Key Takeaways

- Emerging use cases are solving for security challenges in new ways. These use cases include: Cloud Infrastructure Entitlement Management, SaaS Security Posture Management, Cloud Native Protection Platform and Policy as Code.
- Misconfigurations in cloud security remain the biggest cloud security risk, according to 67% of cybersecurity professionals (Fortinet 2021 Cloud Security Report).
- The "cloud skills gap" is a rapidly growing challenge and many organizations will need to adopt a program for evolving their cultures and upskilling their workforce to ensure they are cloud-ready.
- Comprehensive cloud security is a full spectrum spanning from development to runtime, with emerging solutions seeking to provide a single policy engine for seamless continuity.
- The foundation of cloud security is identity; therefore, enterprises creating a cloud strategy should begin with the initial design of an organization's cloud accounts leveraging the principles of Zero Trust.
- While identity solutions are emerging, this is one of the most challenging areas for dynamic environments and we can expect the landscape will evolve to meet the complicated nature of cloud identity security.
- While cloud service provider (CSP) security offerings are generally preferred by enterprises, organizations leveraging multi-cloud prefer third party security vendors, as they provide a unified view into cloud environments.

What is it

Cloud Security is a discipline of cybersecurity providing protection for workloads, data and infrastructure in public, private and hybrid cloud environments. It is composed of: visibility & compliance, compute/workload security, network protections, data security & retention, and identity management. Emerging solutions frequently address new security use cases at the nexus of the NIST Cybersecurity Framework functions of: Identify, Protect, Detect, Respond and Recover.

Why It Matters

Fundamentally, security ensures that entities can only do what they should be able to do. Yet, applying the principal of least privilege for cloud-based workloads is an ever-evolving challenge. Cloud-based services increase an organization's velocity when it comes to serving their clients and staying ahead of their competition, but the tradeoff is a complex paradigm with several new emerging issues every year. As cloud-based services become more sophisticated, the attack surface grows and with it a requirement for greater governance, controls, skill sets and continuous focus on cloud security strategies. Equally dynamic is the technology to support organizations in their security efforts. Comprehensive cloud security requires sophisticated solutions in support of an organization's cloud security strategy. To ensure cloud workloads are secure, it is important for enterprises to proactively adopt the necessary security solutions for their cloud environments.

Approaches

The following section is focused on cloud security, which can be further broken into the established use cases and the emerging areas for securing diverse environments.

Established Use Cases:

Cloud Access Security Broker (CASB) – Software that mediates enterprise user access to cloud services, initially for SaaS applications and has expanded use cases into IaaS & PaaS. CASBs were originally designed to extend on-premise security policies to the cloud environment, preventing the growth of "shadow IT". Today, the CASB market is fully developed with capabilities encompassing visibility, compliance, and threat protection through policies including: authentication, encryption, tokenization, logging, malware detection, and user behavior analytics (UBA).

Cloud Workload Protection Platform (CWPP) – A comprehensive CWPP provides a workload-centric security protection solution for all types of workloads (physical servers, virtual machines, containers and serverless). According to Gartner, CWPP encompasses eight layers of control: 1. Hardening, configuration and vulnerability management, including scanning for vulnerabilities before software is pushed to production. 2. Network firewalling, visibility and micro segmentation. 3. System integrity assurance. 4. Application control and allow listing. 5. Exploit prevention and memory protection. 6. Server workload EDR, behavioral monitoring, and threat detection and response. 7. Host-based IPS with vulnerability shielding. 8. Anti-malware scanning. This visibility across hybrid and multi-cloud environments is furnished from a single pane of glass, and protects enterprise workloads running on any cloud instance.

Cloud Security Posture Management (CSPM) – CSPM protects workloads from the outside (as opposed to inside like CWPP) by assessing secure and compliant configurations of the cloud platform's control plane. A CSPM solution is continuously identifying excessive or unknown risk across an organization's entire cloud estate. There are 6 key capabilities of a CSPM solution: 1. Compliance Monitoring. 2. DevOps Integration. 3. Configuration Monitoring. 4. Asset Inventory. 5. Risk Assessment. 6. Incident Response. Emerging CSPM solutions are offering features such as agentless, risk-based prioritized cloud security risks, suggested and automated remediation as well as inclusive uses cases found in both Cloud Workload Protection Platforms (CWPP) and Cloud Infrastructure Entitlement Management (CIEM).

