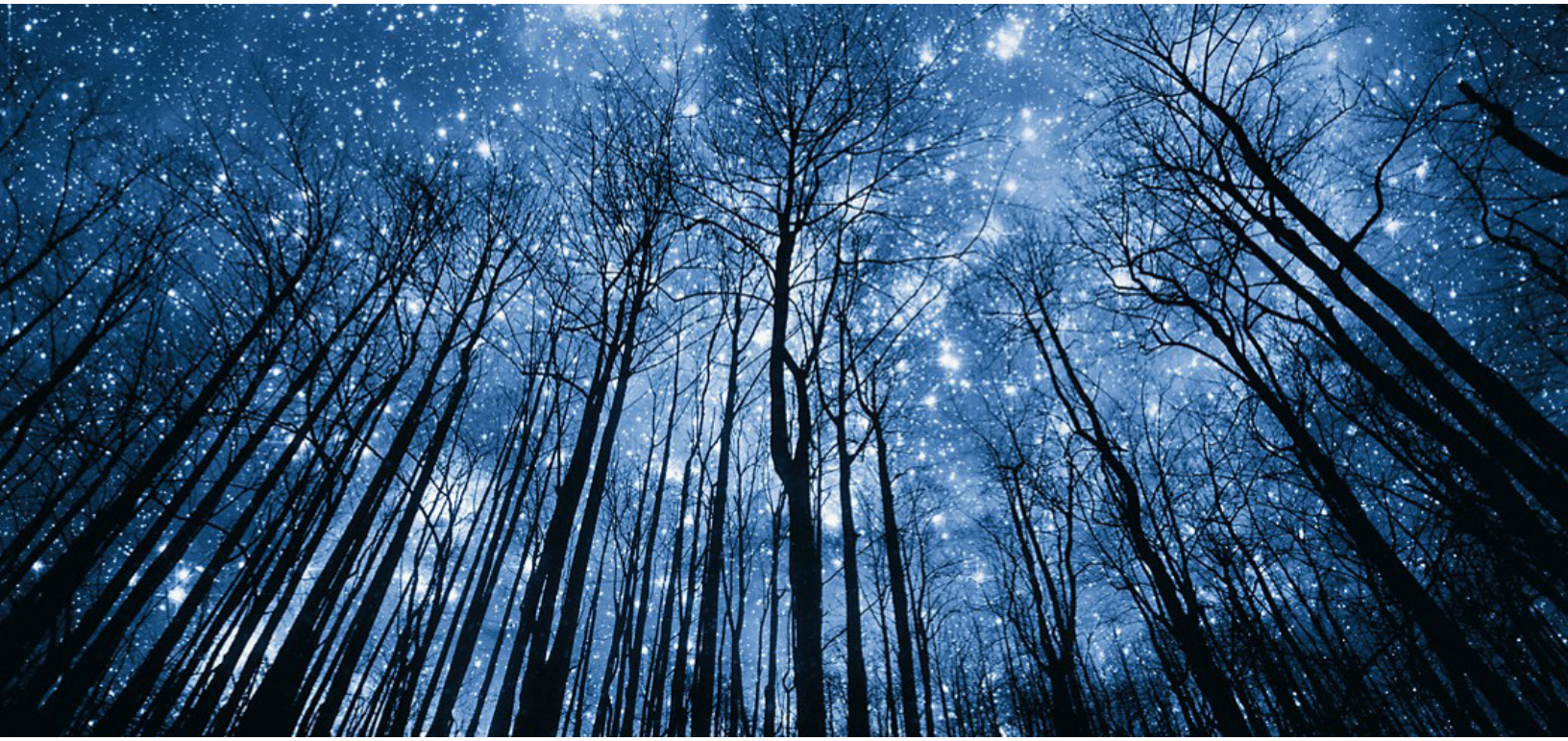
DELL Technologies

THE FUTURE OF CLOUD SECURITY



Nidhi Shree N

DELL Technologies
Proven Professional

Knowledge Sharing Article

Table of Contents

Abstract

As the businesses have accelerated their adoption of new technologies many organizations migrate their data to the cloud as it helps reduce their operations cost at a longer run. The industry is moving in the path of Digital Transformation hence the massive increase in cloud adoption will motivate cybercriminals to target organizations in the cloud environment. Cloud infrastructures have a vast variety of attack surfaces. Though cloud environments are secured with various security measures, improper configuration can still make them vulnerable. Having an appropriate security plan is essential for better cloud security.

Cloud security is a collection of procedures and technology designed to take care of external and internal threats to cloud computing resources in organizations. Every organization needs maximum security as they embrace digital transformation strategy and include cloud-based tools and services into their IT infrastructures. Cloud Security is also a responsibility that is shared between the cloud provider and the customer. With the right cloud security tools in place, we can automate security, prevent internal threats, and lower breach risks.

Future Cloud Security Trends

1. **Cybersecurity Mesh**: A distributed cybersecurity mesh that utilizes zero trust adapts to emerging threats and changing access needs. Threats can be detected in real-time and assets such as data and devices can be protected better than simple VPN passwords.

2. **Zero Trust:** Zero trust policies need to be implemented in every firm, especially in the context of the recent trend of moving everything to the cloud. Firewalls and perimeter security are how businesses safeguard their most precious assets, including user data and intellectual property.

3. **Hybrid and Multi-Cloud Environment:** The hybrid-cloud approach implies that services and applications that can be hosted are configured locally and can be migrated to the cloud. Multi-cloud proves effective when tools like SIEM and threat intelligence are deployed. One environment can contain security-based tools, and the others might have applications and other services.

4. **Merging Security Through DevSecOps:** DevSecOps proves to be secure and fast only with a fully automated software development lifecycle. It also enables businesses to innovate securely. This means that the entire supply chain will be filled with security measures and protocols.

5. **SASE Framework:** SASE is is a framework that provides a cloud-based cybersecurity solution and supports digital enterprises' dynamic, secure access needs. SASE's working structure includes a combination of WAN with multiple security capabilities like anti-malware, security brokers, and securing the network.

