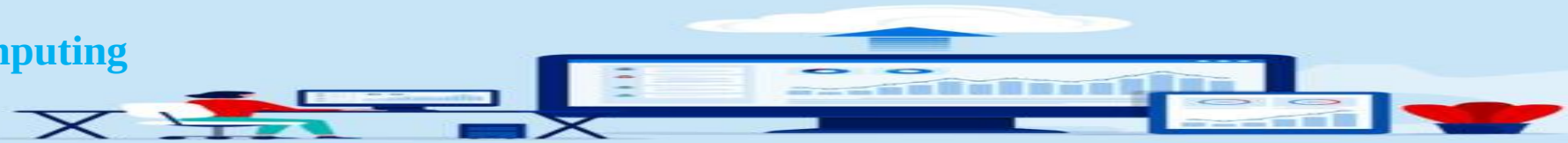
Introduction to Cloud Computing

Dr. Rastgoo

Cloud Computing Defense

Adopting cloud computing for Defence

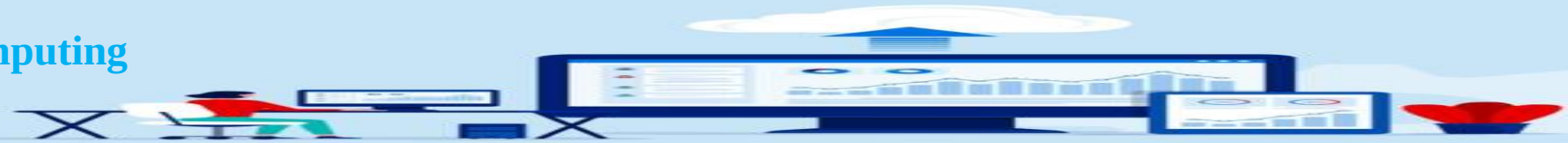
- One of the most critical challenges faced in a congested and contested battlefield is the ability to connect and securely communicate across all domains.
- In order to achieve mission objectives, the defence community need the ability to access and share information seamlessly across the battlespace, to the headquarters in a secure and protected manor.
- Defence computing networks and systems are a notorious and complex set of problems, limited by factors that do not exist in other use cases under normal day to day operations.
- To respond to these challenges, there is a need for a more integrated, digitalized and collaborative operating environment using cloud-based technologies.
- However, when it comes to adopting cloud computing for defence, a number of factors must be taken into consideration.



Cloud Computing

Maintaining trust in Defence

- More often than not, sovereign deployments take place in secure locations where physical access is tightly controlled for devices and people.
- Trust is essential in defence, as is the ability to remove it from people, equipment and systems.
- To maintain trust in defence solutions, identities need to be checked through caching, nodes and other unconventional approaches.
- In defence, rapid deployment of systems with 24/7/365 access is crucial, however can be limited by technology, operations and circumstances.
- In some cases, extreme conditions are endured by systems in deployment, often across multiple environments whether in space, on land, at sea or in air.
- These conditions can mean that availability and other performance indicators cannot be complied with, leading to limitations in analysis.



Cloud Computing

Confidentiality, Integrity, and Availability in Defence solutions

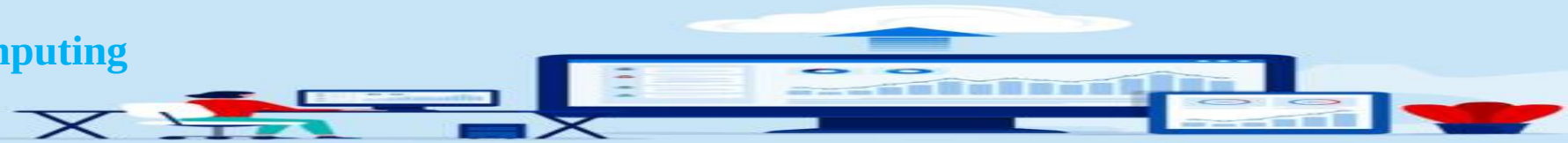
- In defence, security is much tighter than commercial; accreditation has to be achieved and maintained in order for systems to be used, and resources must have mandated security clearance.