Container Security - Traditional practices for securing VMs don't apply to containerized landscapes. Compared to VMs, containers have many more instances, change at a faster rate, and have much more ephemeral networking. For example, containers change IP addresses frequently, meaning they can't be secured by traditional techniques that rely on the static IP addresses usually found in VM and bare metal servers. Container security refers to the ecosystem of solutions that protect, detect, and respond to threats spanning both development and deployment. Container security solutions are often lumped together but may only provide coverage for a particular area. The six key areas in addressing container security are 1. Development process, 2. Image registries, 3. Runtime, 4. Orchestration, 5. Ephemerality, 6. Secrets Management.

Emerging Use Cases:

Cloud Infrastructure Entitlement Management (CIEM) –Defined by Gartner as identity-centric SaaS solutions focused on managing entitlements and data governance in today's hybrid and multi-cloud IaaS set-up. Key attributes of a CIEM solution include discovering all identities, service accounts, IAM users, roles and policies within single or multi cloud IaaS infrastructure. As for the governance part of the solution, CIEM solutions execute routine audits of configurations across cloud environments for the means of policy enforcement and compliance. When adopting CIEM, it is important that organizations go through the exercise to define least privilege policies. While standalone CIEM solutions exist, this use case appears to be heading towards a feature of a large cloud security suite.

SaaS Security Posture Management (SSPM) – SSPM solutions offer tools and automation capabilities that can provide visibility into the security posture of SaaS environments and make it easier to remediate security concerns in those environments. Under the shared responsibility model that SaaS providers follow, the customer is responsible to protect user access and data. The goal of SSPM solutions is to provide visibility and tooling required to adequately manage and protect user access and data in SaaS environments. Key features in SSPM solutions are: 1. Continuous monitoring for risks and violations 2. Detection of misconfigurations in application or privileges. 3. Guided and automated remediation. 4. Built-in security benchmarks. 5. Single pane of glass. There is a symbiotic relationship between CASB and SSPM with many CASB vendors adding SSPM lite capabilities.

Cloud Native Application Protection Platform (CNAPP)- New category coined by Gartner that signifies the converging of CWPP, CSPM, workload-scanning capabilities and shifting left into development. It combines the breadth of CSPM with the depth of CWPP and also includes elements of CIEM to fully protect cloud workloads during development and runtime. The rise of CNAPPs reflects market demand for solutions that support DevSecOps implementation, allowing unified visibility across the development lifecycle.

Policy as Code (PaC) - Policy-as-Code allows an organization to translate the policies into machine-readable definition files, and use them to enforce and validate that the resources provisioned meet those policies. As such, the challenge that policy-as-code is trying to solve is the challenge of as-much-as-possible automation in DevOps practice. PaC automates the policy enforcement while extending the benefits of IaC. By leveraging PaC and defining governance and control activities in code, organizations can systematically declare, test, execute, measure and maintain security – aligning well with complex and dynamic cloud architectures. According to Dr. Chenxi Wang (Rain Capital) "Implementing policy as code does mean that an organization must adopt many of the DevOps methodologies. This includes maintaining controls in a central repository, applying version control, enabling automatic validation in the pipeline, and continuously monitoring performance are crucial elements of PaC." A well-executed PaC strategy can define and validate constraints on cloud systems, limiting the exposure of underlying infrastructure to risks introduced by human error. Example of a security policy that can be expressed and enforced as PaC is "all hosts must use approved standard images" or "google cloud compute instances cannot use the default service account".