The shift to a cloud environment provides companies much need scalability and flexibility to remain competitive in the unstable business environment. At the same time, it exposes the firm to security vulnerabilities if security best practices are not leveraged.

In this article, we will be understanding in depth on cloud security, its threats and how to mitigate them via threat intelligence. We will also discuss about Multiple emerging technologies on cloud security and various approaches that help to maximize the benefits of cloud adoption and make a secure landscape.

Introduction

Cloud security is a rapidly evolving field that encompasses a wide range of measures and technologies designed to protect cloud computing resources from external and internal threats. These threats can include everything from distributed denial of service (DDoS) attacks and malware to hackers and unauthorized access or use of sensitive data and business content. Given the vast variety of attack surfaces present in cloud infrastructures, which can include servers, networks, applications, and data storage, it is essential for organizations to have a comprehensive and robust security plan in place.

As enterprise cloud adoption grows, business-critical applications and data migrate to trusted third-party cloud service providers (CSPs). Most major CSPs offer standard cybersecurity tools with monitoring and alerting functions as part of their service offerings, but in-house information technology (IT) security staff may find these tools do not provide enough coverage, meaning there are cybersecurity gaps between what is offered in the CSP's tools and what the enterprise requires. This increases the risk of data theft and loss.

One of the key components of cloud security is access control, which ensures that only authorized users have access to the data and resources stored in the cloud. This can be achieved through the use of various authentication and authorization mechanisms, such as multi-factor authentication and role-based access control. By implementing these measures, organizations can prevent unauthorized access to their cloud resources and reduce the risk of data breaches.

Another critical aspect of cloud security is the protection of data and business content, such as customer orders, secret design documents, and financial records. This can be accomplished through the use of encryption, which ensures that the data is unreadable to unauthorized parties, and through the use of data loss prevention (DLP) tools, which can help detect and prevent the accidental or intentional leakage of sensitive information. By implementing these measures, organizations can safeguard their sensitive data and maintain the trust of their customers.

In addition to protecting data and content, cloud security also includes measures to protect the underlying cloud infrastructure, including servers, networks, and applications. This can be achieved through the use of firewalls, intrusion detection and prevention systems (IDPS), and security information and event management (SIEM) systems. These tools can help detect and prevent unauthorized access, malware, and other types of cyberattacks. By implementing these measures, organizations can ensure the availability and integrity of their cloud resources.

Putting the right cloud security mechanisms and policies in place is critical to prevent breaches and data loss, avoid noncompliance and fines, and maintain business continuity (BC). A major benefit of the cloud is that it centralizes applications and data and centralizes the security of those applications and data as well. Eliminating the need for dedicated hardware also reduces organizations' cost and management needs, while increasing reliability, scalability, and flexibility.

Because no organization or CSP can eliminate all security threats and vulnerabilities, business leaders must balance the benefits of adopting cloud services with the level of data security risk their organizations are willing to take. Overall, cloud security is a critical aspect of any organization that uses cloud computing. By implementing a comprehensive security plan that includes access control, data and content protection, and the protection of the underlying cloud infrastructure, organizations can protect their sensitive data and business content, as well as the underlying cloud infrastructure, to ensure the confidentiality, integrity, and availability of their cloud resources.

An Overview to Cloud Computing

Cloud technology has revolutionized the way businesses and individuals access, store, and manage their data. The concept of cloud computing, which involves a network of remote servers that can be accessed over the internet for data storage, management, and processing, has been around since the 1950s but it wasn't until the 21st century that it began to gain widespread adoption. The widespread adoption of this technology has brought about many benefits, such as scalability, accessibility, and cost-effectiveness, as well as a few drawbacks. In this article, we will discuss the different types of cloud computing and their unique characteristics and use cases.

One type of cloud computing is Public Clouds, which are owned and operated by third-party providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Public clouds offer a wide range of services, including compute, storage, databases, and analytics, that are designed to be used by multiple customers. They are highly reliable, always accessible, and offer pay-as-you-go pricing, making them an affordable option for small and medium-sized businesses. Public clouds also offer easy scalability, so users can add or remove resources as their needs change. Additionally, public clouds offer built-in disaster recovery and high availability options.

Another type of cloud computing is Private Clouds, which are owned and operated by a single organization and are designed to be used exclusively by that organization. Private clouds can be built on-premises, using the organization's own servers, or hosted by a third-party provider. They offer greater control and security than public clouds as the organization has complete control over its data and applications. This is often a requirement for large organizations that must comply with strict regulatory requirements. However, private clouds are typically more expensive and require more resources to manage. Additionally, private clouds offer more customization options, as they are tailored to the organization's specific needs. Hybrid Clouds are a combination of both Public and Private clouds, allowing organizations to run certain workloads on public clouds while keeping sensitive data and applications on private clouds. This allows for greater flexibility and scalability, as well as the ability to take advantage of the cost savings offered by public clouds. Hybrid clouds are often used by large organizations that need to comply with strict regulatory requirements, but still want to take advantage of the benefits of public clouds. With hybrid clouds, organizations can move workloads between public and private clouds as per the requirement, making it a cost-effective solution.

Community Clouds are shared by a group of organizations that have similar requirements and concerns, such as government agencies or healthcare providers. Community clouds allow organizations to share resources and reduce costs while still maintaining control over their data. This is a good option for organizations that have similar needs but don't want to invest in their own private cloud. Community clouds also offer a higher level of security as they are used by a specific group of organizations.

Multi-cloud is a strategy that uses multiple cloud services from different providers, rather than relying on a single provider. Multi-cloud is used for better flexibility and to mitigate provider lock-in. This approach allows organizations to use the best-of-breed services from multiple providers, rather than being dependent on a single provider.

Cloud Service Models

Cloud service models refer to the different ways in which cloud computing services can be provided to customers. There are three main models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

- IaaS is the most basic form of cloud service, providing customers with virtualized computing resources, such as servers and storage, that can be accessed and managed over the internet. Examples of IaaS providers include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform. IaaS is often used by companies that want to run their own applications on the cloud, but don't want to invest in their own infrastructure.

