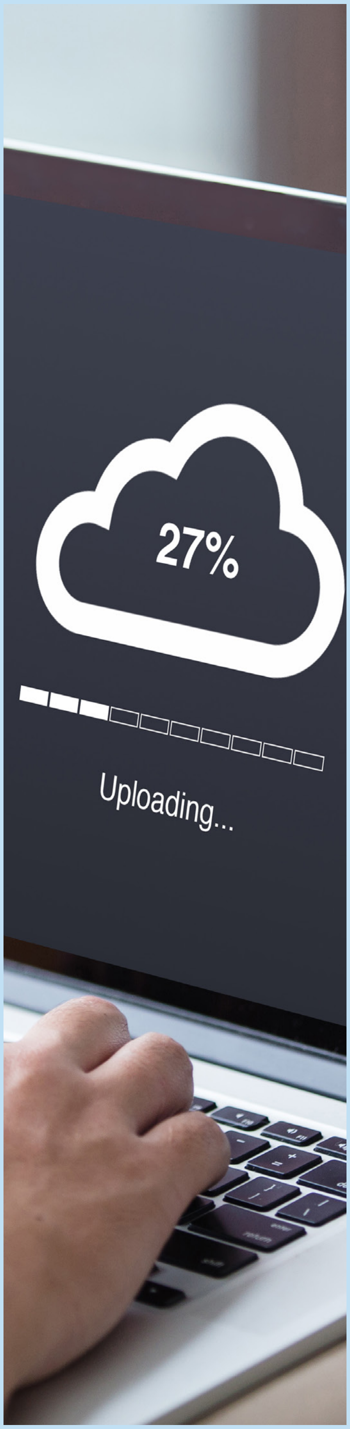
Infosys cobalt

VIEW POINT



SHRINKING THE EXPLOITABLE ATTACK SURFACE ON CLOUD

Abstract

Organizations around the world are racing to adopt cloud – public, private, and hybrid – making it critical to secure cloud infrastructure from cyber-attacks. Many reports show that attacks on cloud assets have doubled in the last few years. This is forcing even small and medium-sized organizations to proactively safeguard their cloud assets. This paper examines the growth potential of the cloud security market. It further describes recent cloud attacks, the repercussions, and key security issues in the cloud. For organizations looking to reduce the attack surface and remediate looming threats, the paper provides best practices to safeguard their customers and business.

Infosys®
Navigate your next

Introduction: Cloud Security Market Review and Outlook

The cloud computing revolution is gathering momentum rapidly with no signs of slowing down. With every passing year, digital technology pervades further into enterprises, transforming how they operate and manage operations. This makes cloud the infrastructure of choice for organizations across different industries. Cloud lowers cost, optimizes resource utilization, and provides easy scalability. When executed well, the total cloud spend is much lower than on-premises infrastructure cost as cloud providers only charge for the resources used. These costs can be further optimized by identifying idle or unused cloud resources and shutting those down. Some organizations leverage heat maps to discover peaks and valleys in computing demand. During peak times, reserved instances can be provisioned for further discounts and to right-size resources for optimized costs. With on-demand resource provisioning, cloud fosters automated and dynamic scaling of computing, allowing organizations to be responsive and agile.

Along with these advantages, however, cloud also brings a higher degree of risk by presenting a wider attack surface for cyber threats. Innovation is driving new cloud applications like serverless computing, quantum computing, digital natives, edge computing, containerization, artificial intelligence, and mobile cloud computing. But concerns continue to haunt organizations faced with phishing, malware, data breaches, unprotected APIs, weak identity and access management, system vulnerabilities, and improper due diligence.

Post Covid-19, it is predicted that the cloud management and security services market size will nearly double from US $34.5 billion in 2020 to US $68.5 billion by 2025. This spurt is being driven by the following factors:

- Organizations want a cloud-first approach but are unaware of the regulatory compliances to be followed in the shared responsibility model
- The threat environment is more sophisticated today with technologies like artificial intelligence being used to execute attacks
- Vulnerability management needs to be automated to continuously monitor the landscape, fix issues in real-time, and assure compliance
- Increasing adoption of 'bring your own device' models and IoT technologies will extend the threat surface in the absence of strong access controls and device security
- There is an increase in demand for DevSecOps or integration of security into the software development cycle

Key Security Issues in Cloud

There are 3 key factors – data, compliance, and talent – that can lead to security issues and hinder smooth adoption of cloud. Data is the most valuable resource in any organization and must be protected through a systematic approach. The dynamic nature of data makes this challenging as data moves between data-at-rest, data-in-motion, and data-in-use. Data must be encrypted when at rest, protected when in motion, and unencrypted when being processed by applications.

