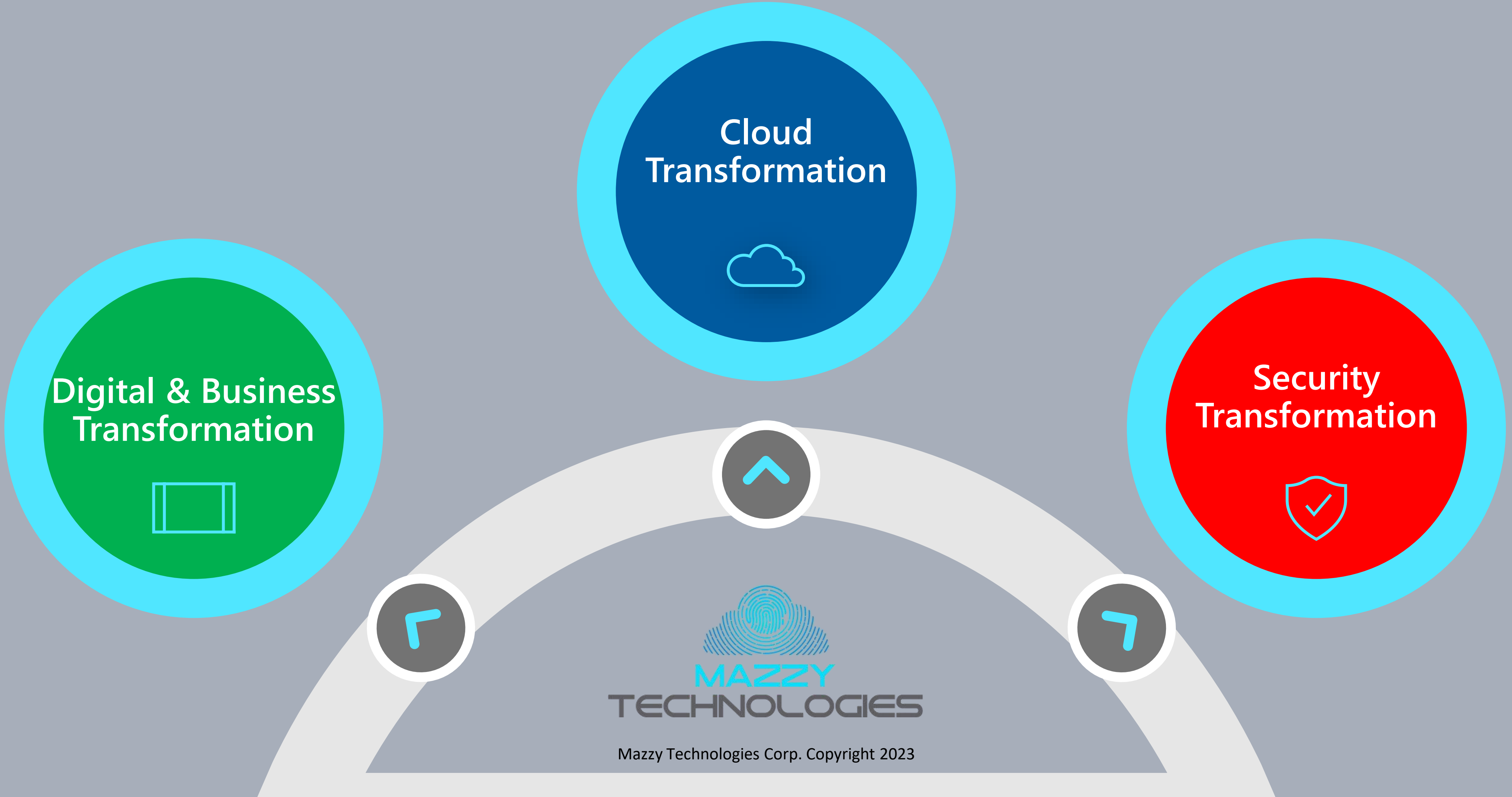
MAZZY TECHNOLOGIES

Azure Penetration Testing

Know your vulnerabilities…

Transformation

As the world goes through amazing transformation so are enterprises and governments.



MAZZY TECHNOLOGIES

Transformation requires Security Transformation

In modern-day enterprises & governments, there has been a growing transition to cloud-based environments and IaaS, PaaS, or SaaS computing models. The dynamic nature of infrastructure management, especially in scaling applications and services, can bring several challenges to organizations when adequately resourcing their departments. These as-a-service models give organizations the ability to offload many of the time-consuming, IT-related tasks.