- Systems operate with limited or no interoperability, in separate domains with widespread use of encryption, and backhaul of data, operational and management to a third party is not acceptable.

- Confidentiality, Integrity, and Availability are key factors in defence solutions and in order to address these, a comprehensive security framework must be in place early on to manage the entirety and consistency of approach. Not only this, but accreditation must be mandated, achieved and maintained.

- All domains whether unclassified, restricted/official or secret, have their uses and rules. Transition from domain to domain is a requirement for defence solutions but must be controlled as dictated by policy and accreditors.

- As such, sub domain multiple models for data is required.



Cloud Computing

Cloud deployment for operations management

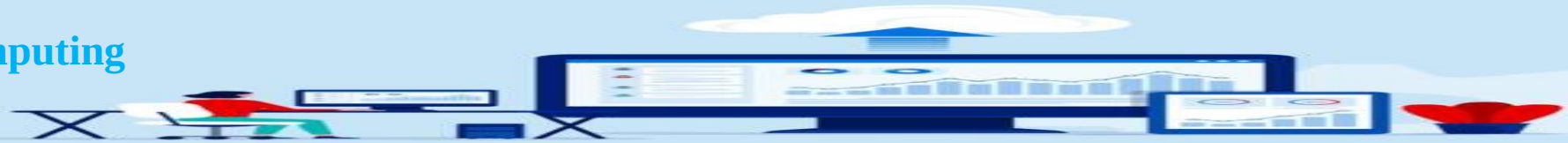
- Schedules for operations and missions require stringent management; if a system is dependent upon an element, then outages are not acceptable to a much more rigorous level, and for some systems, server-less computing will not be acceptable.

- Threats against cloud computing in defence impact more than the aspects of a typical computing system; for example, an attack on the management system will cause widespread disruption.

- The blended attacks of cyber and physical nature are inevitable in defence, occurring simultaneously.

- To prepare for this, risk models will require updates as circumstances change, leading to changes in mitigations and ultimately, technology.

- Interconnects in defence systems are diverse and bearers include satellite, radio link, fixed, commercial and as well as many others; each with its own characteristics and availability all of which need to be taken into consideration in the deployment of cloud infrastructure.

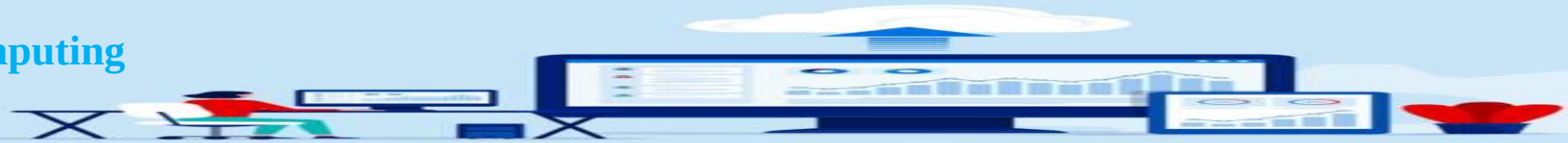


Cloud Computing

Defense-in-depth strategies

- To address critical public cloud data security needs, organizations are turning to defense-in-depth strategies.
- As the amount of data stored in the cloud continues to increase, so too do the challenges of securing that data from malicious attackers.
- According to research from TechTarget's Enterprise Strategy Group, organizations are more confident in their ability to secure on-premises data than data saved in the cloud. Indeed, 54% of organizations surveyed consider their on-premises data security strategies to be more effective than their public cloud infrastructure and application data security.
- This shouldn't be a surprise. Organizations have complete knowledge and control over the on-premises IT infrastructure in which their data resides.

