SharkStriker

Managed Cloud Security Service

| Key Highlights

- Provides unified multi-cloud visibility for AWS, Azure, and Google Cloud.

- Continuous monitoring for cloud misconfigurations.

- Protects cloud workloads from Exploits, Ransomware, and Adversaries.

- Reduces alert fatigue with machine accelerated incident response.

- Assesses the vulnerabilities and baseline.

- Delivers Cloud Monitoring, Posture Management (CSPM), and Workload Protection (CWPP) under one service.

| More visibility for better Security

- Businesses are moving to the cloud due to the vast amount of benefits in form of rapid provisioning, elastic scaling, reduced cost, high flexibility, and high availability. But along with the benefits, it's essential that organization fully understand the security risks associated with the use of any cloud services and requires regular cloud security assessment and monitoring.

- Cloud security issues and challenges may lead to events such as these that could be catastrophic for an organization as it may lead to hacking, theft, or destruction of data. Therefore having a robust cloud security service as a part of the system is vital to combat any attacks.

- SharkStriker's managed cloud security service is a unique combination of Cloud Infrastructure Monitoring, Cloud Security Posture Management (CSPM), and Cloud Workload Protection (CWPP). Service offers 24/7 security monitoring, vulnerability and baseline assessment, threat protection and proactive threat detection with help of machine accelerated human intelligence.

| Worried About Cloud Security?

- Easily manage cloud security risks, protect cloud assets and accelerate growth.

> 66
> Through 2022, at least 95% of cloud security failures will be the customer's fault. 99

- The cloud works on a shared structure between the enterprise and the cloud provider. SharkStriker helps you to secure your business via managing your data security and privacy requirements in the cloud.

- Many organizations struggle with **Three Key** areas in the cloud.

Data Security
Lack of visibility to data, inability to control data, or theft of data in the cloud are the major concerns related to cloud data security.

Compliance
Moving data protected by PCI, HIPPA, or similar regulations to the cloud, achieving and demonstrating regulatory compliance is becoming more difficult.

Expertise
Many companies are still finding it challenging to find resources with cloud knowledge and the expertise they require for security controls in the cloud.

The costs of cloud security solutions, the long procurement life cycle, and the time to train the security teams often impact the purchasing decisions. While security service providers offer security assessment and consulting services involve manual effort, lack of full visibility, and time-consuming. SharkStriker's managed cloud services are fully automated and you can assess your cloud for the best practice control adherence.

| Features of Managed Cloud Security Service

| Cloud Infrastructure Monitoring

- Cloud infrastructure and applications are as susceptible as on-premises solutions. Migrating and expanding to the cloud brings new security challenges and may minimize visibility into the conditions wherein data resides, intensifying risk and makes corporate information more prone to cyber threats. Regardless of where the information is stored, real-time checking and clear visibility are vital for quickly detecting and neutralizing security threats.

  - Fully managed and hosted SIEM
  - Live dashboards
  - Cloud infrastructure monitoring
  - Integrated threat intelligence

| Cloud Security Posture Management (CSPM)

- The quick pace of cloud change, blended with multi-cloud designs and developing compliance requirements, makes the cloud environment unpredictable and botches practically inescapable. One service with a single misconfiguration can rapidly amplify a serious security issue. Nowadays data breaches are becoming a very common and serious issue, so, companies want a singular and complete strategy to address the cloud security challenges.

  - Unified visibility across multi-cloud environment
  - Compliance management
  - Continuous configuration assessment
  - External attack surface assessment

| Cloud Workload Protection Platform (CWPP)

- As defined by [Gartner,](#) the Cloud Workload Protection Platform (CWPP) is a "workload-centric security solution that pursuits the specific protection requirements of workloads in modern enterprise environments." Computing, storage, and networking capabilities are the most specifications required by the applications in the cloud. These cloud workloads have specific security requirements that vary from traditional IT systems, and cloud workload protection platforms (CWPPs) are intended to give security tailored to the needs of workloads deployed in public, private, or hybrid cloud environments. The main goal of the CWPP is to keep the applications secure by giving security for the application and all the other related data capabilities.

  - Endpoint Detection and Response (EDR)
  - ML based signature less Malware Prevention
  - Ransomware & Exploit Protection
  - Adversary Prevention
  - Credential Theft Protection
  - File less or Zero-Footprint attack Prevention
    Vulnerability assessment
  - Baseline configuration assessment

| SOC-as-a-Service

- Cyber threats are increasing day by day. Add in cloud infrastructure and SaaS applications, and the cybersecurity skills you need to have on the prepared and complicated and hard to find. Our cloud-based security orchestration and automation platform reduces noise and prioritizes threats for our SOC, staffed by way of skilled security analysts with a wide range of cyber expertise. You can get the right expertise applied at the proper time, day or night, 7 days a week.

  - 24/7 Threat monitoring
  - Machine accelerated human-led threat hunting
  - Incident investigation and response

| About SharkStriker

SharkStriker is a trailblazing cybersecurity services vendor with a mission to simplify cybersecurity for its partners across industries through its technologically driven human-led open architecture platform STRIEGO. It seeks to cater to some of the industry's most immediate challenges such as siloed cybersecurity, increasing cost of cybersecurity solutions, changing regulatory environment, and increasing reliance on multiple vendors for multiple aspects of cybersecurity and compliance.

With STRIEGO, SharkStriker is able to assist its network of partners and customers through effective augmentation of cybersecurity posture as per use cases, extending visibility, compliance management, and round-the-clock support for incident response.

Through a team of threat-striking experts, they have made their presence across MEA, North America, Europe, and Asia.

| Globally recognized, Globally trusted.

SharkStriker