Trace3 Innovation's Point of View

As organizations scale their cloud resources, cloud security and its dependencies (policies, procedures, controls, and technology) must also evolve. Implementing cloud security not only increases cost and complexity, but the paradigm shift of multi-cloud (inclusive of SaaS) creates an inability to implement centralized policies. Survey data from 451 Research, Fortinet and Trace3 canvas efforts reveal the most reported types of cloud misconfiguration spring from a disconcerting lack of identity and access management basics, such as the use of default passwords and lack of multi-factor authentication. Additional misconfigurations include externally facing workloads subject to port scanning, overly permissive accounts targeted by bad actors, and unauthorized access to services via open ports. This has resulted in data compromises and the introduction of malware, including crypto miners and ransomware. Additionally, a cloud security skills gap is creating real challenges that tooling alone cannot overcome, causing teams to have difficulty in carrying out strategy on infrastructure and evolving features.

Cloud security use cases and the subsequent landscape of solutions are evolving as rapidly as other cloud offerings. As a differentiator, these solutions appear to be taking a "who is the buyer" approach with the focus on three types of buyers: developer centric, security centric and governance centric. Each group has a different lens on the challenges and potentially different budgets. As an example, Policy-as-Code is a potentially disruptive solution targeted towards buyers; however, it is important to understand how PaC can be leveraged to secure assets at scale. With multiple groups of buyers evaluating, this could easily create an overlap in the purchase of tooling features and functionality. Another evolving landscape is identity security and while the market may appear to be signaling that identity security will become a feature of a larger offering (I.e. CNAPP), Trace3 Innovation believes otherwise. Due to identity's challenge in bringing together policy, governance and tooling, investments in more robust, full lifecycle solutions are underway and we expect these identity solutions will continue to evolve their protection capabilities.

For a successful implementation, an organization should not adopt each new use case that is introduced, but rather design a comprehensive cloud security strategy for policies, procedures, controls, and technology. Security strategies can be challenging to create in dynamic hybrid environments; however, Application Relationship Management (ARM) solutions can help by creating continuous visual representation of assets and associated mapping to determine security risks. The Cloud Security Technical Reference Architecture (CSTRA) created by the Cybersecurity and Infrastructure Security Agency is another resource for providing recommendations for cloud migration and data protection with regards to: Shared Services, Cloud Migration and Cloud Security Posture Management. Some key take-aways from CSTRA best practices include: DevSecOps with automated security testing, CSPM and Zero Trust practices to maximize security. Trace3 Innovation firmly believes the best way for organizations to reconcile the extensive options available is to consult their unique hierarchy of cloud needs and recommends continuous, full-cycle security at both development and runtime. To address the cloud skills gap, it is recommended to create a comprehensive training strategy with clear incentivized goals and create a partnership between security and development teams for carrying out security evaluations, as the adoption of an agile framework has created large volumes of distributed workloads with short life spans and multiple iterations.

Enterprises generally prefer to utilize native security capabilities offered by CSPs, since these come at no additional cost or are packaged in a cost-effective manner; however, they should seek to understand their security obligations outlined in the shared responsibility model (SRM), as it is common to overestimate the

accountability CSPs vow to take in security operations. Over half of these enterprises are also turning to third parties in order to create a unified view into their cloud environment. These third-party security vendors are differentiating themselves by focusing on integration to enterprises' CI/CD pipelines, infrastructure as code, and more. Enterprises are also leveraging legacy and hybrid environments, as they require uniform control across many different environments. As larger security platforms acquire other solutions to fit emerging categories, we encourage organizations to fully explore how those acquisitions have been integrated. The goal will be to identify potential gaps and vulnerabilities in a "platform solution".

Solutions

All vendors provided are examples and is not meant to be an exhaustive list. Emerging technologies are subject to significant changes in market share and relative capability.

Cloud Access Security Broker (CASB)

Censornet CASB enables your business to discover, analyze, secure and manage user interaction with cloud applications. Achieve complete visibility and control with a full-featured CASB solution and protect your modern mobile workforce. Integrated with Web Security for visibility and protection at every stage of an attack.

Lookout Cloud Access Security Broker (CASB) provides full visibility into the interactions between users, endpoints, cloud apps and your data. It also enables you to dynamically dial in Zero Trust access controls. With continuous monitoring of user and entity behavior analytics (UEBA), you can detect and respond to insider threats and advanced cyberattacks.

