Designing a secure **Azure solution**

Azure security best practices and design considerations

www.hcltech.com

Table of **Contents**

List of **Figures**

Introduction

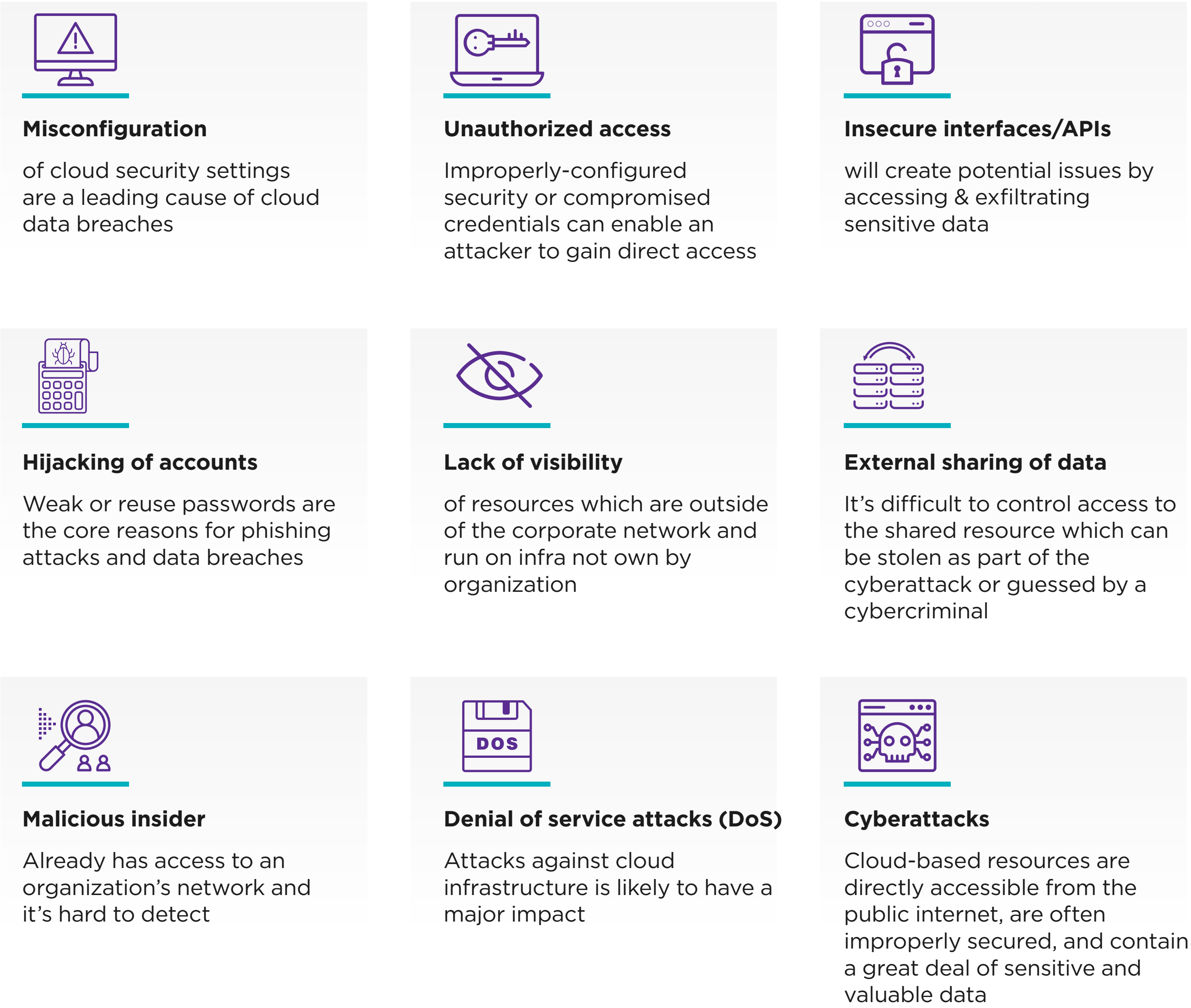
Cloud computing plays an increasingly important role in the operations of organizations of all sizes and industries worldwide. Often, security is a major concern among cloud customers, primarily due to difficulties in getting necessary contractual guarantees of data control, availability concerns, the potential risks of data loss, and the difficulties of enforcing the organization's security policies.

Cloud security is a set of policies, controls, procedures, and technologies that work together to protect cloud-based systems, data, and infrastructure. Information security has always been a complex subject, and it evolves quickly with the creative ideas and implementations of attackers and security researchers. The origin of security vulnerabilities started with identifying and exploiting common programming errors and unexpected edge cases.

Security is one of the most important aspects of any architecture. It provides confidentiality, integrity, and availability assurances against deliberate attacks and abuse of valuable data and systems. Losing these assurances can negatively impact business operations and revenue, and the organization's reputation in the marketplace. One of the best reasons to use Azure for applications and services is to take advantage of its wide array of security tools and capabilities

Typical cloud security issues and threats

Almost every organization has adopted cloud computing to varying degrees within their business. However, with adoption comes the need to ensure protection against top cloud security threats.



Misconfiguration

of cloud security settings are a leading cause of cloud data breaches

Unauthorized access

Improperly-configured security or compromised credentials can enable an attacker to gain direct access

Insecure interfaces/APIs

will create potential issues by accessing & exfiltrating sensitive data

Hijacking of accounts

Weak or reuse passwords are the core reasons for phishing attacks and data breaches

Lack of visibility

of resources which are outside of the corporate network and run on infra not own by organization

External sharing of data

It's difficult to control access to the shared resource which can be stolen as part of the cyberattack or guessed by a cybercriminal

Malicious insider

Already has access to an organization's network and it's hard to detect

Denial of service attacks (DoS)

Attacks against cloud infrastructure is likely to have a major impact

Cyberattacks

Cloud-based resources are directly accessible from the public internet, are often improperly secured, and contain a great deal of sensitive and valuable data

Figure 1 Cloud security issues and threats

How to overcome app security issues in Azure

Azure is built on leading security technologies to help organizations manage and control user identity and access, which are central elements in securing the environment. Azure uses encryption to protect communications and operational processes, including your data in transit and advanced tools to detect and defend against threats.

