How and What on Penetration Testing for Microsoft Azure Cloud Services

ABBAS KUDRATI
APAC CHIEF CYBERSECURITY ADVISOR
@askudrati
https://aka.ms/abbas

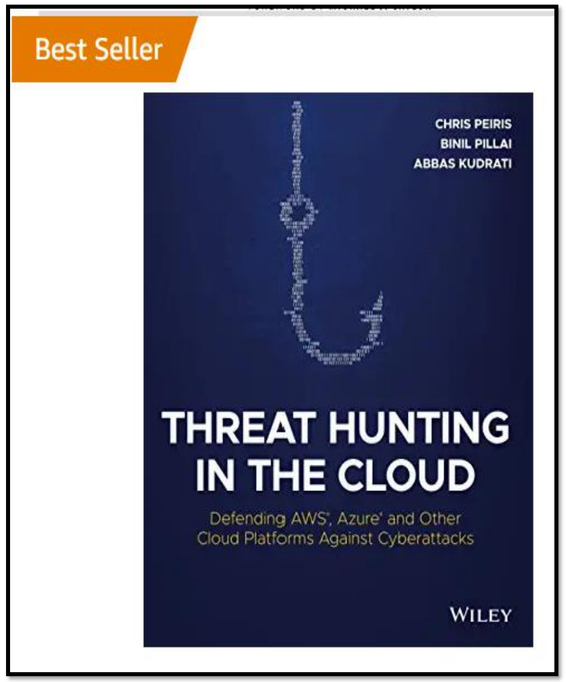
AUSTRALIAN CYBER CONFERENCE 2022

About me

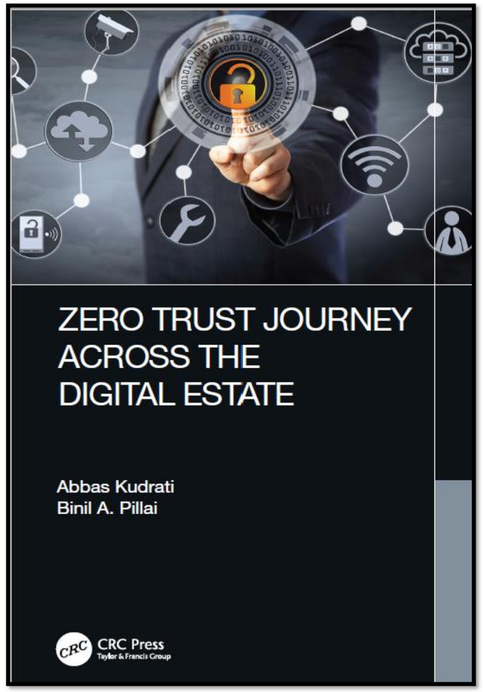
"You join Microsoft, not to be cool
but to make others cool"
Satya Nadella

- **Cybersecurity practitioner and CISO with 25 years of experience in Information / Cybersecurity.**
- **Part time Cybersecurity Professor with Deakin and LaTrobe University in Melbourne, Australia.**
- **Expertise in Zero Trust, Cybersecurity Strategy, Security Operations, Risk, Compliance, Cloud Security and Architecture.**

