Introduction to Cloud Computing

Dr. Rastgoo

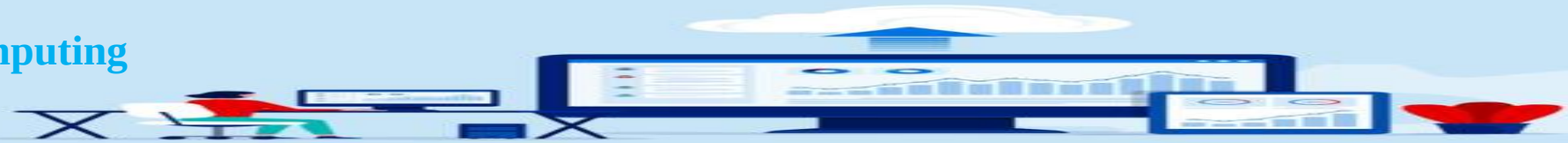
What is Cloud Security?

What is Cloud Security?

- Cloud security refers to the cybersecurity policies, best practices, controls, and technologies used to secure applications, data, and infrastructure in cloud environments.

- In particular, cloud security works to provide storage and network protection against internal and external threats, access management, data governance and compliance, and disaster recovery.

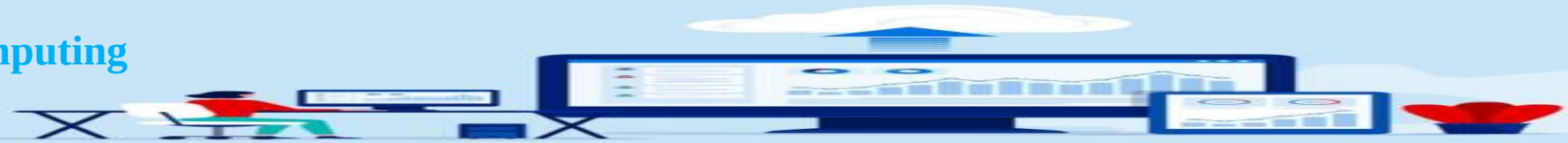
- Cloud computing has become the technology of choice for companies looking to gain the agility and flexibility needed to accelerate innovation and meet the expectations of today's modern consumers. But migrating to more dynamic cloud environments requires new approaches to security to ensure that data remains secure across online infrastructure, applications, and platforms.



Cloud security defined

- Cloud security is the set of cybersecurity measures used to protect cloud-based applications, data, and infrastructure.

- This includes applying security policies, practices, controls, and other technologies like identity and access management and data loss prevention tools to help secure cloud environments against unauthorized access, online attacks, and insider threats.



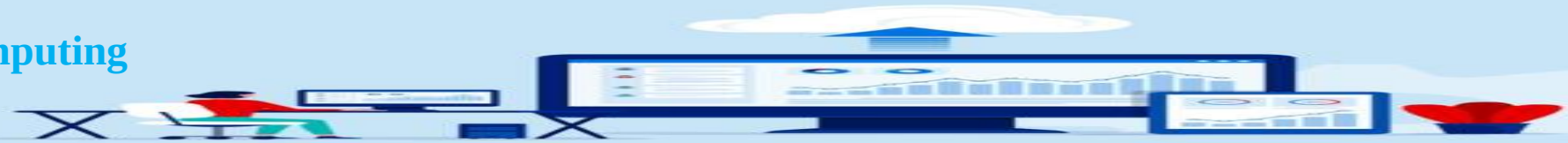
How does cloud security work?

- Cloud security mainly focuses on how to implement policies, processes, and technologies together so they ensure data protection, support regulatory compliance, and provide control over privacy, access, and authentication for users and devices.

- Cloud service providers (CSPs) typically follow a shared responsibility model, which means implementing cloud computing security is both the responsibility of the cloud provider and you—the customer.

- Think of it as a responsibility framework that defines which security tasks belong to the cloud provider and which are the duty of the customer.

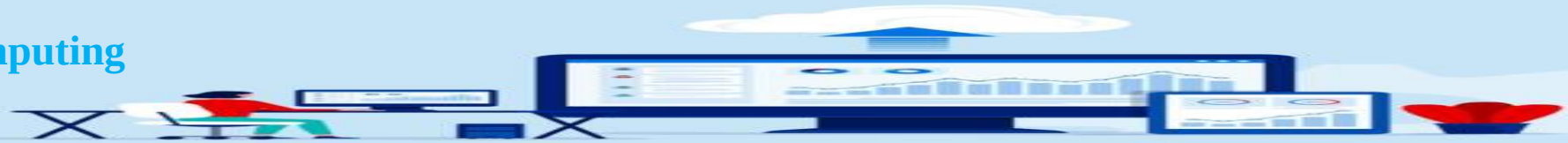
- Understanding where your provider's security responsibilities end and yours begin is critical for building a resilient cloud security strategy.



How does cloud security work?

- Broadly speaking, the CSP is always responsible for the cloud and its core infrastructure, while the customer is expected to secure anything that runs “in” the cloud, such as network controls, identity and access management, data, and applications.

- Shared responsibility models vary depending on the service provider and the cloud computing service model you use—the more the provider manages, the more they can protect.

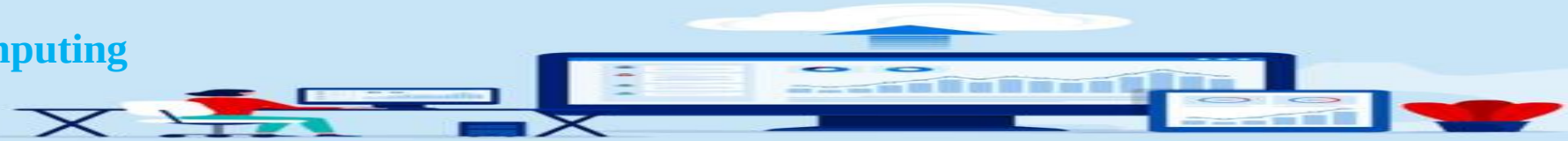


How does cloud security work?

- Here's a look at how this typically works:

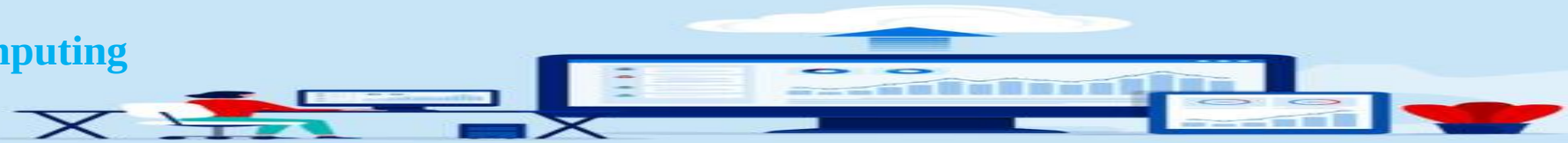
Cloud computing service model	Your responsibility	CSP responsibility
Infrastructure as a service (IaaS)	You secure your data, applications, virtual network controls, operating system, and user access.	The cloud provider secures compute, storage, and physical network, including all patching and configuration.
Platform as a service (PaaS)	You secure your data, user access, and applications.	The cloud provider secures compute, storage, physical network, virtual network controls, and operating system.
Software as a service (SaaS)	You are responsible for securing your data and user access.	The cloud provider secures compute, storage, physical network, virtual network controls, operating system, applications, and middleware.