One must consider the following areas while designing and developing secured apps in Azure to take advantage of its wide array of security tools and capabilities.

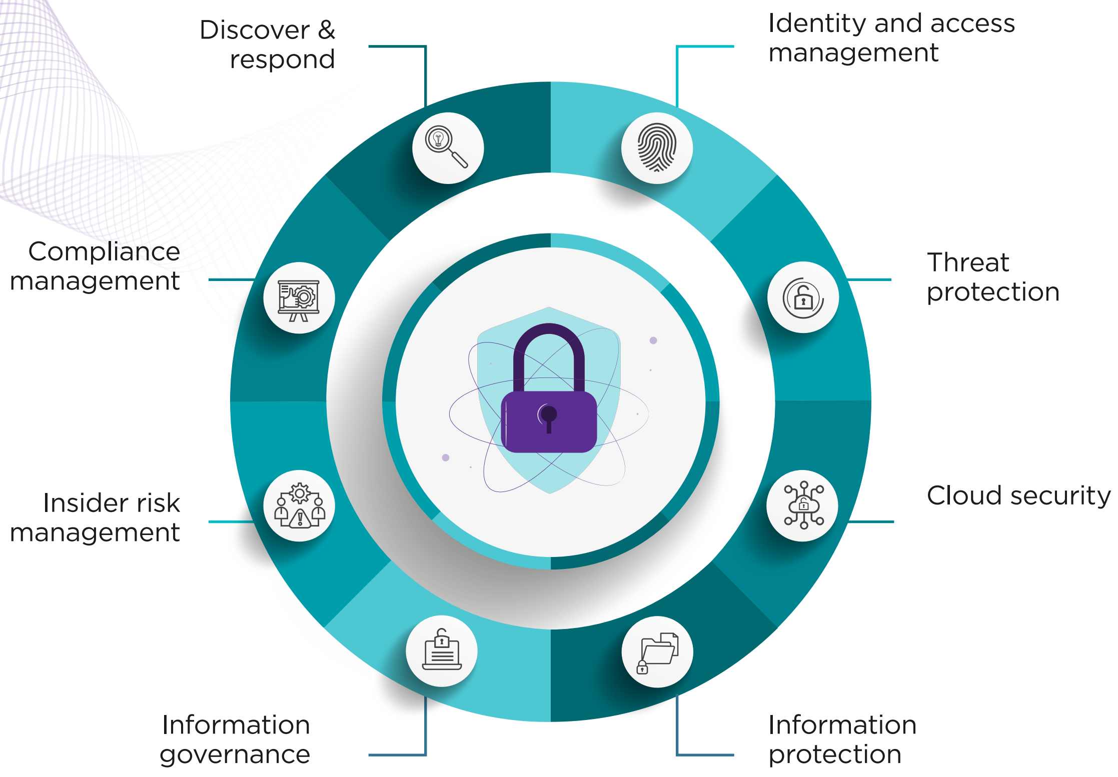
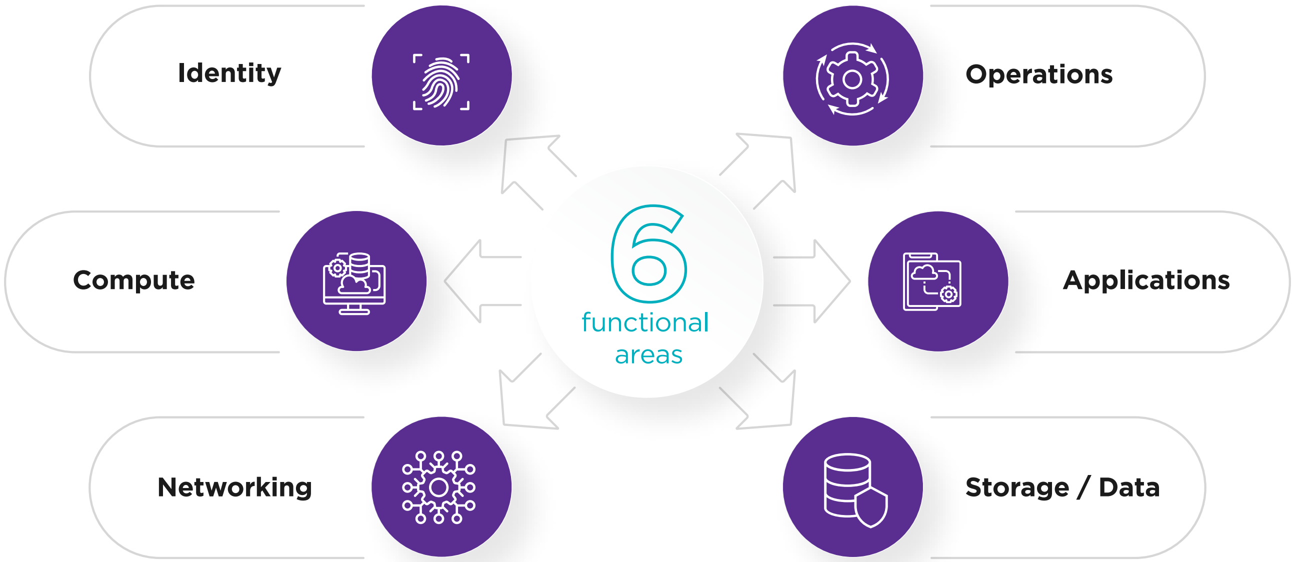


Figure 2 Azure security tools and capabilities

These tools and capabilities make it possible to create Azure security solutions. Microsoft Azure provides confidentiality, integrity, and availability of customer data. From facility to applications, Azure security design can host millions of customers simultaneously, and it provides a trustworthy foundation upon which businesses can meet their security requirements.

Azure platform security capabilities are organized in six functional areas:



Operations

Provide a wide array of configurable security auditing and logging options to help you identify gaps in your security policies and mechanisms.

01 **Azure security center**

Provides integrated security monitoring and policy management across Azure subscriptions.

02 **Azure resource manager**

Provides security, auditing, and tagging features to help you manage your resources after deployment and template-based deployment to improve security solutions.