Further, organizations are often unaware of how cloud providers segregate enterprise data within multi-tenant environments and what processes are used to destroy or delete data when the engagement is over. Understanding this requires qualified and experienced cloud security professionals, a talent that is scarce in the current climate.

Compliance too is a significant hurdle. Organizations must know what regulatory compliances are applicable to them according to region and industry. For instance, there are country-specific as well as industry-specific compliance requirements. GDPR is an example of country-specific compliance while HIPAA is a standard for the American healthcare industry. While cloud service providers comply with various global standards applicable to cloud platforms, there may be certain protocols that organizations should focus on to protect their data, applications, and services.

In summary, trust is an underlying factor for cloud service providers. Organizations entrust their cloud vendors with sensitive data, applications, and assets that are shared in an environment external to the organization. Without a comprehensive approach to cloud security, this leaves them exposed to different kinds of cyber-attacks.

Examples of Cyber-attacks on Cloud Infrastructure

The nature of attacks on cloud platforms varies widely and can range from Distributed Denial of Service (DDoS), ransomware, and malware, to cloud API abuse and unauthorized access to cloud infrastructure as described below:

DDoS attacks

The most common form of attack on cloud computing system is a distributed denial of service or DDoS attack. In DDoS, hackers send thousands of requests in a few seconds to machines via bots, automation, or queries. This overloads the responding machines, breaking the system. Ultimately, the machine is unable to respond, creating a non-availability of service. A recent DDoS attack on Cedexis, a cloud computing company, made headlines among French news channels and magazines. Cedexis is responsible for providing speedy content delivery to media clients including news channels and magazine. The attack happened in a data center located in the USA, bringing down three out of their five networks.

Ransomware attacks

In May 2020, a US-based cloud service provider, Blackbaud, reported a ransomware attack that stole sensitive client data. Blackbaud was forced to pay an undisclosed ransom amount to secure the stolen data and ensure that copies of data were deleted to prevent further cybercrime. Soon after, they took measures to block system access and encrypt data files.

Cloud malware injection

Cloud malware injection is a type of attack where hackers successfully implant malicious code into SaaS or IaaS providers. As users start using this piece of code, it is injected into cloud instances, allowing attackers to steal login credentials, access back-end systems, or even control the cloud server. In 2020, Microsoft reported the existence of this vulnerability in the form of a zero-day attack.

Cloud API attacks

Cloud API attacks are done by hackers who exploit ineffective security practices that, in turn, expose APIs to the world. When developers do not follow API hygiene during cloud hosting, it leads to technical glitches that can cripple the entire cloud infrastructure system, making it vulnerable to attack. In a recent example, Apple's mobile device management API was found to allow unauthorized user access to confidential information. RSA's mobile app API was also shown to be vulnerable, containing hardcoded credentials that allowed access to the database containing contact information of attendees.

What should Cloud Customers Know about the Cloud Attack Surface

Cloud-related attacks target specific areas such as APIs, platforms, infrastructure, databases, and applications.

API integrations

Organizations expose business-critical data and application functionalities to end-consumers through APIs. However, while securing APIs is critical, the scale and flexibility of cloud create different challenges in doing so. An API developer or security administrator should protect APIs from the top 10 risks as listed by the Open Web Application Security Project (OWASP) and enable secure access control. Developers should also control the consumption rate, limit excessive scope, and provide security governance through Role Based Access Control (RBAC) management, global policies, and compliance. A secure-by-design approach is also useful to secure the API SDLC lifecycle.

Platforms

The security of platforms in the cloud or the Platform-as-a-Service (PaaS) cloud model is a shared responsibility between cloud service providers and consumers. Vulnerabilities in the application code, misconfigurations in network controls, identity and directory infrastructure, excessive access privileges of administrative accounts, exposed client endpoints, and applications data have always been the initial enumeration pivot point for hackers to gain persistent access to cloud platforms. Thus, deploying platforms on the cloud requires shifting the focus from infrastructure-centric to identity, application and data-centric perimeter security approaches.

