HORANGI
CYBER SECURITY

The Hitchhiker's Guide To Cloud Security

Deciding Between Native and Third-Party Tools

Report — **May 2021** — **Whitepaper**

What You Need to Know

- **The Move to Remote Work has Accelerated Cloud Computing Adoption.** The COVID-19 pandemic has shifted a majority of companies to remote work, further fueling an already accelerated pace of cloud computing adoption. The number of businesses with more than half of their IT workloads hosted in the cloud is expected to double to 56% within the next year, with a quarter of respondents expecting to have over 75% of their workloads in the cloud by the same period.

- **Cloud Security is the Largest IT Investment Priority for Executives in 2021.** With more companies adopting cloud computing, CCS Insight surveys highlight that companies are now prioritizing IT Security as the largest IT investment moving into 2021. This is driven by the increasing risk of data breaches, potential abuses of cloud resources, and additional compliance regulations enforced unto organizations such as the EU's General Data Protection Regulation (GDPR) and Monetary Authority of Singapore's Third-Party Risk Management (MAS TRM) Guidelines.

- **Types of Cloud Security Solutions: Native Cloud and Third-Party.** There are two categories of services available to end-users in ensuring application-level cloud security. Native Cloud Security, which are security tools offered by Cloud Service Providers (CSP) within their existing infrastructure, and Third-Party Security, which are out-of-the-box solutions offered by non-CSPs.

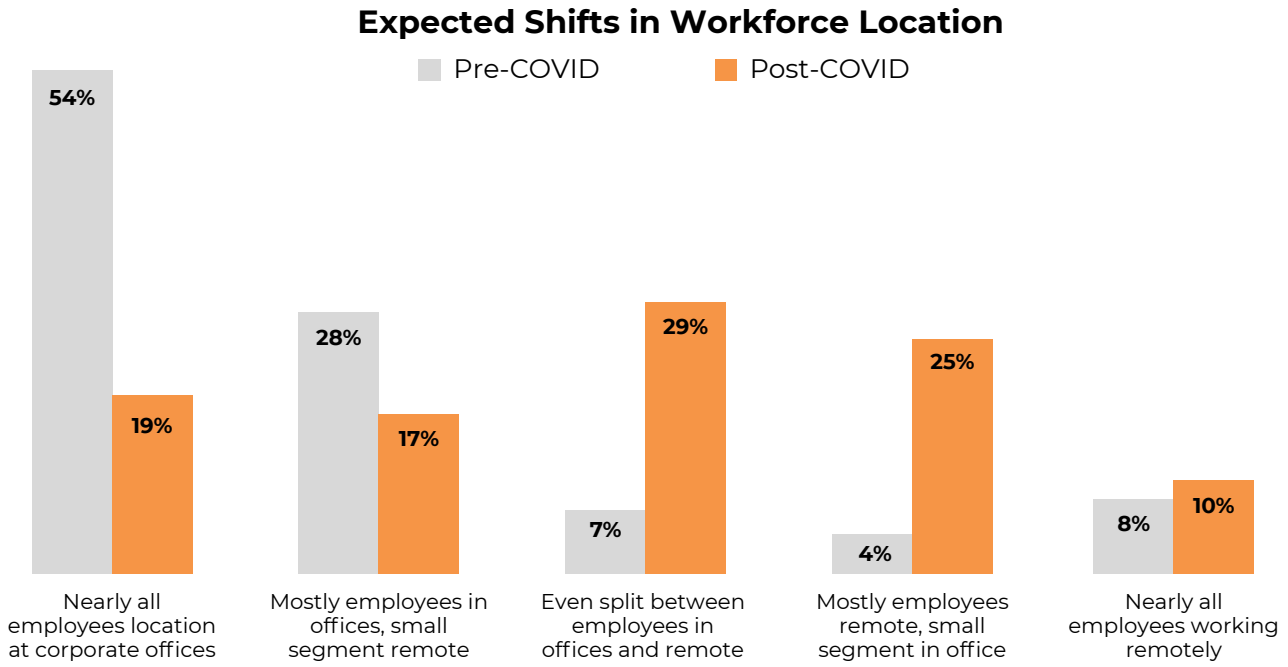
- **Native Cloud Security Solutions May Cover Basic Security Needs But Can Have Gaps.** The top three cloud service providers for Q4 2020 are Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) and each provides its own suite of Native Cloud Security tools. They are often simple to configure for very simple, basic deployments and cover an organization's basic security needs but have gaps when it comes to more complex IT infrastructures, such as multi-cloud environments or a mix of cloud and on-premise security. Additionally, they can be costly when considering the need to hire and maintain in-house cloud security experts to continuously configure and maintain security tools.

- **Third-Party Cloud Security Augments Areas That Native Cloud Security Fall Short At.** These are usually out-of-the-box solutions that aim to address the gaps of Native Cloud Security. They are often more comprehensive and work in any cloud environment. There are three different categories of Third-Party Cloud Security: Cloud Access Security Brokers (CASB) provide visibility and control over cloud usage and access. Cloud Workload Protection Platforms (CWPP) secure workloads and resources across multiple cloud environments. Cloud Security Posture Management (CSPM) uses automation to assess an organization's cloud security, flag potential security threats or compliance violations, and suggest steps to remediate them.

- **Factors When Choosing Native or Third-Party Cloud Security Solutions.** In choosing between the two, decision-makers should take into consideration the company's current resources and cloud security expertise, current IT infrastructure, the expected usage of the cloud, the complexity of the business as well as its regulatory environment, and the sensitivity of data being handled. For companies with relatively simple business operations in a single cloud environment, Native Cloud Security could be sufficient. However, for companies in complex and highly regulated industries such as finance, healthcare, services, and government, Third-Party Cloud Security can provide better security coverage.