- PaaS is a higher-level model, providing customers with a platform for developing, running, and managing applications. In addition to the virtualized computing resources provided by IaaS, PaaS also includes a development environment, a database, and other tools that are needed to create and run applications. Examples of PaaS providers include Heroku, Google App Engine, and AWS Elastic Beanstalk. PaaS is often used by developers and companies that want to create new applications quickly and easily, without having to worry about managing the underlying infrastructure.
- SaaS is the highest-level model, providing customers with access to software applications that are hosted and managed by the service provider. Examples of SaaS providers include Salesforce, Microsoft Office 365, and Google G Suite. SaaS is often used by companies that want to use software applications without having to install and maintain them on their own servers.

Each of these models has its own advantages and disadvantages. IaaS provides the most flexibility and control, but also requires the most technical expertise to manage. PaaS is less flexible, but provides a more streamlined development environment. SaaS is the simplest to use, but also the least customizable.
Choosing the right cloud service model depends on the specific needs of a company. IaaS is a good choice for companies that want to run their own applications on the cloud, PaaS is a good choice for developers and companies that want to create new applications quickly and easily, and SaaS is a good choice for companies that want to use software applications without having to install and maintain them on their own servers.

Shared Responsibility Model

The cloud shared responsibility model is a concept that outlines the responsibilities of both cloud service providers (CSP) and customers in securing and protecting data and resources in a cloud computing environment. The cloud service provider is responsible for the security of the infrastructure and ensuring the platform is updated and configured securely. Customers are responsible for the security of their own data and applications, including encryption, access control, and compliance with laws and industry standards. Although not standardized, the shared responsibility model is a framework that outlines which security tasks are the obligation of the CSP and which are the duty of the customer. Enterprises using cloud services must be clear which security responsibilities they hand off to their provider(s) and which they need to handle in-house to ensure they have no gaps in coverage. Customers should always check with their CSPs to understand what the provider covers and what they need to do themselves to protect the organization. Additionally, both parties must work together to optimize costs, including monitoring resource usage and utilizing cost management tools provided by cloud service providers.

CSP security responsibilities vary by service model, be it SaaS, PaaS or IaaS. Customer responsibility commonly increases from SaaS to PaaS to IaaS. In general, CSPs are always responsible for servers and storage. They secure and patch the infrastructure itself, as well as configure the physical data centers, networks and other hardware that power the infrastructure, including virtual machines (VMs) and disks. These are usually the sole responsibilities of CSPs in IaaS environments. In a PaaS environment, CSPs assume more responsibility, including securing runtime, networking, operating systems (OSes), data and virtualization. In a SaaS environment, CSPs also provide application and middleware security. The details of security responsibilities can vary by provider and customer.

To supplement the CSP security controls, customers are generally responsible for application, middleware, virtualization, data, OS, network and runtime security in IaaS clouds. In PaaS environments, customers take on fewer security tasks, generally only application and middleware security. SaaS environments involve even less customer responsibility. Data security and identity and access management (IAM) are always the responsibility of the customer, however, regardless of cloud delivery model. Encryption and compliance are also the responsibility of the customer. Because CSPs control and manage the infrastructure customer apps and data operate within, adopting additional controls to further mitigate risk can be challenging. IT security staff should get involved as early as possible when evaluating CSPs and cloud services. Security teams must evaluate the CSP's default security tools to determine whether additional measures will need to be applied in-house. Adding a company's own security tools to cloud

environments is typically done by installing one or more network-based virtual security appliances. Customer-added tool sets enable security administrators to get granular with specific security configurations and policy settings. Many enterprises also often find it cost-effective to implement the same tools in their public clouds as they have within their corporate local area networks (LANs). This prevents administrators from having to recreate security policies in the cloud using disparate security tools. Instead, a single security policy can be created once and then pushed out to identical security tools, regardless of whether they are on premises or in the cloud.

Why is Cloud Security important?

Cloud security is important because it protects sensitive information and assets that are stored and processed in the cloud from unauthorized access, use, disclosure, disruption, modification, or destruction. With the increasing use of cloud computing, more and more organizations are moving their data and applications to the cloud, making it a target for cyber criminals.

One of the main reasons cloud security is important is because it helps protect sensitive information such as financial data, personal information, and intellectual property. This information is critical to the operation of a business and its loss or compromise can have serious consequences, including financial losses and damage to a company's reputation.

Another important aspect of cloud security is that it helps to protect against data breaches. Data breaches can lead to the loss or theft of sensitive information, which can have serious consequences for both individuals and organizations. Cloud security measures, such as encryption and access controls, can help to prevent data breaches by making it more difficult for unauthorized individuals to access sensitive information.

Cloud security is also important because it helps to protect against threats such as denial of service (DoS) attacks, which can disrupt the availability of a business's cloud-based services and cause significant financial losses. Cloud security measures, such as firewalls and intrusion detection and prevention systems, can help to protect against DoS attacks by identifying and blocking malicious traffic.

In addition to these specific threats, cloud security is also important for compliance with regulations such as HIPAA, SOC2, PCI DSS, and GDPR. Organizations that operate in certain industries, such as healthcare and finance, are subject to strict regulations regarding the handling of sensitive information and must take appropriate security measures to ensure compliance.

It is important to note that no organization or cloud service provider (CSP) can eliminate all security threats and vulnerabilities. Business leaders must balance the benefits of adopting cloud services with the level of data security risk their organizations are willing to take. Because of this, it is important for organizations to carefully evaluate the security measures offered by their CSPs and to implement additional security measures as needed to ensure the protection of their sensitive information and assets.

Putting the right cloud security mechanisms and policies in place is critical to prevent breaches and data loss, avoid noncompliance and fines, and maintain business continuity (BC). A major benefit of the cloud is that it centralizes applications and data and centralizes the security of those applications and data as well. Eliminating the need for dedicated hardware also reduces organizations' cost and management needs, while increasing reliability, scalability, and flexibility.

How to secure data in the cloud?