Bitglass enables data security on any device without agents for managed applications. Our cloud access security broker (CASB) solution protects data end-to-end, from any cloud app to any device. Enforce access controls, limit sharing, protect against malware, avoid data leakage, and more.

Netskope's industry-leading cloud access security broker (CASB) solution enables you to quickly identify and manage the use of cloud applications, regardless of whether they are managed or unmanaged. Prevents sensitive data from being exfiltrated from your environment by risky insiders or malicious cybercriminals who have breached your perimeter.

Proofpoint Cloud App Security Broker (Proofpoint CASB) helps you secure applications such as Microsoft Office 365, Google Workspace, Box and more. It gives you people-centric visibility and control over your cloud apps, so you can deploy cloud services with confidence. What's more, our powerful analytics help you grant the right levels of access to users and third-party add-on apps based on the risk factors that matter to you.

Zscaler CASB enables organizations to securely adopt and govern the use of SaaS applications, IaaS offerings, and PaaS. It provides real-time visibility and controls access and user activity across sanctioned and unsanctioned applications. The fully integrated platform eliminates overlay architectures and simplifies policy creation and administration, ensuring data is protected and compliance is maintained.

McAfee is a security technology company, headquartered in Santa Clara, California, and delivers proactive and proven solutions and services that secure systems and networks. Built natively in the cloud and for the cloud, MVISION Cloud (CASB) applies persistent protection to sensitive information wherever it goes inside or outside the cloud.

Cloud Security Posture Management (CSPM)

Ermetic offers a new cloud security solution that gives enterprises deep visibility and control over access to critical data and infrastructure, along with policy enforcement, asset management, risk analysis and automated remediation — in single or multi cloud environments. Ermetic enables enterprises to enforce least privilege principles for both user and service identities, across the entire technology stack. With Ermetic, Security and DevOps stakeholders can work together to ensure security without disrupting application continuity or velocity.

Built for today's cloud-scale enterprises, DisruptOps is a Cloud Security Operations Platform to monitor, alert, and respond to security risk in cloud infrastructure. DisruptOps combines the visibility security wants with the automation DevOps teams need.

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. Dig's Governance Automation Engine automates workflow, remediation, and prevention capabilities across cloud and security teams to ensure end-to-end security.

Corestack is a governance platform for cloud services. With its Cloud-as-Code approach, the platform delivers predictable outcomes supporting business agility, adherence to policies, and enforces budgetary compliance. It enables cloud services with a governance platform and an operations manager.

Orca Security is a cloud visibility company. Its Orca Cloud Visibility Platform utilizes its SideScanning technology to deliver full-stack visibility into the entire cloud infrastructure and assets.

Aqua provides self-securing capabilities to ensure your cloud accounts don't drift out of compliance. Get detailed, actionable advice and alerts, or choose automatic remediation of misconfigured services with granular control over chosen fixes.

Threat Stack enables growth-driven companies to scale with confidence by identifying and verifying insider threats, external attacks and data loss in real-time. The fully integrated, cloud-native continuous monitoring solution that gives customers visibility and automatically responds to changes in their environment, Threat Stack provides the coverage needed to run secure and compliant, in all environments, without sacrificing speed and efficiency.

Cloud Workload Protection Platform (CWPP)

NeuVector offers a cloud-native Kubernetes security platform with end-to-end vulnerability management, automated CI/CD pipeline security, and complete run-time security, including the industry's only container firewall to block zero days and other threats. DevOps, DevSecOps, and Security teams have the tools and protection they need to secure the entire container pipeline, from Build to Ship to Run, automatically.

Caveonix is a truly innovative digital risk-management platform designed to govern an enterprise's assets within hybrid and multi-cloud environments. We're powering enterprises to automate and secure their operations, giving teams application-aware visibility, and empowering senior leaders to make the necessary decisions from a reliable data source. With an easy-to-use compliance and audit management solution and continuous security and protection, Caveonix is your single source of truth that helps you govern your digital transformation.