The Move to Remote Work has Accelerated Cloud Computing Adoption

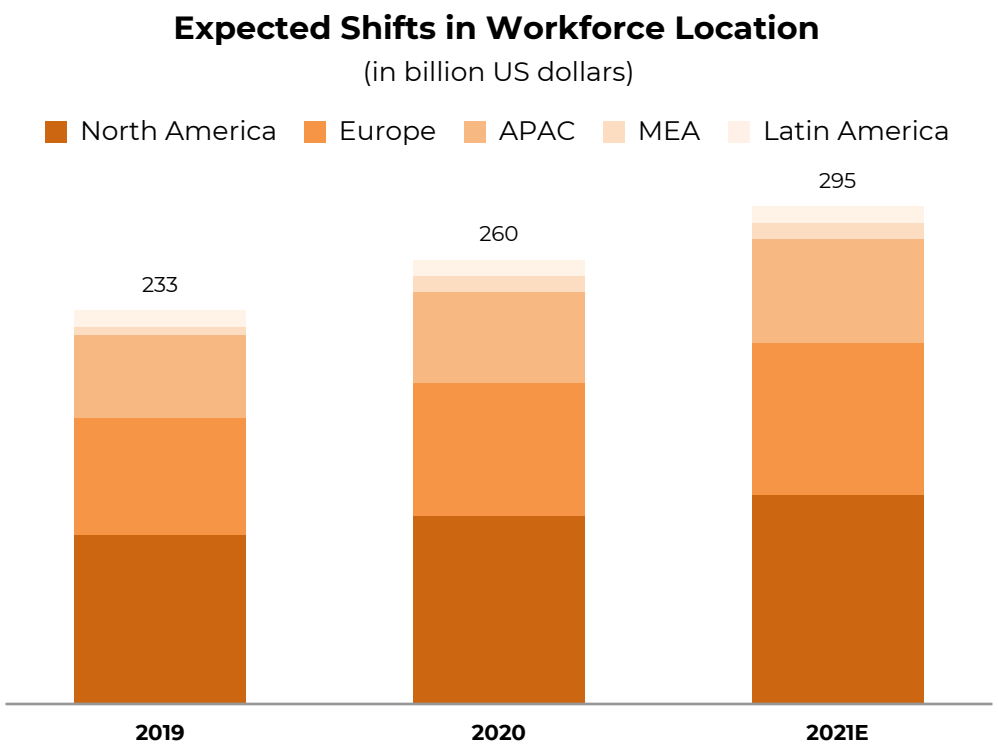
The mass shift to remote work – as a direct result of the COVID-19 pandemic – has served as one of the key catalysts in the already accelerated adoption of cloud computing solutions in 2020. As seen in the chart below, surveys conducted by the Computing Technology Industry Association (CompTIA) show that 64% of companies expect at least half of, if not all, employees will be working remotely in the future, as opposed to only 19% expecting such pre-COVID.



Source: CompTIA (November 2020), Zero One

Given this, companies around the world have been forced to rapidly reconfigure their operations to better enable their employees to work remotely, which is made easier by adopting cloud-based systems. After all, the cloud reduces dependency on on-premises data centers, is highly scalable and flexible, and ensures data and applications are always available from anywhere.

According to CCS Insight, the number of businesses with more than half of their IT workloads hosted in the cloud is expected to double to 56% within the next year, with a quarter of respondents expecting to have over 75% of their workloads in the cloud by the same period. Overall, the cloud computing market is expected to rise from US$233 billion in 2019 to US$295 billion by 2021, at a Compound Annual Growth Rate (CAGR) of 12.5%, according to MarketsandMarkets.



Source: Markets and Markets (April 2020), Zero One

Cloud Security is the Largest IT Investment Priority for Executives in 2021

With more and more people working remotely via the cloud, the number of risks that companies face has drastically increased. According to IBM Security, a remote workforce as a result of COVID-19 was found to increase the average total cost of a data breach by nearly US$137,000. See below for the average cost of a data breach for selected regions for the years 2020 and 2019.

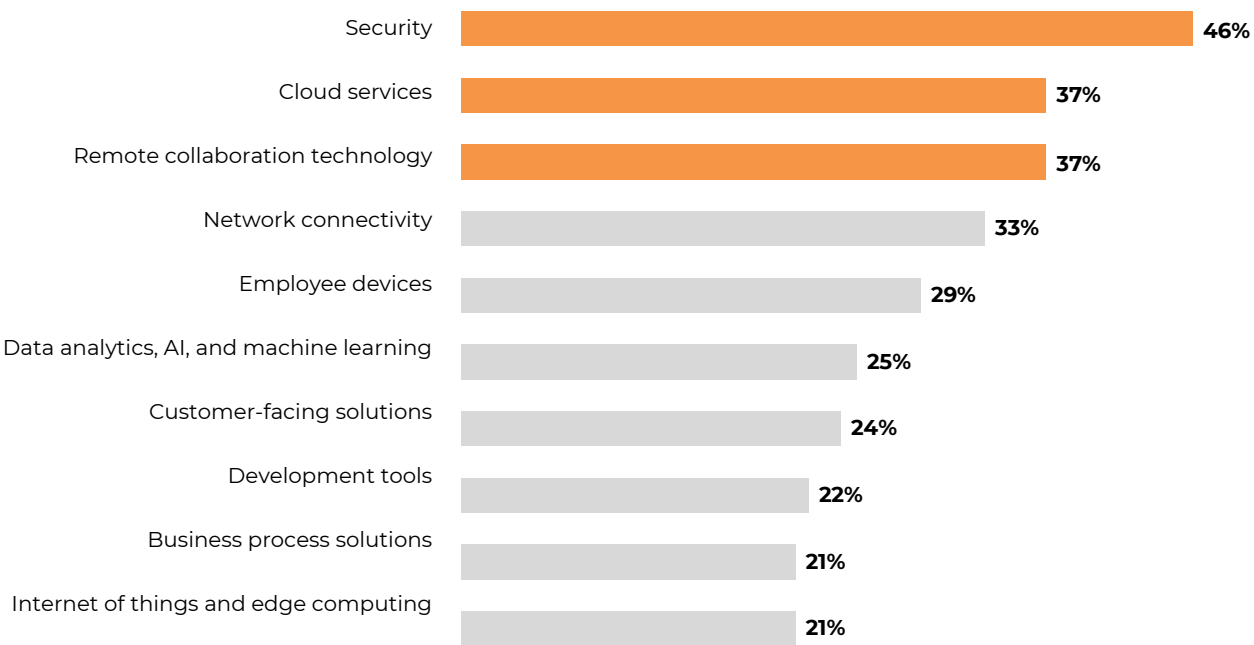
Average Cost of a Data Breach for Selected Regions (in million US$)