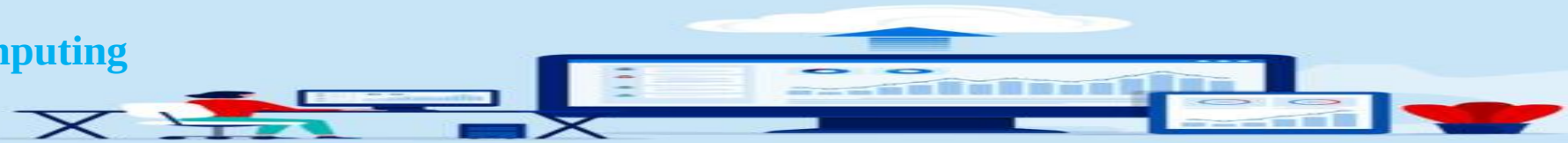
On-premises data refers to private data that companies house in their own facilities and maintain themselves.



Cloud Computing

Defense-in-depth

- Organizations also have developed trusted relationships with many third-party security vendors and are familiar with their capabilities.
- The same can't be said of their cloud-resident data.
- Organizations must assess how well their Cloud Service Provider's (CSP) native tools and controls secure their cloud-resident data.
- While survey respondents were confident in their CSP's monitoring and logging, their level of confidence in other key activities for securing data -- including risk assessments, encryption and access policies -- was lower.



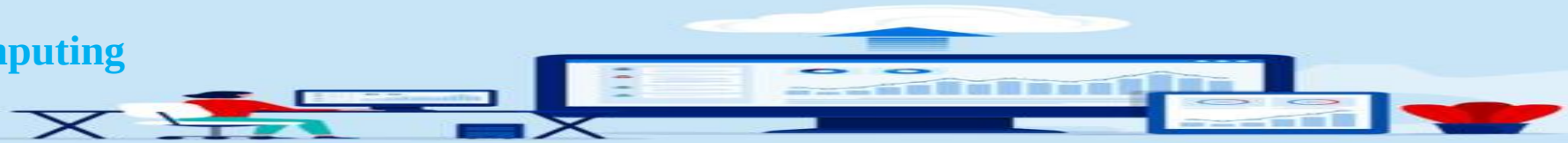
Cloud Computing

Preference for defense in depth

- The lukewarm confidence in CSP-native controls for securing sensitive data and the perception that third-party tools provide better security capabilities are evident when looking at how organizations currently secure cloud-resident data.

- More than half (51%) of organizations said they use a combination of CSP-native controls and third-party controls, with nearly a quarter relying on a Managed Service Provider (MSP) for some or all of their cybersecurity controls.

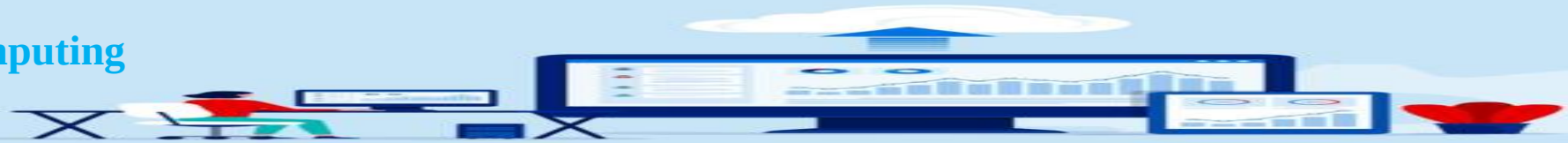
- The preference to employ multiple CSP-native and third-party tools not only reflects an organization's confidence in selecting third-party vendors but also shows organizations recognize defense-in-depth strategies improve their ability to secure sensitive data in the cloud.



Cloud Computing

Defense in depth offers better outcomes

- A defense-in-depth strategy helps reduce data breaches.
- The research found organizations that relied only on CSP-native controls were twice as likely (55%) to have lost data as those using a combination of CSP-native and third-party tools.
- SaaS, IaaS, and PaaS are complex cloud environments with large attack surfaces.
- Multiple, often overlapping, tools provide a better security outcome for organizations.