03 **Application insights**

To monitor live web applications and automatically detect performance anomalies. It monitors application all time it's running, during testing, published or deployed.

04 **Azure monitor**

Provides visualization, query, routing, alerting, auto scale, and automation on data both from the Azure subscription & Azure resources

05 **Azure monitor logs**

To see metrics and logs for an entire environment in one place and able to quickly search through large amounts of security-related entries with a flexible query approach

06 **Azure advisor**

To help improve the performance, security, and reliability of Azure resources and provides security recommendations which can significantly improve security

07 **Microsoft Defender for Cloud**

Brings advanced, intelligent, protection of Azure & hybrid resources and workloads.

08 **Microsoft Sentinel**

A scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Sentinel delivers intelligent security analytics and threat intelligence across the enterprise.

Applications

Understand and evaluate the security advantages of hosting applications and focus from a network-centric to identity-centric with best practices.

01 **Web application vulnerability scanning**

Testing for vulnerabilities on App Service app is to use the integration with Tinfoil security to perform one-click vulnerability scanning on app and view the test results.

02 **Penetration testing**

To enhance the security of applications to make the entire Azure ecosystem more secure and comply with the Microsoft cloud penetration testing rules.

03 **Web application firewall (WAF)**
WAF in Azure application gateway helps protect web applications from common web-based attacks like SQL injection, cross-site scripting attacks, and session hijacking.

04 **Authentication and authorization in Azure App service**
Provides a way for application to sign in users so that they don't have to change code on the app backend.

05 **Layered security architecture**
App service environments provide an isolated runtime environment deployed into an Azure Virtual Network; developers can create a layered security architecture providing differing levels of network access for each application tier.

06 **Web server diagnostics and application diagnostic**
App service web apps provide diagnostic functionality for logging information from both the web server and the web application.

07 **Azure information protection**
A cloud-based solution to discover, classify & protect documents/emails through labels to content.

08 **API management**
To create consistent & modern API gateways for existing back-end services.

09 **Azure confidential computing**
To isolate sensitive data while it’s being processed in the cloud.

10 **API management**
To create consistent & modern API gateways for existing back-end services.

Storage/data

Covers the major areas of encryption, including encryption at rest, encryption in flight, and key management with Azure Key Vault.

01 **Azure role-based access control (Azure RBAC)**
To secure storage account with Azure role-based access control (Azure RBAC) and use of Azure built-in roles, such as Storage Account Contributor, to assign privileges to users.

02 **Shared access signature (SAS)**
Provide delegated access to resources in storage account and grant a client limited permission to objects in storage account for a specified period and with a specified set of permissions.

03 **Encryption in transit**
A mechanism of protecting data when it is transmitted across networks. With Azure data can be secured using – transport-level encryption, wire encryption and client-side encryption.

04 Encryption at rest

It is a mandatory step towards data privacy, compliance, and data sovereignty and it provides storage service encryption, client-side encryption and Azure disk encryption.

05 Storage analytics

Performs logging and provides metrics data for a storage account and this data can be used to trace requests, analyze usage trends, and diagnose issues.

06 Enabling browser-based clients using CORS

A mechanism that allows domains to give each other permission for accessing each other's resources. The user agent sends extra headers to ensure that the JavaScript code loaded from a certain domain can access resources located at another domain.

07 Azure backup

Simple, secure & cost-effective solution to back up data & recover it from Azure cloud.

08 Azure storage service encryption

Automatically encrypts & decrypts the data while storing & retrieving.

09 Azure information protection

A cloud-based solution to discover, classify & protect documents/emails through labels to content.

10 Azure confidential computing

To isolate sensitive data while it's being processed in the cloud.

Networking

Process of protecting resources from unauthorized access or attack by applying controls to network traffic.

01 Network layer controls

it's the act of limiting connectivity to and from specific devices or subnets and represents the core of network security.

02 Network security group (NSG)

To control traffic moving between subnets within an Azure virtual network and traffic between an Azure virtual network and the internet.

03 Route control and forced tunneling

To control routing behavior on Azure virtual networks is a critical network security and access control capability. Forced tunneling is commonly used to force outbound traffic to the internet to go through on-premises security proxies and firewalls.

04 Azure virtual network (VNet)

Allows full control the IP address blocks, DNS settings, security policies, and route tables within this network.

05 Azure private link

Enables to access Azure PaaS services and Azure hosted customer-owned/partner services privately in virtual network over a private endpoint.

06 Express route

A dedicated WAN link to extend on-premises networks into the Microsoft cloud over a dedicated private connection facilitated by a connectivity provider.

07 Application gateway

Provides an Application Delivery Controller (ADC) as a service, offering various layer 7 load balancing capabilities for application.

08 Web application firewall

Provides protection to web applications that use application gateway for standard Application Delivery Control (ADC) functions.

09 Traffic manager

To control the distribution of user traffic for service endpoints in different data centers and a range of traffic-routing methods to suit different application needs, endpoint health monitoring, and automatic failover.

10 Azure load balancer

Delivers high availability and network performance to applications, Load balance incoming Internet traffic to virtual machines and forward external traffic to a specific virtual machine.

11 Azure DDoS protection standard

To defend against DDoS attacks & automatically tuned to help protect Azure resources in a virtual network.

12 Key vault managed HSM

A fully managed & highly available service to safeguard cryptographic keys for cloud apps.

13 Azure service bus

A fully managed enterprise message broker with message queues and publish-subscribe topics.

Compute

Helps identify and remove viruses, spyware, and other malicious software. Also, it generates alerts when known malicious or unwanted software tries to install itself or run-on Azure systems.

01 Antimalware & antivirus

Provide protection capability that helps identify and remove viruses, spyware, and other malicious software.

02 Hardware security module

Simplify the management and security of critical secrets and keys by storing them in Azure Key Vault. Key vault provides the option to store keys in hardware security modules (HSMs) certified to FIPS 140-2 Level 2 standards.

03 Virtual machine backup

Protects application data with zero capital investment and minimal operating costs. With Azure Backup, virtual machines running Windows and Linux are protected.

04 Azure site recovery

Helps orchestrate replication, failover, and recovery of workloads and apps so that they are available from a secondary location if primary location goes down.