Region	2020	2019	% Increase YoY
Global	3.86	3.9	(1%)
ASEAN	2.71	2.15	26%
Australia	2.15	2.13	1%
India	2	1.83	9%

Source: IBM Security (April 2020), Zero One.

As businesses continue to migrate towards cloud computing, coupled with a regulatory climate and cyber-threat landscape constantly in flux, CCS Insight surveys have identified IT Security as the largest IT investment priority for companies as they move forward into 2021.

IT Investment Priorities for 2021

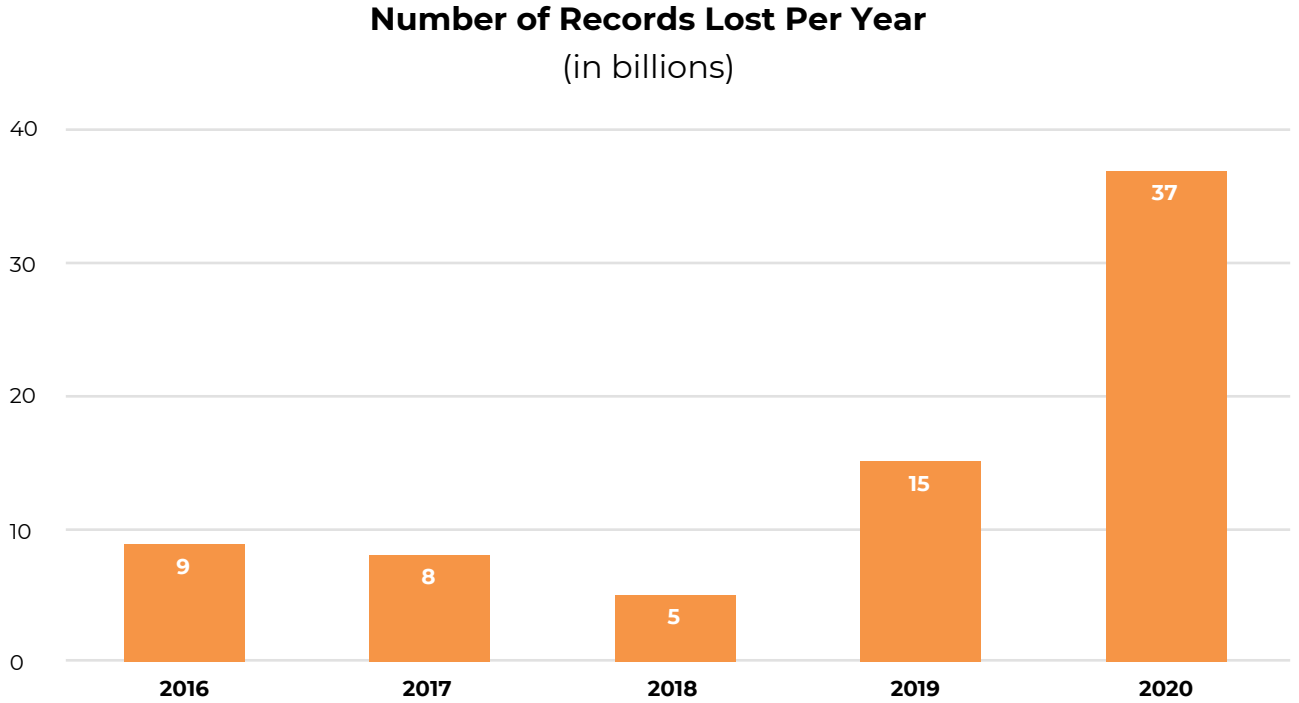


Source: CCS Insight (November 2020), Zero One

We take a deeper dive below into some of the key factors that will continue to drive IT Security:

1. Increasing Risk of Data Losses & Breaches

The quickened pace of cloud adoption has created more vulnerabilities and holes for exploitation. According to security firm Risk Based Security (RBS), the volume of records that were compromised by data breaches globally jumped by 141% to 37 billion records exposed in 2020, the largest number seen by RBS since 2005. The type of records loss can range from personal or publicly identifiable information of customers or employees, to even an organization's intellectual property or trade secrets.



Source: Risk Based Security (January 2021), Zero One

In particular, ransomware coupled with data theft has seen a 100% increase, growing from 337 confirmed data breach events to 676 in 2020. Ransomware involves the encryption of business data and systems stored in the cloud by malicious actors, where they then hold these for ransom. These data losses and breaches have the potential for serious reputational and financial implications for organizations, depending on the amount and sensitivity of the data that was stolen.

2. Heightened Abuse of Cloud Resources

Beyond data leaks and losses, the increased pace of cloud adoption could lead to various types of unsanctioned use of an organization's cloud resources, whether by malicious actors or employees. Third-party attackers who gain access to a company's cloud infrastructure could manipulate the resources to conduct their own criminal activities such as hosting malware or launching Distributed Denial-of-Service (DDoS) attacks, leaving a company unknowingly complicit or even liable to these crimes.