Tigera is the industry leader in Kubernetes security and observability, and the inventor and maintainer of Calico Open Source. We enable organizations of all sizes in various industries to secure, observe, and troubleshoot cloud-native applications in Kubernetes environments. Our solutions are used by leading companies, including AT&T, Discover, Merck, ServiceNow, HanseMerkur, RealPage, L3Harris, and Mindbody.

BluBracket is an enterprise security solution for code in a software-driven world. BluBracket gives companies visibility into where source code introduces security risk while also enabling them to fully secure their code—without altering developer workflows or productivity.

Sysdig provides an intelligence platform to deliver monitoring, security, and troubleshooting in a microservices-friendly architecture used by a community of developers, administrators, and other IT professionals looking for visibility into systems and containers.

Cloud Infrastructure Entitlement Management (CIEM)

Ermetic prevents cloud data breaches by automating the detection and remediation of identity and access management risks in AWS, Microsoft Azure, and Google Cloud. It automatically discovers all user and service identities, and analyzes their entitlements, as granted by roles/scope and policies, using a continuous lifecycle approach. By combining analytics with granular, full stack insight, Ermetic makes it possible to enforce least privilege access at scale even in the most complex public cloud environments.

Britive's platform empowers teams across cloud infrastructure, DevOps, and security functions with a dynamic and intelligent privileged access administration solution. Using deep API-based integrations, our technology orchestrates permissions for the modern enterprise cloud infrastructure and applications. Britive helps organizations implement cloud security best practices like just-in-time (JIT) access and zero standing privileges (ZSP) to prevent security breaches and operational disruptions.

With centralized visibility and automated policy enforcement as part of a complete identity solutions, SailPoint makes it easy to control and govern user access across AWS, Azure, and Google Cloud Platform. And with their identity driven ecosystem of connectors and integrations, organizations can gain complete visibility of access to all your systems, users, and their roles.

Saviynt offers complete access governance and intelligence solutions for critical data, workloads, devops resources, and access to critical applications on cloud and enterprise. Saviynt combines granular application access, risk and usage analytics, real-time prevention with out-of-box risk signatures and SOD rules to address security and compliance needs for the enterprise.

SaaS Security Posture Management (SSPM)

Grip Security brings the industry's most comprehensive visibility across an enterprise's entire SaaS portfolio – known or unknown for SaaS applications, users, and their interactions – with extreme accuracy and deployment in minutes. Armed with deep visibility, Grip's enforceable endpoint-centric approach secures all SaaS application access regardless of device or location as well as maps data flows to apply security policies – including data loss prevention.

Adaptive Shield enables security teams to see and fix configuration weaknesses quickly in their SaaS environment, ensuring compliance with company and industry standards. Adaptive Shield provides a system that is able to detect all incorrect security configurations in all the applications that are in the organization. The system then offers automatic corrections to those configurations, and provides continuous monitoring and alerts in case of changes that could be a future opening for information leakage.

Vectrix is an easy-to-use, online security platform that gives users an effective way to scan and monitor their SaaS vendors for security issues, like insecure settings, suspicious activity, and best practices violations. No-code Vectrix scans are designed to be the fastest, easiest way to have your security needs covered, both today and tomorrow.

AppOmni provides unprecedented data access visibility, management, and security of SaaS solutions, enabling organizations to secure mission-critical and sensitive data. AppOmni's technology deeply scans APIs, security controls, and configuration settings to evaluate the current state of SaaS deployments and compare against best practices and business intent. With AppOmni, organizations can establish rules for data access, data sharing, and third-party applications that will be continuously and automatically validated.

Obsidian delivers best-in-class SSPM, enabling you to strengthen your security posture proactively. The platform offers unified visibility and monitoring of accounts, privileges and activity. Using Obsidian, organizations can prune inactive accounts and fix common application misconfigurations to reduce risk. A lower risk profile not only reduces

the chance of a costly breach, but also lowers the indirect costs of ongoing security efforts.