Many of the security tools and mechanisms that are used in on-premises environments can also be used in the cloud, although there may be cloud-specific versions of these tools available. Some of the tools that are commonly used in both on-premises and cloud environments include encryption, IAM (Identity and Access Management), single sign-on (SSO), data loss prevention (DLP), intrusion prevention and detection systems (IPSes/IDSes), and public key infrastructure (PKI).

When it comes to cloud-specific security tools, there are a few that are commonly used to protect workloads in the cloud. One example is cloud workload protection platforms (CWPPs), which are designed to protect virtual machines (VMs), applications, and data in a consistent manner. Another example is cloud access security brokers (CASBs), which act as a gatekeeper between cloud customers and cloud services, enforcing security policies and adding an extra layer of security. Additionally, cloud security posture management (CSPM) is a group of security products and services that monitor cloud security and compliance issues, and aim to combat cloud misconfigurations. Other security models that are gaining popularity in the cloud environment are Secure Access Service Edge (SASE) and zero-trust network access (ZTNA)

Security as a service, often referred to as SaaS or SECaaS, is a subset of software as a service that provides security-related services. The Cloud Security Alliance (CSA) has defined 10 SECaaS categories, which include Identity and Access Management (IAM), Data Loss Prevention (DLP), web security, email security, security assessments, intrusion management, security information and event management (SIEM), encryption, Business Continuity/Disaster Recovery (BCDR), and network security. These services may include firewall as a service, cloud-based virtual private networks (VPNs), and key management as a service (KMaaS).

It's important to note that the steps required to secure data in the cloud vary. Factors, including the type and sensitivity of the data to be protected, cloud architecture, accessibility of built-in and third-party tools, and number and types of users authorized to access the data must be considered. The approach to securing data in the cloud should be tailored to the specific needs of the organization and its data.

Some general best practices to secure business data in the cloud include:

- Encrypting data at rest, in use and in motion.
- Using two-factor authentication (2FA) or multifactor authentication (MFA) to verify user identity before granting access.
- Adopting cloud edge security protections, including firewalls, IPSes, and antimalware.
- Isolating cloud data backups to prevent ransomware threats.
- Ensuring data location visibility and control to identify where data resides and to implement restrictions on whether data can be copied to other locations inside or outside the cloud.
- Logging and monitoring all aspects of data access, additions and changes.
- Considering emerging cybersecurity tools such as network detection and response (NDR) and artificial intelligence (AI) for IT operations (AIOps) which can collect cloud infrastructure health and cybersecurity information, and alert administrators of abnormal behavior that could indicate a threat.

Cloud Security challenges

Cloud computing has become increasingly popular in recent years due to its many benefits, such as cost savings, scalability, and flexibility. However, it also poses many cybersecurity challenges that organizations must be aware of and prepared to address. Some of the key challenges include:

- **Insider threats:** Employees with access to sensitive data and systems can intentionally or unintentionally cause damage, whether through malice or carelessness. For example, an employee who has access to sensitive data may steal it or share it with unauthorized parties, or an employee who is not aware of security best practices may inadvertently cause a data breach.
- **Data loss and data breaches:** Data loss can occur due to hardware failure, human error, or malicious attacks, while data breaches can happen due to weak security controls, lack of monitoring, or unpatched vulnerabilities.
- **Identity and access management (IAM):** IAM controls who has access to what data and systems, and it's essential to ensure that only authorized users have access to sensitive data and that their access is limited to what they need to do their job.
- **Key management:** Encryption keys are used to protect data at rest and in transit, and it's essential to ensure that these keys are properly managed, stored, and rotated.
- **Access control:** Organizations need to have controls in place to ensure that only authorized users have access to sensitive data and systems, and that access is limited to what they need to do their job.
- **Phishing and malware:** Phishing attacks attempt to trick users into providing sensitive information or installing malware, while malware is malicious software that can cause damage to systems or steal sensitive data.
- **Shadow IT:** Shadow IT refers to the use of IT resources and services without the knowledge or approval of the IT department. This can lead to security risks as users may use unapproved and unsecured services, such as cloud storage or SaaS.
- **DDoS attacks:** DDoS attacks attempt to overwhelm a website or network with traffic, causing it to become unavailable to legitimate users.
- **Insecure APIs:** APIs are used to allow different systems and applications to communicate with each other, and if they're not properly secured, they can be used to gain unauthorized access to sensitive data.
- **Cloud-specific challenges:** Cloud account hijacking, lack of cloud visibility and control, working with cloud security tools that in-house administrators may be unfamiliar with, tracking and monitoring where data is located both in transit and at rest, misconfigurations, weak cloud control plane, challenges understanding the shared responsibility model, nefarious use of cloud services, multi-tenancy concerns, incompatibilities with on-premises environments, cloud compliance, and cloud governance.

Some of the advanced cloud-native security challenges and the multiple layers of risk faced by today’s cloud-oriented organizations include:

- **Increased Attack Surface:** The public cloud environment presents a large and attractive attack surface for hackers who exploit poorly secured cloud ingress ports to access and disrupt workloads and data. This includes a range of malicious threats such as malware, Zero-Day attacks, and account takeover.
- **Lack of Visibility and Tracking:** In the Infrastructure as a Service (IaaS) model, cloud providers have full control over the infrastructure layer and do not expose it to their customers. This lack of visibility and control is further extended in the Platform as a Service (PaaS) and Software as a Service (SaaS) cloud models, making it difficult for customers to effectively identify and quantify their cloud assets or visualize their cloud environments.

- **Ever-Changing Workloads:** Cloud assets are provisioned and decommissioned dynamically, at scale, and at velocity. Traditional security tools are often not equipped to enforce protection policies in such a flexible and dynamic environment with ever-changing and ephemeral workloads.
- **DevOps, DevSecOps, and Automation:** Organizations that have embraced the highly automated DevOps culture must ensure that appropriate security controls are identified and embedded in code and templates early in the development cycle. Security-related changes implemented after a workload has been deployed in production can undermine the organization's security posture as well as lengthen time to market.
- **Granular Privilege and Key Management:** Cloud user roles are often configured very loosely, granting extensive privileges beyond what is intended or required. This can include giving database delete or write permissions to untrained users or users who have no business need to delete or add database assets. At the application level, improperly configured keys and privileges expose sessions to security risks.
- **Complex Environments:** Managing security in a consistent way in the hybrid and multicloud environments favoured by enterprises these days requires methods and tools that work seamlessly across public cloud providers, private cloud providers, and on-premise deployments. This includes branch office edge protection for geographically distributed organizations.
- **Cloud Compliance and Governance:** Cloud providers align themselves with accreditation programs such as PCI 3.2, NIST 800-53, HIPAA, and GDPR, but customers are responsible for ensuring their workloads and data processes are compliant. Given the poor visibility and dynamics of the cloud environment, compliance audit process becomes difficult unless tools are used to achieve continuous compliance checks and issue real-time alerts about misconfigurations.