Another abuse of cloud resources often seen is unlawful cryptomining. Malicious actors will gain access to an organization's high-bandwidth cloud infrastructure to mine cryptocurrencies for their personal benefit, ballooning the organization's cloud fee.

Even employees, who have been granted cloud access could abuse an organization's cloud resources by using storage space or even cloud instances for personal projects, leading to increased costs to the business.

3. Additional Compliance and Enforcement Regulations

Since the EU's General Data Protection Regulation (GDPR) took effect in May 2018, the world of data privacy has shifted its focus from guidance to stepped-up enforcement. Organizations are now held liable for data breaches by third party actors due to inadequate controls, with potential fines of up to 4% of annual revenue or US$22 million, whichever is greater. In 2019, multinational companies such as H&M and Marriot were fined as much as US$56 million for GDPR violations.

5 Biggest GDPR Fines as of Date

Company	Country	Violation Fine
Google Inc.	France	US$56M
H&M Hennes & Mauritz	Germany	US$40.2M
TIM - Telecom Provider	Italy	US$31.2M
British Airways	United Kingdom	US$24.7M
Marriott International	United Kingdom	US$22.9M

Source: Data Privacy Manager (January 2021), Zero One

Additionally, organizations in highly regulated industries such as finance, healthcare, services, or government have their own set of compliance standards that need to be adhered to, lest they risk losing their license to operate. Examples of such compliance standards include the Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and the Monetary Authority of Singapore's Third-Party Risk Management (MAS TRM) Guidelines. Other compliance requirements such as ISO 27001 or SOC 2 certifications may be prerequisites for doing business with larger enterprises with strict vendor management processes in place.

Types of Cloud Security Solutions: Native Cloud and Third-Party

Following the Shared Responsibility Model, the move to cloud computing assigns the responsibility of physical security and infrastructure security (Security of the Cloud) to Cloud Service Providers (CSPs). However, cloud users are still responsible for application-level security such as data encryption and user access (Security in the Cloud). Some of the most important application-level security controls and tools that organizations need to consider in a cloud context are the following:

- Identity and access control
- Network access control: Firewalls and anti-DDoS
- Data Security: Encryption at rest & in transit, secrets management
- Logging
- Auditing and monitoring
- Security operations centers, configuration & compliance

There are two categories of services available to end-users in ensuring application-level cloud security. Native Cloud Security, which are security tools offered by CSPs within their existing infrastructure, and Third-Party Security, which are out-of-the-box solutions offered by non-CSPs. We summarize in the table below the differences between the two:

	Native Cloud Security	**Native Cloud Security**
Implementation	Simple to deploy a tool, as it's already integrated with other CSP products. However, it needs heavy customization depending on the user's infrastructure.	Implementation is often supported by vendor's team of security experts
Maintenance	Requires an extensive in-house security team to keep security policies up-to-date and relevant.	Solutions continuously scan existing cloud configuration for potential threats. Vendors often provide 24/7 customer support.
Pricing	Sometimes offers a free version with very limited features. Paid version has additional features but with pricing based on usage.	Variety of flexible pricing such as subscription per user account, GB storage, rule, or resource.
Applicable IT Infrastructure	Applicable only for its corresponding cloud environment.	Can interface and cover multi-cloud environments or infrastructures with a mix of cloud and on-premise security.

Native Cloud Security Solutions Are Simple to Deploy and Cover Basic Security Needs But Can Have Gaps

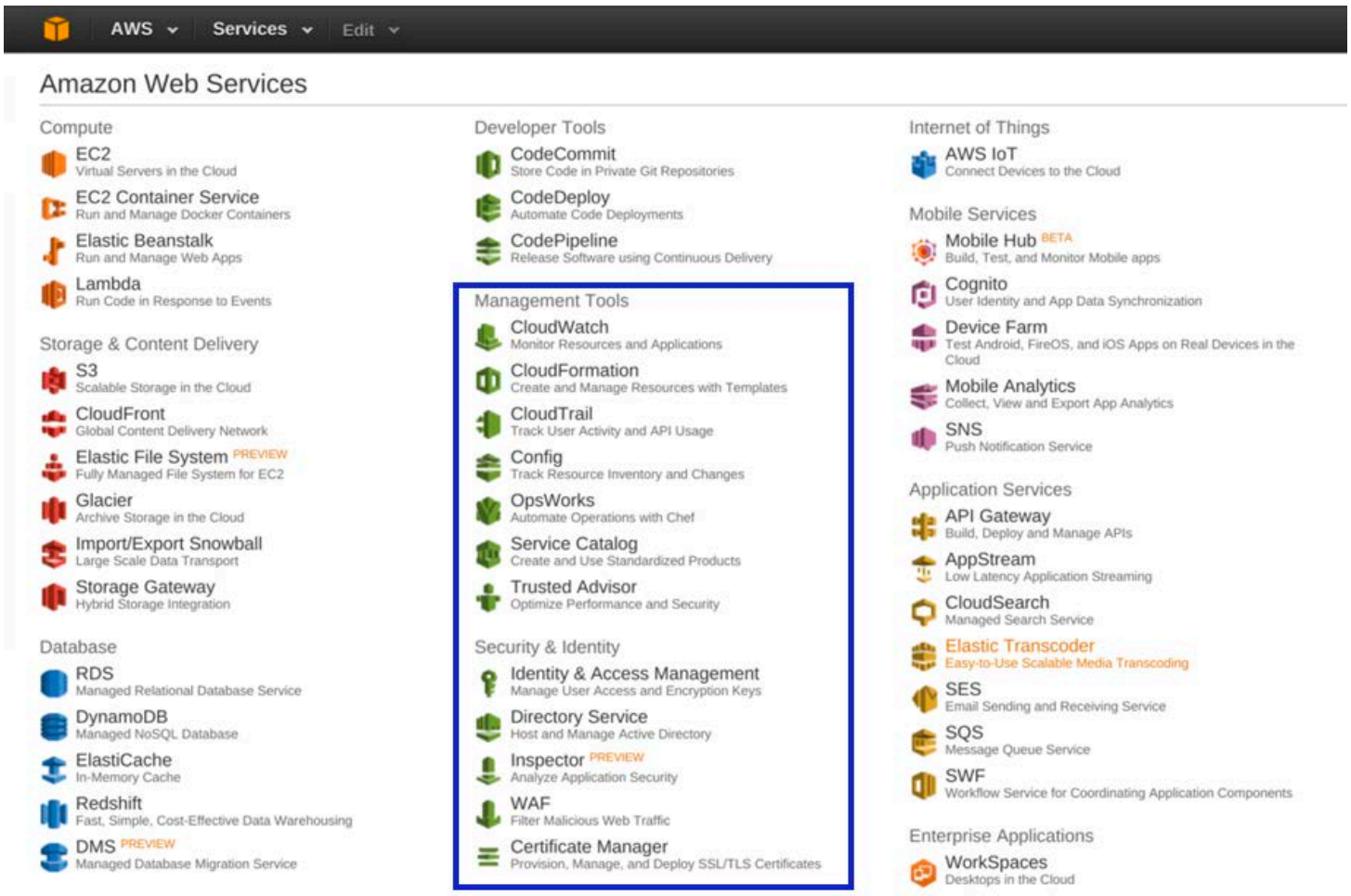
Native Cloud Security Solutions are cloud security tools that are built and designed by a CSP for its own cloud infrastructure. Oftentimes, they are already inbuilt in the cloud infrastructure provided by CSPs, and only need to be enabled and configured by end-users. We provide below a run-through of available cloud security tools from the top three cloud service providers for Q4 2020: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