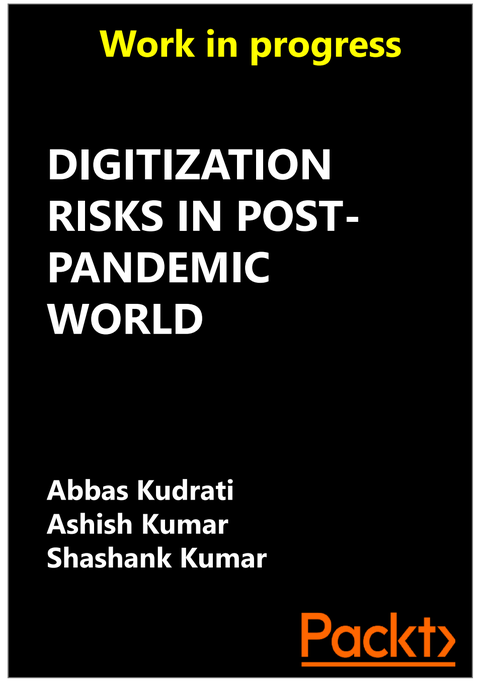
My Publications



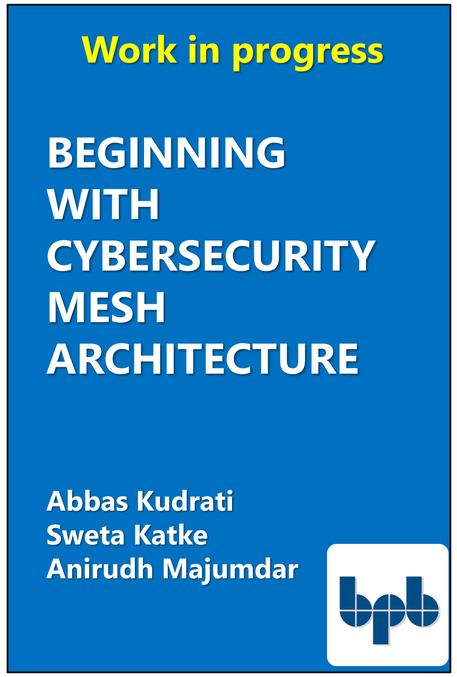
[Get it on Amazon](#)
Or send me a request for a free copy



[Order on Amazon](#)



Releasing soon by Dec 2022



Releasing soon by March 2023

Cloud computing challenges, and

Shared Responsivity Model

Cloud Computing Challenges

- Are the appropriate security controls set up on the Cloud?
- Are customers storing sensitive data in the Cloud and protecting them properly?
- Azure providing appropriate controls to monitor events and attacks attempts?

A Cloud Provider Inherits…

Customer Regulations

ISO 27001 · ISO 27018 · ISO 27017 · ISO 22301 · SOC 1 Type 2 · SOC 2 Type 2 · SOC 3 · CSA STAR Self-Assessment · CSA STAR Certification · CSA STAR Attestation

Moderate JAB P-ATO · High JAB P-ATO · DoD DISA SRG Level 2 · DoD DISA SRG Level 4 · DoD DISA SRG Level 5 · SP 800-171 · FIPS 140-2 · Section 508 VPAT · ITAR · CJIS · IRS 1075

PCI DSS Level 1 · CDSA · MPAA · FACT UK · Shared Assessments · FISC Japan · HIPAA / HITECH Act · HITRUST · GxP 21 CFR Part 11 · MARS-E · IG Toolkit UK · FERPA · GLBA · FFIEC

Argentina PDPA · EU Model Clauses · UK G-Cloud · China DJCP · China GB 18030 · China TRUCS · Singapore MTCS · Australia IRAP/CCSL · New Zealand GCIO · Japan My Number Act · ENISA IAF · Japan CS Mark Gold · Spain ENS · Spain DPA · India MeitY · Canada Privacy Laws · Privacy Shield · Germany IT Grundschutz workbook

…

Customer Adversaries

…

Shared Responsibility & Cloud Providers

Two key priorities when working with cloud providers:

Implement Shared Responsibility Model

Security work is shared between you and cloud provider.

