TAG Insights Report: Overview of the Cloud Security Commercial Market

Prepared by
Dr. Edward Amoroso
Chief Executive Officer, TAG Infosphere
Research Professor, NYU
eamoroso@tag-cyber.com

Version 1.0
February 17, 2024

Introduction

This TAG Insights Report on *Cloud Security* is intended to help companies, managers, practitioners, researchers, investors, and commercial vendors better understand current trends, issues, and market opportunities in this area. A list of representative commercial vendors working in various areas of cloud security is included. The five specific areas of covered in this report include:

1. Cloud Data Fragmentation (CDF)
2. Cloud Infrastructure Entitlement Management (CIEM)
3. Cloud Security Posture Management (CSPM)
4. Cloud Workload Protection Platform (CWPP)
5. Microsegmentation

This report is intended for general and unrestricted use, but interested readers are encouraged to connect with the TAG research and advisory team for more information on the private TAG Research as a Service (RaaS) community that covers, discusses, and shares information on these topics in more depth and includes a wider range of startups, vendors, and companies.

TAG Taxonomy

We organize this TAG Insights Report as per our updated TAG Taxonomy which includes twenty categories of modern solution areas where stakeholders and buyers can find suitable commercial products and services for purchase and use. Each category has five subcategories

that correspond to the main areas in which practitioners can focus. These subcategories are discussed below.

1 Application Security 1.1 API Security 1.2 Application Security Testing 1.3 Application Security Posture Mgmt. 1.4 Runtime Application Security 1.5 SBOM/SCA	**6 Email Security** 6.1 Anti-Phishing Tools 6.2 DMARC 6.3 Email Encryption 6.4 Phish Testing and Training 6.5 Secure Email Gateway	**11 Identity and Access Management** 11.1 Authorization 11.2 IAM Platforms 11.3 identity, Anti-Fraud, and KYC 11.4 Identity Governance and Admin. 11.5 Privileged Access Management	**16 Operational Technology Security** 16.1 ICS/OT Device Security 16.2 ICS/OT Visibility 16.3 Unidirectional Gateway 16.4 Vehicle Security 16.5 Zero Trust OT
2 Attack Surface Management 2.1 Bug Bounty Services 2.2 External Attack Surface Management 2.3 Automated Pen Testing/Red Teams 2.4 Breach and Attack Simulation 2.5 Security Ratings Platforms	**7 Encryption and PKI** 7.1 Certification Authority (CA) 7.2 Data Encryption 7.3 Key and Secret Management 7.4 Key and Certificate Protection 7.5 Post-Quantum Cryptography	**12 Security Operations and Response** 12.1 Data Forensics and eDiscovery 12.2 Incident Response 12.3 SIEM Platforms 12.4 SOC/SOAR Support 12.5 Threat Hunting	**17 Security Professional Services** 17.1 Penetration Testing 17.2 Security Assessments 17.3 Security Research and Advisory 17.4 Security Training 17.5 Value Added Resellers
3 Authentication 3.1 Biometrics 3.2 Multifactor Authentication 3.3 Passwordless Authentication 3.4 Password Management 3.5 Single Sign-On	**8 Endpoint Protection** 8.1 Antivirus Software 8.2 Browser Isolation 8.3 Content Disarm and Reconstruction 8.4 Endpoint Detection and Response 8.5 Security Enhanced Browser	**13 Managed Security Services** 13.1 DDOS Security 13.2 Managed Detection and Response 13.3 Managed Security Services Platform 13.4 Network Detection and Response 13.5 XDR Services	**18 Software Lifecycle Security** 18.1 AI/MLOps Security 18.2 Container/Kubernetes Security 18.3 Container Scanning 18.4 DevSecOps Platforms 18.5 Infrastructure-as-Code Security
4 Cloud Security 4.1 Cloud Data Fragmentation 4.2 Cloud Infrastructure Entitlement Mgmt. 4.3 Cloud Security Posture Management 4.4 Cloud Workload Protection Platform 4.5 Microsegmentation	**9 Enterprise IT Infrastructure** 9.1 Asset Inventory 9.2 Backup Platform 9.3 Infrastructure Resilience 9.4 Physical Security 9.5 Secure Sharing and Collaboration	**14 Mobility Security** 14.1 IOT Security 14.2 Mobile App Security 14.3 Mobile Device Management 14.4 Mobile Device Security 14.5 Mobility Infrastructure Security	**19 Threat and Vulnerability Management** 19.1 Digital Risk Protection 19.2 Security Scanning 19.3 Third Party Risk Management 19.4 Threat and Vulnerability Platform 19.5 Threat Intelligence
5 Data Security 5.1 Cloud Data Security Posture Mgmt. 5.2 Data Access Governance 5.3 Data Discovery and Classification 5.4 Data Leakage Protection 5.5 Data Privacy Platform	**10 Governance, Risk, and Compliance** 10.1 Continuous Compliance 10.2 Cyber Insurance 10.3 Incident Reporting 10.4 GRC Platform 10.5 Risk Management Platform	**15 Network Security** 15.1 Network Access Control 15.2 Next Generation Firewalls 15.3 Secure Access Service Edge (SSE) 15.4 Virtual Private Networks 15.5 Zero Trust Network Access	**20 Web Security** 20.1 Bot Management 20.2 Content Security 20.3 Secure Web Gateway 20.4 Web Application Firewall 20.5 Website Scanning