	AWS	Azure	GCP
Identity & Access Control	• AWS Identity and Access Management (IAM) • AWS Security Token Service (STS) • AWS Microsoft AD • Cognito	• Azure Active Directory (Azure AD) • Access Keys, Temp Tokens	• GCP Cloud Identity • GCP Identity and Access Management (IAM) • GCP Identity-Aware Proxy • GCPIdentity Platform • Managed Service for Microsoft AD • GCP Titan Security Key
Network Access Controls	• Security Groups • Access Control List (ACL) • AWS Shield: DDoS Protection Service • AWS WAF	• Network Security Groups • Azure Firewall • Access Control List (ACL) • Azure DDoS Protection Service • WAF/App Gateway WAF	• Google Cloud Armor • Google Firewalls • Application Gateway
Data Security & Encryption	• AWS Key Management Service (KMS) • AWS Cloud Hardware Security Module (HSM) • AWS Certificate Manager Private Certificate Authority • AWS Secrets Manager	• Azure Key Vault • Key Value Certificate Management	• GCP Key Management Service (KMS) • GCP Certificate Authority Service • GCP Confidential Computing • Google Secret Manager
Logging	• AWSCloudTrail • AWS X-Ray • VPC Flow Logs	• Azure Resource Manager: Activity Logs, Diagnostic Logs, Storage Access Logs • NSG Flow Logs	• GCP Cloud Logging • GCP Access Transparency • GCP Network Telemetry
Audit and Monitoring	• CloudWatch • Amazon Macie • Trusted Advisor • AWS IAM Access Advisor • Guard Duty • Security Hub	• Azure Security Center • Azure Advanced Threat Protection • Azure Sentinel • Azure Network Watcher	• GCP Cloud Data Loss Prevention • GCP Cloud Operations Suite • GCP Cloud Console • GCP Network Intelligence Center • GCP Cloud Monitoring
Security Operations Center	• AWS Config • AWS Security Hub	• Azure Security Center • Azure Policy	• GCP Security Command Center • GCP Policy Intelligence

Key Features of Native Cloud Security

1. Simple to Deploy, Complicated to Customize and Maintain

Native Cloud Security tools – since they're already integrated with the respective cloud infrastructure of the CSP – are often easy to deploy individually. For example, with AWS, cloud security tools are accessible from the main console without any need to install separate software or access a separate domain.



Source: Amazon Web Services

However, despite the availability of these native cloud security tools, configuring them to suit the needs of the business and its compliance environment is still up to the cloud user, not the CSP. According to the (ISC)² Cybersecurity Workforce Study, 64% of organizations report staff shortages for cybersecurity professionals, with the estimated cybersecurity workforce gap at 3.12 million – the region with the largest gap being Asia-Pacific with 2 million. Without the proper staff and skills to properly configure and monitor cloud security, organizations open themselves up to potential data breaches.

According to IBM Security, misconfigured cloud servers served as one of the leading threat vectors, responsible for 19% of data breaches, alongside compromised credentials (19%). Gartner estimates that by 2023, 99% of cloud security failures will be the customer's fault, up from 95% in 2017. 75% of these security failures in 2023 will result from inadequate identity and access management, up from 50% in 2020.

Even with competent in-house cloud security experts, an ever-changing regulatory environment coupled with evolving cybersecurity risks demands constant review, monitoring, and maintenance of the existing cloud security policies, which – depending on the scale and size of an organization – could prove to be costly and time-consuming.

