ENSIGN INFOSECURITY

Ensign InfoSecurity Cloud Security Services

Securing your data wherever it lives – in public, private or hybrid environment

The adoption of cloud technology has been increasing exponentially as businesses gain awareness of its benefits in terms of cost, scalability, availability and flexibility. Alongside the private sectors that are leading the cloud computing revolution, the government is also embarking on a journey to migrate their IT systems on to the Cloud to leverage its global ecosystem of solutions and services. Despite the advantages brought about by the Cloud movement, there are, however, growing concerns about how organisations store, manage and process critical data on cloud systems.

Common challenges of cloud technology adoption:

- Abuse and misuse of cloud computing
- Insecure Application Programming Interfaces (APIs)
- Compromised credentials due to insider threats
- Use of unsanctioned cloud platforms
- Data ownership, accountability, and risk
- Data replication and lack of visibility
- Security in public cloud environments

SERVICES & FEATURES

Powered by unparalleled threat intelligence, Ensign's comprehensive cloud security solutions can help organisations protect their critical and sensitive data, defend against advanced threats, and maintain information integrity as it moves to the Cloud.

OUR KEY CAPABILITIES INCLUDE:

1. Cloud Security Consulting

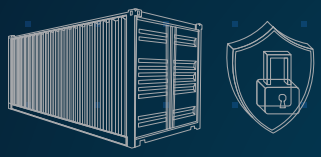
Ensign's cloud security experts can help you design and develop a holistic security strategy to navigate the multi-cloud environment. We will help you assess your data protection policies and cloud security architecture. At the same time, we can assist you in identifying risks and improving network visibility. This can be achieved with the following components:

- Cloud security strategy and roadmap
- Cloud security policy build and review
- Cloud data protection assessment
- Cloud security architecture assessment and design
- Cloud security incident response

2. Cloud Access Security Broker (CASB)

Ensign's CASB solution protects your public cloud workloads and data in sanctioned cloud applications through various modes of access and policy enforcement points. Ensign's CASB solution addresses:

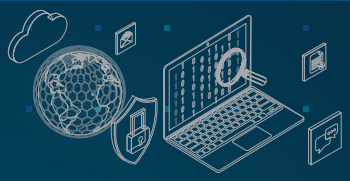
- Visibility of Shadow IT
- Cloud services compliance
- User activity monitoring
- Data leakage protection
- Threat protection



3. Container Security (CS)

Ensign's CS solution can help secure the containers on your DevSecOps in your on-premise and cloud environments. The CS platform integrates with the CI/CD environment and Container Registry, providing the following competencies during runtime:

- Vulnerability management
- Runtime protection
- Secrets management
- Embedded CI/CD scanning
- Workload firewall
- Compliance and auditing



4. Cloud Security Monitoring

Providing real-time monitoring and clear visibility of your data across on-premise and hybrid Cloud environments, Ensign's cloud security monitoring strengthens your cloud security posture while helping you detect and neutralise security threats. Our cloud security monitoring capabilities include:

- 24/7 policy-based monitoring of applications, devices and servers in the cloud
- Anomaly detection
- Advanced security analytics
- Proactive escalations and contextual alerts of suspicious cloud usage
- Runtime defence
- Compliance reporting
- Cloud forensic
- Single-pane view of your cloud, on-premise and hybrid environments threats

BENEFITS

Ensign takes a holistic aprroach in addressing your cloud security challenges. We can provide a full suite of capabilities, from gathering insights to architecting and designing solutions to help safeguard your cloud infrastructure.

Regulatory compliance
Cloud Security controls protect your data in the cloud. This is governed by regulatory standards such as GDPR, HIPAA, PCI-DSS, and more.

Single, logical view of multi-cloud resources
Gain complete visibility across all cloud environments by assessing data and threat alerts in real time.

Consistent security assessment
Audit and monitor your security configurations, resources, and services across your cloud environments.

Insider threat protection
Leverage machine learning to detect activities signalling negligent and malicious behaviour including insiders stealing sensitive data. Design and implement policies prohibiting data exfiltration from unmanaged cloud storages.

Data loss prevention (DLP)
Prevent confidential data from being leaked by identifying and restricting attempts of users to upload or share sensitive corporate data to an unsanctioned managed cloud storage bucket or blob.

About Ensign:

Ensign InfoSecurity is the largest pure-play, end-to-end cybersecurity service provider in Asia. Headquartered in Singapore, Ensign offers bespoke solutions and services to address their clients' cybersecurity needs. Their core competencies are in the provision of cybersecurity advisory and assurance services, architecture design and systems integration services, and managed security services for advanced threat detection, threat hunting, and incident response. Underpinning these competencies is in-house research and development in cybersecurity. Ensign has two decades of proven track record as a trusted and relevant service provider, serving clients from the public and private sectors in the Asia Pacific region.

For more information, visit *www.ensigninfosecurity.com* or email *marketing@ensigninfosecurity.com*