Figure 1. TAG Taxonomy for Cybersecurity

Overview of Cloud Security Solutions

The following emerging global commercial opportunities involving cloud security solutions are covered in this report, including the listing of several viable commercial entities providing solutions on the market today:

- Cloud Data Fragmentation bolsters enterprise cybersecurity by dispersing sensitive data across multiple cloud environments, ensuring that even if one fragment is compromised, the integrity and confidentiality of the complete data set remain intact. This fragmentation serves as a complex puzzle that unauthorized entities find difficult to piece together, significantly reducing the risk of a complete data breach.
- CIEM provides enterprises with a detailed oversight of who is entitled to what within their cloud infrastructure, enabling meticulous management of identities and access rights. By continually analyzing permissions and ensuring that they adhere to the principle of least privilege, CIEM minimizes the risk of insider threats and unauthorized access to sensitive systems and data.
- CSPM tools automate the identification and remediation of risks across cloud infrastructures, providing enterprises with continuous compliance monitoring and security governance. This vigilance ensures that security configurations are not only set up correctly from the outset but are also maintained over time as the cloud environment evolves and new threats emerge.

- CWPP safeguards enterprise cloud environments by offering comprehensive protection tailored to the unique requirements of cloud workloads. It detects and mitigates threats in real-time, ensuring that applications and services running in the cloud are shielded from vulnerabilities and attacks that could compromise data or disrupt business operations.
- Microsegmentation fortifies enterprise cybersecurity by dividing the cloud network into distinct security segments down to the individual workload level. This strategy ensures that in the event of a breach, the lateral movement of threat actors is confined, thereby limiting the extent of the attack, and protecting critical assets from unauthorized access.

Focus Area: Cloud Data Fragmentation (CDF)

Cloud Data Fragmentation (CDF) is an emerging concept in the realm of cybersecurity, addressing the challenges posed by the increasing decentralization of data storage in the cloud. As organizations migrate more of their operations to cloud environments, they often utilize multiple cloud services, resulting in data being scattered across various platforms and locations. This fragmentation can create both challenges and opportunities for cybersecurity.

From a security perspective, Cloud Data Fragmentation presents a complex landscape. Each cloud service provider has its own security protocols and standards, making it difficult for organizations to maintain a consistent security posture across all platforms. This heterogeneity can lead to gaps in security, as some data fragments might be less protected than others. Additionally, tracking and managing data across multiple cloud environments can be challenging, increasing the risk of data breaches or loss.