As companies continue to migrate to the cloud, understanding the security requirements for keeping data safe has become critical. While third-party cloud computing providers may take on the management of this infrastructure, the responsibility of data asset security and accountability doesn't necessarily shift along with it.

By default, most cloud providers follow best security practices and take active steps to protect the integrity of their servers. However, organizations need to make their own considerations when protecting data, applications, and workloads running on the cloud.

Security threats have become more advanced as the digital landscape continues to evolve.

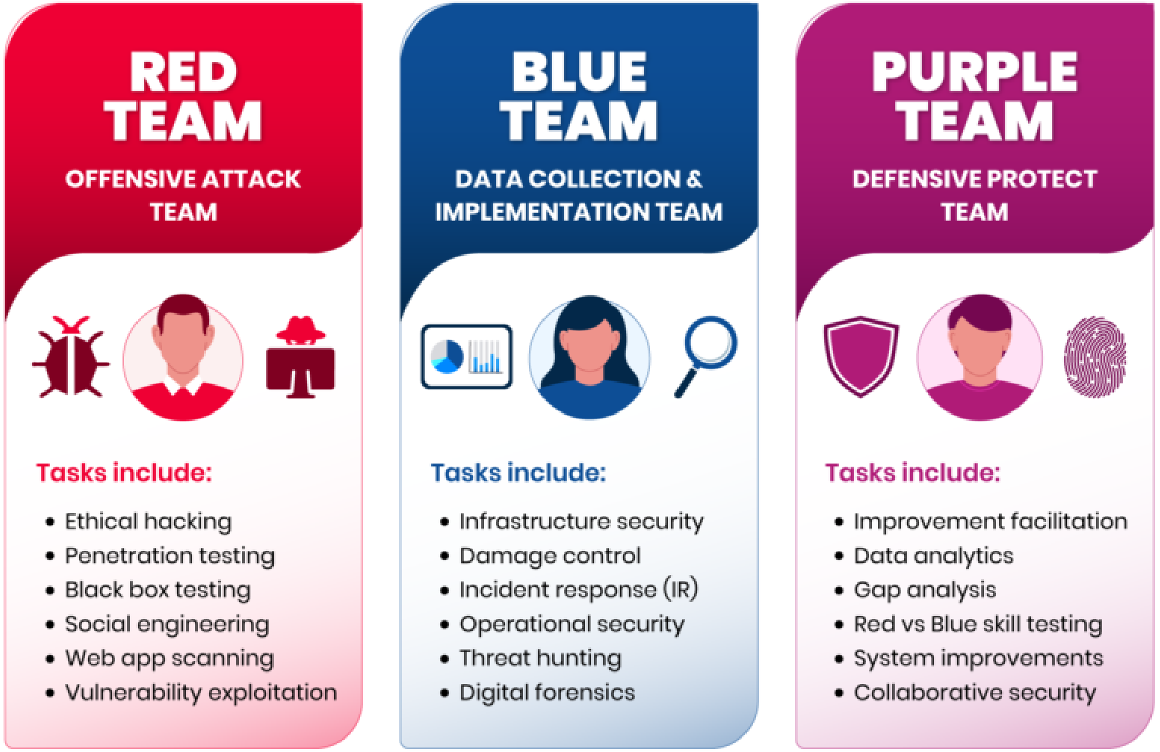
Whether it is for compliance/regulations purposes or just piece of mind, know the risks with MT’s Vulnerability Assessment and Azure Penetration Testing combination.

*Note this specific solution just includes Azure Penetration Testing, contact MT for details on other services

MAZZY TECHNOLOGIES

A Multiteam Protection is Necessary

Mazzy Technologies Red teams will utilize Pen Testing to attempt to defeat corporate cybersecurity controls – as would a malicious hacker – to find cybersecurity weaknesses and implement fixes before real hackers can exploit them.