2. Covers Core Security Needs within its Cloud Environment but Can have Gaps in More Complex or Hybrid Infrastructures

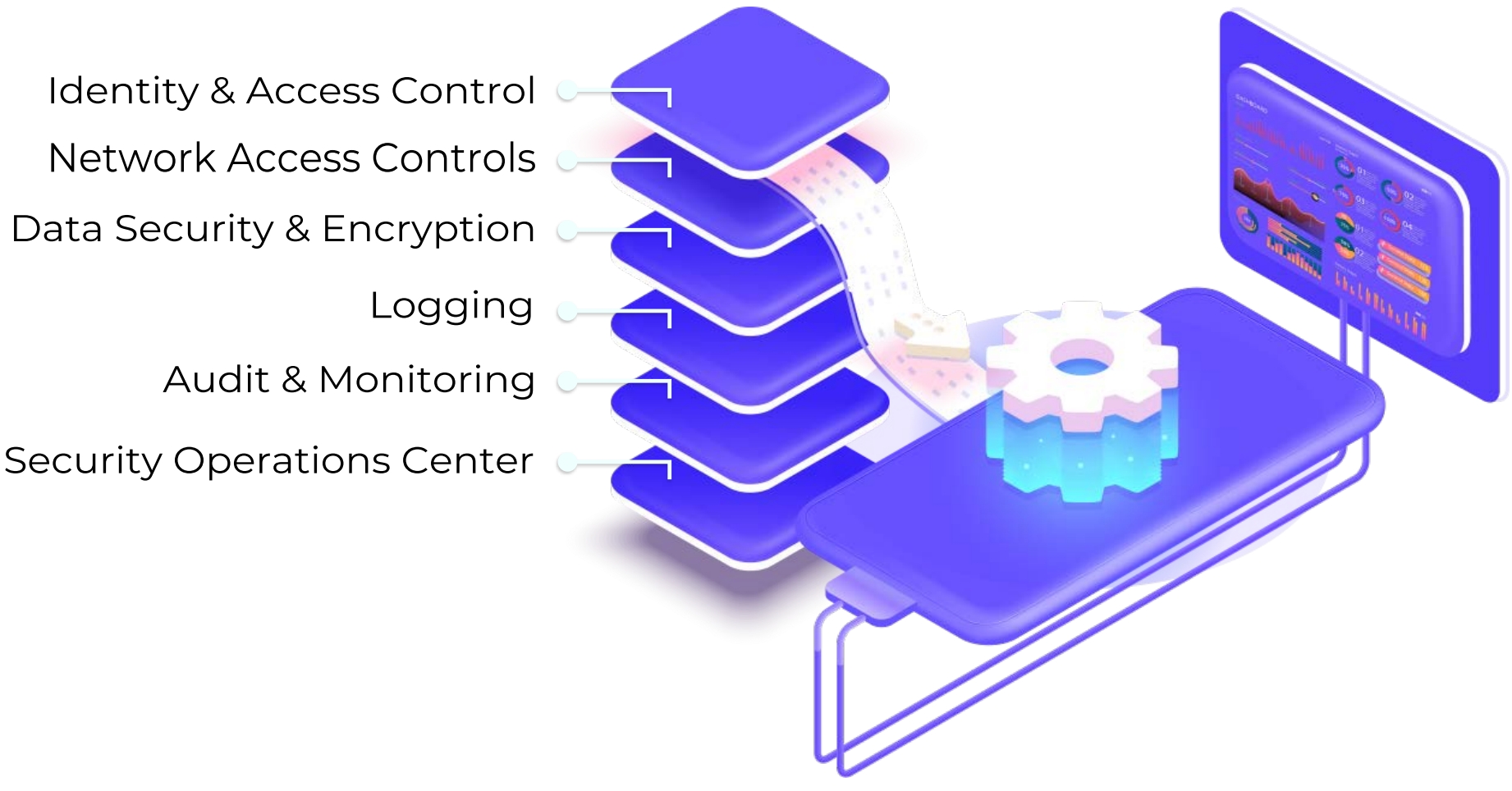
Native Cloud Security tools more or less cover core security needs such as API activity monitoring, basic threat intel, web application firewalls (WAF), among others. Some of these offerings even come with prebuilt security policies. For instance, Google's Cloud Armor offers several pre-configured WAF rules — tested and ready to use — to protect against SQL injection, Cross-Site Scripting (XSS), remote file inclusion, and remote code execution attacks.

However, the scope and effectiveness of Native Cloud Security provided by CSPs are often limited to that singular cloud environment. If an organization's IT infrastructure has a mix of on-premise data centers, private cloud, or public cloud, Native Cloud Security tools wouldn't be able to secure applications and workloads as they move across multiple environments and CSPs. According to Gartner, 80% of companies use two 2 or more cloud providers for their computing needs.

3. Free or Per-Use Pricing is Affordable in the Short-run but can be Expensive with Large Workloads

Lastly, Native Cloud Security tools are often already bundled with the CSP service agreement, making them — in essence — free since the cloud user doesn't have to pay any additional fees to enable Native Cloud Security tools. For example, AWS Shield Standard is available to all AWS users for free.
However, other advanced features are usually gated behind fees, and become more costly as they are used more extensively. Azure Web Application Firewall charges $5 monthly for each policy and add-on charges of $1 per month and $20 per month for custom rules and managed rulesets, respectively.

Third-Party Cloud Security Augments Areas That Native Cloud Security Fall Short At



Third-Party Cloud Security Solutions are cloud security tools that are offered by service providers separate from an organization's CSP. These are usually out-of-the-box tools that can work in any CSP environment, a multi-cloud infrastructure, or even a mix of cloud and on-premise. For this report, we will be covering third-party tools that address cloud-specific problems, and have no equivalent on-premise solution.

1. Cloud Access Security Brokers (CASB)

As the pandemic has forced companies into remote work, databases and resources that have previously only been accessible on-premises must now be made available off-premises and through an employee's device. While this better enables employees to work remotely, it opens up new risks for companies to address such as unauthorized access or download of company files by a user beyond their authorization level. This makes monitoring and controlling the usage and access to cloud applications all the more essential to enterprise security.

Cloud Access Security Broker (CASB) tools and services mediate between cloud services, cloud infrastructure (SaaS, IaaS, PaaS), and the devices of employees: ensuring incoming and outgoing network traffic complies with an organization's security policies. They are generally deployed as proxies, which allow them to have visibility and control over the enterprise usage and access of cloud resources.