However, Cloud Data Fragmentation can also offer cybersecurity advantages. By distributing data across multiple locations, organizations can achieve a form of security through obscurity. In the event of a cyberattack on one cloud service, only a portion of the organization's data is exposed, reducing the overall impact. This distribution can act as a natural barrier against massive data breaches, making it more difficult for attackers to access the entirety of an organization's sensitive information.

Another advantage is the potential for enhanced resilience. By having data stored in multiple cloud environments, organizations can mitigate the risks associated with single points of failure. If one cloud service experiences downtime or a security incident, other fragments of data remain accessible, ensuring business continuity.

However, to effectively leverage the benefits of Cloud Data Fragmentation, organizations must implement robust data management strategies. This involves establishing clear data governance policies, ensuring compliance with various regulatory standards, and employing advanced security tools designed for multi-cloud environments. These tools can include cloud access security brokers (CASBs), which provide visibility and control over data across different cloud services, and sophisticated encryption techniques to protect data in transit and at rest.

Focus Area: Cloud Infrastructure Entitlement Management (CIEM)

Cloud Infrastructure Entitlement Management (CIEM) is a crucial aspect of cybersecurity in the cloud computing era. As organizations increasingly adopt cloud services, managing access and entitlements in these environments becomes more complex and critical. CIEM solutions are designed to address these challenges, providing enhanced security and compliance in cloud infrastructures.

CIEM primarily focuses on identity and access management within cloud environments. It involves the understanding, controlling, and managing of permissions and entitlements for users and systems across various cloud platforms. As cloud environments can be dynamic and sprawling, traditional access management systems often fall short in providing the necessary visibility and control. CIEM fills this gap by offering tools and frameworks to manage cloud access comprehensively.

One of the key benefits of CIEM in cybersecurity is the reduction of excessive permissions, often referred to as "permission bloat." In many cloud environments, users and services are granted more permissions than necessary for their role or function. This over-provisioning of access rights can pose significant security risks, as it increases the attack surface for potential exploiters. CIEM helps in rightsizing these permissions, ensuring that entities have only the access they need to perform their duties, thereby adhering to the principle of least privilege.

CIEM also plays a crucial role in detecting and mitigating security risks associated with misconfigured cloud resources. Misconfigurations are a common cause of data breaches in cloud environments. CIEM solutions can continuously monitor cloud infrastructures for such misconfigurations and alert security teams or automatically rectify these issues, thus enhancing the overall security posture.

Another aspect of CIEM is its contribution to regulatory compliance. Many industries are subject to stringent regulatory requirements regarding data access and privacy. CIEM helps organizations ensure that their cloud environments comply with these regulations by providing clear insights into who has access to what data, how this access is being used, and whether it aligns with compliance standards.

Focus Area: Cloud Security Posture Management (CSPM)

Cloud Security Posture Management (CSPM) is an essential cybersecurity approach tailored for the cloud computing environment. As organizations increasingly shift their operations to the cloud, ensuring the security of their cloud infrastructure becomes paramount. CSPM addresses this need by providing continuous visibility into and management of the security posture across various cloud services.

CSPM systems primarily focus on identifying and mitigating risks associated with cloud resource configurations. As cloud environments grow in complexity and scale, the likelihood of misconfigurations, which can lead to security breaches, also increases. CSPM tools automate

the process of identifying such misconfigurations and non-compliance with security best practices and regulatory standards. This automated monitoring is crucial for maintaining a strong security posture in dynamic cloud environments, where manual oversight is often impractical.

One of the main benefits of CSPM is its ability to provide a comprehensive view of the security status across multiple cloud environments. This holistic perspective is vital for organizations using hybrid or multi-cloud strategies, as it helps identify blind spots and security gaps that could be exploited by attackers. By centralizing the visibility of the cloud infrastructure, CSPM enables security teams to manage and secure their cloud resources more effectively.