Infrastructure

Many organizations opt for the infrastructure-as-a-service (laaS) cloud model to host application workloads as it is more flexible, saves cost, and offers control and security advantages. But it also places all the responsibility of securing cloud workloads on the cloud customer. To reduce the attack surface, organizations must ensure security across all cloud layers bearing in mind the key design principles. These include zero-trust approach, secure by design, least privilege and separation of duties, security governance, audit traceability, data protection in transit and at rest, and security monitoring. The cloud layers include infrastructure, network, endpoints, API/applications, and data. All of these form the attack surface for adversaries who look for ways to penetrate through cloud-native security services or external security solutions.

Databases

Data is critical for organizations, clients, and end-users. Cloud security architects should clearly identify data-specific security requirements on cloud and establish defense strategies across each layer. These layers include network access security with firewall rules, Access Control Lists (ACLs), security groups, access management with SQL or AD authentication, assigned roles and permissions, row level security, threat protection, and information protection at rest and in-transit with TLS/SSL, encryption keys, and certificates.

Cloud applications

By default, applications deployed on the cloud have direct privileged access to the internal ecosystem that consists of systems, databases, networks etc. Application vulnerabilities and misconfigurations open doors for attackers to gain unauthorized access to cloud infrastructure. To prevent this, organizations must identify input and output attack surface areas in applications during the threat modelling process. They must also ensure security best practices and guidelines are followed to fix application vulnerabilities and misconfigurations before being deployed into cloud. This will prevent applications from executing extraneous behavior and leaking sensitive details. Additionally, web application firewalls and DDoS protection such as cloud-native security services help protect applications from live DDoS attacks and exploitable code.

Addressing Security Issues in the Cloud

Managing cloud security is a shared responsibility between the enterprise, customer and the cloud service provider. Enterprises should be apprised of the various security protocols when embarking on cloud transformation journeys. For example, they should know how physical security is being managed at the data centers by the cloud security provider. They should also understand who is responsible for security in different cloud models like IaaS, PaaS, and SaaS. Further, compliances must be delineated between those met by the cloud service provider and those that lie with the enterprise or organization.

Here are some guidelines to follow:

Secure the data

Encryption and tokenization can be used for data in storage or data at rest. In this way, even if data is copied from a server or database for unauthorized use, it remains incomprehensible and cannot be read. When data is in transit, moving between servers and applications, VPN technologies can be used to encrypt data. While under processing by any application, confidential computing can be used to encrypt data in memory and outside of the CPU.

Secure the environment

Enterprises should conduct periodic risk and cloud assessments along with vulnerability management for their cloud applications and infrastructure. This will enable threat protection through a combination of SIEM, endpoint security, threat intelligence services, threat hunting services, etc.

Secure the infrastructure

Cloud service providers are sometimes unaware of enterprise virtual instances. Thus, it is up to the organization to protect their applications and perimeters within the cloud tenant. This can be done on two levels – network as well as host. Network-level security includes segmentation, topology, perimeter firewalls, and access control lists. Some considerations are penetration testing for cloud infrastructure, certifying a production rollout, entry and exit points for cloud infrastructure, types of firewalls, WAF, load-balancing, etc. While providing host-level security for SaaS and PaaS is the responsibility of the cloud service provider, the onus of ensuring IaaS security is on the cloud customer. Server security, operating system security, container security, and virtual software security are some examples of host-level security in an IaaS environment.

Secure the applications

DevSecOps allows application and infrastructure security to be embedded within the software development lifecycle. DevSecOps is a shift-left principle for security in DevOps. It allows code vulnerabilities to be identified early in the development stage by embedding security in the CI/CD pipelines, thereby creating Secure Software Development LifeCycles (SSDLC).

Best Practices to Minimize the Attack Surface on Cloud

As more and more companies adopt cloud, the number of workloads residing on cloud infrastructure increases exponentially, presenting a wider target for cyber-attacks. Thus, ensuring that all cloud assets are secure on the cloud should be the topmost priority for cloud security teams.