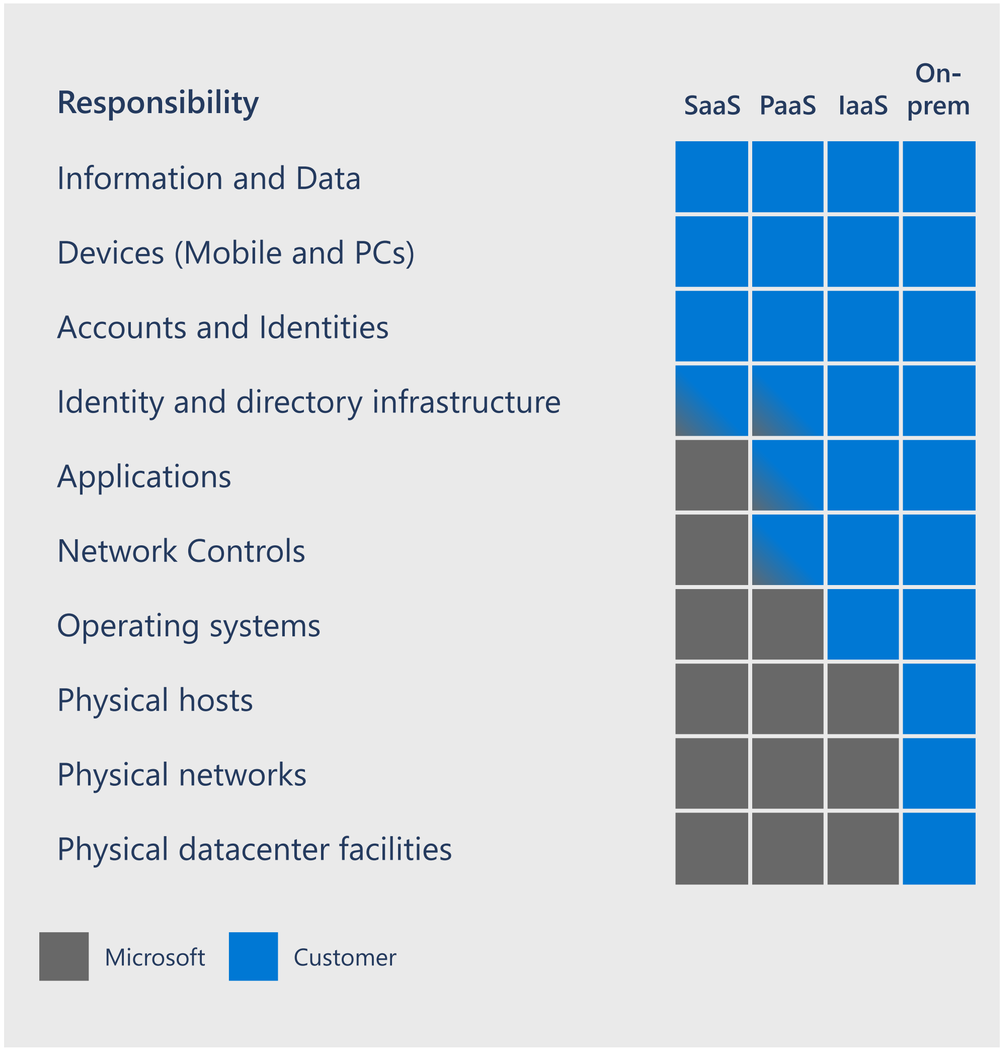
- Adjust your security strategy, planning, processes, controls, and more to this reality and build a unified common defense

Evaluate and Monitor Cloud Provider Security

Security of business-critical assets may rely on provider security practices

- Take a holistic view of cloud provider security that considers compliance, approach