- More recently, a new model for cloud computing security is emerging which sees shared responsibility models shifting to shared fate models. Under shared fate, a cloud provider provides more comprehensive guidance, resources, and tools to help customers sustain secure use of the cloud, rather than leaving customers to navigate risk management in cloud-native environments.



Why is cloud security important?

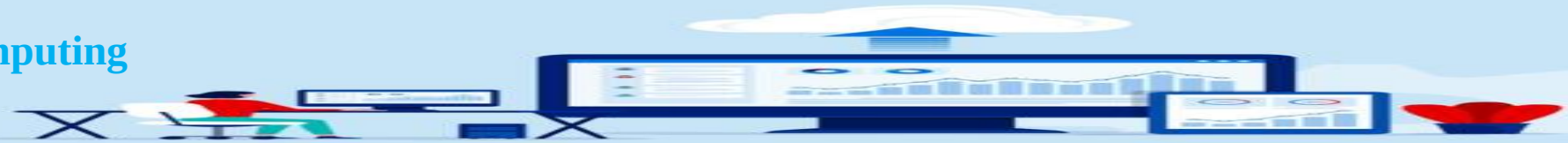
- It’s imperative to rethink security approaches as more companies move to the cloud from on-premises environments, especially with data governance and compliance under the regulatory microscope.
- In an increasingly hybrid and multi-cloud world, you have more freedom than ever to build where and when you want.
- But it also means, security is a lot more complicated than stopping someone from accessing your network.
- Unfortunately, many organizations tend to treat security as an afterthought and may forgo best practices in favor of chasing after faster digital transformation.



Why is cloud security important?

- As a result, attackers see cloud-based targets as a potentially easy path to big gains and are adapting their tactics to exploit vulnerabilities accordingly.

- While cloud security can never guarantee complete prevention of attacks and vulnerabilities, a well-designed cloud security strategy can go a long way toward preventing breaches or mitigating damage, improving compliance, and building stronger customer trust.

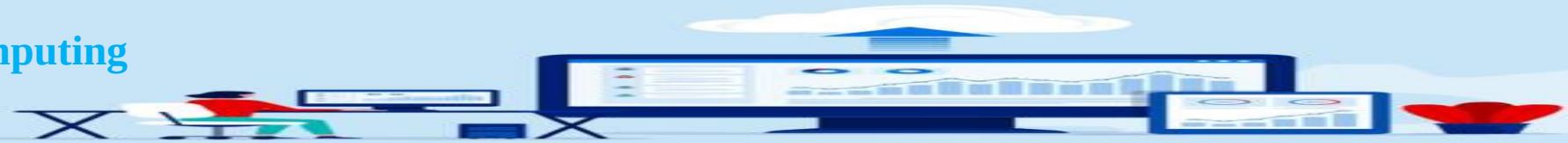


Cloud security risks and challenges

- Cloud suffers from similar security risks that you might encounter in traditional environments, such as insider threats, data breaches and data loss, phishing, malware, DDoS attacks, and vulnerable APIs.

- However, most organizations will likely face specific cloud security challenges, including:

- **Lack of visibility:** Cloud-based resources run on infrastructure that is located outside your corporate network and owned by a third party. As a result, traditional network visibility tools are not suitable for cloud environments, making it difficult for you to gain oversight into all your cloud assets, how they are being accessed, and who has access to them.

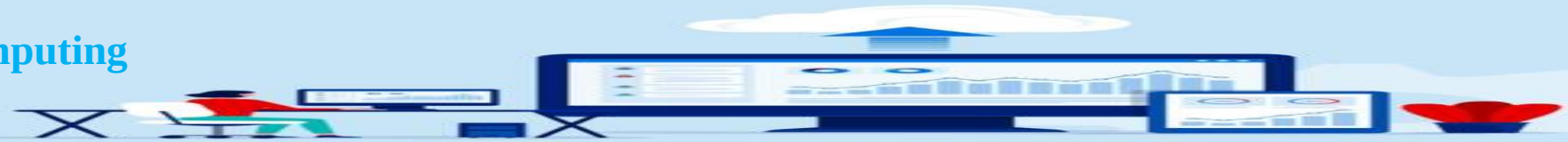


Cloud security risks and challenges

- Misconfigurations: Misconfigured cloud security settings are one of the leading causes of data breaches in cloud environments. Cloud-based services are made to enable easy access and data sharing, but many organizations may not have a full understanding of how to secure cloud infrastructure. This can lead to misconfigurations, such as leaving default passwords in place, failing to activate data encryption, or mismanaging permission controls.

- Access management: Cloud deployments can be accessed directly using the public internet, which enables convenient access from any location or device. At the same time, it also means that attackers can more easily gain authorized resources with compromised credentials or improper access control.

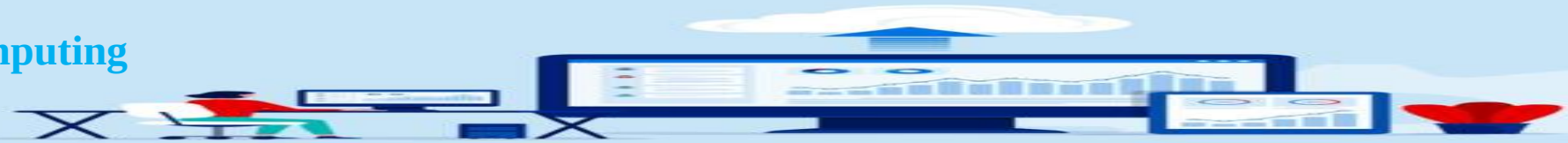
- Multitenancy: Public cloud environments house multiple client infrastructures under the same umbrella, so it's possible your hosted services can get compromised by malicious attackers as collateral damage when targeting other businesses.



Cloud security risks and challenges

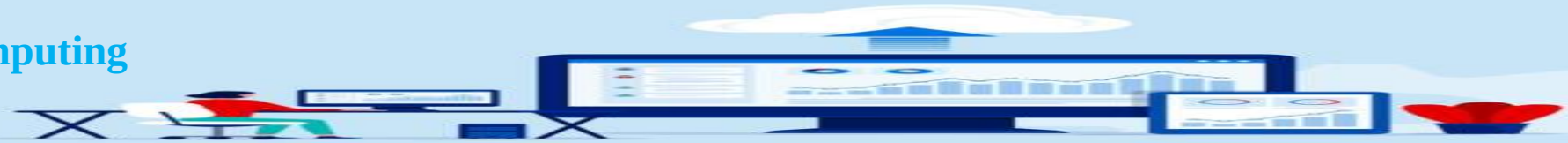
- Dynamic workloads: Cloud resources can be provisioned and dynamically scaled up or down based on your workload needs. However, many legacy security tools are unable to enforce policies in flexible environments with constantly changing and ephemeral workloads that can be added or removed in a matter of seconds.

- Compliance: The cloud adds another layer of regulatory and internal compliance requirements that you can violate even if you don't experience a security breach. Managing compliance in the cloud is an overwhelming and continuous process. Unlike an on-premises data center where you have complete control over your data and how it is accessed, it is much harder for companies to consistently identify all cloud assets and controls, map them to relevant requirements, and properly document everything.