CSPM also aids in compliance management. With various industries subject to stringent regulations regarding data protection and privacy, CSPM tools help ensure that cloud deployments are in line with these regulatory requirements. They do this by continuously monitoring the cloud environment against compliance frameworks, thus facilitating adherence to industry standards, and reducing the risk of non-compliance penalties.

Furthermore, CSPM contributes to enhancing overall cybersecurity by integrating with other security systems, cybesuch as Cloud Access Security Brokers (CASBs) and Security Information and Event Management (SIEM) systems. This integration allows for a more coordinated and proactive approach to cloud security, enabling rapid response to potential threats and vulnerabilities.

Focus Area: Cloud Workload Protection Program (CWPP)

A Cloud Workload Protection Platform (CWPP) is a cybersecurity solution specifically designed to secure workloads in cloud environments. As organizations increasingly move their data and applications to the cloud, traditional security measures often fall short in providing the necessary protection for these dynamic and scalable environments. CWPP addresses this gap by offering specialized security capabilities tailored to protect cloud workloads.

The primary function of a CWPP is to safeguard various types of workloads, including virtual machines, containers, and serverless functions, across public, private, and hybrid cloud environments. It does this by continuously monitoring for threats, vulnerabilities, and misconfigurations. This continuous monitoring is essential in cloud environments where workloads are frequently created, modified, and moved.

One of the key benefits of CWPP is its ability to provide consistent security across diverse cloud environments. With the proliferation of multi-cloud strategies, organizations often struggle to maintain a unified security posture. CWPP solutions enable centralized management and security policy enforcement across different cloud platforms, ensuring consistent protection regardless of where the workloads are deployed.

CWPP also focuses on protecting against advanced threats that specifically target cloud-native technologies. This includes securing container orchestration tools like Kubernetes and managing the security of serverless functions. By addressing the unique challenges of these environments, such as the ephemeral nature of containers and the fine-grained access controls of serverless architectures, CWPP ensures that these cutting-edge technologies are not left vulnerable to exploitation.

Another significant aspect of CWPP is its role in compliance management. Many industries are subject to specific regulatory requirements regarding data security and privacy. CWPPs help organizations ensure that their cloud workloads comply with these regulations by providing tools for compliance monitoring and reporting.

Focus Area: Microsegmentation

Microsegmentation is a cybersecurity approach that involves dividing a network into distinct security segments down to the individual workload level. This granular partitioning allows for more precise control of intra-network traffic, significantly enhancing overall security. As network environments become increasingly complex, particularly with the adoption of cloud and hybrid infrastructures, microsegmentation becomes a vital strategy in an organization's cybersecurity toolkit.

The primary benefit of microsegmentation is the substantial increase in internal network security. Traditional network security models operate on the principle of a trusted internal network perimeter, which can be vulnerable to lateral movement by attackers once they breach the perimeter defenses. Microsegmentation addresses this issue by applying strict access controls and policies to each segment, thus limiting the potential for attackers to move laterally across the network.

By isolating workloads, applications, and processes into distinct segments, microsegmentation also minimizes the attack surface. In the event of a breach, the impact is contained within that small segment, significantly reducing the overall risk to the network. This containment is especially crucial in environments that handle sensitive or regulated data, as it can prevent widespread data breaches.

Another advantage of microsegmentation is its role in compliance and regulatory adherence. By segregating network segments that handle sensitive data, organizations can ensure that specific regulatory standards are met within those segments, simplifying compliance efforts. This is particularly important for industries subject to stringent data protection regulations, such as healthcare and finance.

Microsegmentation also enhances visibility into network traffic. With more defined segments, it becomes easier for security teams to monitor and understand traffic patterns, identify anomalies, and detect potential threats. This improved visibility is crucial for timely threat detection and response.

Companies and Contributions

The companies listed below emerged as part of our research at TAG. Our goal in listing these fine firms is to provide a starting point for buyers, advocates, stakeholders, and researchers trying to make sense of the commercial landscape for Cloud Security as a means for driving toward a more secure global ecosystem.