Overall, these challenges require a comprehensive and holistic approach to cloud security that includes continuous monitoring, real-time threat detection, incident response, and recovery capabilities. Additionally, organizations must adopt a culture of security with a strong focus on security education, training, and awareness to ensure that employees are aware of the risks and know how to mitigate them.

6 Pillars of Cloud Security

While cloud providers such as Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP) offer a wide range of security features and services that are native to their respective platforms, these alone are not enough to provide the level of security required to protect enterprise cloud workloads from breaches, data leaks, and targeted attacks. This is because the dynamic and distributed nature of cloud environments requires a more comprehensive approach to security that goes beyond the basic security measures provided by cloud providers.

To achieve enterprise-grade protection of cloud workloads, it is essential to supplement the security features and services offered by cloud providers with third-party solutions. These solutions can provide additional layers of security and help to close any gaps in the security provided by the cloud provider. By using a combination of cloud-native and third-party security tools, organizations can gain centralized visibility and detailed control over their cloud environments, which is necessary to implement the industry-standard 6 Pillars of Robust Cloud Security:

- **Granular, policy-based controls for authentication and access privileges**, this means using groups and roles instead of individual IAM level, so it's easy to update IAM definitions as business requirements change, grant minimal access privileges to assets and APIs that are essential for a group or role to carry out its tasks. The more extensive privileges, the higher the levels of authentication, and enforcing good IAM hygiene such as strong password policies, permission time-outs, etc.
- **Zero-trust network security across isolated networks and micro-segments**, this means deploying business-critical resources and apps in logically isolated sections of the provider's cloud network, such as Virtual Private Clouds (AWS and Google) or vNET (Azure), using subnets to micro-segment workloads from each other, with granular security policies at subnet gateways, also using dedicated WAN links in hybrid architectures, and

static user-defined routing configurations to customize access to virtual devices, virtual networks and their gateways, and public IP addresses.

- **Enforcement of virtual server protection policies and processes** such as change management and software updates, Cloud security vendors provide robust Cloud Security Posture Management, consistently applying governance and compliance rules and templates when provisioning virtual servers, auditing for configuration deviations, and remediating automatically where possible.
- **Safeguarding all applications with a next-generation web application firewall**, this will granularly inspect and control traffic to and from web application servers, automatically updates WAF rules in response to traffic behavior changes, and is deployed closer to microservices that are running workloads.
- **Enhanced data protection**, this includes encryption at all transport layers, secure file shares and communications, continuous compliance risk management, and maintaining good data storage resource hygiene such as detecting misconfigured buckets and terminating orphan resources.
- **Threat intelligence** that detects and remediates known and unknown threats in real-time, Third-party cloud security vendors add context to the large and diverse streams of cloud-native logs by intelligently cross-referencing aggregated log data with internal data such as asset and configuration management systems, vulnerability scanners, etc. and external data such as public threat intelligence feeds, geolocation databases, etc. They also provide tools that help visualize and query the threat landscape and promote quicker incident response times. AI-based anomaly detection algorithms are applied to catch unknown threats, which then undergo forensics analysis to determine their risk profile. Real-time alerts on intrusions and policy violations shorten times to remediation, sometimes even triggering auto-remediation workflows.

Cloud Security Trends

1. Cybersecurity Mesh

A distributed cybersecurity mesh, also known as Cybersecurity Mesh Architecture (CSMA), is a network security model that utilizes the concept of zero trust. Zero trust is a security model that assumes that all network traffic, whether it originates from inside or outside the network, should be treated as untrusted until proven otherwise. This approach adapts to emerging threats and changing access needs by detecting them in real-time and protecting assets such as data and devices better than simple VPN passwords.

Cybersecurity mesh, also known as Cybersecurity Mesh Architecture (CSMA), is a method that focuses on creating a flexible security-oriented architecture that utilizes safety or risk-mitigation arrangements without causing any delay. It can be applied to distributed systems and components, such as IoT devices, cloud technology, remote workers, and the internet.

The purpose of CSMA is to promote interoperability among all the stand-alone security-related products so that they all work towards designing a trustworthy and all-inclusive digital safety policy for enterprises. It focuses more on protecting every technology endpoint separately.

CSMA encourages businesses to give more priority to a centrally-manageable security mechanism that has various components integrated for various purposes.

It achieves this goal by: Strategizing ways that encourage fragmented creation of policies for communication and collaborative working. These fragments help in designing of a dynamic and all-inclusive policy. This means that it allows multiple security tools to work together and share information, creating a more comprehensive security strategy.

Creating a more customizable security posture that can be altered as the pace of digitization increases. With the rapid pace of digitalization, traditional security models can become top-heavy and cumbersome, making it difficult to keep up with the evolving digital landscape. Cybersecurity mesh allows for a more modular and adaptable approach to security that can evolve with the organization's digital needs.

Improving the organization’s defensive stand by introducing tools for continual monitoring and early mitigation of risks. Cybersecurity mesh provides a foundation for real-time threat detection and response, allowing organizations to quickly identify and address potential security breaches before they cause significant damage.Generating an ecosystem that promotes the swift and need-based deployment of key security aids digitally. Cybersecurity mesh allows for more efficient deployment of security tools, reducing the need for duplicated efforts and resources.

Removing replicated tasks and letting organization save money and efforts, while deploying the people/resources in better security or non-security operations. By streamlining security efforts and reducing the need for duplicated tasks, organizations can save money and resources while focusing on more important security or non-security operations.