Benefits of cloud security

- Although cloud security has often been framed as a barrier to cloud adoption, the reality is that cloud is no more or less secure than on-premises security.
- In fact, cloud computing security offers many advantages for businesses that can improve your overall security posture.
- The top cloud providers have secure-by-design infrastructure and layered security that is built directly into the platform and its services, including everything from zero-trust network architecture to identity and access management to multi-factor authentication, encryption, and continuous logging and monitoring.
- Plus, the cloud helps you to automate and manage security at an enormous scale.

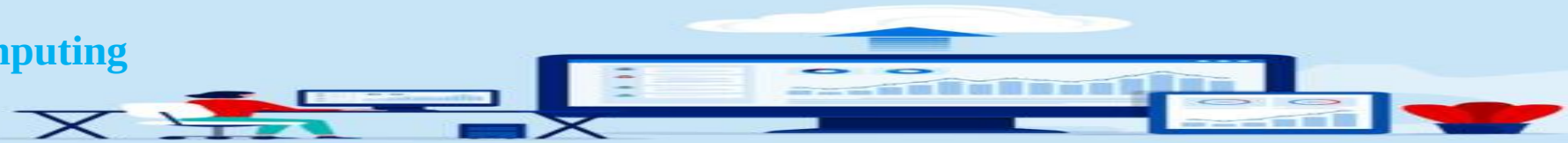


Benefits of cloud security

- Other common cloud security benefits include:

- Greater visibility: Only an integrated cloud-based security stack is capable of providing the centralized visibility of cloud resources and data that is vital for defending against breaches and other potential threats. Cloud security can provide the tools, technologies, and processes to log, monitor, and analyze events for understanding exactly what's happening in your cloud environments.

- Centralized security: Cloud security allows you to consolidate protection of cloud-based networks for streamlined, continuous monitoring and analysis of numerous devices, endpoints, and systems. It also enables you to centrally manage software updates and policies from one place and even implement and action disaster recovery plans.

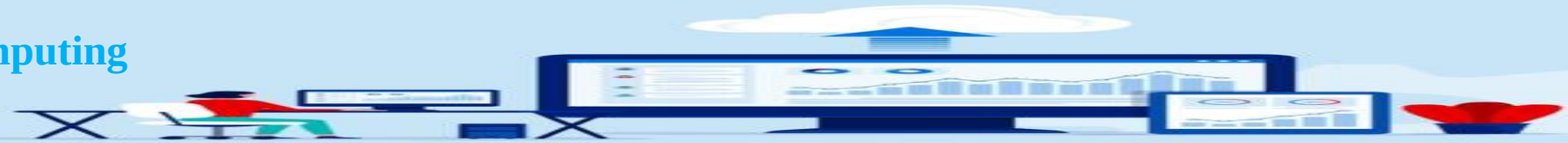


Benefits of cloud security

- Other common cloud security benefits include:

- Reduced costs: With cloud security, you don't have to pay for dedicated hardware to upgrade your security or use valuable resources to handle security updates and configurations. CSPs provide advanced security features that allow for automated protection capabilities with little to no human intervention.

- Data protection: The best cloud computing providers will provide data security by design, offering strong access controls, encryption for data at rest and in transit, and data loss prevention (DLP) to secure your cloud data wherever it's located or managed.

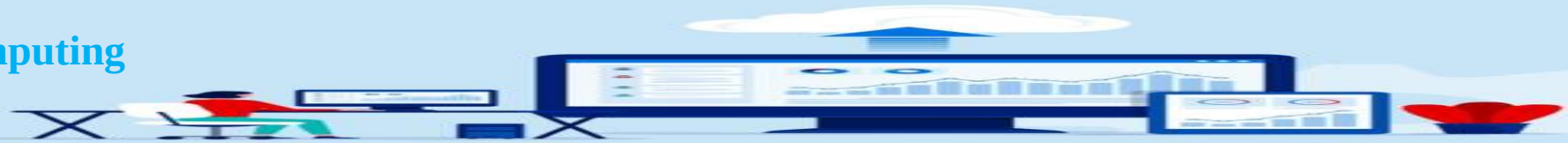


Benefits of cloud security

- Other common cloud security benefits include:

- Cloud compliance: Cloud providers go to great lengths to comply with both international and industry compliance standards, often undergoing rigorous independent verifications of their security, privacy, and compliance controls.

- Advanced threat detection: Reputable CSPs also invest in cutting-edge technologies and highly skilled experts to provide real–time global threat intelligence that can detect both known and unknown threats in the wild and in your networks for faster remediation.

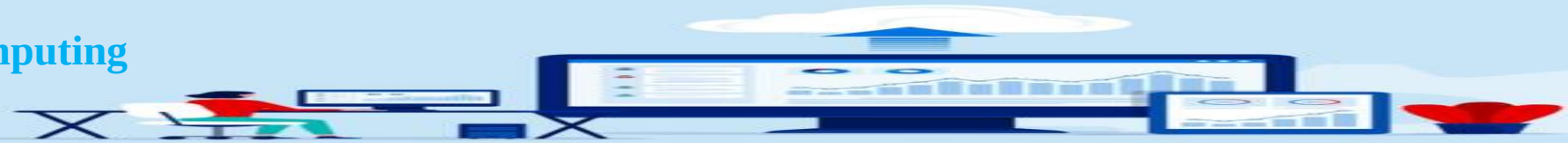


Types of cloud security solutions

- Cloud security is constantly evolving and adapting as new security threats emerge. As a result, many different types of cloud security solutions are available on the market today, and the list below is by no means exhaustive.

- Identity and access management (IAM): IAM services and tools allow administrators to centrally manage and control who has access to specific cloud-based and on-premises resources. IAM can enable you to actively monitor and restrict how users interact with services, allowing you to enforce your policies across your entire organization.

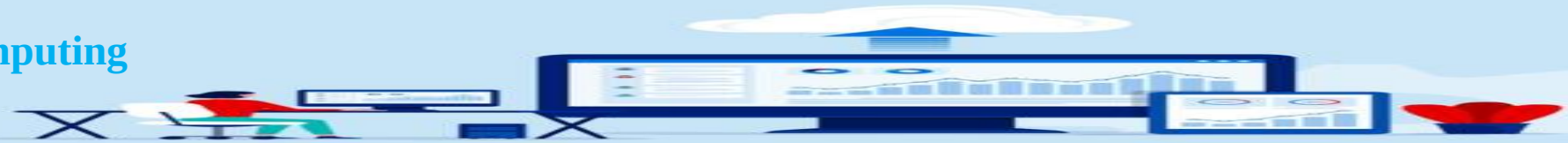
- Data Loss Prevention (DLP): DLP can help you gain visibility into the data you store and process by providing capabilities to automatically discover, classify, and de-identify regulated cloud data.



Types of cloud security solutions

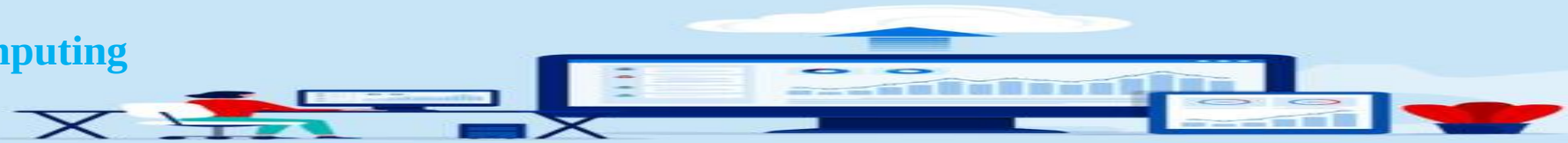
- Security Information and Event Management (SIEM): SIEM solutions combine security information and security event management to offer automated monitoring, detection, and incident response to threats in your cloud environments. Using AI and ML technologies, SIEM tools allow you to examine and analyze log data generated across your applications and network devices—and act quickly if a potential threat is detected.