RED TEAM

OFFENSIVE ATTACK TEAM

Tasks include:

- Ethical hacking
- Penetration testing
- Black box testing
- Social engineering
- Web app scanning
- Vulnerability exploitation

BLUE TEAM

DATA COLLECTION & IMPLEMENTATION TEAM

Tasks include:

- Infrastructure security
- Damage control
- Incident response (IR)
- Operational security
- Threat hunting
- Digital forensics

PURPLE TEAM

DEFENSIVE PROTECT TEAM

Tasks include:

- Improvement facilitation
- Data analytics
- Gap analysis
- Red vs Blue skill testing
- System improvements
- Collaborative security

*Please contact MT for additional services if needed across teams

Out of Scope Areas (Prohibited by Microsoft)

- Scanning or conducting tests on other Azure customer assets
- Accessing data that is not completely self-owned
- Conducting any DDoS attacks
- Conducting any intensive network fuzzing against Azure virtual machines
- Any tests that generate a huge amount of traffic through automated testing methods
- Attempt phishing or any social engineering attacks on Microsoft’s employees
- Utilizing any services that violate the acceptable usage policies as mentioned in the online usage terms

In Scope as per Microsoft

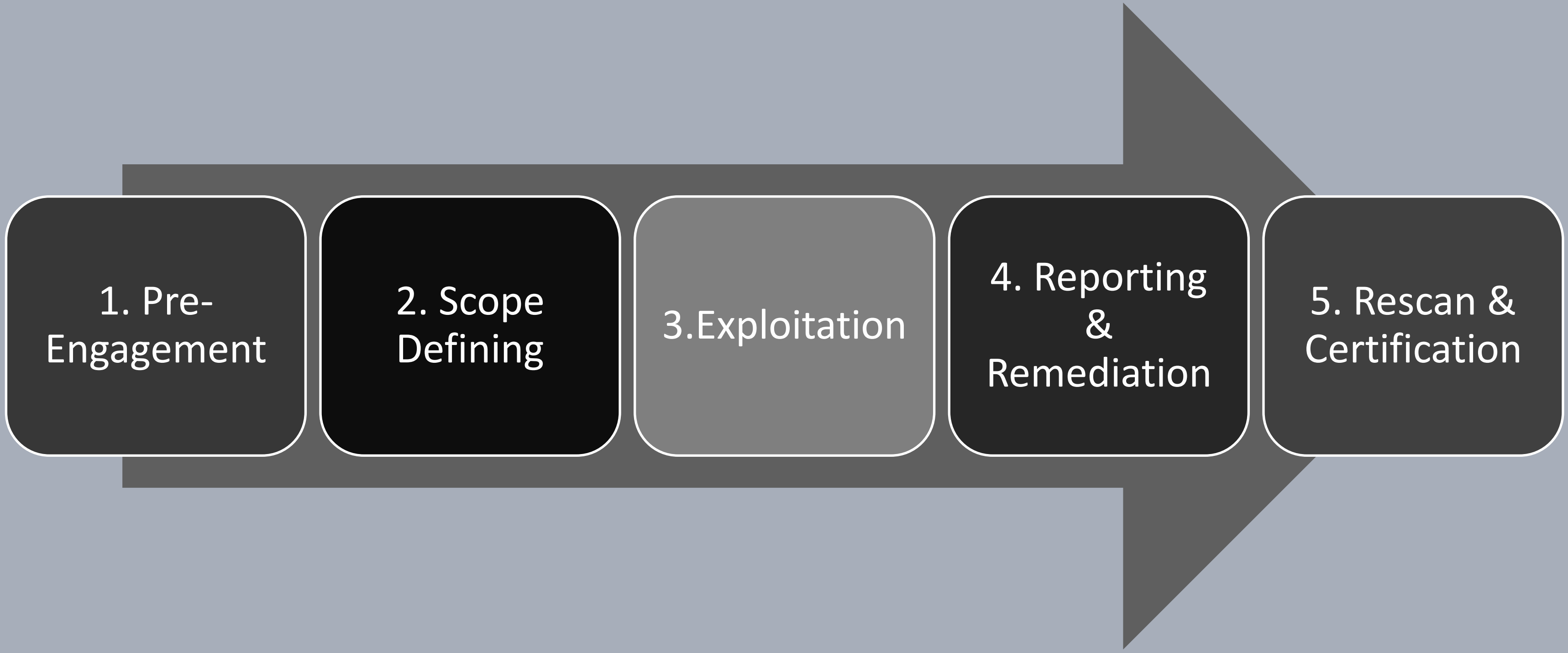
- Create multiple test or trial accounts to test cross-account access vulnerabilities.
- Running vulnerability scanning tools, performing port scans, or fuzzing on your virtual machine.
- Testing your account by generating traffic that is expected to match regular working periods and can also include surge capacity.
- Try to break out of Azure services to access other customer assets. If any such vulnerability is found, you should inform Microsoft and cease any further tests.