Cloud Data Fragmentation Vendors

1. AWS (Amazon Web Services): AWS facilitates data sharing through data spaces, offering a decentralized and secure data exchange across organizations and industries.
2. Cohesity: Cohesity provides a cloud-based platform that addresses data fragmentation, enabling a consistent experience across clouds with its data management solutions.
3. Dell Technologies: Dell Technologies offers a range of cloud solutions and services that help address the challenges of data fragmentation and secure data sharing.
4. Druva: Druva offers Cloud Data Protection and Management, addressing data fragmentation through backup, disaster recovery, and archival solutions in the cloud.
5. Google Cloud: Google Cloud offers services that facilitate secure data sharing and management, helping organizations deal with data fragmentation in cloud computing.
6. HPE (Hewlett Packard Enterprise): HPE provides cloud services and solutions for managing data fragmentation, particularly in storage and data management across hybrid cloud environments.
7. IBM: IBM provides cloud and data management solutions that focus on secure data sharing and addressing data fragmentation across multiple cloud environments.
8. Microsoft Azure: Microsoft Azure provides various cloud services, including tools and platforms for secure data sharing and managing cloud data fragmentation.
9. NetApp: NetApp's cloud data services manage and unify data across different cloud environments, addressing data fragmentation in cloud storage and file sharing.
10. Oracle: Oracle offers cloud solutions and services that address the challenges of data fragmentation and secure data sharing across its cloud environments.
11. Rubrik: Rubrik provides cloud data management and enterprise backup solutions that help organizations tackle data fragmentation, ensuring data security and compliance.
12. ShardSecure: ShardSecure specializes in data resilience in the cloud, providing security through a process of breaking up data into discrete components for distribution across multiple public clouds.
13. Snowflake: Snowflake also provides data exchanges for secure data collaboration, breaking down data silos and enabling control over data consumption and monetization.
14. Veeam: Veeam offers cloud data management solutions that address data fragmentation, particularly in backup and disaster recovery scenarios.

Cloud Infrastructure Entitlement Management (CIEM) Vendors

1. BeyondTrust: Specializes in multicloud entitlements reconciliation, entitlements optimization, monitoring, and remediation.

2. CrowdStrike: Provides centralized management and identity governance to manage cloud entitlements across multi-cloud environments.
3. CyberArk: Provides solutions to improve visibility and remediate IAM misconfigurations in single and multi-cloud environments.
4. Lacework: Offers solutions to understand and manage user permissions in the cloud, identifying risky entities and right-sizing entitlements.
5. Okta: Specializes in identity and access management, providing CIEM solutions for cloud security and compliance.
6. One Identity: Offers a range of identity governance and administration solutions, including cloud entitlement management.
7. Palo Alto Networks: Offers Prisma Cloud with CIEM capabilities for managing cloud access risks and integrating with identity provider services.
8. Rapid7: Delivers CIEM solutions that focus on administration-time controls for managing entitlements in hybrid and multi-cloud environments.
9. SailPoint: Specializes in identity governance, offering solutions to manage and secure cloud infrastructure entitlements.
10. Saviynt: Provides a specialized identity-centric SaaS solution for managing cloud access risk using time-limited access controls.
11. Sonrai Security: Sonrai Security offers CIEM services for customers which includes full identity and permissions inventory, continuous activity log monitoring, effective permissions engines, and least privilege enforcement.
12. Tenable: Focuses on multi-cloud asset management and full-stack risk assessment, offering automated remediation customized to organizational needs.
13. Wiz: Offers enhanced visibility and robust security posture through their CIEM tool, ensuring streamlined access to cloud resources.
14. Zscaler: Focuses on deep visibility into cloud entitlements alongside automated remediation to maintain least-privileged access.