There are numerous applications of cybersecurity mesh, resulting in increased flexibility, adaptability, and an overall stronger security posture for an organization. For example, using this strategy in IT development enables an organization to centralize its security policy management. Additionally, it can be integrated with the organization's network, making it safer and more prepared for future risks. By selecting cybersecurity technologies that facilitate integration, for example, plug-in application programming interfaces (APIs) that allow customization and extensions, as well as extensible analytics, an organization can be positioned to respond to future security risks. Furthermore, by using current and emerging security standards, it can close any security gaps due to weaknesses and vulnerabilities in different solutions.

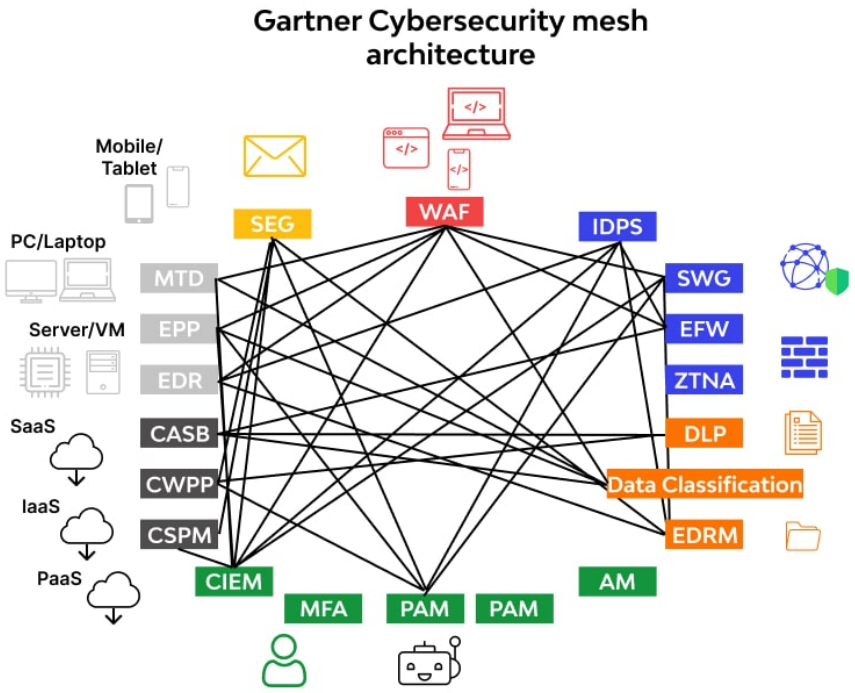


Image Source: https://assets.website-files.com/5ff66329429d880392f6cba2/6283d2273969ea65eab8f831_Cybersecurity%20Mesh%20Architecture.jpg

2. Zero Trust

The zero-trust security model is a cybersecurity approach that prioritizes the assumption that any user, device, or network is untrusted until it can be verified and authenticated. This contrasts with traditional security models which rely on a perimeter-based approach, where access to internal resources is granted based on a user's location within the network.

What is the zero-trust security model?

The zero-trust security model is a cybersecurity approach that denies access to an enterprise's digital resources by default and grants authenticated users and devices tailored, siloed access to only the applications, data, services, and systems they need to do their jobs. Gartner has predicted that by 2025, 60% of organizations will embrace a zero-trust security strategy.

This approach is known as zero-trust network access (ZTNA) and applies zero-trust concepts to an application access architecture, allowing organizations to establish secure remote access to cloud services and applications.

ZTNA solutions use a variety of technologies and protocols, such as multi-factor authentication, single sign-on, identity and access management, and secure remote access technologies to verify user identity, device security posture and network location, before granting access to resources. This helps to prevent unauthorized access and limit the potential damage if a breach does occur.

One key component of ZTNA is the use of a controller or trust broker to enforce an organization's pre-established access policies. This controller acts as a gatekeeper, facilitating or denying connections between users and apps based on the access policies. It also hides the network's location (i.e., IP address), making it more difficult for attackers to locate and target specific resources.

ZTNA solutions also use a variety of contextual variables to determine whether a user, device or network is trustworthy, such as device security postures, times of day, geolocations, and data sensitivity. This allows the ZTNA to make dynamic access decisions based on the current state of the user, device, or network, and adjust access policies accordingly. Suspicious context could prompt a ZTNA broker to deny even an authorized user's connection request.

ZTNA solutions prevent users from seeing any services and applications they do not have permission to access. This allows ZTNA to protect against lateral movement attacks, in which compromised credentials or endpoints allow an attacker to move to other services and systems.

3. Hybrid and Multi-Cloud Environment

The hybrid-cloud approach implies that services and applications that can be hosted are configured locally and can be migrated to the cloud as needed. This allows organizations to take advantage of the benefits of both on-premises and cloud-based infrastructure, and to optimize their IT resources based on their specific needs.

Multi-cloud is an extension of the hybrid-cloud approach, and it proves effective when tools like SIEM (Security Information and Event Management) and threat intelligence are deployed. In a multi-cloud environment, different clouds can be used for different purposes: one environment can contain security-based tools, and the others might have applications and other services. This allows organizations to take advantage of the strengths of different cloud providers and to avoid vendor lock-in.

Using a hybrid-cloud or multi-cloud approach can provide several benefits for organizations, including:

- Reduced operational overhead by managing applications and infrastructure with the same toolsets across clouds. This includes the creation of “skill portability” where developers and operators can use the same skills across multiple cloud platforms.
- Improved observability at all layers consistently across clouds, which in turn can improve application performance and security.
- Enhanced security posture by leveraging a Zero Trust architecture and secure software supply chains.
- Increased application portability opportunities via consistent services and APIs.

Hybrid cloud security involves protecting data, applications, and infrastructure, both on-premises and in the public cloud. This includes business processes, workloads, and management across multiple IT environments. Enterprises sometimes assume that their cloud provider handles all aspects of cloud security, but in reality, cloud security is a shared responsibility. Cloud providers provide security for their infrastructure, but enterprises are responsible for protecting the application layer, and their sensitive data.