Cloud Access Security Brokers (CASB) typically leverage the following technologies:

- **Firewalls** - for identifying malware and blocking the entrance to the corporate network.
- **Authentication** - verifying user credentials and controlling access to unauthorized content.
- **Web Application Firewall (WAFs)** - implemented to prevent and block attacks originating at the application level.
- **Data Loss Prevention (DLP)** - helps prevent unauthorized transmissions of sensitive information outside of the organization's authorized pools of data.

Sample Cloud Access Security Broker (CASB): NetSkope Security Cloud

Netskope's cloud access security broker (CASB) solution enables organizations to identify and manage the use of enterprise cloud applications, regardless of whether they are managed or unmanaged, thereby preventing sensitive data from being brought out from its environment by malicious actors.

Netskope deployment options, from an API-only deployment to several real-time options. It gives visibility of all SaaS, IaaS, and web traffic, even from sync clients, mobile apps, and TLS-encrypted traffic.

2. Cloud Workload Protection Platforms (CWPP)

While migrating workloads from on-premise to cloud servers provide significant gains for organizations, it also it also exposes organizations to more threats. Distributing workloads to various off-premise locations means more risks and an expanded attack surface while lowering visibility due to the short-lived nature of containers. Traditional solutions and manual processes no longer suffice, especially considering organizations that opt for multi-cloud strategies.

Cloud Workload Protection Platforms (CWPP) tools and services monitor and protect an organization's capabilities or workloads running in a cloud instance. There are a variety of CWPP capabilities across vendors but they usually include functionalities such as system hardening, vulnerability management, host-based segmentation, system integrity monitoring, and application allow lists. These overall enable visibility and security control management across multiple public cloud environments from a single console.

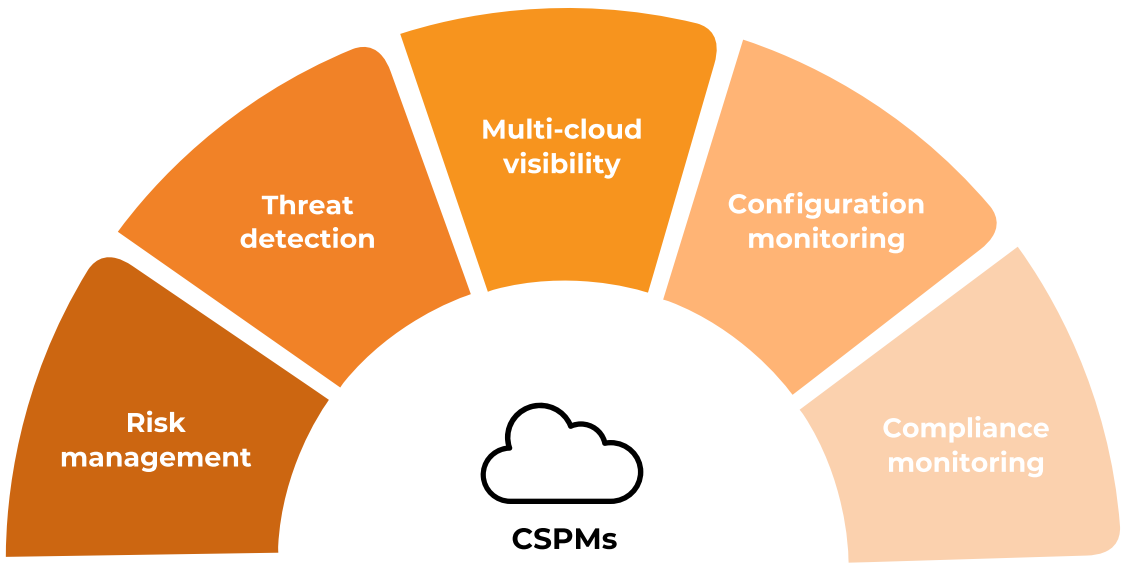
Cloud Workload Protection Platforms (CWPP) achieves the following objectives:

- Protects cloud workloads, i.e. containers or serverless functions
- Provide a consistent view across all cloud environments
- Boost portability and ensure security no matter what or where the workload is

Sample Cloud Workload Protection Platform (CWPP): Check Point CloudGuard

CloudGuard Workload Protection automates workload protection for modern cloud workloads, including serverless functions and containers. CloudGuard Workload Protection offers observability by continuously scanning an organization's serverless functions, automating least privilege protection for containers, logs, databases, etc., and providing active threat protection such as pattern matching, allow listing, blocklisting, among others.

3. Cloud Security Posture Management (CSPM)



Significant automation in the public cloud (IaaS and PaaS) has magnified the importance of cloud configuration and compliance. With a cyber threat landscape and regulatory climate constantly in flux, a single mistake can expose thousands of systems or large amounts of sensitive data.

Additionally, a lack of comprehensive visibility into programmatic cloud infrastructure means that incorrect and non-compliant configurations could go undetected for extended periods. These leave organizations at the risk of losing future business and liable to fines from regulatory agencies.

Cloud Security Posture Management (CSPM) tools and services continuously assess and improve an organization's cloud security to reduce the likelihood of successful attacks from malicious actors. Additionally, Cloud Security Posture Management (CSPM) solutions can assess the cloud infrastructure throughout the life cycle of cloud applications against relevant compliance standards and uniformly apply security best practices across multiple cloud environments.

Cloud Security Posture Management (CSPM) achieves the following objectives:

- Constant visibility and enforcement of security controls across multi-cloud providers
- Discovery and identification of cloud workloads and services
- Threat detection and alerts
- Cloud risk management, risk visualization, and risk prioritization capabilities
- Continuous compliance monitoring against a variety of industry or geography-specific regulations

Sample Cloud Security Posture Management (CSPM): Horangi Warden

Horangi Warden is a multi-cloud Cloud Security Posture Management (CSPM) solution that helps organizations manage their security and compliance risks without requiring any cloud security expertise. While usable from anywhere in the world, Warden is especially relevant for organizations based in the Asia Pacific region because of the unique compliance standards supported, namely MAS TRM, MAS Cyber Hygiene, APRA, and BNM-RMiT aside from international standards such as PCI-DSS and ISO 27001.