05 SQL VM TDE

Transparent data encryption (TDE) and column level encryption (CLE) are SQL server encryption features and requires customers to manage and store the cryptographic keys you use for encryption.

06 VM disk encryption

Helps encrypt Windows and Linux IaaS virtual machine disks. It applies the industry standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks.

07 Virtual networking

A logical construct built on top of the physical Azure network fabric. Each logical Azure virtual network is isolated from all other Azure virtual networks.

08 Security policy management and reporting

To prevent, detect, and respond to threats, and provides increased visibility into, and control over, the security of Azure resources.

Identity and access management

Secure systems, applications, and data begin with identity-based access controls and provide an overview of the core Azure security features that help with identity management.

01 Secure identity

Microsoft uses multiple security practices and technologies across its products and services to manage identity and access – Multi-factor authentication, MS Authenticator, Password policy enforcement, Token-based authentication, Azure role-based access and hybrid identity.

02 Secure apps and data

Helps secure access to data in applications on site and in the cloud and simplifies the management of users and groups. It combines core directory services, advanced identity governance, security, and application access management, and makes it easy for developers to build policy-based identity management into their apps.

03 Azure AD identity protection

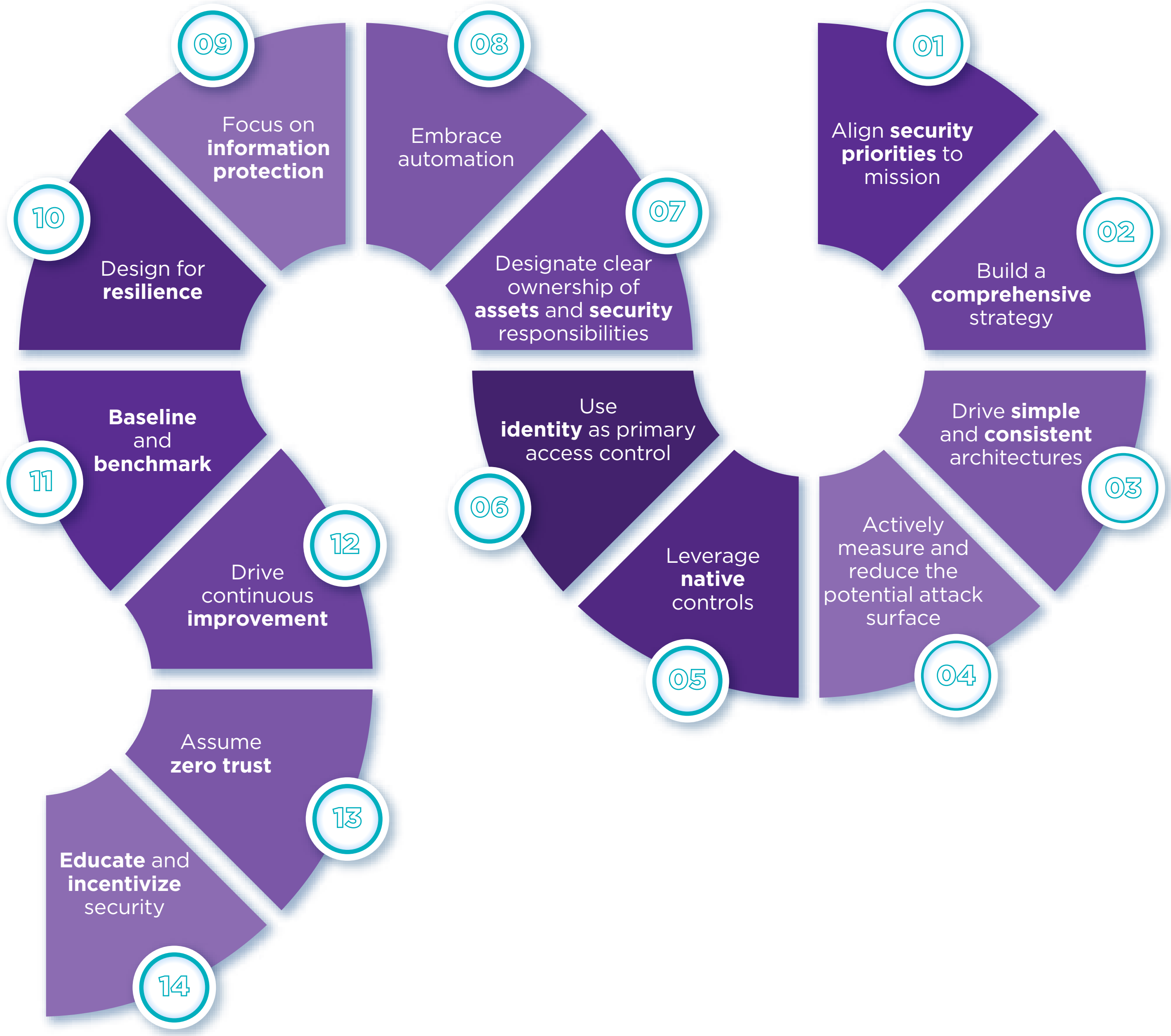
To automate the detection & remediation of identity-based risks which can be further analyzed.

04 Azure AD external identities

To allow external users to access apps & resources by leveraging Azure AD B2B collaboration while Azure AD B2C supports millions of users & billions of authentications per day and automatically handling threats.

App security principles and design considerations

Microsoft provides technical guidance for protecting applications and data from threats available under Microsoft Well- architected framework. The following security principles describe a securely architected system hosted on cloud or on-premises data centers (or a combination of both) and maintain assurance of confidentially, integrity, and availability.