and processes, relevant business model(s), and results / outcomes.

Shared Responsibility Model



What it is – Planning model for identifying which security elements are provided by different parties (e.g. cloud platform and cloud customers)

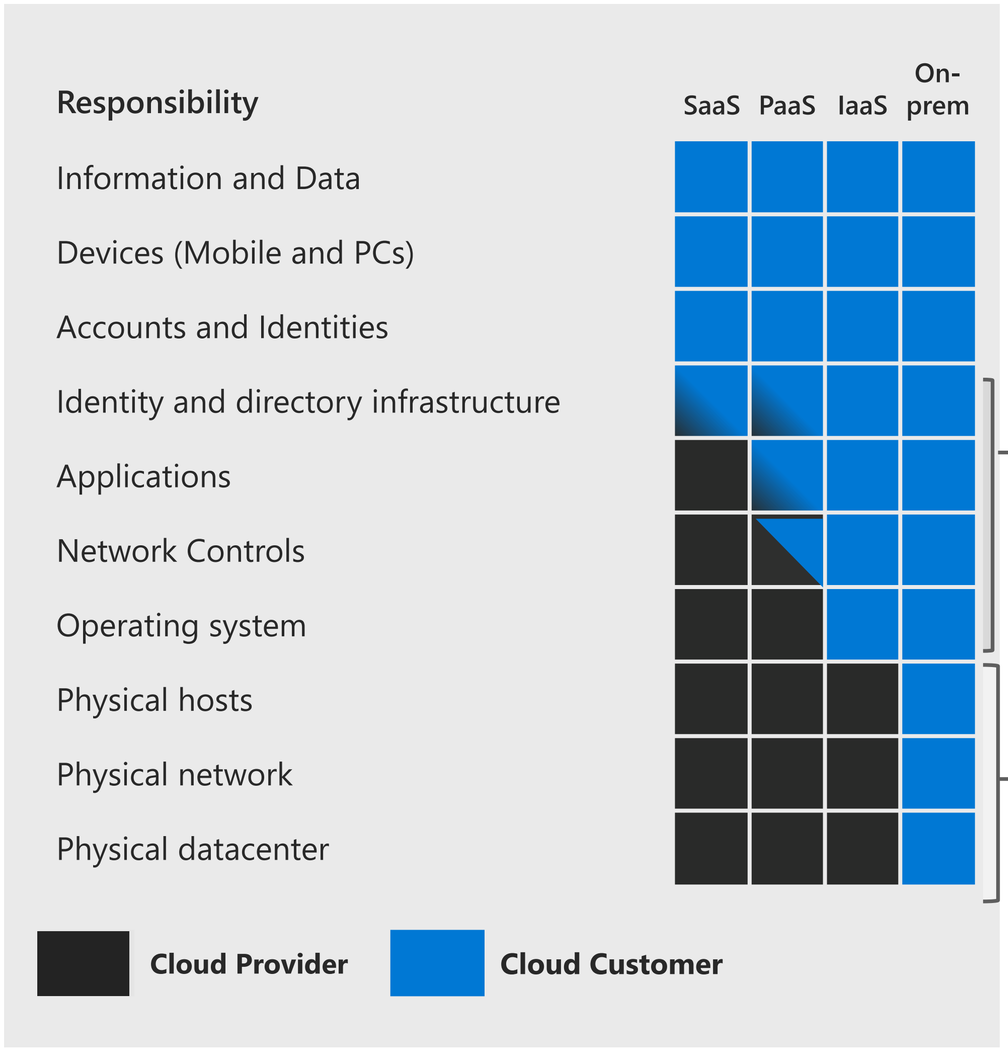
Prevalence – Frequently used by security teams during first adoption of cloud services