Protecting the application layer involves implementing security measures such as access controls, encryption, and monitoring. It also includes regularly reviewing and updating security policies and procedures and ensuring that all employees are aware of and comply with them. Additionally, organizations should implement incident response plans to be able to quickly detect and respond to security breaches.

4. Merging Security Through DevSecOps

DevSecOps is a methodology that incorporates security into every aspect of the software development lifecycle (SDLC) from the very beginning. This approach is known as "shifting security to the left" and it aims to address security issues at the earliest possible stages, rather than waiting until later stages like in traditional DevOps. This method is more efficient and cost-effective as it is less expensive and difficult to implement to integrate security at the end of the development process.

DevSecOps pipeline consists of four main stages: building, testing, infra & compliance scan, and deployment. In the building stage, static scanning of source code or Static Application Security Testing (SAST) is performed. This helps developers to identify vulnerabilities and issues related to code, and sends a feedback report back to developers to resolve issues such as backdoors, poor source code, etc. This stage prevents passing on the vulnerabilities to the production team.

The next stage is the testing stage which is equally crucial for software development. In this stage, dynamic application scanning testing (DAST) is performed. DAST simulates or imitates malicious intrusion from outside an application. The feedback report enumerates the possible ways of how a hacker can breach the secure confinement of the software. These issues need to be resolved before actually deploying the software to framework seal protection from cyber threats.

The next stage is the infrastructure & compliance analysis stage. Infrastructure scans focus on configuration settings and the system’s infrastructure. The compliance scan analyzes a system’s conformity with specific regulations such as HIPAA or HITRUST. Adherence to such specific regulations allows to disclose the security stance of software.

The final stage of DevSecOps is the deploy/release stage. During this stage, an application is integrated with a Web Application Firewall (WAF) which prevents the application from cross-site scripting (XSS), cross-site forgery, file inclusion, and SQL injection which can result in a cyber incursion.

Image Source: https://www.nic.in/wp-content/uploads/2022/03/DevSecOPs_1-1024x859.png

5. SASE Framework

Secure Access Service Edge (SASE) is a framework that provides a comprehensive, cloud-based cybersecurity solution for digital enterprises. It combines software-defined wide area networking (SD-WAN) with various security capabilities such as anti-malware, security brokers, and network protection. SASE is designed to secure access to cloud services, private applications, and websites, and reduce the complexity of endpoint protection, making it particularly useful for virtual workforces, digital customer experiences, and digital-first businesses.

SASE offers a range of features, including access controls for endpoints, advanced threat protection, security monitoring, and data security. It also provides centralized controls for acceptable use, which are enforced through API-based integration. SASE is typically delivered as a cloud service, but some vendors also offer on-premises and agent-based components.

SASE solutions are designed to provide zero-trust and least-privileged access based on context and identity, as defined by Gartner. This means that users are only granted access to the resources they need, based on their specific role and location. This level of granular access control is essential in today's distributed and dynamic work environments, where employees are accessing resources from a variety of locations and devices.

SASE also includes several other core security features such as Secure Web Gateways (SWGs), which protect the cloud from unwanted internet traffic, Cloud Access Security Brokers (CASBs), which protect applications from unauthorized access, and Next-Generation Firewalls (NGFWs). Some SASE architectures may also include additional safeguards such as advanced threat detection and data loss prevention (DLP).

Image Source: https://ngs-sec.com/images/services/cloud-security-sase.png

Cyber Threat Intelligence

Cyber threat intelligence can be described as the process of gathering, analyzing and interpreting information about potential cyber threats and vulnerabilities within a system or network, in order to make informed decisions and take action to mitigate or prevent attacks. It involves the collection of data from a variety of sources, such as open-source intelligence, network traffic, and incident reports, as well as the use of analytical techniques to identify patterns, trends, and potential indicators of compromise (IoCs).

There are three main types of threat intelligence:

- **Strategic threat intelligence:** This type of threat intelligence provides a broad overview of the cyber threat landscape and is typically used by executives and other decision-makers to inform their cybersecurity strategy and policies. It can include information about the types of threats and actors that are most likely to target a particular organization, as well as the trends and patterns that are currently emerging in the cyber threat landscape.
- **Tactical threat intelligence:** This type of threat intelligence is more focused on the tactics, techniques, and procedures (TTPs) of cyber threat actors. It is typically used by security personnel to understand the specific methods that attackers are using, so that they can develop more effective defenses and response plans. This type of threat intelligence can include information about specific malware families, phishing campaigns, and other tactics that attackers are using.
- **Operational threat intelligence:** This type of threat intelligence provides detailed information and analysis on cyberattacks or previous cyber events, and is primarily used by incident response teams to understand the nature, intent, and possible timing of a specific attack. It can include information about the specific tools and techniques that were used, as well as the indicators of compromise that were detected.

At its core, cyber threat intelligence is all about using information to make better security decisions. The data that is collected and analyzed for evidence of threat intelligence contains valuable insights into potential attackers, their attack vectors, intents, motives, and capabilities. This information can be used to identify and prioritize risks, develop more effective defenses, and respond more quickly and effectively to incidents.

Integrating cyber threat intelligence into cloud security can be a powerful way to improve the security of cloud-based systems and data. The process of collecting, analyzing and interpreting threat intelligence is essentially the same, but

the focus is on cloud-specific data resources such as static indicators and TTPs. This information can be used to identify and mitigate cloud-specific threats and vulnerabilities, such as misconfigured cloud resources, and to develop more effective security controls and incident response plans.

The Future of Cloud Security

The future of cloud security is a topic of increasing importance as more and more companies move their data and operations to the cloud. With the rise of cloud computing, the security of data stored in the cloud has become a major concern for organizations of all sizes. In order to protect their data and operations, companies will need to adopt new strategies and technologies to secure their cloud environments.

One of the key trends in cloud security is the use of artificial intelligence (AI) and machine learning (ML) to detect and respond to security threats. These technologies can analyze large amounts of data in real-time to identify patterns and anomalies that may indicate a security threat. This allows organizations to quickly respond to potential threats and take steps to prevent them from causing harm.