- Public Key Infrastructure (PKI): PKI is the framework used to manage secure, encrypted information exchange using digital certificates. PKI solutions typically provide authentication services for applications and verify that data remains uncompromised and confidential through transport. Cloud-based PKI services allow organizations to manage and deploy digital certificates used for user, device, and service authentication.



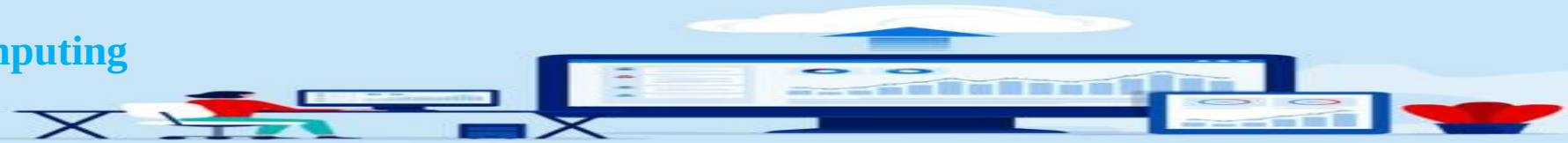
How should you approach cloud security?

- The way to approach cloud security is different for every organization and can be dependent on several variables.
- However, the National Institute of Standards and Technology (NIST) has made a list of best practices that can be followed to establish a secure and sustainable cloud computing framework.
- The NIST has created necessary steps for every organization to self-assess their security preparedness and apply adequate preventative and recovery security measures to their systems.
- These principles are built on the NIST's five pillars of a cybersecurity framework: Identify, Protect, Detect, Respond, and Recover.



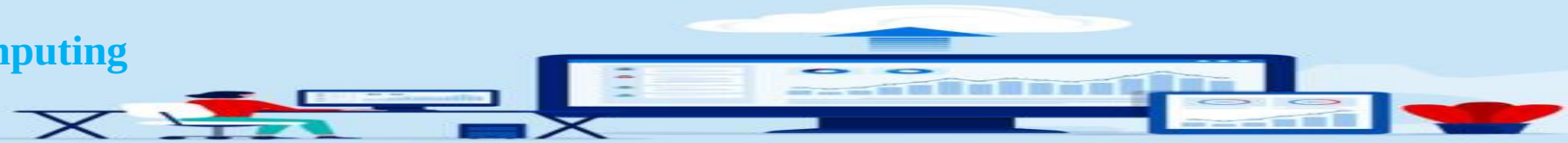
How should you approach cloud security?

- Another emerging technology in cloud security that supports the execution of NIST's cybersecurity framework is Cloud Security Posture Management (CSPM).
- CSPM solutions are designed to address a common flaw in many cloud environments - misconfigurations.
- Cloud infrastructures that remain misconfigured by enterprises or even cloud providers can lead to several vulnerabilities that significantly increase an organization's attack surface.
- CSPM addresses these issues by helping to organize and deploy the core components of cloud security.
- These include identity and access management (IAM), regulatory compliance management, traffic monitoring, threat response, risk mitigation, and digital asset management.



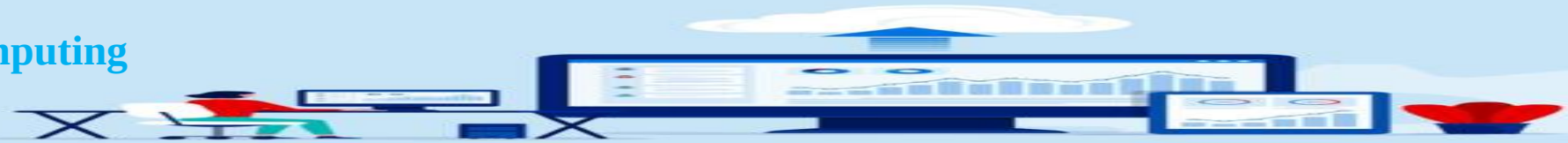
What are cloud security services?

- Cloud security services are a set of services designed to mitigate risk and improve compliance of cloud environments.
- Since these environments can be quite complex, involving a wide range of technologies and processes and, at the same time, exposed to a variety of threats, they can't be protected by a one-size-fits-all solution.
- Rather, most of these services tackle specific areas.
- Technically speaking, these services are actually managed cloud-security services, meaning, they're managed and operated by third parties.



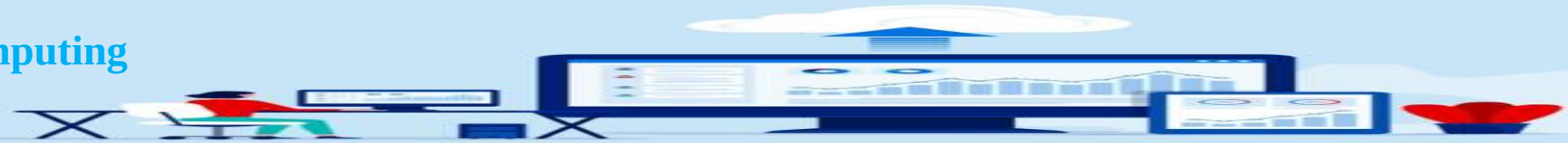
What are cloud security services?

- Offloading security operations to a third party has several benefits, including:
- Threats can be monitored, detected, and responded to by experts who actually know what to do. This ensures threats are dealt with properly and completely.
- Managed cloud security services providers are usually also trained to help organizations achieve regulatory compliance—an area that's normally also outside of an organization's expertise.
- Your IT staff no longer have to handle cyber incidents and can focus instead on supporting your core business operations.



What Are Some Types of Cloud Security Services?

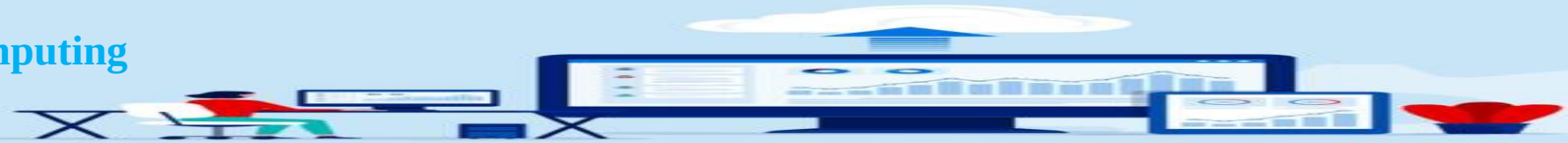
- Cloud environments can be quite complex, consisting of a mishmash of technologies and processes.
- At the same time, they're exposed to a wide range of threats.
- Hence, you normally don't find a one-size-fits-all cloud security service.
- Rather, most of these services tackle specific areas.
- Some of the most common types of cloud security services include Data Loss Prevention (DLP), Identity and Access Management (IAM), email security, web security, and intrusion detection.



What Are Some Types of Cloud Security Services?