Primary Use Cases –

- Helps transform mindset and strategy/plan/architecture from “in control of everything” to “shared responsibility” mode
- Derivative models can define inter-team and inter-organizational security responsibilities

Known limitations – Framing exercise only, requires expertise for detailed planning and execution, requires threat modelling to ensure controls are collectively complete

Security responsibilities transfer to the cloud



Transferred for SaaS & PaaS

- Security Patches
- Feature Upgrades
- VMs/Containers security – OS and middleware installation, maintenance, troubleshooting, etc.

Transferred for SaaS, IaaS & PaaS

- Racking/Stacking Servers, Adding Capacity
- Fabric/Virtualization Patching, Maintenance & Troubleshooting
- Fabric Availability / Uptime

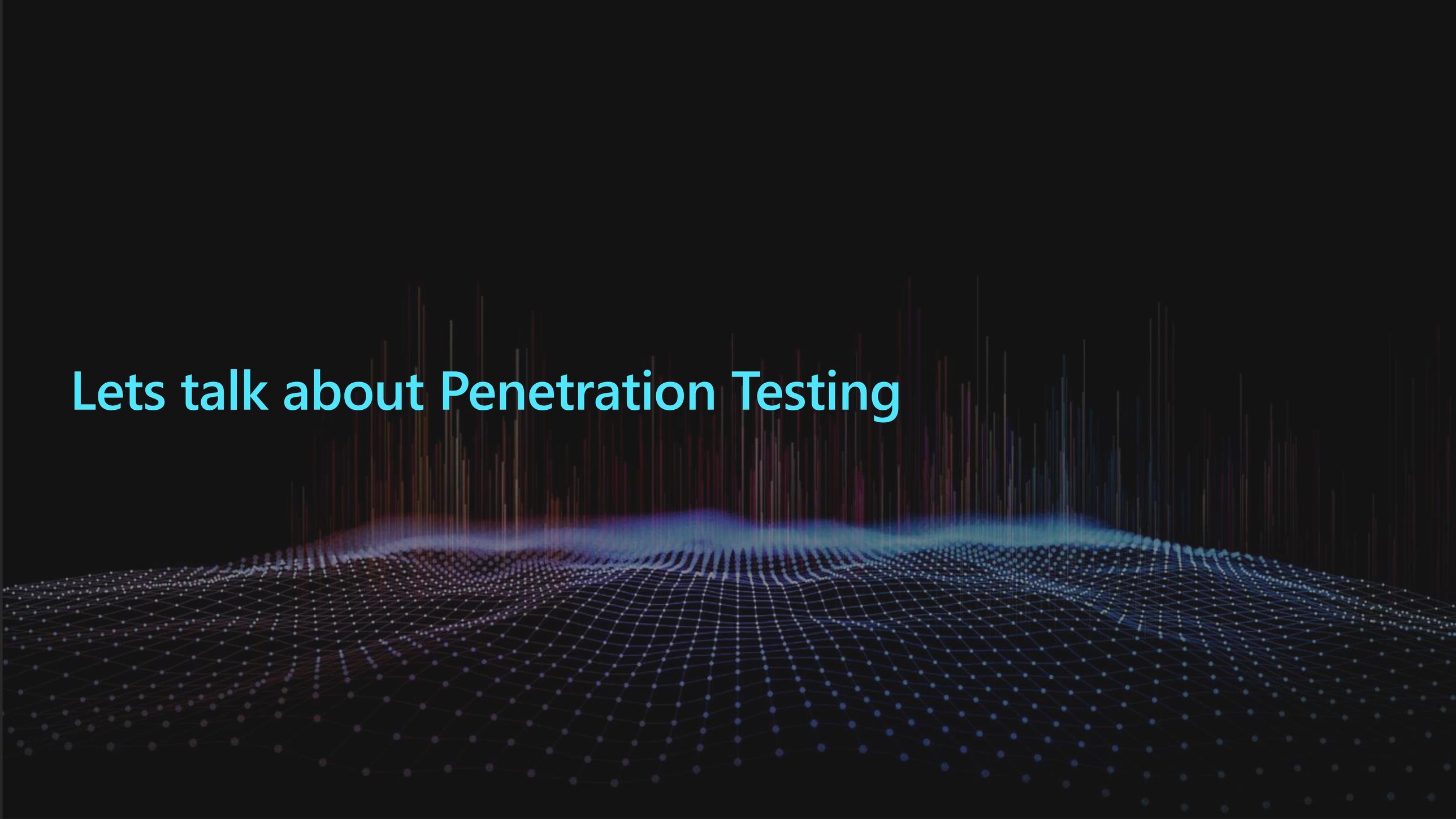
Attacks on

- Physical Location
- Virtualization Fabric
- Hardware/Firmware
- Network Infrastructure

"Customers should be able to reduce administration effort because the cloud service provider will be responsible for maintaining the hardware and software. This helps IT transition to higher-value activities and boost morale"

Forrester

Lets talk about Penetration Testing



Why Penetration Testing is important?

- Allows companies to view its critical infrastructure from the perspective of a hacker
- Provides more power in the security field
- Enables regulations and compliance
- Measures Cyber Maturity Accurately
- Indicates where the organization stands in terms of risk exposure

Why is Penetration Testing needed?

- Technologies evolve over time
- Vulnerabilities also change and evolve over time and get more sophisticated on the hackers' hands
- Penetration testing is really a form of QA that looks for flaws in network architecture and design, operating system and application configuration, application design, and even human behaviour as it relates to security policies and procedures.
- This can range from testing network and application access controls, to software code and IT operational processes.

What to have in a Penetration Testing?

Pen-testing plan

- Penetration Testing Methodology and Processes
- Select Penetration Testing tools
- Define customer needs and expectations
- Approval by appropriate business and IT management

