

Learnings and  
best practices to

# Overcome Cloud Security Challenges













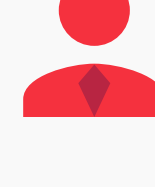
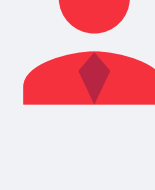

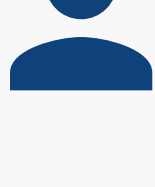








## Cloud Security:

# It takes two to tango

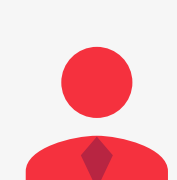
Cloud is evolving at a fast pace and so are the considerations for security, data protection, and regulatory compliance. The effort involved in securing applications and infrastructure demands a shared responsibility model, where the responsibilities for various aspects of cloud deployment are shared by the customer and the cloud service provider (CSP). The shared model relieves customers of tasks such as management of physical networks, servers, virtual networks, and middleware.

With cloud becoming integral to business transformation, every attempt to innovate presents a security risk. Therefore, a harmonized partnership between the customer and the CSP is very important to take such challenges head on.

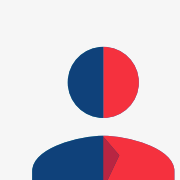
Responsibility	SaaS	PaaS	IaaS	On-prem
Data governance and rights management				
Client endpoints				
Account and access management				
Identity and directory infrastructure				
Application				
Network controls				
Operating system				
Physical hosts				
Physical network				
Physical datacenter				



Managed by you



Managed by vendor



Managed by both

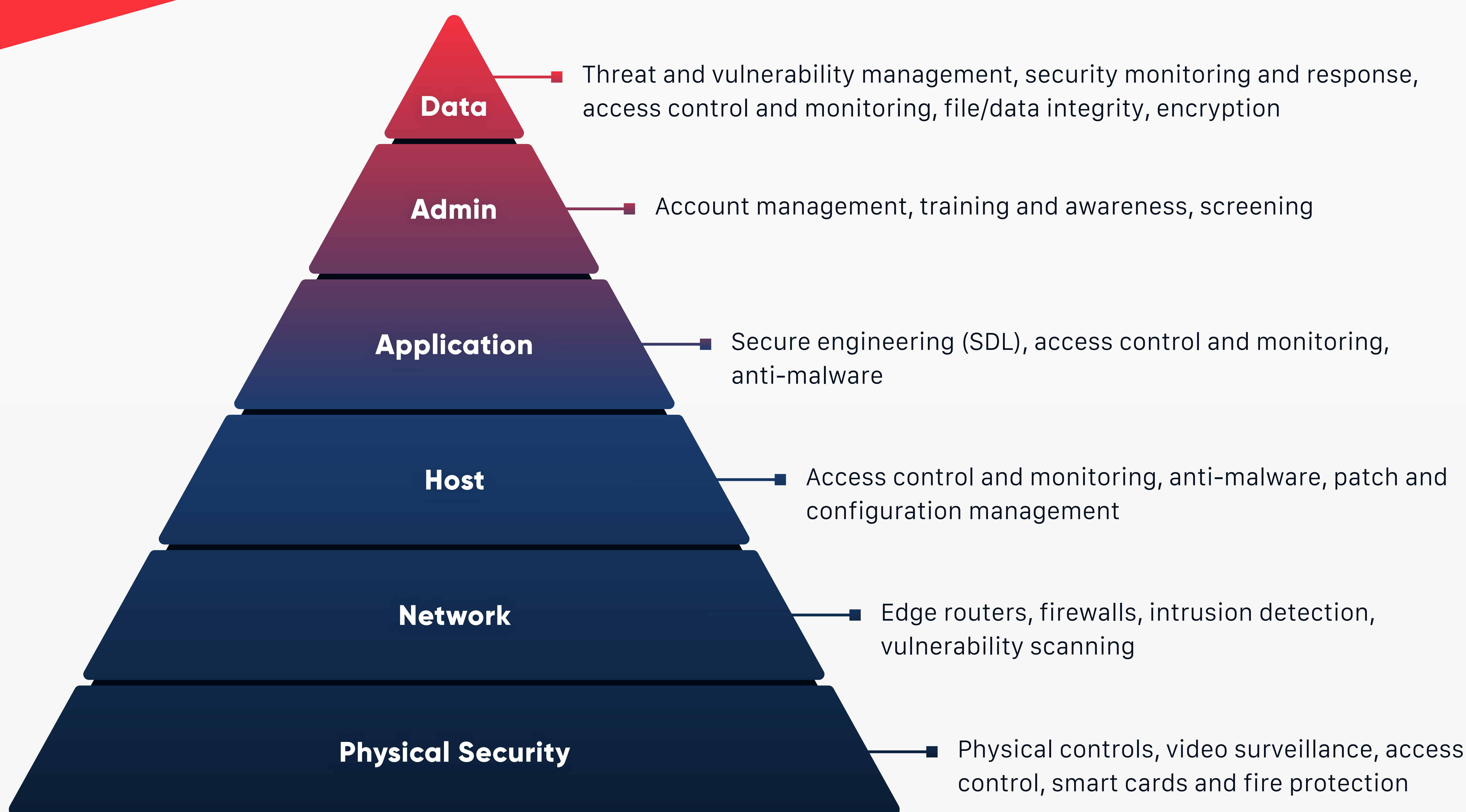
# Defense in depth

A defense-in-depth strategy ensures the presence of security controls across layers of services. In the event of a failure, compensating controls maintain security at all times. This includes strategies to identify and mitigate security threats before they happen. This involves continuous improvements to service-level security features.