Penetration Testing Frameworks & Methodologies

Mazzy Technologies aligns the framework based on your business

- (ISSAF) Information System Security Assessment Framework
- (NIST) The National Institute of Standards and Technology
- (PTES) Penetration Testing Methodologies and Standards
- (OSSTMM) Open-Source Security Testing Methodology Manual
- (OWASP) Open Web Application Security Project

External Penetration Testing Methodology



1. Pre-Engagement

2. Scope Defining

3.Exploitation

4. Reporting & Remediation

5. Rescan & Certification

Defining security objectives & outcomes

Recognizing assets that would undergo the test

Simulating attacks on the system

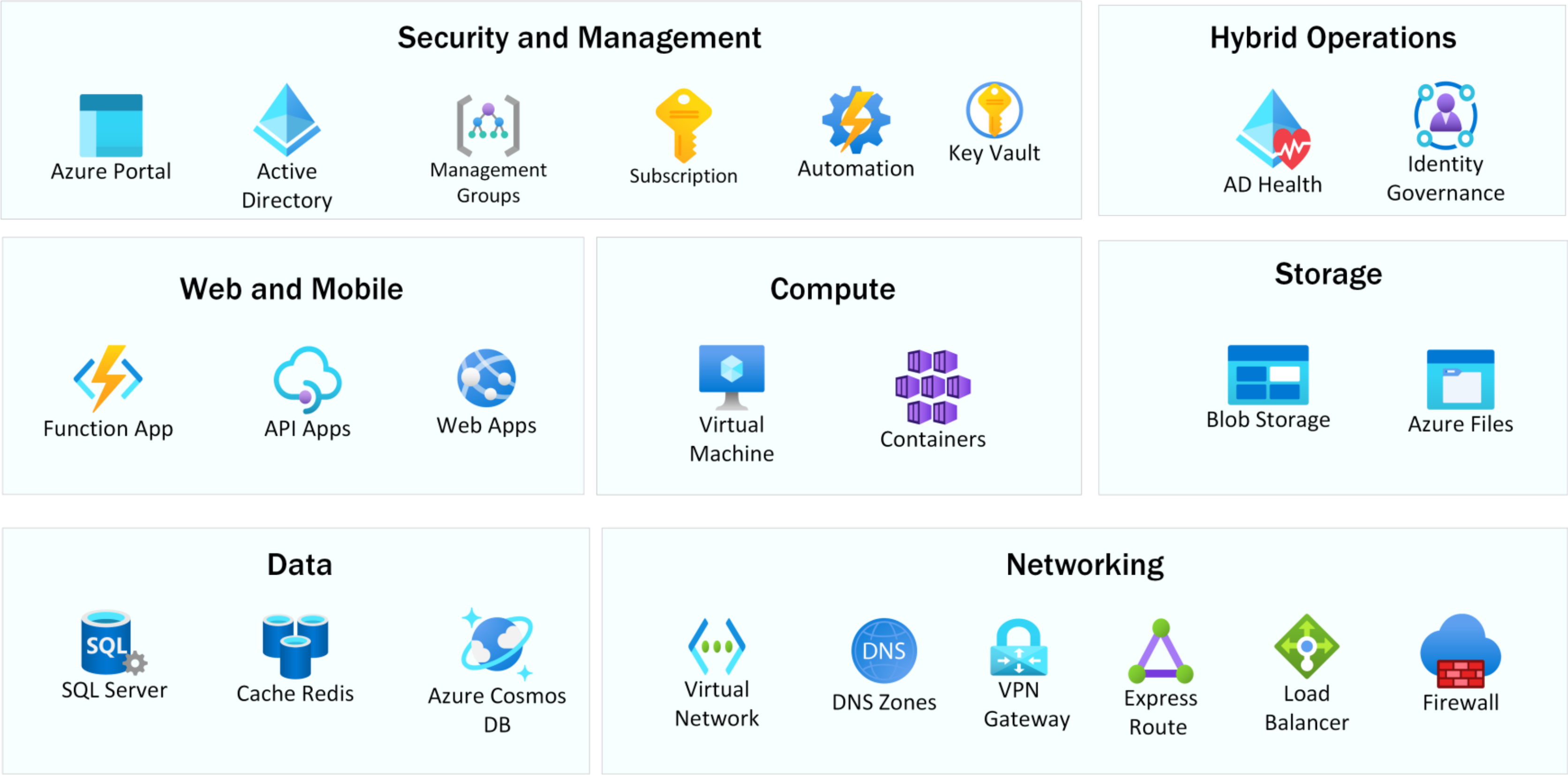
Document the findings and working on fixing