Cloud Security Posture Management (CSPM) Vendors

1. AWS Marketplace: Hosts a range of CSPM solutions focusing on continuous monitoring and assessment of security posture in AWS environments.
2. Aqua Security: Aqua Security secures applications in cloud-native containers, CI/CD pipelines, and DevOps.
3. Arctic Wolf: Arctic Wolf provides a concierge security-as-a-service (SaaS) cloud-based SIEM and incident response solutions for business customers.
4. Check Point: Offers a product called CloudGuard that provides CSPM solutions with a focus on compliance, offering comprehensive cloud security and posture management tools.
5. Cloudflare: Specializes in securing complex cloud deployments and reducing manual effort in managing cloud infrastructure security.
6. CrowdStrike: Integrates CSPM with cybersecurity solutions, focusing on threat detection, guided remediation, and cloud security integrations.

7. Cynet: Cynet collects indicators and supports enterprise analysis for detection and mitigation of advanced threats.
8. Cyscale: Known for cloud security mapping, Cyscale provides a user-friendly CSPM solution supporting AWS, Azure, Google Cloud Platform, and Alibaba configurations.
9. Exabeam: Offers CSPM solutions for continuous, automated detection of cloud misconfigurations leading to data leaks and breaches.
10. Fedelis Security: Offers security and compliance solutions designed for the cloud, focusing on automated security and compliance for cloud assets.
11. F5: Offers CSPM solutions tailored for cloud builders, automating cloud security at scale.
12. Lacework: Known for automating cloud security, Lacework provides CSPM solutions focusing on managing cloud identities and entitlements.
13. Microsoft: Offers Microsoft Defender for Cloud that provides CSPM features like attack path analysis, agentless scanning, and data-aware security posture across Azure, AWS, and GCP.
14. Obsidian Security: Obsidian offers a platform that delivers data engineering, data science, and threat research so security teams can focus on protecting SaaS environments.
15. Orca Security: Orca Security offers a cloud security platform that identifies, prioritizes, and remediates security risks and compliance issues across a cloud environment spanning AWS, Azure, Google Cloud and Kubernetes.
16. Palo Alto Networks: Offers CSPM capabilities in Prisma Cloud, focusing on network threat detection and user entity behavior analytics across multicloud environments.
17. Qualys: Qualys provides cloud-based security and compliance functions through its Qualys Cloud Platform.
18. Rapid7: Provides CSPM solutions identifying and remediating threats in cloud environments, with a focus on risk assessment, incident response, and DevOps integration.
19. Skyhigh Security: Delivers Zero Trust security solutions that are data-aware and simple to use, focusing on data use and providing visibility and control.
20. Sonrai Security: Sonrai Security delivers an enterprise security platform for AWS, Azure, Google Cloud, and Kubernetes.
21. Sysdig: Sysdig provides unified posture management and threat detection in a single cloud security platform
22. Tenable: Provides a risk-based view of IT, security, and compliance postures, helping to quickly identify and prioritize critical assets and vulnerabilities.
23. Trend Micro: Offers a unified cloud security solution targeting cloud builders and integrating into users' DevOps processes across major cloud platforms.
24. Wiz: Provides CSPM solutions for enterprises with a full range of world-class capabilities for multi-cloud cyber risk management.
25. Zscaler: Specializes in identifying and remediating cloud misconfigurations and vulnerabilities across major public cloud providers.