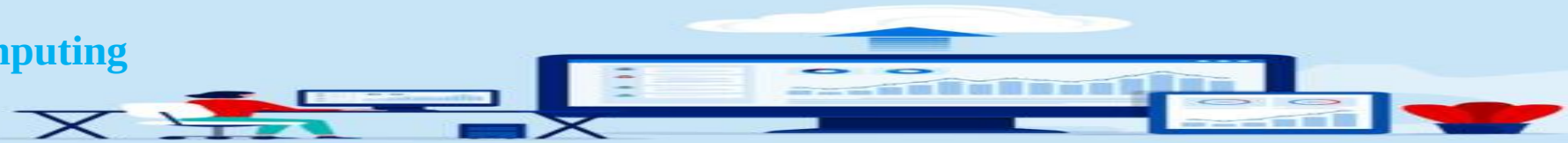


Cloud Computing

Defense in depth offers better outcomes

- Having several tools have could solve some problems that organizations incurred, including the following:
- Misconfiguration
- 33% lost data through SaaS misconfigurations.
- 32% lost data through IaaS and PaaS misconfigurations.
- Policy violations
- 33% had a data-exposure event due to data misclassification.
- 26% had data exposed via unsanctioned apps or services.
- 25% had incorrect or insufficient security policies.
- Access controls
- 26% lost data to an attacker masquerading as an employee via stolen credentials.
- 23% lost data via unauthorized access by an over-provisioned account.

- It's hard to build a single security tool that can defend against the myriad ways data is lost. Instead, using multiple overlapping layers of defense proves to be much more effective than a single point of defense.



Cloud Computing

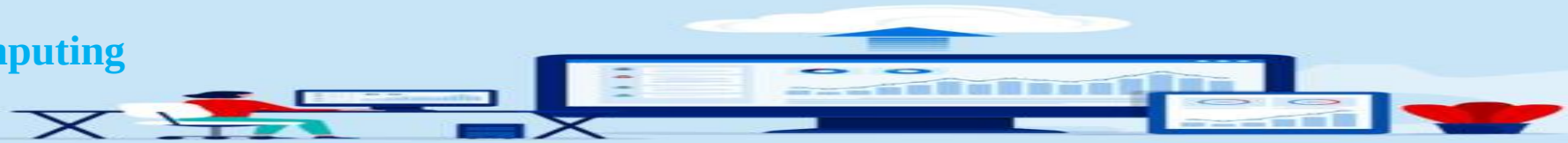
Managed Service Providers (MSPs) provide an additional layer of defense!

- Organizations that relied only on CSP-native controls were three times as likely to have lost data compared to organizations using a combination of CSP-native and third-party tools managed by an MSP.

- MSPs provide the following two advantages:

- MSPs have the time, staff, and resources to become experts in each security tool and can use their experience with the tools across multiple disparate environments to tune them and their operations to get the best outcomes.

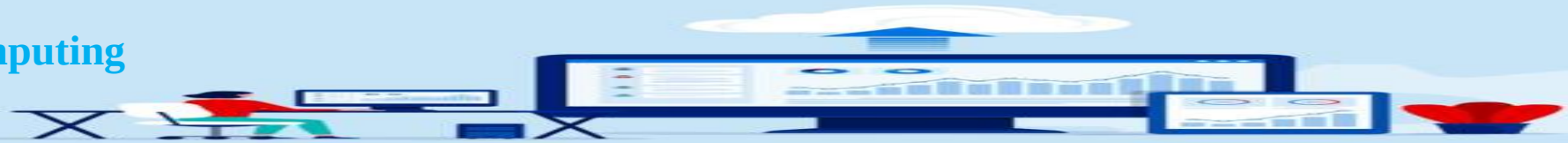
- As the proverbial saying goes, a rising tide lifts all boats. In the MSP realm, they can apply to all their customers their experience in identifying, responding to and mitigating an attack against one of their customers, often before multiple customers get targeted.