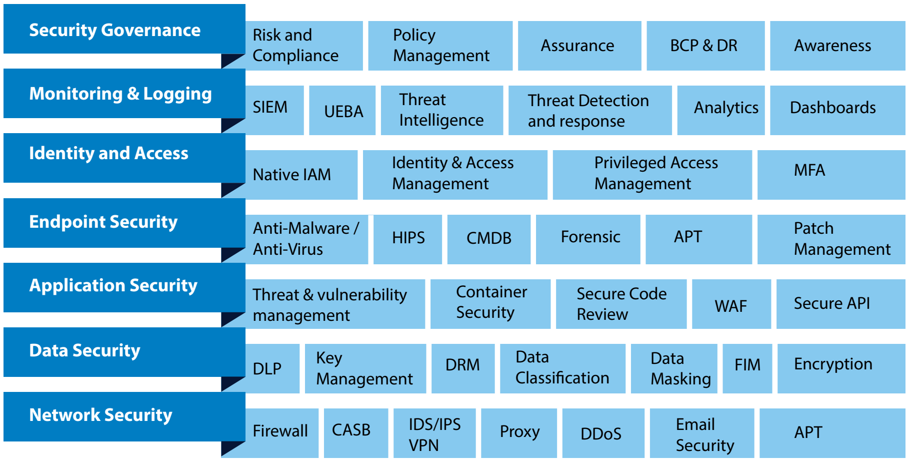
The overarching approach should aim to reduce the attack surface, thereby reducing the scope and risk of exploitation from outsiders. Infosys recommends using layered architecture that does not expose assets to the internet unless required. Such architecture will also have the ability to withstand DDoS attacks and mitigate loss of business and reputation.

Here are some best-practices that enterprises can use to narrow the exploitable attack surface of their cloud ecosystems:

Use cloud security frameworks for in-depth defense

It is important to follow a security framework that covers aspects such as security governance, monitoring, logging, network security, and application security. Policy management within security governance helps restrict cloud assets from being victims of external attacks. Equally important is the network security that controls, inspects, and monitors both ingress and egress traffic with IDS/IPS capabilities. Tools for detection and remediation of DDoS attacks also play a vital role.

A multi-layered approach focusing on in-depth defense will enhance overall security. Areas such as network security controls with network segmentation, data encryption when at rest, end-point security, monitoring, and behavior analysis are the key elements for achieving a 'defense-in-depth' architecture.



Security Governance	Risk and Compliance	Policy Management	Assurance	BCP & DR	Awareness		
Monitoring & Logging	SIEM	UEBA	Threat Intelligence	Threat Detection and response	Analytics	Dashboards	
Identity and Access	Native IAM	Identity & Access Management	Privileged Access Management	MFA			
Endpoint Security	Anti-Malware / Anti-Virus	HIPS	CMDB	Forensic	APT	Patch Management	
Application Security	Threat & vulnerability management	Container Security	Secure Code Review	WAF	Secure API		
Data Security	DLP	Key Management	DRM	Data Classification	Data Masking	FIM	Encryption
Network Security	Firewall	CASB	IDS/IPS VPN	Proxy	DDoS	Email Security	APT

Reference architecture of cloud security framework: Defense-in-depth

Embed secure-by-design

Creating a robust cloud security framework with proper design principles is important, particularly when migrating to public cloud. Design principles should incorporate key security approaches such as Identity and Access Management (IAM), principle of least privileges, zero-trust model, data security in transit and at rest, secure development environment, logging and monitoring, risk assessment and continuous compliance. It should also include SIEM solution to handle security incidence, threats, vulnerabilities, and endpoint security.

Minimize attack entry points

It is important to set up cloud infrastructure and applications with minimum entry points. The network should be designed in a way that limits the number of routes to sensitive systems. Organizations can leverage cloud-native elastic load balancers and Content Delivery Network (CDN) services like AWS CloudFront or Azure Front Door that have in-built capabilities to withstand DDoS attacks.

Perform network segmentation

Segmentation of cloud networks will make it difficult for an attacker to traverse deep within the infrastructure and gain access to sensitive and protected data. Organizations must protect the network at different layers with network security groups and network access control lists that restrict both inbound and outbound traffic across subnets. Micro-segmentation of networks helps isolate workloads from each other, thus making it more secure. This also follows the zero-trust approach. The best use case for micro-segmentation is separation of development, test, and production workloads as well as the implementation of hybrid cloud environments.