Cloud Workload Protection Platform (CWPP) Vendors

1. Aqua Security: Specializes in securing cloud-native workloads, including scanning for vulnerabilities in container images, VM images, and functions, and providing native controls for containers and serverless functions.
2. Bitdefender: Provides a holistic security approach ensuring timely detection of threats across various container architectures and cloud environments.
3. Caveonix: Provides CWPP solutions that facilitate visibility and security control across hybrid multicloud networks, including VMs, containers, and serverless workloads.
4. Cloud Raxak: Provides automated security for cloud workloads, simplifying compliance and reducing risk across cloud environments.
5. Cloudflare: Offers CWPP solutions that detect and remove threats across various types of cloud infrastructures, including virtual machines, containers, and serverless functions.
6. CloudPassage: is an automated, portable, scalable, on-demand security and compliance company. Delivered as a service, the Halo security orchestration engine includes automated security controls for instant visibility and continuous protection in any combination of data centers, private clouds and public clouds.
7. CrowdStrike: Recognized for its cloud security offerings, CrowdStrike provides comprehensive visibility into workloads, containers, serverless workloads, and hosts.
8. Checkpoint: Specializes in network security and threat management for cloud environments, offering comprehensive protection for cloud infrastructures.
9. Entrust: Provides solutions for securing cloud infrastructure and data, focusing on workload security and compliance in cloud environments.
10. Fedelis Security: Offers security and compliance solutions designed for the cloud, focusing on automated security and compliance for cloud assets.
11. Fortinet: provides a powerful network security platform that helps protect against sophisticated threats and malicious attacks. Fortinet's comprehensive portfolio of security solutions includes advanced firewalls, secure access solutions, secure web gateways, endpoint security, cloud security, and more.
12. Microsoft Security: Offers CWPP solutions as part of a larger cloud-native application protection platform, integrating with SIEM and CIEM solutions for multicloud workload protection.
13. Palo Alto Networks: Their Prisma Cloud platform offers integrated security optimized for cloud-native architectures, focusing on runtime policies and container access control.
14. Sonrai Security: Sonrai Security delivers an enterprise security platform for AWS, Azure, Google Cloud, and Kubernetes. The Sonrai Dig platform is built on a sophisticated graph that identifies and monitors every possible relationship between identities and data that exists inside an organization’s public cloud.
15. Sophos: Provides real-time protection against malware, viruses, ransomware, and other cyber threats, with a focus on network security and unified threat management.
16. Tigera: Focuses on securing workloads in cloud environments and offers solutions that integrate with CI/CD pipelines for a comprehensive security approach.
17. VMWare: Focuses on maintaining, managing, and securing cloud-based workloads, offering increased visibility and data sharing between security and operations departments.

Microsegmentation Vendors

1. Akamai Technologies: Specializes in microsegmentation to reduce attack surfaces by isolating environments and segmenting workloads.
2. Algosec: AlgoSec provides a suite of enterprise firewall management tools for policy, configuration, and analysis of rules, configuration, and design.
3. Appgate: Provides Appgate SDP, a solution recognized for its flexibility and robust configuration capability in microsegmentation.
4. Check Point: Provides comprehensive security solutions, including microsegmentation to protect cloud and network environments.
5. Cisco: Cisco Secure Workload offers robust microsegmentation capabilities, providing 100% telemetry coverage and full visibility of activities on endpoints and networks.
6. Elisity: Elisity was designed to help companies' security needs within cloud, mobility, and connected devices.
7. F5: Specializes in application services and network security, including microsegmentation to secure data and applications.
8. Fortinet: Provides microsegmentation capabilities that enhance network security and control within cloud and on-premise environments.
9. Illumio: Focuses on microsegmentation to enhance cybersecurity, limiting the lateral movement of threats within network environments.
10. Juniper Networks: Offers solutions that focus on securing network traffic and implementing microsegmentation in complex network environments.
11. Nutanix: Provides Nutanix Flow, a solution focused on network and process-level policies for safeguarding critical applications.
12. Palo Alto Networks: Specializes in microsegmentation with a focus on role-based access control, image signing, and runtime protection for containers.
13. Truefort: TrueFort develops products focused on application and cloud workload protection using a unified, application-context approach and behavioral analytics engine.
14. Varmour: vArmour provides software-based distributed security controls such as segmentation and deception to virtual and cloud environments.
15. VMware: Offers microsegmentation solutions as part of its broader network security and cloud infrastructure services.

About TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations in cybersecurity, artificial intelligence, and sustainability to enterprise teams, government agencies, and commercial vendors.