01
Align security priorities to mission
02
Build a comprehensive strategy
03
Drive simple and consistent architectures
04
Actively measure and reduce the potential attack surface
05
Leverage native controls
06
Use identity as primary access control
07
Designate clear ownership of assets and security responsibilities
08
Embrace automation
09
Focus on information protection
10
Design for resilience
11
Baseline and benchmark
12
Drive continuous improvement
13
Assume zero trust
14
Educate and incentivize security

Figure 3 Security design principles for systems hosted on cloud or on-premises

Application of these principles will dramatically increase the likelihood of security architecture and maintain assurances of confidentiality, integrity, and availability. A more detailed description is provided below:

01 Align **security priorities** to prioritize efforts and assurances by aligning security strategy and technical controls to the business using classifications of data and systems

02 Build a **comprehensive strategy** to consider investments in culture, processes, and security controls across all system components

03 **Drive simplicity** by aligning with simple and consistent architecture and implementations

04 **Design for attackers** to actively measure and reduce the potential attack surface that is a target for exploitation of resources within the environment

05 **Leverage native controls** built into cloud service over external controls from 3rd party

06 Use an **identity-based** authentication and authorization for access controls

07 Designate clear ownership of assets and security responsibilities to ensure **accountability**

08 **Embrace automation** of tasks decreases the chance of human error that can create risk

09 **Focus on information protection** to classify information and assets to enable security prioritization, using strong access control and encryption technology, and meeting business needs

10 **Design for resilience** requires several approaches to be work together such as balanced investment, ongoing investment, defense in depth, and least privilege, etc.

11 **Baseline and benchmark** to evaluate strategy and configuration against external references

12 Drive **continuous improvement** to improve the continuous digital transformation of the enterprise

13 Access requests must be **granted conditionally** based on the requestor's trust level and the target resource's sensitivity

14 **Educate** and **incentivize security** to support the security assurance goals of the system

Security design considerations

Microsoft has provided a list of key security design considerations, as summarized below.

Governance, risk, and compliance-related considerations

Enforce creation and deletion of services and their configuration through Azure policies.

Ensure consistency across the enterprise by applying policies, permissions, and tags across all subscriptions through careful implementation of the root management group.

Periodically perform external and or internal workload security audits and have compliance checks as part of the workload operations.

Zero-trust landing zone in Azure for isolation by creating segments and isolating assets at several layers from Azure.

Utilize the Azure Blueprint service to rapidly and consistently deploy application environments that are compliant with your organization's policies and external regulations.

Administrative account security is the practice of monitoring, maintaining, and operating IT systems to meet service levels that the business requires.

Require all critical impact admins to use passwordless authentication or multifactor authentication (MFA).

Regularly simulate attacks against administrative users with current attack techniques to educate and empower them.

Identity and access management considerations

01 Use **identity management services** to authenticate and grant permission to users, partners, customers, applications, services, and other entities.

02 Support a **single enterprise directory** and keep the cloud and on-premises directories synchronized, except for critical-impact accounts.

03 Consider the **built-in roles in Azure** before creating custom roles to grant the appropriate permissions to VMs and other objects.

04 **Policy management across some or all resources** to monitor and enforce compliance with external (or internal) regulations, standards, and security policy, assign appropriate permission to those roles.

05 **Grant permissions to the central IT department** to create, modify and delete resources like virtual machines and storage.

06 **Central networking group across network resources** to ensure consistency and avoid technical conflicts.

07 Enable **MFA** for all users and login methods with Azure AD security defaults.

Data protection

01 Usage of **Azure encryption models**, including server-side encryption that uses service-managed keys, customer-managed keys in **Key Vault**.

02 Usage of **client-side encryption**, which can be able to manage and store keys on-premises or in another secure location.

03 Azure **disk protection** to protect Windows and Linux virtual machines.

04 **Azure Storage Service Encryption** (SSE) to automatically encrypt data before it is stored, and automatically decrypt the data when you retrieve it.

05 Usage of **Transport Layer Security** (TLS) protocol to protect data when it’s traveling between the cloud services and customers.

06 **Encryption of data** in transit to, from, and between VMs that are running Windows.

07 **Key Vault** for managing and controlling access to encryption keys used by cloud services.

Application and services

Identify and classify key organizational applications according to organizational impact.

Securing that **application code** requires identifying and mitigating risks from the design and implementation of the application.

Use **native security** capabilities built into cloud services instead of adding external security components, such as data encryption, network traffic filtering, threat detection, and other functions.

Do a **comprehensive analysis** to identify threats, attacks, vulnerabilities, and countermeasures.

Evaluate the security advantages of platform as a service (PaaS) versus other cloud service models.

Change your security focus from a network-centric to an **identity-centric** perimeter security approach.

Adopt a secure DevOps approach

DevOps has replaced siloed development and operations to create multidisciplinary teams that work together with shared and efficient practices, tools, and KPIs. To deliver highly secure apps and services in this fast-moving environment, it is critical for security to move at the same speed. One way to achieve this is to build **security in development (SDL) and operations (OSA) processes.**

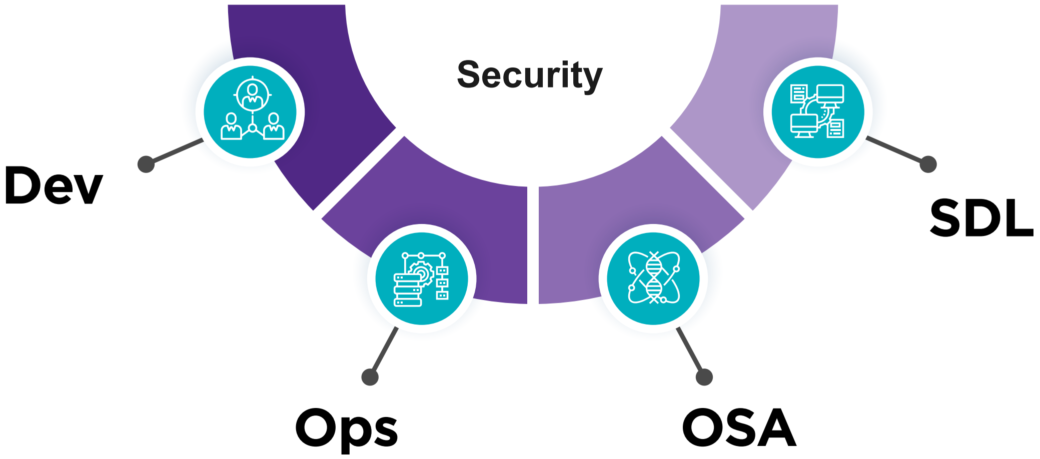


Figure 4 DevSecOps in Azure

DevSecOps combines GitHub and Azure products and services to help **DevOps** and **SecOps** teams collaborate in building more secure apps. Here are the DevSecOps practices to make application development more secure across people, processes, technology to ensure enterprise and teams are productive and efficient.