Warden provides visibility of cloud posture across major cloud service providers AWS, GCP, and Azure including IAM, Amazon S3, ElasticSearch, ELBv2, CloudFront, Cloud Storage, Compute Engine, Firewall Rules, and more. Risky configurations are automatically detected and alerts are sent to the team in charge, together with risk prioritization and actionable remediation steps for DevOps to triage issues. This is supported by Warden's integration with GitHub, GitLab, Slack, Jira, and Bitbucket.

Key Features of Third-Party Cloud Security

1. Continuous Customer Support by Third-Party Security Experts

Third-Party Security solutions often come with customer support from cloud security experts. These teams help minimize potential misconfigurations in cloud security upon setup and provide continuous support for companies who may lack the necessary skills or expertise in their own in-house security team.

Additionally, system updates and maintenance to Third-Party Cloud Security tools are handled by the vendor, ensuring that security is up to the standard of constantly evolving threats, with some even providing 24/7 support to continually support cloud users.

2. Comprehensive Security Coverage in Complex or Hybrid Cloud Infrastructures

For organizations with significant on-premise security or who have a mix of hybrid or multi-cloud infrastructures, relying on Native Cloud Security alone can be cumbersome, as users would have to reconfigure each cloud environment separately and ensure its consistency with an organization's security policy.

Third-Party Cloud Security solutions can consolidate the security and risk monitoring in a centralized dashboard. Using APIs with existing Cloud environments, Third-Party Cloud Security ensures that access levels are consistent throughout the cloud infrastructure and that workloads are protected and comply with relevant compliance requirements. Additionally, specific solutions such as Cloud Security Posture Management (CSPM) even enable assessment and monitoring against select compliance standards and regulatory frameworks.

3. Flexible Pricing Allows Organizations to Scale Up or Down

While native cloud tools often charge on usage and require heavy investment for in-house security staff, Third-Party Cloud Security solutions offer a variety of different pricing options, such as subscription per account, GB storage, rule, or resource. This provides organizations the flexibility to adjust their cloud security as needed. For instance, in an industry that sees high growth such as e-Commerce, a third-party cloud security solution could offer significant economies of scale as opposed to hiring additional staff. On the other hand, in contracting industries such as hospitality, third-party cloud security solutions let businesses scale down their security needs, as opposed to maintaining an overstaffed in-house cloud security team.

Factors When Choosing Native or Third-Party Cloud Security Solutions

1. The Organization's Current Resources and Cloud Security Expertise

An organization's current resources and expertise in cloud security are major factors in determining what cloud security solutions can be deployed and maintained. For instance, companies that have large IT security teams with the necessary expertise can opt to solely use Native Cloud Security, and instead create Cloud Security Posture Management (CSPM) or CWPP functionalities in-house. However, for companies that are only just starting to invest in cloud computing and may not have extensive expertise in cloud security, Third-Party Cloud Security might be a preferable choice because of its ease of use and expert support provided by vendors.

2. The IT Infrastructure Context

If an organization uses only one CSP such as AWS, Azure, or GCP, then Native Cloud solutions could be sufficient for its security needs.

However, organizations that use a multi-cloud strategy, or have an extensive presence on-premises and in the cloud are better off using Third-Party options. In this scenario, native cloud security tools alone are not enough because Third-Party providers offer greater parity in securing both multi-cloud-based and on-premises resources.

3. The Forecasted Usage of Cloud Computing

If an organization only has a few workloads running in the cloud and doesn't expect any significant changes, it may be feasible to secure them with CSP native security tools alone. In most cases, this approach is faster to set up because the security tools are natively integrated with its cloud services. However, if an organization expects its cloud footprint to grow steadily, or if it needs the flexibility to move to other clouds, a Third-Party security service will offer greater agility.

4. The Complexity of Business and Regulatory Environment

The choice between Native Cloud Security or Third-Party Security depends on the complexity of a business and the regulatory environment an organization operates in. For relatively straightforward businesses that aren't under regulatory scrutiny, Native Cloud Security can be enough for cloud security needs.

However, for businesses in industries with strict compliance requirements such as finance, healthcare, services, or government, Third-Party Security is often preferred with its ability to provide better visibility over cloud security and adhere to relevant compliance standards such as the Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and the Monetary Authority of Singapore's Technology Risk Management (MAS TRM) Guidelines.

5. The Sensitivity of Data Being Handled

All organizations handle data and should follow proper cloud security and data privacy regulations, but the extent of security policies required depends on the sensitivity of data handled by the organization. For organizations that handle little to no sensitive data, Native Cloud Security alone could be sufficient. However, for organizations that handle highly sensitive data such as bank accounts, personal identification, etc. the more robust security of Third-Party Security may provide better coverage.

Low Sensitivity	Medium Sensitivity	High Sensitivity
Public website content, press releases	Research details, financial information, contracts, intellectual property	Social security numbers, credit card numbers, bank accounts, personal identification, health information

Conclusion

In conclusion, cloud security has quickly risen as a priority for many companies, due to the increased risk of data breaches and ever-changing regulatory requirements. Native Cloud Security, which comes with an organization's native CSP, can be sufficient in some cases. However Third-Party Cloud Security Solutions offer substantial advantages such as ease of use, continuous threat protection, and the ability to function in a multi-cloud environment. In choosing one's cloud security, decision-makers should take into consideration the company's current resources and cloud security expertise, current IT infrastructure, the expected usage of the cloud, the complexity of the business as well as its regulatory environment, and the sensitivity of data being handled.