Cloud Computing

MSPs provide an additional layer of defense

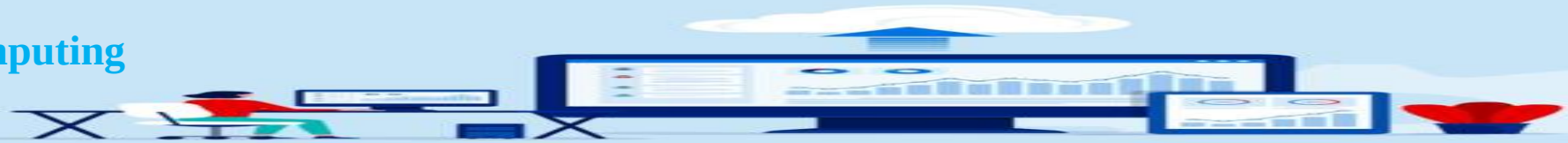
- Because many organizations have expressed concerns about relying solely on CSP-native data security controls, defense-in-depth strategies have taken hold.
- And these strategies have proven to be successful, as much as two times more effective in preventing data loss.
- A defense-in-depth strategy isn't perfect, however.
- It can often require additional investments in tools, people to run the tools and people to stitch the tools into a coherent cybersecurity stack.
- The security architects should approach their defense-in-depth strategy with an eye toward balancing the investments against their desired outcomes.



Cloud Computing

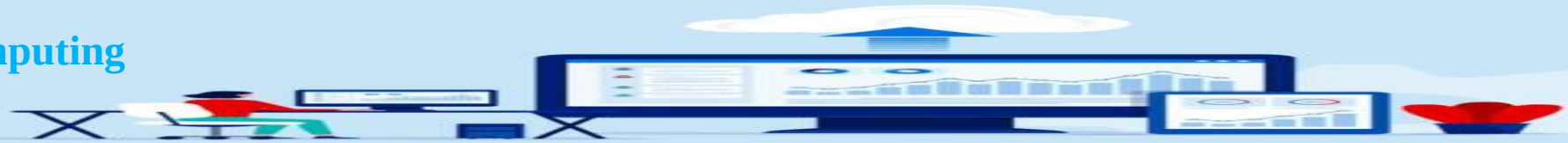
Defence Strategies for a Cloud-first Computing Era

- The uncontested benefits of digitization have pushed the envelope for cloud adoption.
- Organizations are increasingly choosing to become cloud-first by moving most or all their existing infrastructure to the cloud and adopting the latest technologies without making large investments, by paying only for the services they use.
- This gives them flexibility and is cost-effective.
- Unfortunately, it also increases the attack surfaces exposing them to various threats.
- Dynamically evolving threat vectors in the cloud environment have compelled organizations to continuously rework both security controls and processes. This continuous adaption requires a pivot strategy for defense controls to rapidly discover, comprehend, and reposition the enterprise baseline.



Defence Strategies for a Cloud-first Computing Era

- Since a cloud-first computing environment differs from on-premise infrastructure, it is not adequate to merely replicate the security controls of on-premise into the cloud.
- Cloud-native microservices applications, diverse workloads, identity explosions, and cloud data posture need focused attention.
- Focus areas define the security quad of Posture, Identity, Data, and Code.
- The Security Quad forms the four pillars on which cloud security strategy stands.
- We need dynamic security controls, enforcement points, and granular governance to align these security tenets with the modern dynamic era.