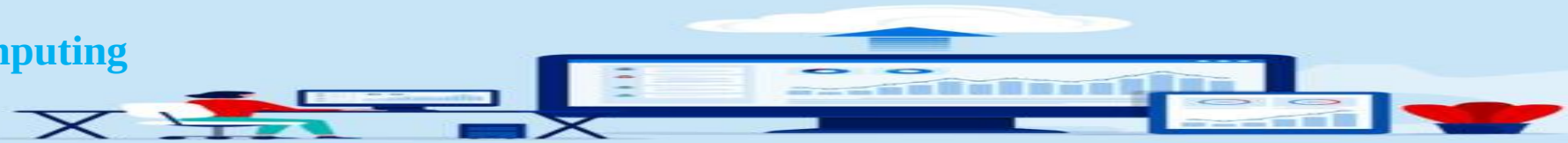
- Data Loss Prevention: With so much data being uploaded to and generated by cloud services, and with so many applications and devices accessing that data, the chance of data loss is enormous. DLP services are built to detect the presence of sensitive data—credit card data, electronic Protected Health Information (ePHI), social security numbers, etc.—and prevent them from falling into the wrong hands.

- Identity and Access Management: IAM services ensure that users adhere to the principle of least privilege, meaning they force users to access cloud resources and perform actions that are permissible to their designated role or function. For instance, an ordinary user shouldn't be able to create instances or delete snapshots. An IAM service can enforce that policy. By using an IAM service, administrators can create permission policies and then associate them with a user or group of users.



What Are Some Types of Cloud Security Services?

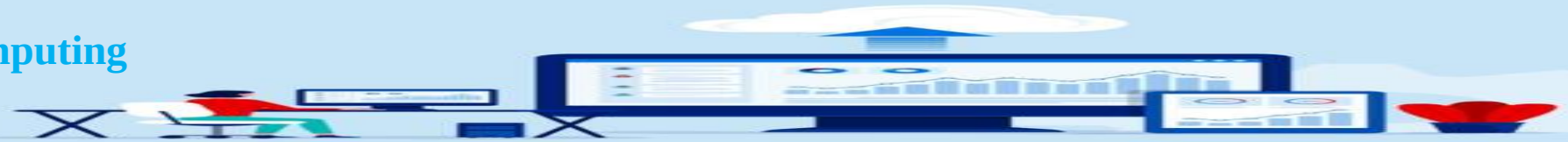
- Email Security: As the weakest link in the security chain, users are often the targets in cyberattacks. And because practically all users use email, many of these attacks—such as phishing and Trojans—are carried out through that medium. Some of these attacks may compromise your cloud environment. For instance, a spear phishing attack may be aimed at acquiring cloud administrator credentials. One way to mitigate these threats is by employing a capable email security service that can detect phishing emails and malicious attachments.



What Are Some Types of Cloud Security Services?

- Web Security: Increased usage of cloud services is an added burden to IT administrators, who now have to deal with a much larger attack surface. Users access cloud services from different locations—in their headquarters, at home, in branch offices, or just about anywhere. Web security solutions, which sit between users (regardless of location) and the internet in typical scenarios, provide administrators the means to secure these connections and protect them against cyber threats.

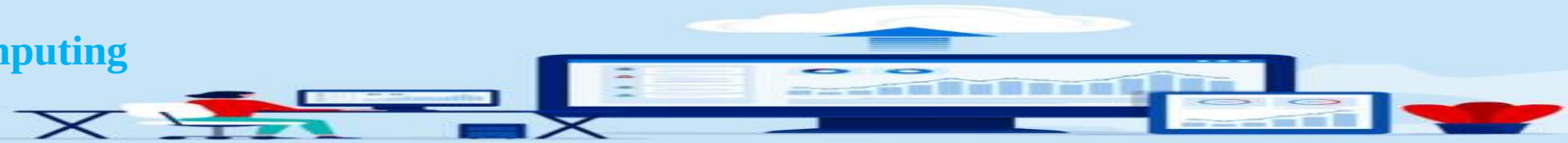
- Intrusion Detection: Intrusion-detection solutions monitor inbound and outbound traffic for suspicious activities and detect potential threats. Usually, detection is done through pattern recognition mechanisms that identify specific signatures and behaviors. Traditional intrusion detection is usually applied to the network layer. However, we're now seeing more solutions applying this kind of protection to the host layer (i.e., to the virtual machines themselves). By detecting threats before they can exploit vulnerabilities, businesses can prevent threat actors from establishing a beachhead in the targeted system.



What about Security Information and Event Management?

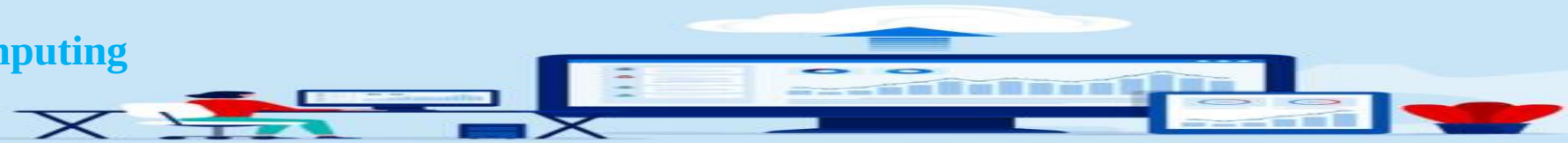
- A Security Information and Event Management (SIEM) solution collects log and event data from various security tools and network devices (e.g., antivirus solutions, DLP software, intrusion detection solutions, firewalls, routers, switches) in real-time, correlates all aggregated data, and then generates alerts based on predefined rules.

- It's one of the key tools of threat detection and incident response teams, enabling them to respond quickly to threats.



Encryption

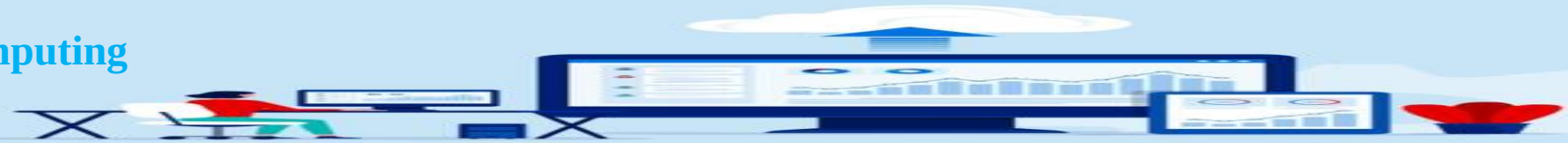
- Encryption, which protects data by rendering it unreadable, is a highly sought security control, not only because it preserves data confidentiality, but also because this functionality is one of the basic requirements for compliance with data privacy/protection laws and regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and General Data Protection Regulation (GDPR).



What about Business Continuity and Disaster Recovery?

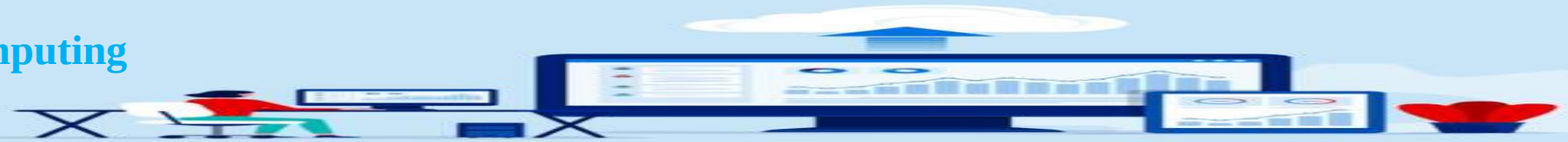
- Despite the High Availability (HA) capabilities of cloud environments, unforeseen events can still disrupt business operations.
- A server instance may fail, ransomware may encrypt files in your cloud storage, a Distributed Denial-of-Service (DDoS) attack may render your services unreachable, and so on.
- Business continuity and disaster recovery services can help ensure you can continue doing business as usual or recover in the quickest possible time should an unforeseen disruptive event occur.