Testing the fixes and issuing pen-test certificate

Most common Azure Services that will be Attacked

- App Services
- Storage Accounts
- Automation Accounts
- Key Vaults
- Azure SQL
- Virtual Machines
- Azure Contain Registry / Azure Container Instances

Services within Scope



Security and Management

- Azure Portal
- Active Directory
- Management Groups
- Subscription
- Automation
- Key Vault

Hybrid Operations

- AD Health
- Identity Governance

Web and Mobile

- Function App
- API Apps
- Web Apps

Compute

- Virtual Machine
- Containers

Storage

- Blob Storage
- Azure Files

Data

- SQL Server
- Cache Redis
- Azure Cosmos DB

Networking

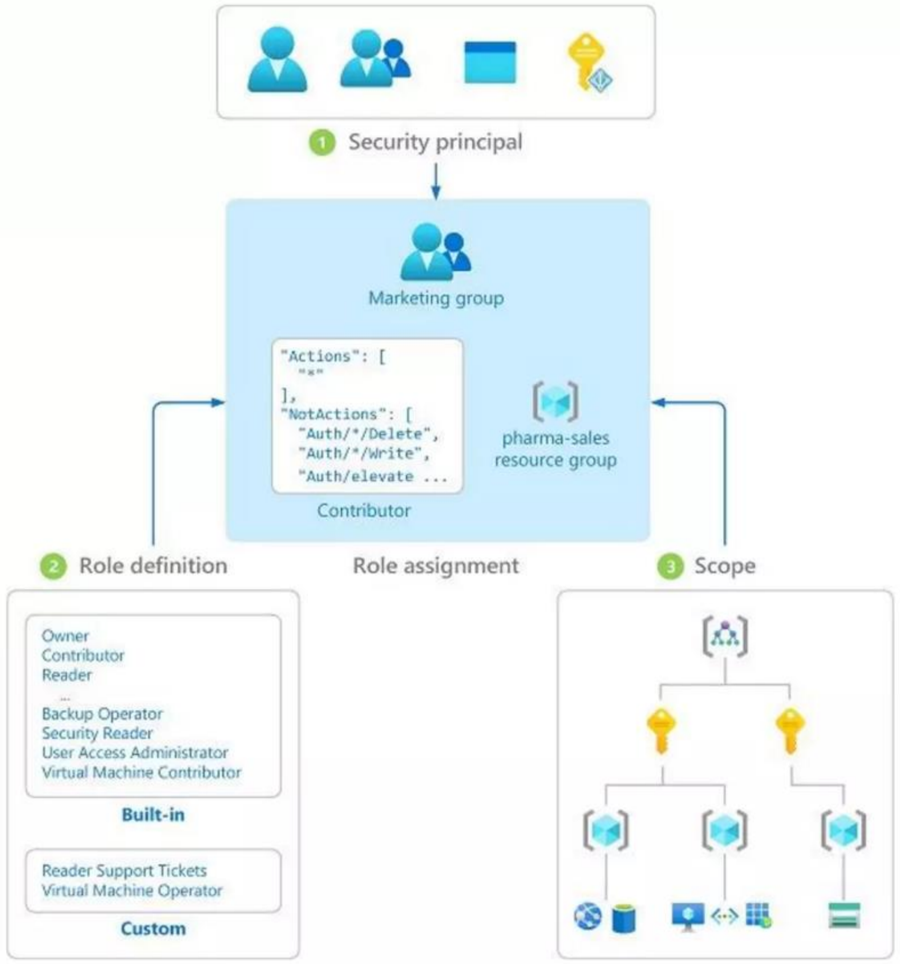
- Virtual Network
- DNS Zones
- VPN Gateway
- Express Route
- Load Balancer
- Firewall

MAZZY TECHNOLOGIES

Azure Penetration Testing Scopes

- Anonymous external testing
- Read-only configuration review
- Internal network testing
- Architectural review

Assessing Azure Cloud Services



```
"Actions": [
  "*"
],
"NotActions": [
  "Auth/*/Delete",
  "Auth/*/Write",
  "Auth/elevate ...
```