Outlining the Security Quad: Posture, Identity, Data, and Code

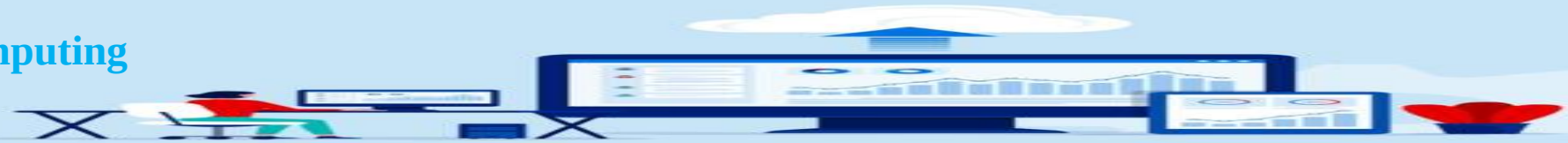
- The first order of the strategy is to look at architectural design and design solutions that align with the zero-trust principle to minimize the attack surface.

- Posture or architecture design helps manage the overall security framework using standardized controls, responsibilities, and security configurations, which can be deployed across common use cases.

- Next is identity, which covers knowledge of users, business environments, vulnerabilities, and threats. Solutions powered by Artificial Intelligence (AI) or Machine Learning (ML) can address modern threat vectors. Along with traditional controls, Data Security Posture Management (DSPM) or Cloud Infrastructure Entitlement Management (CIEM) helps address specific cloud problems.

Data security posture management (DSPM) is a comprehensive approach to safeguarding an organization's sensitive data from unauthorized access, disclosure, alteration, or destruction.

Cloud Infrastructure Entitlement Manage (CIEM) solutions automate the process of managing user entitlements and privileges in cloud environments. This makes them an integral part of an organization's identity and access management and cloud security posture management (CSPM) infrastructure.

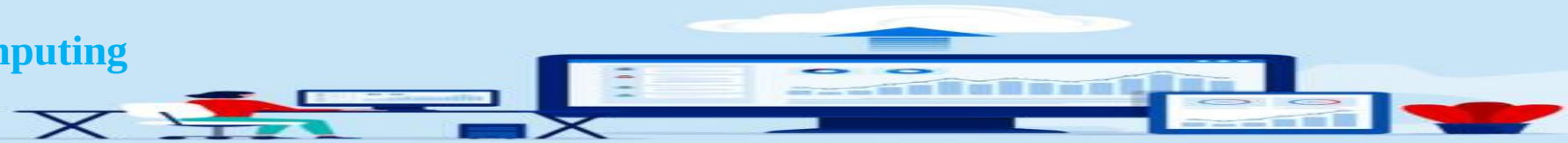


Outlining the Security Quad: Posture, Identity, Data, and Code

- The third pillar of the security quad is data, which needs to be encrypted, whether at rest or whether it is being transmitted between internal and external cloud connection points, to reduce the risk of breaches.

- The fourth component is code, where security is automated and embedded across the entire development life cycle through various checks and tests to secure cloud workloads with speed and agility and prevent manual error.

Zero Trust: Regardless of where the request originates or what resource it accesses, Zero Trust teaches us to "never trust, always verify." Every access request is fully authenticated, authorized, and encrypted before granting access.



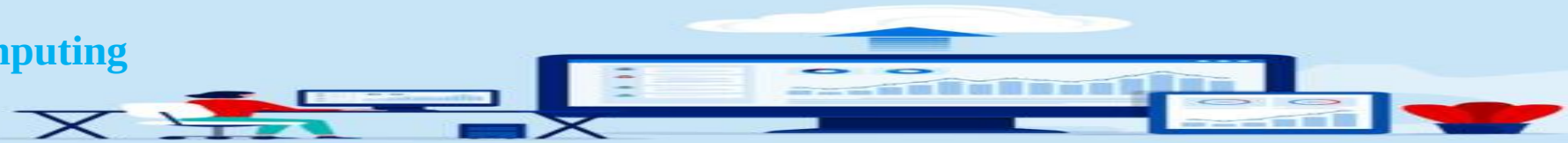
Cloud Computing

Effective Cloud-first Defence Strategies

- While selecting security controls is important, one must emphasize how these controls are delivered.