*External factors and security-specific threats are converging to influence the overall security and risk landscape, so leaders in the space must properly prepare to improve resilience and support business objectives.*

- Gartner

## Continuous improvements to service level security





# Application and data security

The major challenges in application and data security include safeguarding data from theft/ unauthorized access, ensuring uninterrupted access to data when unforeseen errors/failures occur, and avoiding exposure of data that was deleted. Some of the steps that can be taken to overcome these challenges are:

- **Least privilege - deny by default:** By limiting access privileges to the IT environment, security breaches can be contained at the affected level.
- **Protecting data at rest and in motion:** Server-side encryption of data ensures security in situations where storage media is compromised. Token-based authentication is used to authorize user access. For data in motion, Transport Layer Security (TLS) is used to encrypt data.
- **Cloud access security brokers (CASBs):** Implement API-based CASB solutions to secure data and monitor network traffic to ensure conformance with security and policy guidelines.
- **Tagging:** Data is classified based on its value and significance. This is done by assigning tags/labels (low to high) to data based on risk. Tags/labels are a feature offered by most CSPs for tagging resources.
- **Find, secure, and manage secrets:**
  - Keep secrets outside of code and configuration
  - Ensure secrets are encrypted
  - Centralize secrets with a cloud-based Key Management Service (KMS)
  - Integrate a centralized log management system to aggregate, store, and analyze data
  - Secure container secrets
    - Avoid using secrets for the container image
    - Use volume mounts to pass secrets to containers at runtime
    - Plan rotation of secrets and ensure they are encrypted
- **Be aware of cloud zombies:** Review your CSP's data policy as well as the technology used to securely dispose of data.



# Cloud Identity and Access Management (IAM)

A cloud IAM solution facilitates security while connecting and managing multiple identities across different applications. It comprises:

- Identity federation and SSO
- Adaptive authentication
- Account management and identity provisioning
- API and microservices security
- Privacy regulation
- Access control

## Network security

Network security should be done using a layered approach to ensure multiple levels of protection.

- Centralize management of core network functions such as VPCs and subnets
- Zero trust approach - ensure validation of trust based on device, network location, and identity
- Network segmentation and segregation to restrict access to sensitive data
- Deploy perimeter zones to add additional layers of security for distributed denial of service (DDoS) prevention and intrusion detection
- Customize routing configurations based on deployment scenario
- While configuring Egress Filtering, start with a 'default deny policy' where all types of outbound traffic is blocked unless a policy states otherwise
- Utilize add-on services that can be used to assess network security, check code quality, and conduct runtime security analysis

# Audit checklist

Area	Details
Governance	Review organizational strategy and risk appetite, roles and responsibilities, insurance, and governance tasks.
Data management	Perform a data flow and privacy assessment by reviewing the data life cycle.
Data environment	Where are the data centers located? Can the CSP commit to specific privacy requirements?
Cyber threat	What are patch and vulnerability management program practices? How does the CSP ensure these program practices do not create a security risk for client infrastructure?
Infrastructure	Is there restricted and monitored access to assets all the time?
Logs and audit trails	How long are logs and audit trails kept?
Availability	What service level guarantee does the CSP offer for Disaster Recovery/Business Continuity?
Identity and access management	Provide information regarding authentication, restriction of access, or implementation of segregation of duties (SOD) for cloud provider staff.
Encryption	Ensure connection points 'to and from' data with encryption for data in transit, data at rest, and type of encryption.
Privacy	How are digital identities and credentials protected?
Regulatory compliance	Can the provider demonstrate compliance with regulatory requirements?
Legal	Is there an engagement agreement?



# Cloud security services at QBurst

## Cloud security assessment

By limiting access privileges to the IT environment, security breaches can be contained at the affected level.

## Cloud security monitoring

Mitigate risks and indicators of compromise, initiate remediation, advanced analytics to baseline normal behavior, detect anomalies and remove false positives.

## Cloud incident response

Proactive incident management to detect, respond, and prevent future incidents; bot-centric reporting to better analyze and understand bot traffic.

## Cloud security management

Implement firewalls, identity and access management processes including SSO capabilities, multi-factor authentication.

## Cloud endpoint security

Increase visibility to protect endpoints, find threats and vulnerabilities, stop malware before it reaches networks or endpoints.

## Disaster Recovery

Custom DRM solution for data backup and restoration with business continuity in mind.

## Why QBurst?

Experience in AWS, Azure, and Google Cloud Platform

Certified cloud security professionals

Multi-cloud security and tools expertise

Strong capabilities in pragmatic risk and compliance management

Experience in migrating applications from various hosting solutions to public clouds

Experience in developing and managing microservices-based applications

Experience in delivering DevOps services



# About us

QBurst is a full-service software development and consulting partner for some of the world's most innovative companies. We bring to the table deep experience in DevOps, cloud services, microservices-based application development, cloud security, AI and machine learning, blockchain development, and big data analytics.



USA | UK | UAE | India | Singapore | Japan | Australia

[www.qburst.com](http://www.qburst.com) | [info@qburst.com](mailto:info@qburst.com)