Secure your Cloud Environment

Modern cloud services, such as AWS or Azure, give your organization the opportunity to be more secure and information resilient than ever before. They can provide enhanced security and privacy services to manage and protect your data. They also change your risk profile with new ways of potentially exposing your data.

This requires a new strategic approach to governance structure, policies and processes to manage the provider's technology.

If you are adopting cloud technologies and services, we can support you in addressing these new security and privacy risks to enable you to take advantage of these cloud services.

How secure is your cloud environment?

Plan your security road map to strengthen your cloud security posture.

Whatever the stage of your cloud journey, our cloud security team can help you identify and mitigate the risks facing your organization such as:

- Attack surface for cybercriminals (Infrastructure and Application)
- Ineffective shared responsibility model
- Security misconfigurations and process weaknesses
- Lack of visibility and defence in depth protection
- Data loss and corruption
- Insecure cloud architectures
- Business Continuity and Incident Response
- Inappropriate data privacy governance
- Inadequate privacy and security by design

Key services

- Threat models, risk assessments, cloud security model and requirements
- Security gap analysis of policies, processes, and maturity posture
- Technical security architecture, configuration and baseline assessment
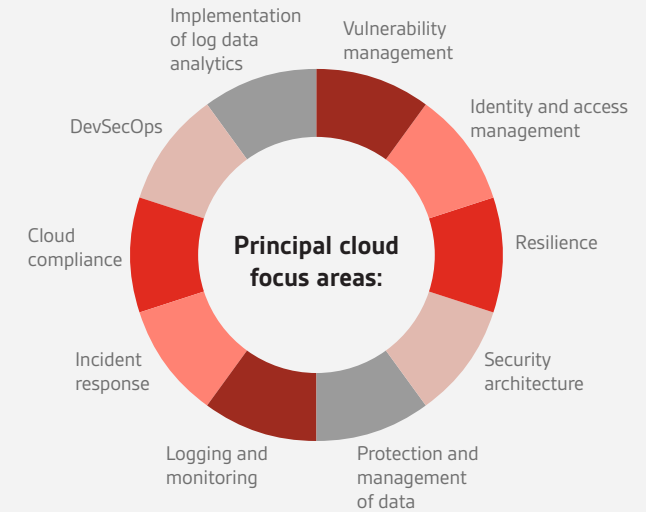- Third party due diligence
- Data privacy assessment

Security technologies

Working with our trusted security technology partners, we provide insight and proactive engagements to support our client's requirements.

- Secure Web Gateway as a Service
- Cloud Access Security Broker and Cloud DLP
- Identity and Access Management
- Security Information and Event Management / User and Entity Behavioural Analytics / Security Orchestration, Automation and Response
- Email security and Security Awareness Training

Why BSI?

For more than 15 years, BSI's information security practice has provided Cyber Risk and Advisory services allowing clients to meet a wide range of standards-based data security and data privacy requirements. We also have a CREST/CHECK/OSCP certified penetration testing team, capable of testing networks and infrastructure, applications, and web services, mobile and IoT, and cloud-based systems.

Principal cloud focus areas:

- Implementation of log data analytics
- Vulnerability management
- Identity and access management
- Resilience
- Security architecture
- Protection and management of data
- Logging and monitoring
- Incident response
- Cloud compliance
- DevSecOps

Our cloud services include:

Start

- Management reporting
- Cloud security governance review
- Security requirements design and review
- Threat modelling and risk analysis
- Security maturity improvement roadmap
- Secure architecture design and assessment
- Security configuration assessment
- Penetration testing
- Attack simulation analysis and incident response
- Third party due dilligence
- Cloud privacy review

bsi.

zscaler™ okta druva proofpoint. McAfee Together is power. exabeam