Cloud Native Application Protection Platform (CNAPP)

Wiz analyzes all layers of the cloud stack to reveal actionable insights about high-risk attack vectors in your cloud so you can prioritize and fix them. Wiz uses a unique technology to scan deep within VMs and containers without needing an agent, analyzing all of your workloads even if a resource isn't online. You can connect Wiz to all of your cloud environments, whether public cloud like Amazon Web Services, Microsoft Azure, and Google Cloud Platform or on premises like OpenShift.

Orca Security, the cloud security innovation leader, provides cloud-wide, workload-deep security and compliance for AWS, Azure, and GCP. Orca treats your cloud as an interconnected web of assets, prioritizing risk based on the severity of the underlying security issue combined with environmental context. Our SideScanning™ technology reads your cloud configuration and workloads' runtime block storage out-of-band, detecting vulnerabilities, malware, and misconfigurations.

Uptycs provides a cloud-native security analytics platform for security analysts, site reliability engineers, incident response teams and IT professionals to observe and secure their cloud workloads and endpoints -- all from the same place. The Uptycs platform includes capabilities in CSPM, CWPP, XDR, insight & inventory, audits, and compliance & governance.

The Aqua Cloud Native Security Platform provides prevention, detection, and response automation across the entire application lifecycle to secure the build, secure cloud infrastructure and secure running workloads wherever they are deployed. Aqua checks your cloud services, Infrastructure-as-Code templates, and Kubernetes setup against best practices and standards, to ensure the infrastructure you run your applications on is securely configured and in compliance.

The Threat Stack Cloud Security Platform delivers full stack security observability across the cloud management console, host, container, orchestration, managed containers, and serverless layers. Threat Stack provides the flexibility to consume telemetry within existing security workflows — or manages it with you through the Threat Stack Cloud SecOps Program, so you can respond to security incidents and improve your organization's cloud security posture over time.

MVISION is the industry's first platform to bring application and risk context to converge Cloud Security Posture Management (CSPM) for public cloud infrastructure, and Cloud Workload Protection (CWPP) to protect hosts and workloads including VMs, containers, and serverless functions. McAfee MVISION CNAPP extends MVISION Cloud's data protection – both Data Loss Prevention and malware detection – threat prevention, governance and compliance to comprehensively address the needs of this new cloud-native application world thereby improving security capabilities and reducing the Total Cost of Ownership of cloud security.

Policy as Code

Manage you cloud security, compliance, and operations through a single pane of glass, leveraging Secberus' policy-first Enterprise Governance Platform. Secberus' continuous adaptive policy assessment framework enables you to assess, respond, adapt and prevent cloud misconfigurations and risk at enterprise scale.

Magalix sets out to accelerate the implementation of innovative technologies and products by powering developers and security teams with the tools for them to codify security and compliance in their software development lifecycle."

Stacklet is a cloud governance company that provides operational efficiencies and increased manageability for organizations that want to embrace policy as code at scale

Concourse Labs automates cloud governance, protecting enterprise data, controlling risk, and accelerating success in the cloud. Concourse pinpoints the root cause of each risk, specifying the code and configuration that needs to be corrected so developers can immediately fix non-compliant applications.

Styra enables enterprises to define, enforce, and validate security across their Kubernetes environments. With a combination of Open Source (Open Policy Agent) and commercial solutions (Declarative Authorization Service), Styra provides compliance guardrails to secure applications and ease compliance. Styra's policy-as-code solution lets DevOps and Security teams mitigate risks, reduce human error, and accelerate app development.

Fugue simplifies cloud operations with its software-defined system for orchestrating and enforcing cloud infrastructure at scale. Teams can use Fugue to declare the desired state of cloud infrastructure and policies in a collaborative, human-friendly programming language and

Fugue

automate the provisioning, management and teardown of complex cloud environments, while continuously enforcing infrastructure state and policy compliance.

accurics™
Immutable Security™

Accurics helps companies secure cloud native infrastructure throughout the DevOps lifecycle and eliminate risk posture drift.

checkov
by bridgecrew

Checkov scans cloud infrastructure configurations to find misconfigurations before they're deployed.
Checkov uses a common command line interface to manage and analyze infrastructure as code (IaC) scan results across platforms such as Terraform, CloudFormation, Kubernetes, Helm, ARM Templates and Serverless framework.