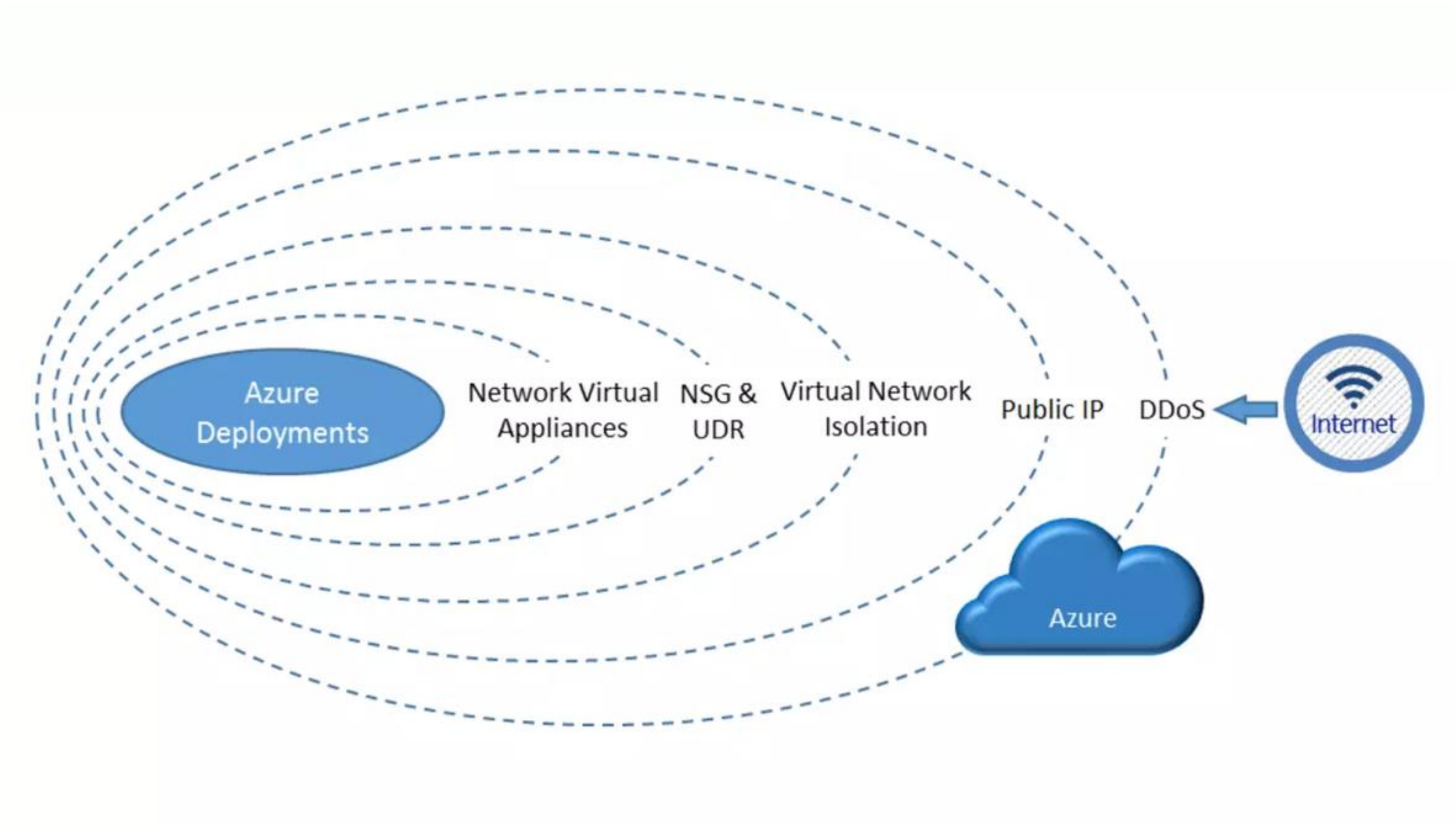
Owner
Contributor
Reader
...
Backup Operator
Security Reader
User Access Administrator
Virtual Machine Contributor

Built-in

Reader Support Tickets
Virtual Machine Operator

Custom

Securing the Database



Azure Penetration Testing Tools

Windows or Linux administration tools

- JQ, httpie, wget, curl, unzip, powerShell etc…

General Penetration testing tools

- Gobuster, nmap, dnscan and hydra

Azure specific Penetration testing tools

- Microbust, Lava, Koboko, PowerZure, Stormspotter, and BloodHound

Thank you!

Contact us:

Phone: **1.888.992.1062**

sales@mazzytechnologies.com

https://mazzytechnologies.com

MAZZY TECHNOLOGIES