Distributed denial-of-service (DDoS) attacks leverage a wide web of computers or devices infected with malware to launch a coordinated barrage of meaningless online requests, blocking legitimate access.



Can Cloud Security Services Help with Network Security?

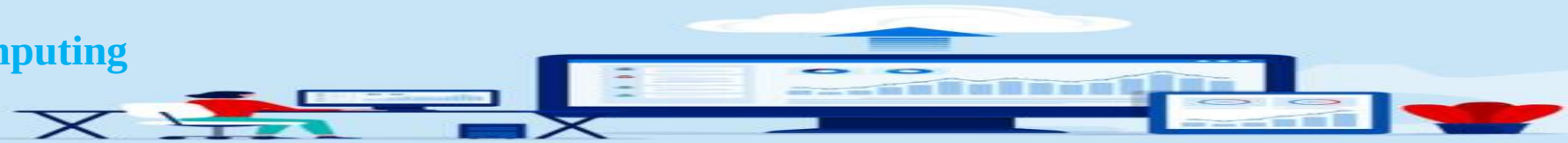
- We all know that scalability is a key characteristic of the cloud.
- Internet as a Service (IaaS) users can spin up a bunch of servers with ease.
- Auto-scaling takes that capability even further by enabling organizations to deploy hundreds if not thousands of instances rapidly, again with relative ease.
- But that scalability comes with a cost. It now means IT teams have a much larger attack surface to secure, a responsibility that's made even more challenging with the increased adoption of more complex hybrid cloud infrastructures.
- Network security services help businesses address vulnerabilities in user-to-cloud as well as intra-cloud and inter-cloud data exchanges.



What Are Best Practices when Using Cloud Security Services?

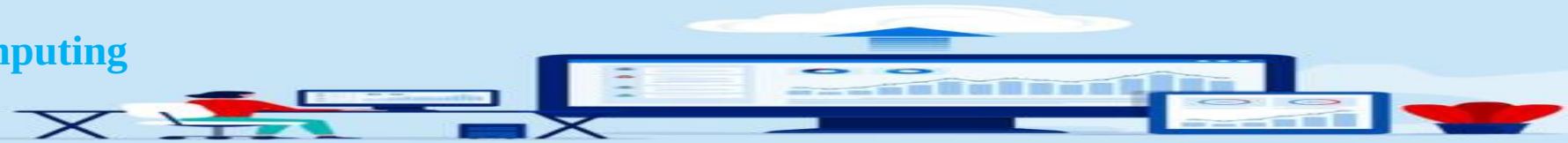
- With so many different cloud security services in the market today, it can be difficult to put them together into an effective layer of defense.

- In the following, we'll share some best practices that will help you make the most of using cloud security services.



Recognize Your Shared Security Responsibility Model

- Before you embark on any cloud security program, it's important to understand your role in the shared security responsibility model.
- It defines what portions of the cloud environment are your responsibility and which ones are for your cloud provider.
- Generally speaking, your provider will supervise the security of the cloud, and you will be responsible for security in the cloud.
- Different cloud service offerings like Software as a Service (SaaS) and IaaS have different takes on this model, so make sure you're looking at the right one.
- Your provider should have this information.

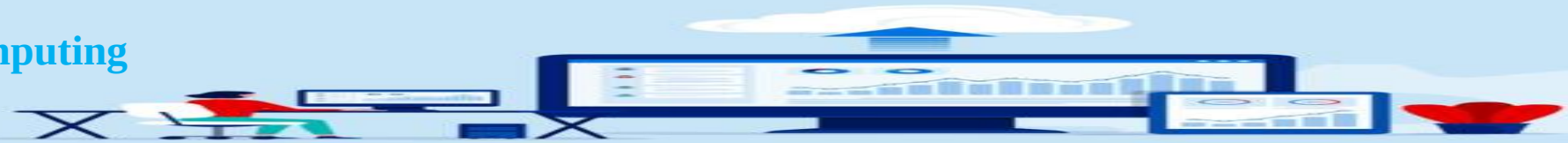


Clarify Concerns about Security Measures and Procedures in Place

- While large cloud providers have several security controls in place, the presence of these controls and the extent of their coverage may vary from one provider to another.

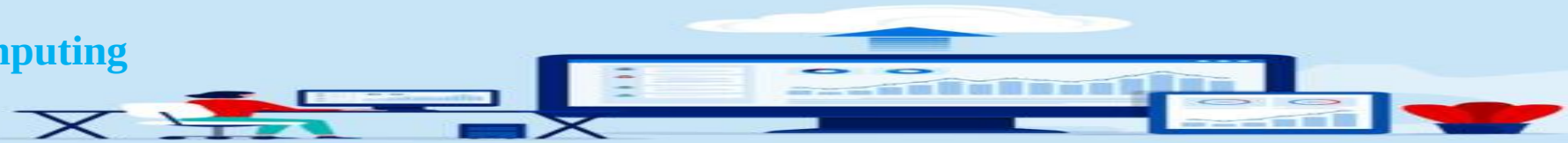
- Hence, it's important to know exactly which controls exist as well as the details pertinent to these controls.

- What's their disaster recovery plan?
- Do they have information that maps their security controls with specific regulatory requirements?
- What access control, encryption, and backup mechanisms are readily available?
- What is the extent of their technical support?
- Do they have 24/7 support?
- These are some of the questions you should ask.



Utilize an Identity and Access Management Solution

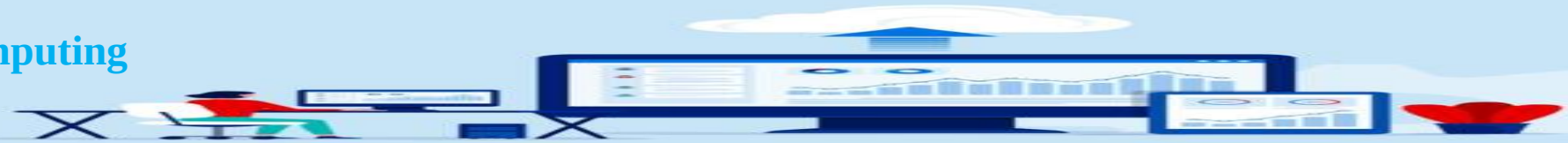
- The recent Cost of a Data Breach Report identified cloud misconfigurations as the third-most common initial attack vectors.
- What's alarming is that many of these misconfigurations aren't even intentional.
- One way to minimize this particular risk is to limit privileged access to only those who absolutely need it.
- Better yet, limit the scope of administrative functions to specific administrators.
- Conversely, you shouldn't be granting absolute administrative rights to just one person.
- All this can be achieved by using an IAM solution.