- By aligning with zero-trust principles, where implicit trust is eliminated, and every stage of the digital interaction is continuously validated, organizations can minimize the attack surface by pushing the service edge and policy enforcement close to the user and away from the application stack.

- A decentralized structure for security controls is another way forward, and possible with the use of Continuous Integration (CI) and Continuous Delivery (CD). With this, security teams can devote their efforts towards governance, guaranteeing baseline hygiene and security consistency while reducing the cloud attack surface to a large degree.



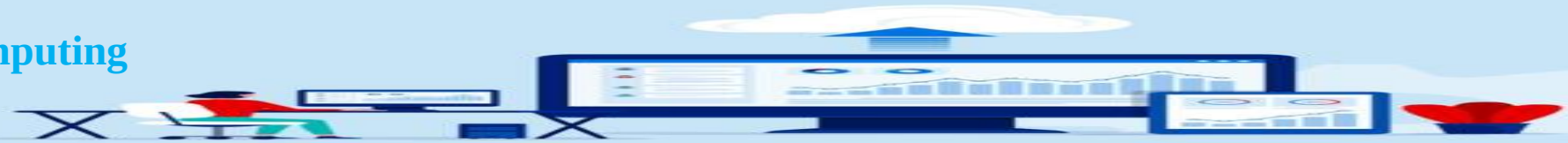
Cloud Computing

Effective Cloud-first Defence Strategies

- Whether code pipelines (CD services that model, visualize, and automate the release of security codes) are configured using gating controls or baseline mandate definitions, they must adhere to the organization's security and compliance objectives.

- Governance can also be extended to the operation space by shifting to Managed Detection and Response (MDR) services that cover all cloud assets from infrastructure, application, and IoT landscape, with built-in AI and ML algorithms.

Managed Detection and Response (MDR) is a category of a Security-as-a-Service offering, where an organization outsources some of its security operations to a third-party provider. As its name suggests, it goes beyond simply detecting threats to actually working to remediate them on an organization's network.

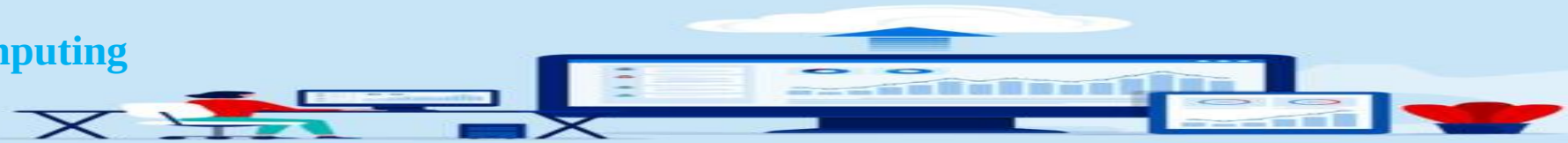


Cloud Computing

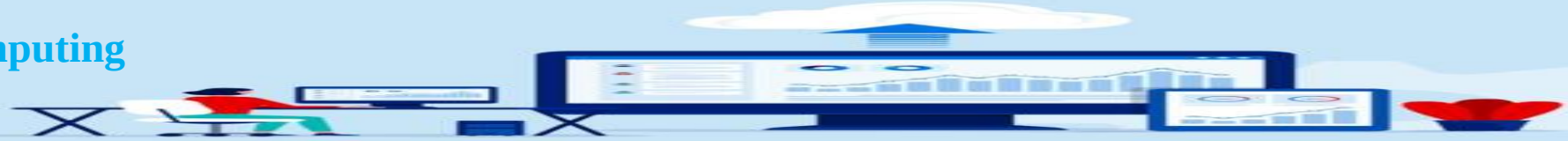
Conclusion

- Organizations should strive to protect themselves from potential security and privacy threats by implementing robust security best practices.

- The most effective defense strategy for a cloud-first computing era would be zero trust, with a strong emphasis on governance to regulate all the events, flows, and movements within the cloud landscape.



Cloud Computing



Cloud Computing