People

- Education
- Security first mindset
- Assumed breach
- Protect credentials

Process

- Secure development lifecycle
- Threat modeling
- Security assessment
- Red-Blue team exercises (pen test)
- Code reviews
- Limited production access
- Immutable infrastructure
- Progressive exposure / canary deployments

Technology

- Release automation
- Infrastructure / config as code
- Static app security testing (SAST)
- Dynamic app security testing (DAST)
- Credential scanning secrets management
- Known vulnerabilities
- License risks

Figure 5 Azure DevSecOps practices

Security service map to create secured solutions/apps

Security service map in Azure helps meet the security needs of businesses and protect users, devices, resources, data, and applications in the cloud.

Azure Security Benchmark program is a collection of high-impact security recommendations that can help secure the services in Azure. The security services map organizes services by the resources and group services into the following categories –

Secure and protection

This collection of security services and capabilities provide a way to understand and improve security posture across Azure environment

Detect threats

Services to identify suspicious activities and facilitate mitigation the threat

Investigate and respond

Services to pull logging data to access a suspicious activity and respond

Here are the potential services which are typically followed by any service provider to build the secured applications for an enterprise.

01 Performing an initial assessment to determine security and risk tolerance.

02 Building a comprehensive, holistic security strategy and architecture.

03 Collaborating to identify a set of security processes that can work public cloud/hybrid cloud, satisfy industry and regulatory needs, and map to key business practices.

04 To identify the right set of apps to deploy in the public cloud (like Azure) by assessing security and risk tolerance and establishing identity and access management to streamline and control access to cloud services.

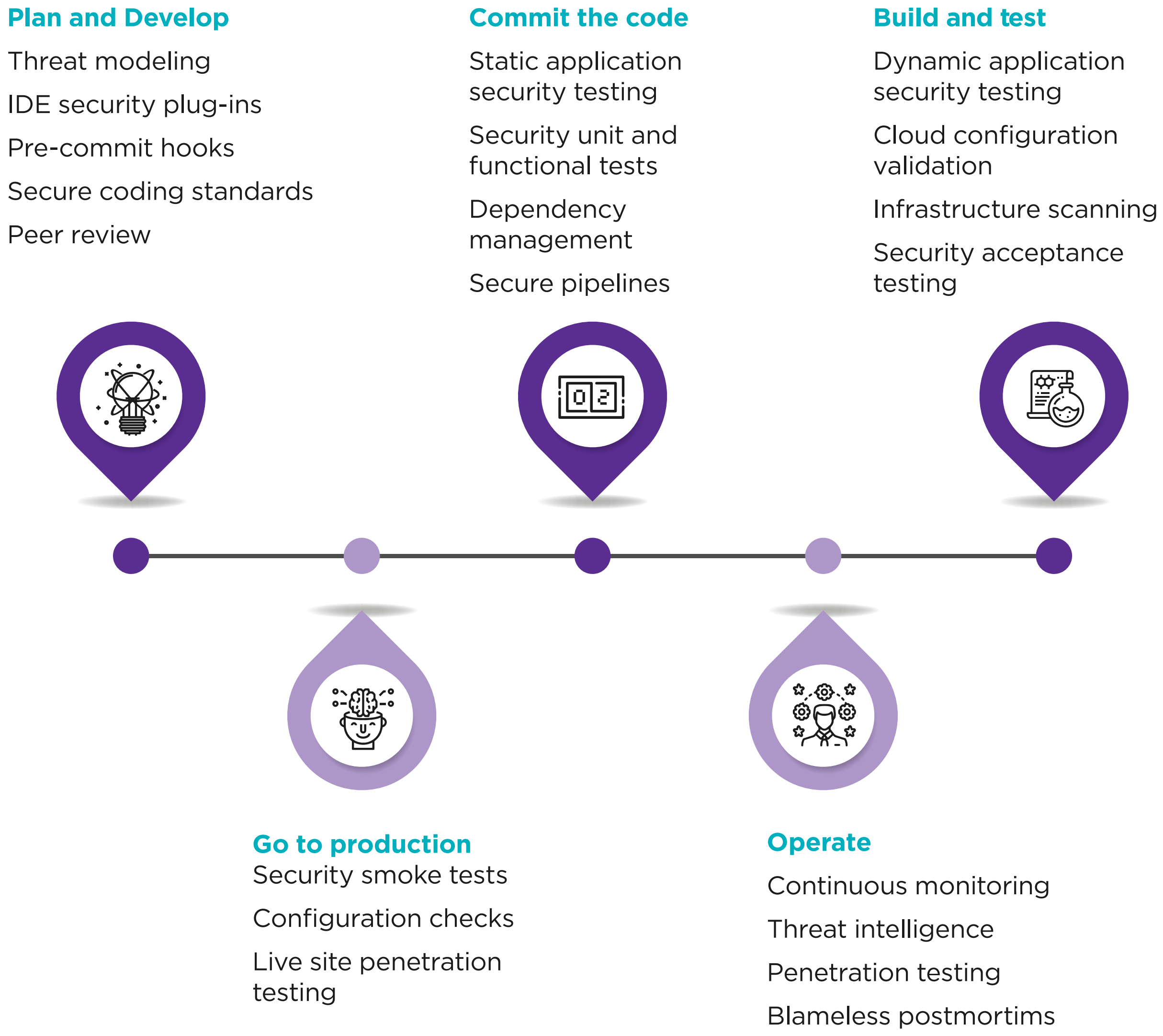
05 Specify recommendations for ease of orchestration across platforms.