Train Employees to Recognize Threats

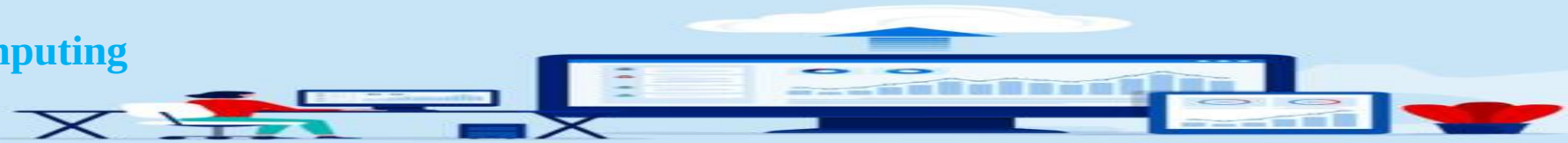
- Since users are the weakest link in the security chain, something must be done to strengthen that link. Otherwise, your cloud security initiatives will only go to waste. Now, since it's their lack of security awareness that's likely exposing them to threats, education is the best solution.

- Ensure all your users undergo security awareness training, and keep them updated with the latest threats, particularly those that target end users (e.g., phishing, spear phishing, and other social engineering attacks). You can even incorporate it into your onboarding process so that they can be equipped with the right mindset from day one.



Document and Apply Cloud Security Policies

- To facilitate a smooth implementation of your cloud security program, document all relevant policies, processes, and procedures.
- These will serve as guard rails for all members of your organization to follow.
- However, those policies shouldn’t be left to gather dust.
- Leadership must take it upon themselves to inspire employee buy-in and spearhead the implementation of those security policies.

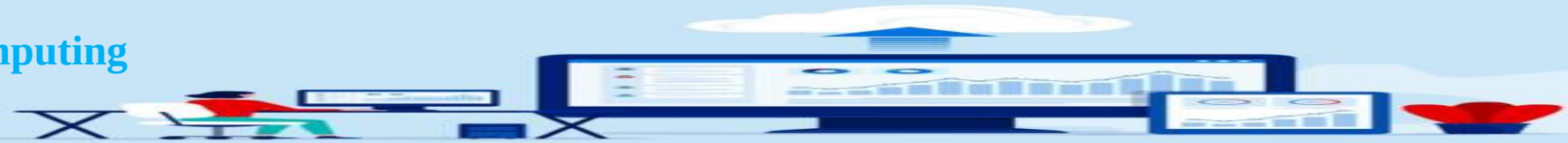


Automated In-Depth Defense Strategy

- Current cyber threats operate mostly with a high degree of sophistication. Thus, for your cloud security services to be effective against them, you need to incorporate them into an in-depth defense strategy. This means a strategy that layers several security mechanisms that can counter sophisticated threats should one defense fail.

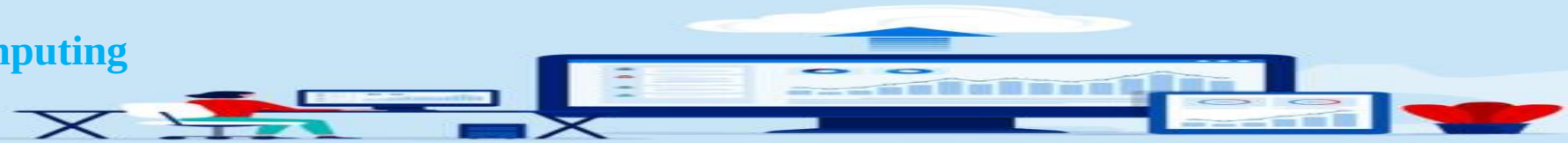
- For greater efficacy, those security solutions should be integrated, automated, and orchestrated.

- This will eliminate manual and time-consuming processes, streamline security operations, optimize threat monitoring, ensure faster detection and incident response, and lower the Total Cost of Ownership (TCO).



Outsource Your Cloud Service Security

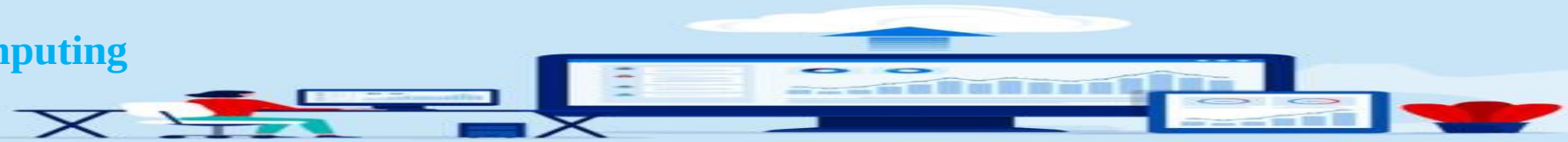
- Not all organizations have dedicated cybersecurity teams, let alone a full-fledged Security Operations Center (SOC), that can architect and implement a defense-in-depth strategy as well as manage its cloud security solutions and take charge of threat monitoring, detection, and response.
- If you lack (or have no) in-house cybersecurity staff, the best option would be to outsource cloud security services.
- Third parties such as Managed Security Service Providers (MSSPs) can manage existing cloud security services and also offer cloud security services themselves.
- By outsourcing your security responsibilities, you can focus more on your core business.



Parallels Remote Application Server (RAS): Virtualize Your Infrastructure, and Enhance Your Cloud Security

- As businesses increase the adoption of remote and hybrid work environments, cloud-based applications and desktops are taking center stage more often.
- This is giving rise to cloud-ready Virtual Desktop Environment (VDI) solutions such as Parallels® Remote Applications Server.
- There are several advantages of using a VDI solution like Parallels RAS, especially from a cloud security standpoint.

Parallels RAS is application virtualization software produced by Parallels that allows Windows applications to be accessed via individual devices from a shared server or cloud system. Parallels RAS was first released in 2014.

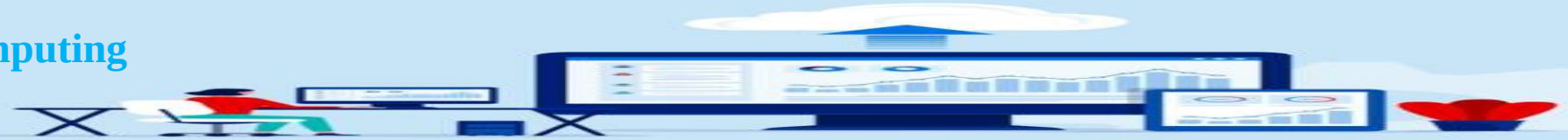


Parallels Remote Application Server (RAS): Superior Encryption

- Data-in-motion encryption is an essential security control in any cloud-based use case.
- That's because user sessions usually pass through the internet and, hence, are exposed to several network-based threats such as man-in-the-middle attacks.
- Parallels Remote Application Server (RAS) protects these sessions with strong Transport Layer Security/Secure Sockets Layer (SSL/TLS) encryption and uses cryptographic elements that comply with the Federal Information Processing Standard (FIPS) 140-2 to provide enterprise-grade security and hide confidential information from network eavesdroppers.

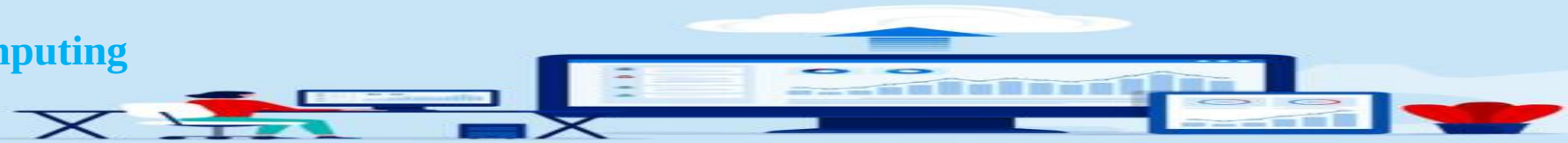
SSL/TLS encrypts communications between a client and server, primarily web browsers and web sites/applications. SSL (Secure Sockets Layer) encryption, and its more modern and secure replacement, TLS (Transport Layer Security) encryption, protect data sent over the internet or a computer network.

