SALUS

CYBER

CLOUD SECURITY SERVICES

WWW.SALUSCYBER.COM

GET BETTER CONTROL OVER YOUR CLOUD INFRASTRUCTURE

Cloud Technology is core to the way Businesses and Governments now operate. Cloud services have revolutionised the way we interact and conduct our work, both internally and externally.

Cloud computing comes in various deployments such as; public (shared services and infrastructure with other organisations), private (used by a single organisation) and hybrid (a combination of both public and private).

Cloud services also come in three forms - Infrastructure as a service (IaaS), Software as a service (SaaS) and Platform as a service (PaaS).

IaaS gives organisations a pay-as-you-go option to obtain IT infrastructure services from a cloud vendor. This means organisations can save on costly on-site installations. Examples include Google Compute Engine and Microsoft Azure VM.

SaaS services are widely used amongst businesses that acquire software apps over the internet that do not require any onsite installation or download. Household names include: Salesforce, Slack, Microsoft 365 and Adobe creative cloud.

PaaS is a service that delivers hardware and software tools over the internet. Many companies use this to develop new applications or environments such as web and mobile apps and databases. Well-known vendors include Microsoft Azure Web Apps and Amazon Web Services (AWS).

Although Cloud services gives organisations greater benefits such as cost savings and scalability, they also need to understand the risks that come with moving to a modern way of working. Shared ownership of risk, personal ownership of risk and supplier ownership of risk all need to be properly balanced and understood.

83% of organisations say they need to improve their cloud security.

Source: The 2020 Cloud Security Alliance report commissioned by Proofpoint.

Cloud security and why it's problematic

Cloud security requires certain processes and technologies that aim to protect your cloud infrastructure and stop unauthorised access to data and applications.

There are however, many challenges that come with this such as:

- **Complex infrastructures - Difficulty knowing which vulnerabilities might be exposed.**
- **Less visibility - Data and applications are stored outside your organisations network.**
- **Compliance issues - Not knowing if a cloud provider is adhering to specific regulations.**
- **Lack of data control - Unaware who has access to sensitive data.**

Protecting your cloud infrastructure is crucial, as any attack footprint can rapidly expand. Ensuring you have the right security measures can help mitigate these common cloud security challenges.

CLOUD SECURITY SERVICES

Cloud Security Architectural Design

Due to the increased number of innovative services, both security-related and functional, within cloud environments, ensuring your newly developed solution is secure-by-design is now an increasing challenge for architects.

When reviewing designs, our consultants can ensure that environments are designed in-line with vendor guidance, and that all appropriate security considerations have been built in, whilst reducing the administrative overhead by utilising time-saving cloud products within the environment.

This review is a paper-based exercise, conducted in communication with client design resources in order to verify and justify decisions made in the process of solution development.

Cloud Security Assessment

With the mass migration by a wide variety of businesses to cloud-native infrastructure and application stacks, modern security attacks are often looking to exploit these services. Most security issues relating to cloud services are due to misconfigurations surrounding the security features of these cloud platforms.

Many platforms will, by default, be configured in a mostly open state to allow rapid setup and configuration of the platform by prospective users, however these configurations are not always removed or hardened in a secure manner.

As such a cloud configuration review is primarily concerned with the access controls and permissions granted on specific objects within a cloud provider environment (Azure, AWS, Google Cloud). This entails reviews of access controls used within virtual networks and access controls within the configuration used to grant permissions to resources and data.

CLOUD SECURITY SERVICES

Threat Profiling

At an unprecedented pace, cloud computing has simultaneously transformed business and Government, and created new security challenges. The COVID pandemic also led to more rapid transition home working than many companies were ready for. The shift from traditional client/server to service-based models is transforming the way technology departments think about, designing, and delivering computing technology and applications.

However, the improved value offered by cloud computing advances have also created new security vulnerabilities, including security issues whose full impacts are still emerging. Such issues are often the result of the shared, on-demand nature of cloud computing.

Salus Cyber security testers maintain an up to date understanding of the core threats, risks and vulnerabilities in the cloud and monitor the work of the Cloud Security Alliance. We undertake security threat research and testing to help companies minimise:

- **Data Breaches**
- **Misconfiguration and Inadequate Change Control**
- **Lack of Cloud Security Architecture and Strategy**
- **Insufficient Identity, Credential, Access, and Key Management**
- **Account Hijacking**
- **Insider Threat**
- **Insecure Interfaces and APIs**
- **Weak Control Plane**
- **Metastructure and Applistructure Failures**
- **Limited Cloud Usage Visibility**
- **Abuse and Nefarious Use of Cloud Services**

MICROSOFT OFFICE 365 SECURITY ASSESSMENT

Office 365 Review

Office 365 provides an easy way for users to access organisational information from anywhere with internet access, a necessity in the modern workforce. But this means that attackers are also targeting these systems more aggressively, as the opportunity for exploit is now much greater.

Salus Cyber's Office 365 review will check that the data stored within Office 365 has appropriate protections in place to protect access and prevent data exfiltration, as well as checking that all other inter-connecting systems within 365 have best practice controls in place for the following:

- **Conditional Access Policies (MFA)**
- **SharePoint Document Controls**
- **DLP / Sensitivity Labels**
- **External Sharing Policies**
- **MDM Device Policies**
- **Password Policy**
- **Email Security (Threat Protection + Verification DKIM / SPF / DMARC)**
- **Reviewing Audit Log Settings**
- **Mailbox Access Review**

SALUS

CYBER

CLOUD SECURITY SERVICES

WWW.SALUSCYBER.COM
01242 374087

CYBER ESSENTIALS CERTIFIED PLUS

THE CYBER SCHEME

Assured Service Provider
in association with National Cyber Security Centre

CHECK
IT Health Check Service

Crown Commercial Service Supplier

ISOQAR REGISTERED
UKAS MANAGEMENT SYSTEMS 0026
Certificate Number 18737
ISO 9001