06 Training to required teams/end users in the nuances of security and compliance in Azure cloud.

07 Deliver managed service model to managed operations and support services while maintaining the security practices.

Assess security workload

Microsoft provides technical guidance for securing applications available under MS Azure Well-Architected Framework and shown below as part of the **Microsoft Security Development Lifecycle (SDL).**



Plan and Develop

Threat modeling

IDE security plug-ins

Pre-commit hooks

Secure coding standards

Peer review

Commit the code

Static application security testing

Security unit and functional tests

Dependency management

Secure pipelines

Build and test

Dynamic application security testing

Cloud configuration validation

Infrastructure scanning

Security acceptance testing

Go to production

Security smoke tests

Configuration checks

Live site penetration testing

Operate

Continuous monitoring

Threat intelligence

Penetration testing

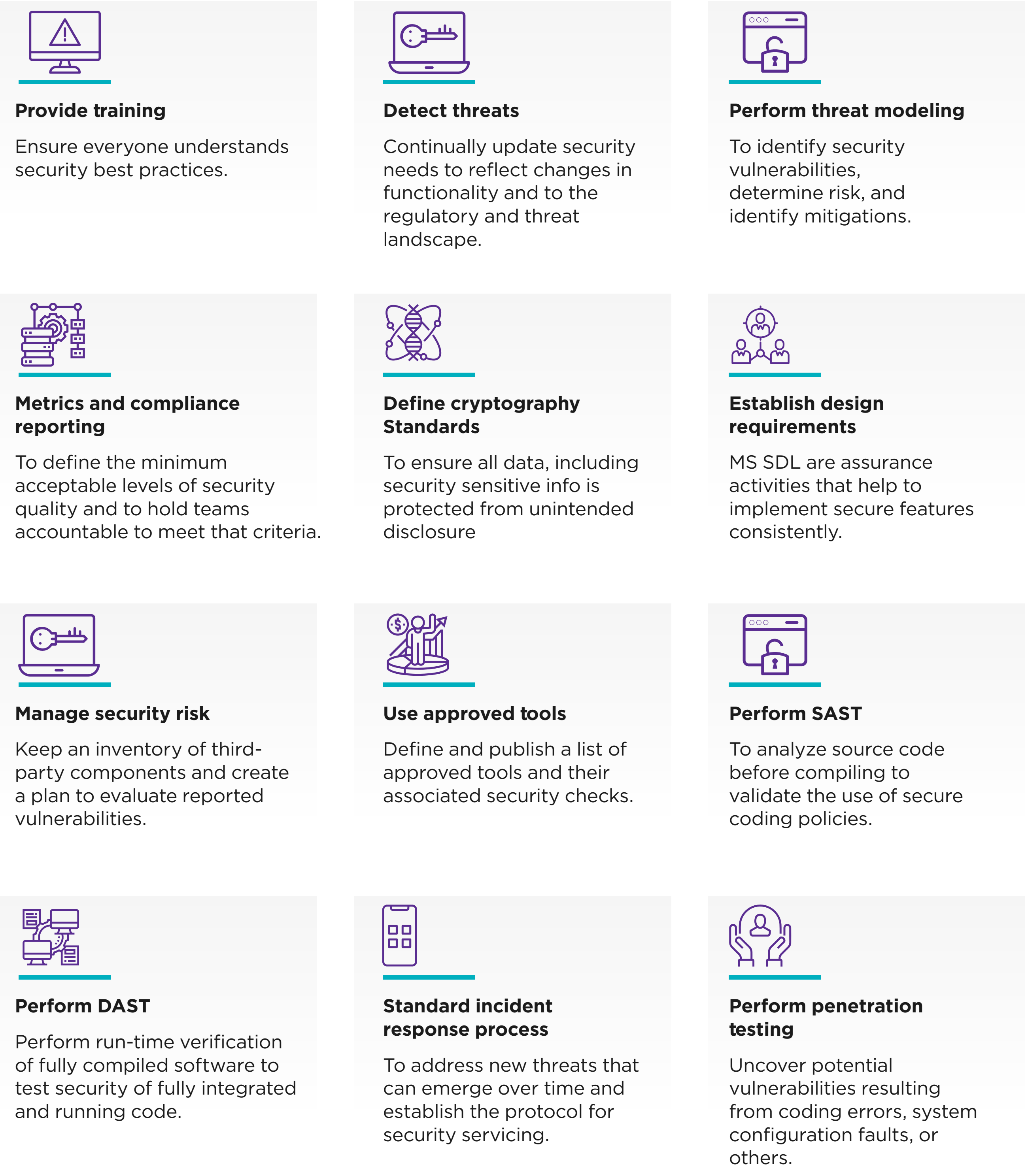
Blameless postmortims

Figure 6 MS Security Development Lifecycle (SDL)

The Security Development Lifecycle comprises a set of practices that support security assurance and compliance requirements. It helps developers build more secure apps by reducing the number and severity of vulnerabilities.

MS Operational Security Assurance (OSA)

Microsoft Operational Security Assurance (OSA) provides a set of practices that improve operational security in cloud-based services. It is a framework that provides security engineering practices that enterprises should adopt. Here is the high-level view of these practices to follow –



Provide training

Ensure everyone understands security best practices.

Detect threats

Continually update security needs to reflect changes in functionality and to the regulatory and threat landscape.

Perform threat modeling

To identify security vulnerabilities, determine risk, and identify mitigations.

Metrics and compliance reporting

To define the minimum acceptable levels of security quality and to hold teams accountable to meet that criteria.

Define cryptography Standards

To ensure all data, including security sensitive info is protected from unintended disclosure

Establish design requirements

MS SDL are assurance activities that help to implement secure features consistently.

Manage security risk

Keep an inventory of third-party components and create a plan to evaluate reported vulnerabilities.

Use approved tools

Define and publish a list of approved tools and their associated security checks.

Perform SAST

To analyze source code before compiling to validate the use of secure coding policies.

Perform DAST

Perform run-time verification of fully compiled software to test security of fully integrated and running code.

Standard incident response process

To address new threats that can emerge over time and establish the protocol for security servicing.