Another trend in cloud security is the use of multi-factor authentication (MFA) to secure access to cloud-based resources. MFA requires users to provide multiple forms of identification, such as a password and a fingerprint or a token, in order to gain access to a system. This adds an additional layer of security and makes it more difficult for attackers to gain unauthorized access to sensitive data.The use of encryption is also becoming increasingly important in cloud security. Encryption allows organizations to protect their data by converting it into a code that can only be deciphered by those with the appropriate key. This makes it much more difficult for attackers to access sensitive data, even if they are able to penetrate a cloud-based system.

Another important aspect of cloud security is the use of virtual private networks (VPNs) to secure communications between different parts of an organization. VPNs allow employees to securely access data and resources from any location, which is particularly important for companies with employees working remotely.

In addition to the trends mentioned earlier, the use of blockchain technology and quantum computing is also expected to play a significant role in the future of cloud security.

Blockchain, the technology behind cryptocurrencies like Bitcoin, is essentially a digital ledger that is decentralized and distributed across a network of computers. This means that there is no central point of failure, and it is extremely difficult for hackers to alter or manipulate the data stored on the blockchain. This makes blockchain an ideal technology for securing cloud-based systems and applications.

Quantum computing is a new technology that uses the principles of quantum mechanics to perform calculations much faster than traditional computers. It has the potential to revolutionize the way we think about security and encryption, as quantum computers can easily crack even the most advanced encryption algorithms used today. However, the same technology can be used to create new and more powerful encryption methods that can withstand quantum attacks.

As more and more companies move to the cloud, the need for robust cloud security will continue to grow. Organizations will need to adopt new technologies and strategies to protect their data and operations in the cloud. By staying up to date on the latest trends in cloud security, companies can ensure that they are well-prepared to protect their sensitive data and operations in the cloud.

Conclusion

In conclusion, the future of cloud security is a topic of increasing importance as more and more companies move their data and operations to the cloud. With the rise of cloud computing, the security of data stored in the cloud has become a major concern for organizations of all sizes. In order to protect their data and operations, companies will need to adopt new strategies and technologies to secure their cloud environments.Cloud security is gaining centre stage, and attackers are growing more sophisticated. Luckily, the security industry is rising to the challenge with new security tools and platforms: In 2022 and beyond, organizations will adopt these new technologies to address a new wave of cloud threats, and secure the core of our evolving digital economy.

One of the key trends in cloud security is the use of artificial intelligence (AI) and machine learning (ML) to detect and respond to security threats. These technologies can analyses large amounts of data in real-time to identify patterns and anomalies that may indicate a security threat. This allows organizations to quickly respond to potential threats and take steps to prevent them from causing harm.

Another trend in cloud security is the use of multi-factor authentication (MFA) to secure access to cloud-based resources. MFA requires users to provide multiple forms of identification, such as a password and a fingerprint or a token, in order to gain access to a system. This adds an additional layer of security and makes it more difficult for attackers to gain unauthorized access to sensitive data. The use of encryption is also becoming increasingly important in cloud security. Encryption allows organizations to protect their data by converting it into a code that can only be deciphered by those with the appropriate key. This makes it much more difficult for attackers to access sensitive data, even if they are able to penetrate a cloud-based system.

In addition to these trends, the use of blockchain technology and quantum computing is also expected to play a significant role in the future of cloud security. Quantum computing, on the other hand, has the potential to revolutionize the way we think about security and encryption, as quantum computers can easily crack even the most advanced encryption algorithms used today. However, the same technology can be used to create new and more powerful encryption methods that can withstand quantum attacks.

Integrating cyber threat intelligence into cloud security can be a powerful way to improve the security of cloud-based systems and data. The process of collecting, analysing and interpreting threat intelligence is essentially the same, but the focus is on cloud-specific data resources such as static indicators and TTPs. This information can be used to identify and mitigate cloud-specific threats and vulnerabilities, such as misconfigured cloud resources, and to develop more effective security controls and incident response plans.

As more and more companies move to the cloud, the need for robust cloud security will continue to grow. Organizations will need to adopt new technologies and strategies to protect their data and operations in the cloud. By staying up to date on the latest trends in cloud security, companies can ensure that they are well-prepared to protect their sensitive data and operations in the cloud.

Bibliography

- “Box.” Box, www.box.com/resources/what-is-cloud-security. https://www.box.com/en-in/resources/what-is-cloud-security

- “What Is Cloud Security?” Security, 1 Feb. 2021 https://www.techtarget.com/searchsecurity/definition/cloud-security

- “The Evolution and Future of Cloud Security | Teradata.” The Evolution and Future of Cloud Security | Teradata, www.teradata.com/Trends/Cloud/Future-of-Cloud-Security. https://www.teradata.com/Trends/Cloud/Future-of-Cloud-Security

- “What Is Cloud Security? Understand the 6 Pillars - Check Point Software.” Check Point Software, /cyber-hub/cloud-security/what-is-cloud-security. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/#ZeroTrust

- “The Future of Cloud Security: 2022 and Beyond.” ReadWrite, 12 Nov. 2021, readwrite.com/the-future-of-cloud-security-2022-and-beyond. https://readwrite.com/the-future-of-cloud-security-2022-and-beyond/

- “Cyber Threat Intelligence.” https://www.eccouncil.org/cyber-threat-intelligence/

- “How Cyber Threat Intelligence Can Help to Protect Against Cloud Security Threats | Tripwire.” How Cyber Threat Intelligence Can Help to Protect Against Cloud Security Threats | Tripwire, www.tripwire.com/state-of-security/how-cyber-threat-intelligence-can-help-to-protect-against-cloud-security-threats. https://www.tripwire.com/state-of-security/how-cyber-threat-intelligence-can-help-to-protect-against-cloud-security-threats

- “DevSecOps-Securing Cyber Security | National Informatics Centre.” DevSecOps-Securing Cyber Security | National Informatics Centre, www.nic.in/blogs/devsecops-securing-cyber-security. https://www.nic.in/blogs/devsecops-securing-cyber-security/