware recovery engagements revealed insufficient privilege access and lateral movement controls.

Eventually it boils down to data:
Organisations struggle to implement an effective data protection strategy which aligns with their business needs. None of the impacted organisations implemented proper administrative credential segregation and least privilege access principles via dedicated workstations during the management of their critical identity and high value assets, such as proprietary systems and business-critical applications.

CWSI.

Why have a Security Review?

Operationally, the cloud service provider takes on responsibility for physical security, hardware resilience and in the case of SaaS and PaaS services, they will also secure the operating system and application. However, this does not absolve the cloud customer from the ownership of their security. Depending on what services in the cloud the customer is using, security configuration and management remain in the remit of the customer for example, ultimately, every cloud customer must have confidence in their own security architecture, configuration and security operations.

As cloud providers compete to offer more services and get more "sticky" with their customers, cloud services continue to evolve and add functionality. As these new functions and features are made available, this can lead to the security posture of the cloud customer needing to be reviewed. Any cloud customer who doesn't do a periodic analysis of their cloud footprint is opening themselves up to the risk of a devastating attack.

What is covered with a review?

As part of the security review, we cover the following aspects:

| Identity & Access Control | Defender for Cloud | Network Security | Data Security, Encryption & Storage | Operational Security |

Do I need a full Security Review?

CWSI provide an Azure Security Assessment as an alternative to a full review. This is a cutdown version of the review and covers the 70 most significant configuration elements, providing a high-level report of where remediation focus should be.

Why CWSI

When it comes to information protection, you need an experienced partner.

Founded in 2010, CWSI is a mobile and cloud security specialist, providing IT security, mobility and managed service solutions that support the modern workplace. From offices in Ireland, United Kingdom, Belgium, Luxembourg and the Netherlands, we provide consulting, professional services, and managed services to Europe's most respected organisations in a range of industries.

CWSI has deep technical expertise in the design, deployment, integration, and management of industry-leading software solutions and is a Microsoft Solutions partner. CWSI helps companies to thrive and stay secure in a mobile world and has enabled hundreds of organisations and thousands of employees to work productively and securely from anywhere, and on any device.

Microsoft Solutions Partner

Member of Microsoft Intelligent Security Association
Microsoft Security

Microsoft Partner
Microsoft Ireland Partner of the Year 2022 Winner
Security

UK: +44 1189 344 300   info@cwsi.co.uk | **BE:** +32 2 669 95 00   info@mob.co
IRE: +353 1 293 2500   info@cwsi.ie | **LUX:** +353 1 293 2500   info@mob.co
NL: +31 88 030 9030   hello@blaud.com | **cwsisecurity.com**