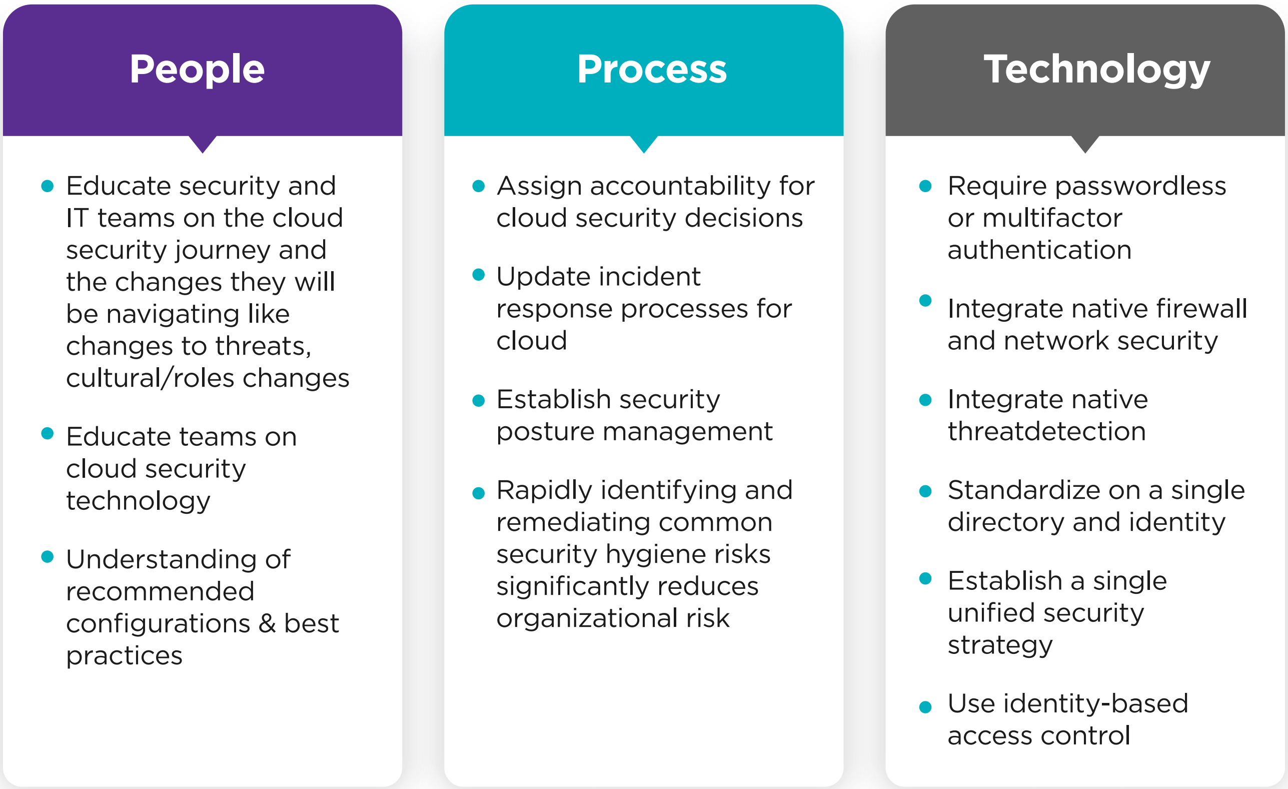
Perform penetration testing

Uncover potential vulnerabilities resulting from coding errors, system configuration faults, or others.

Figure 7 MS OSA practices

Security best practices

Here are the top Azure security best practices across people, processes, and technology that Microsoft recommends based on lessons learned across customers -



People

- Educate security and IT teams on the cloud security journey and the changes they will be navigating like changes to threats, cultural/roles changes
- Educate teams on cloud security technology
- Understanding of recommended configurations & best practices

Process

- Assign accountability for cloud security decisions
- Update incident response processes for cloud
- Establish security posture management
- Rapidly identifying and remediating common security hygiene risks significantly reduces organizational risk

Technology

- Require passwordless or multifactor authentication
- Integrate native firewall and network security
- Integrate native threatdetection
- Standardize on a single directory and identity
- Establish a single unified security strategy
- Use identity-based access control

Figure 8 Azure security best practices

Conclusion

Security, in general, has been a concern for businesses entering into cloud platform(s). Enterprises have been concerned with public cloud providers (Azure/AWS/G-Cloud) and the cloud, in general, to ensure that their applications/data are secured.

Organizations are struggling to address security challenges around identity and access control, monitoring and responding to threats, data leakage, governance, security skills shortages, and shadow IT adoption. But MS Azure, through a combination of its security capabilities and services across the six areas highlighted in this paper, has tried to address all the typical security concerns and challenges.

HCL, as a partner for Microsoft with deep competency on Azure and core security capabilities, can help enterprise customers overcome all these security concerns by guiding them on Azure security capabilities, configuring and enabling secure solutions, and hand-holding enterprise customers across their solution journey.

References

1. https://docs.microsoft.com/en-us/azure/architecture/framework/

2. https://azure.microsoft.com/en-us/solutions/devsecops/#overview

3. https://csahkm.files.wordpress.com/2021/01/csa-devops-security-best-practices-with-microsoft-azure-20210128.pdf

4. https://www.microsoft.com/en-us/securityengineering/sdl/practices#practice12

5. https://docs.microsoft.com/en-us/security/benchmark/azure/

HCL Technologies (HCL) empowers global enterprises with technology for the next decade today. HCL's Mode 1-2-3 strategy, through its deep-domain industry expertise, customer-centricity and entrepreneurial culture of ideapreneurship™ enables businesses to transform into next-gen enterprises.

HCL offers its services and products through three lines of business - IT and Business Services (ITBS), Engineering and R&D Services (ERS), and Products & Platforms (P&P). ITBS enables global enterprises to transform their businesses through offerings in areas of Applications, Infrastructure, Digital Process Operations, and next generation digital transformation solutions. ERS offers engineering services and solutions in all aspects of product development and platform engineering while under P&P. HCL provides modernized software products to global clients for their technology and industry specific requirements. Through its cutting-edge co-innovation labs, global delivery capabilities, and broad global network, HCL delivers holistic services in various industry verticals, categorized under Financial Services, Manufacturing, Technology & Services, Telecom & Media, Retail & CPG, Life Sciences, and Healthcare and Public Services.

As a leading global technology company, HCL takes pride in its diversity, social responsibility, sustainability, and education initiatives. As of 12 months ending on December 31, 2021, HCL has a consolidated revenue of US $ 11.18 billion and its 197,777 ideapreneurs operate out of 52 countries. For more information, visit www.hcltech.com

www.hcltech.com