Enable strong alerting and automation

Any breach of compliance rules that violate an organization's security frameworks must be alerted on time and supported with automated remediation. For example, any SSH/RDP ports opened to the internet should be immediately and automatically remediated with notifications sent to important stakeholders. Most cloud service providers offer artificial intelligence and machine learning-based native cloud solutions that provide end-to-end SIEM as well as Security Orchestration Automation and Response (SOAR) solutions. This eliminates the overheads of managing the infrastructure. Advanced threat detection and management solutions combined with automation are highly recommended. Some examples include Guard Duty and Azure Advanced Threat Protection

Regularly audit assets and network traffic

Regular audits help identify misconfigured assets, Indicator of Compromise (IoC), and outdated software, all of which are prone to high vulnerabilities. Third-party cloud security assessment tools can provide insights into an organization's security posture along with proper remediation guidelines. It is important to note that continuous compliance plays a vital role in ensuring that cloud environments maintain a healthy state of security. Regular monitoring enables timely alerting and auto-remediation of breaches. Leveraging cloud-native services like AWS Security Hub and Azure Security Center helps maintain a strong security posture. These monitor the common industry-standard regulatory compliance protocols like PCI DSS, ISO 27001, SOC TSP, etc.

Conduct periodic network scans

Organizations must invest in tools that run network scans, identify key weaknesses within the network, and categorize these according to different risk levels. The scan results can be compared against the security compliance framework that organizations adhere to.

Implement application security

OWASP mentions top 10 vulnerabilities that can be mitigated by proper application firewall rules. These rules can also protect from attacks at the application layer 7 of the OSI model. The underlying approach is one of three A's – authentication, authorization, and auditing, which safeguards against unauthorized access. Single sign-on based authentication (SSO) instead of the prevalent Lightweight Directory Access Protocol (LDAP) can help manage users more effectively from a central location, thereby improving governance.

Enhance API security

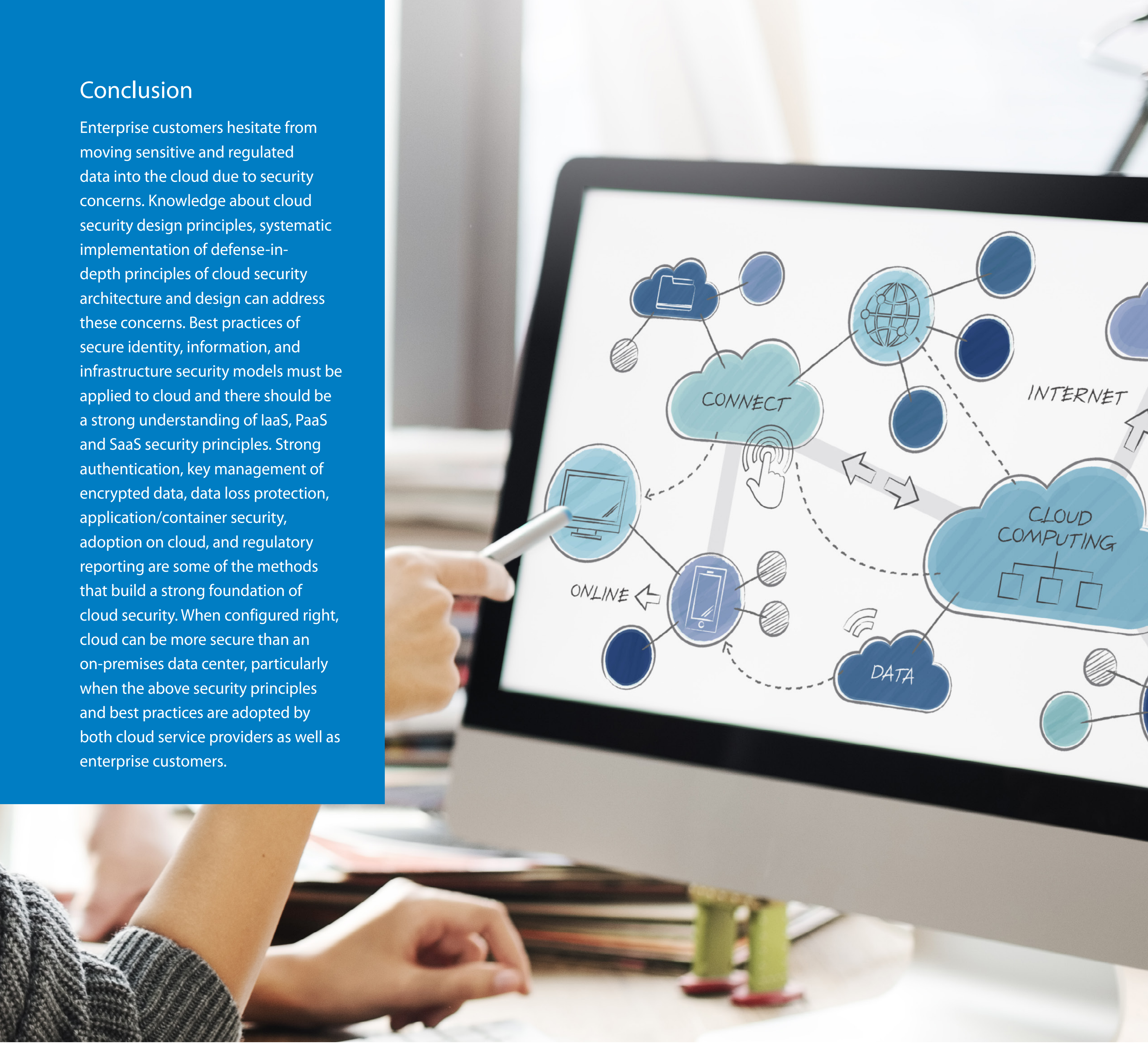
From an API security and governance standpoint, two focus areas to consider are request-based security implementation and authentication. The first dictates policies and constraints on API consumption to gatekeep who can consume data and how much. The second area of authentication dictates policies and constraints on authentication and authorization in terms of who the consumer is and what they can access. For example, Google offers a cross-cloud Apigee API management platform that secures enterprise assets such as internal and external users, data, and backend systems in the API program. In 2020, Google (Apigee) was named a 'Leader' in Gartner's Magic Quadrant for full lifecycle API management. Apigee protects against hackers, bots, and suspicious behavior, and verifies API keys at runtime. It also generates OAuth tokens and implements JSON threat protection through policies that extend security for API protection. Gartner has also named other leaders in API management such as MuleSoft, Kong, IBM, Software AG, Axway, and Microsoft that offer similar security capabilities on multi-cloud platforms to protect against various API threats.

