ALTIMETRIK®

Datasheet
CloudSecurity

Introduction and Overview

In 2023, data breaches involving cloud-stored data, whether in public, private, or multiple environments, comprised a staggering 82% of reported incidents. Cloud environments became prime targets for threat actors, with 39% of breaches impacting multiple environments, often resulting in a higher-than-average cost of USD 4.75 million.

Cloud misconfiguration and business email compromise constituted notable initial attack vectors, accounting for 11% and 9% of attacks, respectively. The implications of these breaches varied based on the storage location of the compromised data. Specifically, breaches that extended across multiple environments, including cloud and on-premises infrastructures, incurred heightened costs and prolonged identification and containment durations for data breaches.

The prevalence of breaches predominantly impacted data stored across various environments. A significant 39% of breaches encompassed data across multiple environments, overshadowing the combined 34% attributed solely to private cloud or on-premises environments. This trend emphasizes the vulnerability of data spread across multiple cloud environments.

Among these breaches, those affecting public clouds and multiple environments exhibited higher costs. These incidents registered an average cost of USD 4.75 million, notably surpassing the lowest cost of USD 3.98 million associated with data breaches in private cloud environments. Such incidents across multiple environments also surpassed the average cost of a data breach, indicating substantial financial implications.

Cloud Security Challenges

Even companies with robust cloud security measures in place can fall victim to cyberattacks for several reasons. Despite implementing stringent security protocols, vulnerabilities can arise from human error, misconfigurations, or overlooked weaknesses within the cloud infrastructure. Sophisticated attackers are adept at exploiting novel attack vectors, such as social engineering techniques or zero-day vulnerabilities and can bypass even the most advanced security defenses.

There is a higher risk for organizations as services used by employees are now facing publicity. Also, there are now more ways to authenticate to cloud providers than just username and password. API keys and credentials can be found in publicly accessible code repositories.

Additionally, the complexity of multi-cloud and hybrid environments can introduce unforeseen risks, making comprehensive security management challenging for organizations.

Cloud Native Application Protection Platforms

The Cloud Native Application Protection Platforms (CNAPP) approach ensures in-depth coverage across all aspects of your environment from proactive validation of workloads to auditing the policies on the public cloud platforms. Key focus areas include:

Development Artifact Scanning

Comprehensive Software Composition Analysis (SCA) and Application Security Testing (SAST/DAST/IAST) of source code or compiled libraries to flag the version and license of the library in use and then list any common vulnerabilities and exposures (CVEs) and their rating

Infrastructure as Code (IaC) scanning

Scanning of infrastructure automation templates such as CloudFormation (AWS), ARM (Azure), Google Cloud Foundation (GCP), Kubernetes manifests, Docker files, or Terraform plans to find security flaws before they make it to production and cause problems

Cloud workload protection platform (CWPP)

Detect and remove threats such as Malware, vulnerabilities, and unauthorized applications across all types of infrastructure - physical servers, virtual machines, containers, and serverless functions.

Cloud infrastructure entitlement management (CIEM)

The most important protective area of managing access rights, permissions, or privileges for the identities of a single or multi-cloud environment to avoid risks resulting from privileges being higher or broader than they should be – to ensure compliance, detection and remediation, Governance and visibility.

Cloud Detection and Response (CDR)

Continuously analyse various cloud infra logs (Application, System, System logs, etc.) to detect patterns that match malicious behaviour – and act on security events and potential threats to help secure your workload.

Cloud Security Posture Management (CSPM)

Identify and remediate risks by automating and enabling monitoring for continuous threat detection and configuring remediation workflows for any misconfigurations across diverse cloud environments/infrastructure.

Altimetrik
Cloud Security Services

Zero Trust Network Architecture Implementation

Altimetrik implements Zero Trust Network Architecture (ZTNA) methodologies with Identity and Access Management (IAM) as a crucial aspect of cloud security, ensuring that only authorized users and applications have access to sensitive resources. Implementing effective ZTNA practices is essential for safeguarding data, preventing unauthorized access, and maintaining compliance regulations. We implement robust ABAC controls to manage user access and permissions ensuring that only authorized individuals have access to sensitive data and resources. Also implementing least privilege access by granting users only the minimum level of access required for their specific roles and reducing the attack surface, blast radius and minimizing potential damage in case of unauthorized access.

Cloud Security Testing and Assessments

Our experts specialize in single-platform and multi-cloud security testing and assessments for AWS, Azure and GCP. The cloud provides a unique environment for security testing as traditional attacks are approached from different angles. There is more room for misconfigurations and a higher risk due to many employee services that have now become public-facing. Your attack surface is assessed by our experts to locate potential attack vectors and work with stakeholders to remediate these issues.