The Federal Information Processing Standards (FIPS) are a set of US Government security requirements for data and its encryption. FIPS are publicly shared and encouraged by the US Federal Government, and overseen by the National Institute of Standards and Technology (NIST) of the Department of Commerce.



Parallels Remote Application Server (RAS): Monitoring Tools

- Parallels RAS also provides monitoring tools that enable IT administrators to gain in-depth visibility into user sessions.
- This allows them to monitor what users are doing on the network.
- In addition, Parallels RAS also auto-baselines its VDI environment.
- You can use this to trigger alert notifications should user activities deviate from the baseline, i.e., when abnormal actions are detected.



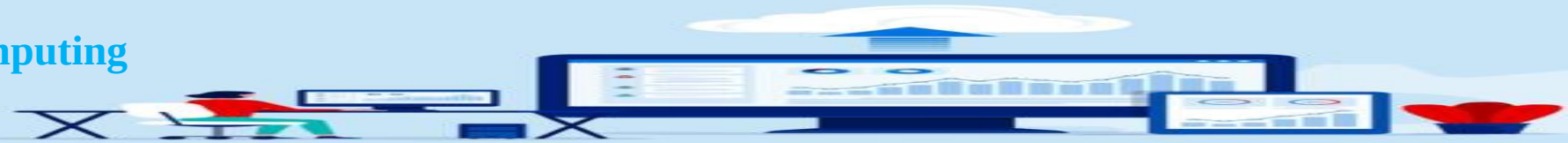
Parallels Remote Application Server (RAS): Hardened Access with Multifactor Authentication

- Since users access cloud-based VDI desktops and applications remotely from any device, it's important to make sure that the person logging in is really who that user claims to be.

- Parallels RAS mitigates the risk of unauthorized logins by adding several multifactor authentication (MFA) options, including Azure MFA, Duo, FortiAuthenticator, TekRADIUS, RADIUS, Deepnet, Google Authenticator, or Gemalto (formerly SafeNet).

- With MFA, even if a threat actor manages to acquire a legitimate user's login password, that person will still be unable to log in if the second factor fails to match what Parallels RAS expects.

Multifactor authentication (MFA) adds a layer of protection to the sign-in process. When accessing accounts or apps, users provide additional identity verification, such as scanning a fingerprint or entering a code received by phone.

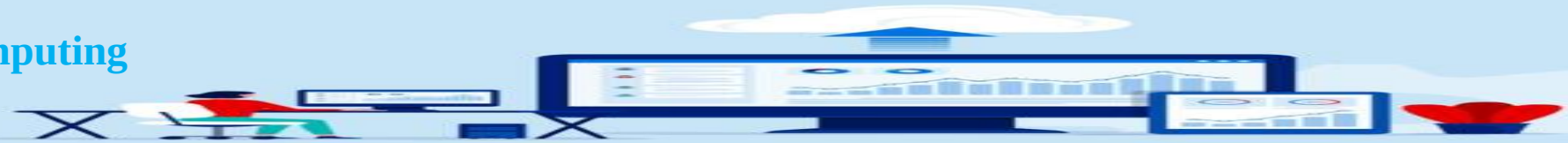


Parallels Remote Application Server (RAS): Advanced Permissions Filtering

- In addition to MFA, Parallels RAS further minimizes the chances of unauthorized access by enabling administrators to create granular filtering rules for user access to a Parallels RAS farm.

- Administrators can specify who can access a published resource based on several criteria, including user, IP address, client device name, client device OS, media access control (MAC) address, and gateway.

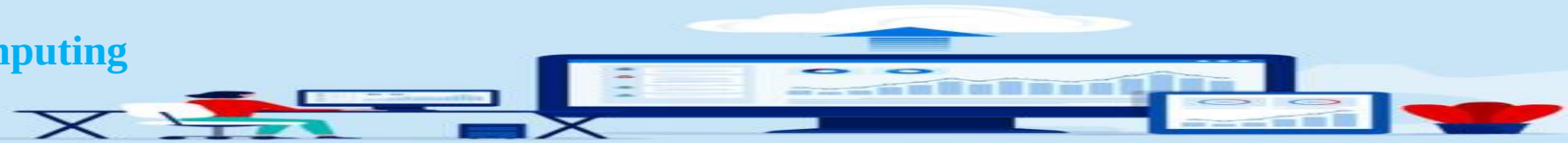
- Only users that can satisfy the specified criteria are granted access.



Parallels Remote Application Server (RAS): Client Policies

- One major advantage of delivering virtual applications and desktops from a centralized location such as the cloud is that it simplifies endpoint device management and security.

- Parallels RAS makes it much easier by allowing administrators to add users to a group, create client policies, and then apply those policies to that group, thereby ensuring policy enforcement.

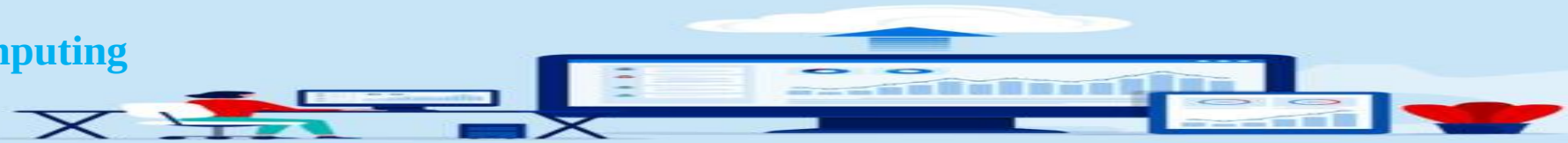


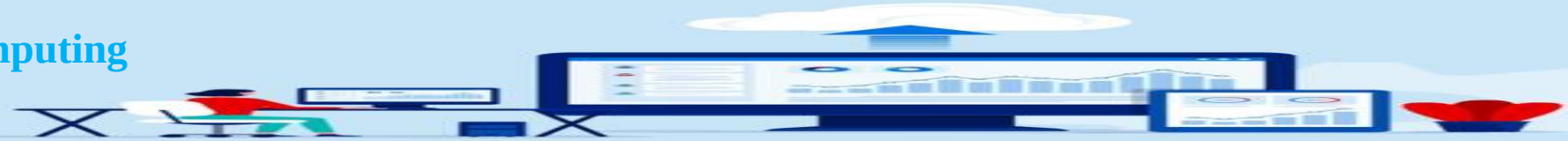
Parallels Remote Application Server (RAS): Security Compliance with the data privacy/protection laws and regulations

- The Parallels RAS assemblage of security features, which includes enterprise-grade encryption, multifactor authentication, advanced permissions filtering, and others, enables companies to conform with data privacy/protection laws and regulations.

- When delivering virtual applications and desktops from the cloud, it's not enough to rely on cloud security services.

- Enhance the protection provided by your cloud security services with a highly secure, cloud-ready VDI solution.





Cloud Computing