Foster cybersecurity awareness among employees

Human error multiplies the risk to sensitive enterprise assets. Unsafe user behavior such as clicking on phishing links allows malicious malware to be installed on cloud assets or expose employee credentials that can then be used by cybercriminals to exploit and steal sensitive data. Conducting regular employee awareness programs on cloud hygiene will help reduce exposure to attacks.

Conclusion

Enterprise customers hesitate from moving sensitive and regulated data into the cloud due to security concerns. Knowledge about cloud security design principles, systematic implementation of defense-in-depth principles of cloud security architecture and design can address these concerns. Best practices of secure identity, information, and infrastructure security models must be applied to cloud and there should be a strong understanding of IaaS, PaaS and SaaS security principles. Strong authentication, key management of encrypted data, data loss protection, application/container security, adoption on cloud, and regulatory reporting are some of the methods that build a strong foundation of cloud security. When configured right, cloud can be more secure than an on-premises data center, particularly when the above security principles and best practices are adopted by both cloud service providers as well as enterprise customers.



References

1. https://www.marketsandmarkets.com/PressReleases/cloud-security.asp
2. https://www.prnewswire.com/news-releases/cloud-security-market-worth-68-5-billion-by-2025--exclusive-report-by-marketsandmarkets-301107486.html
3. https://medium.com/cloud-management-insider/7-cloud-computing-trends-you-should-follow-in-2020-7c7231e81645
4. https://www.zymr.com/top-cloud-security-trends
5. https://www.microsoft.com/security/blog/2019/12/03/microsoft-security-leader-5-gartner-magic-quadrants/
6. https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#8c21ad36261a
7. https://platform.keesingtechnologies.com/malware-attacks/

About the Authors

Soumitri Mishra
Project Manager

Satyajeet Hambirrao Mohite
Senior Associate Consultant

For more information, contact askus@infosys.com

Infosys®
Navigate your next