Cloud Architecture Risk Analysis

We specialize in Cloud Architecture Risk Analysis, our service is designed to comprehensively assess the security and resilience of your cloud infrastructure. Leveraging our expertise in cloud

technologies and security, we conduct thorough evaluations of your cloud architecture, identifying potential vulnerabilities, misconfigurations, and compliance gaps that may expose your systems to security risks. Our team employs industry best practices and robust methodologies to evaluate the architecture's design, data flow, access controls, and resilience against potential threats. Through our analysis, we provide actionable insights and recommendations aimed at enhancing your cloud security posture, ensuring regulatory compliance, and strengthening your infrastructure against evolving cyber threats.

Threat Detection and Continuous Monitoring

We provide threat detection, continuous monitoring, and automated security auditing for proactive identification and swift response to potential risks. We ensure in-depth coverage across all facets of your cloud environment, verifying workload validation and auditing public cloud platform policies. Count on our cloud security experts to continuously improve your cloud security posture and safeguard your operations against emerging cyber threats.

Vulnerability Management

Our Vulnerability Management Program is tailored to proactively identify and mitigate potential vulnerabilities within your cloud infrastructure. Our program involves a systematic approach that includes continuous scanning, assessment, and remediation of security weaknesses across your cloud environment. Leveraging cutting-edge tools and methodologies, our expert team conducts regular vulnerability scans, identifying weaknesses, misconfigurations, and potential entry points for cyber threats. We prioritize and classify these vulnerabilities based on their severity and potential impact, offering a detailed remediation plan to address critical issues promptly.

Security Governance Risk and Compliance

Our experts will help ensure compliance with relevant industry regulations and data privacy laws to maintain data confidentiality and integrity such as GDPR, HIPAA, and PCI DSS. SGRC services include IT Security Policy Development, SOC2, HITRUST and HITECH compliance audits, 3rd Party Risk Assessments, Security Awareness Training, Incident Response Planning, Business Impact Analysis and Business Continuity Planning.

Benefits of Altimetrik Cloud Security Services

Enhanced security

Our services are designed to protect cloud-based applications and data from unauthorized access, malware, and other threats. Clients will benefit from a significantly improved cybersecurity posture for their cloud environments. This enhanced security will safeguard critical infrastructure, reduce vulnerabilities, and protect against a wide range of cyber threats.

Improved compliance

We help organizations comply with a variety of industry regulations, such as HIPAA, PCI DSS, and SOC 2. Our experts have a deep understanding of these regulations and can help provide the necessary documentation and controls to help you meet compliance requirements

Reduced costs

Our experts will help tailor custom solutions and plans to help your organization reduce costs by eliminating the need to invest in and maintain on-premises security infrastructure. By identifying vulnerabilities and implementing robust security controls, Altimetrik security services help clients mitigate risks associated with cyberattacks, operational disruptions, and data breaches. This risk reduction minimizes potential financial losses and reputational damage.

Increased Agility

Our approach increases agility by focusing on quickly provisioning and de-provisioning security resources as needed. This can be particularly beneficial for organizations that are constantly adding and removing applications and data.

Cyber Threat Hunting

Clients benefit from continuous, real-time monitoring and threat hunting, allowing for early detection and proactive response to emerging threats. This capability minimizes the potential damage of cyber incidents.

Incident Response Preparedness

Clients gain confidence in their ability to respond effectively to cybersecurity incidents. Our incident response procedures and threat detection capabilities ensure swift identification, containment, and resolution of security breaches.

Scalability and Automation

Once a framework and workflow has been established our team will create an automation workflow that can be scaled up or down as needed to meet the changing security needs of your organization. This can be particularly beneficial for organizations that are experiencing rapid growth.

Conclusion

Altimetrik is your trusted partner in Cloud Security. As technology advances so do the threats to cloud infrastructure. We are committed to empowering organizations with tailored solutions that enhance security, reduce vulnerabilities, and fortify their cloud environments. With a comprehensive suite of services, spanning from architecture risk analysis, vulnerability management, penetration testing, threat hunting, incident response planning and compliance, we provide the expertise and support needed to safeguard operations, protect assets, and maintain the resilience of business-critical services.

Contact

For more information, please visit us at:
www.altimetrik.com

About Altimetrik

Altimetrik is a data and digital engineering services company focused on delivering business outcomes with an agile, product-oriented approach. Our digital business methodology provides a blueprint to develop, scale, and launch new products to market faster. Our team of 5,500+ practitioners with software, data, cloud engineering skills help create a culture of innovation and agility that optimizes team performance, modernizes technology, and builds new business models. As a strategic partner and catalyst, Altimetrik quickly delivers results without disruption to the business.