Scoping

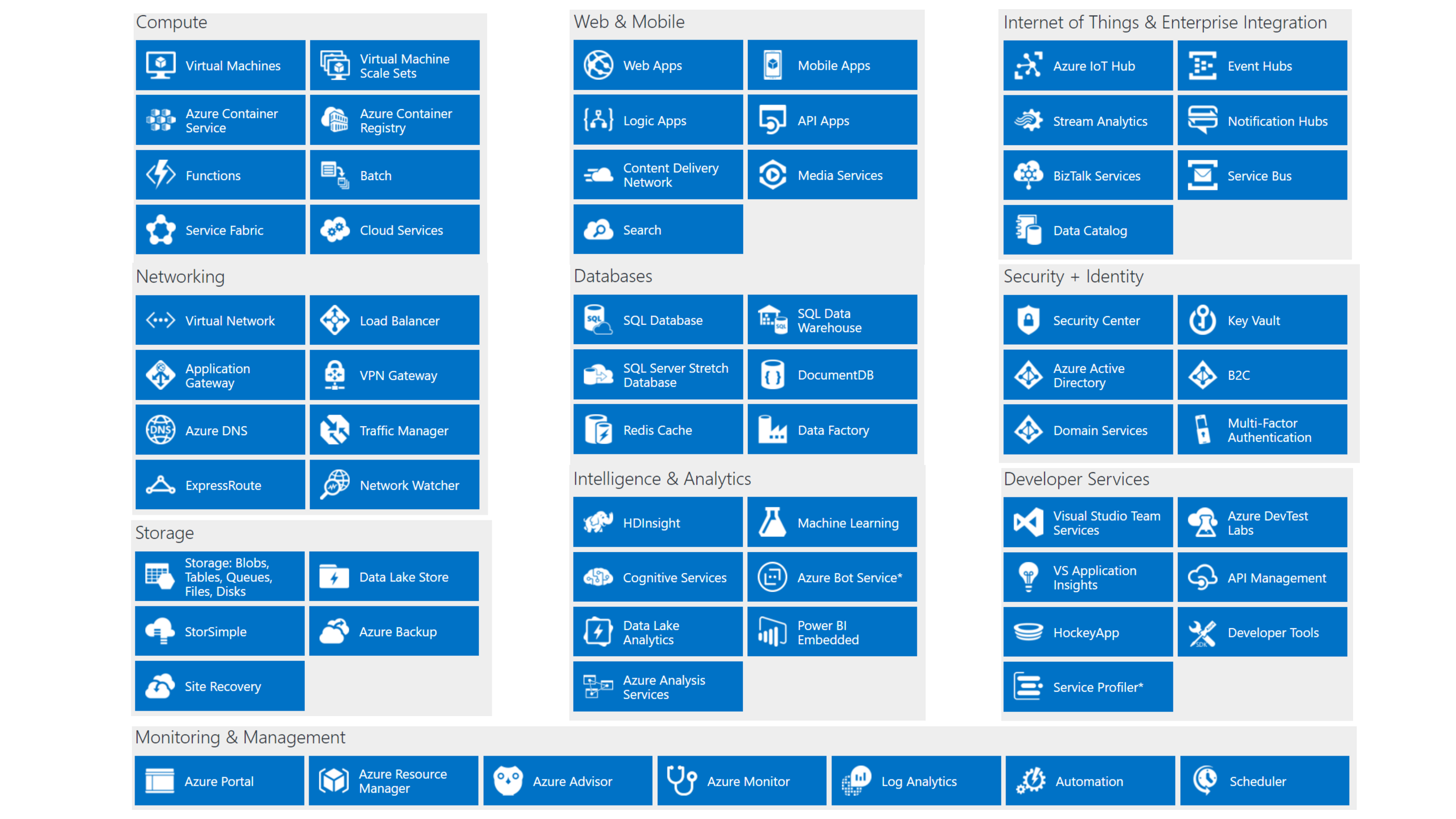
- Exploitation of targeted software
- Web Applications
- APIs, endpoints
- Databases
- Main-systems, enterprise-wide
- Real-world exploits

Compliance

- Some industries and types of data are regulated
- Regulator will insist on a penetration test as part of a certification process.
- Some standards will specify the requirements for penetration testing.

Penetration Testing Methodology

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


Compute
Virtual Machines
Virtual Machine Scale Sets
Azure Container Service
Azure Container Registry
Functions
Batch
Service Fabric
Cloud Services
Networking
Virtual Network
Load Balancer
Application Gateway
VPN Gateway
Azure DNS
Traffic Manager
ExpressRoute
Network Watcher
Storage
Storage: Blobs, Tables, Queues, Files, Disks
Data Lake Store
StorSimple
Azure Backup
Site Recovery
Web & Mobile
Web Apps
Mobile Apps
Logic Apps
API Apps
Content Delivery Network
Media Services
Search
Databases
SQL Database
SQL Data Warehouse
SQL Server Stretch Database
DocumentDB
Redis Cache
Data Factory
Intelligence & Analytics
HDInsight
Machine Learning
Cognitive Services
Azure Bot Service*
Data Lake Analytics
Power BI Embedded
Azure Analysis Services
Internet of Things & Enterprise Integration
Azure IoT Hub
Event Hubs
Stream Analytics
Notification Hubs
BizTalk Services
Service Bus
Data Catalog
Security + Identity
Security Center
Key Vault
Azure Active Directory
B2C
Domain Services
Multi-Factor Authentication
Developer Services
Visual Studio Team Services
Azure DevTest Labs
VS Application Insights
API Management
HockeyApp
Developer Tools
Service Profiler*
Monitoring & Management
Azure Portal
Azure Resource Manager
Azure Advisor
Azure Monitor
Log Analytics
Automation
Scheduler

Azure Security Services and Capabilities*

Network Security

- Virtual Network Service Endpoints
- DDoS protection
- Network Security Groups
- NSG service tags
- NSG Application Security Groups
- NSG Augmented Rules
- Global Virtual Network Peering
- Azure DNS Private Zones
- Site-to-site VPN
- Point-to-site VPN
- ExpressRoute
- Azure Virtual Networks
- Virtual Network Appliances
- Azure Load Balancers
- Azure Load Balancer HA Ports
- Azure Application Gateway
- Azure Web Application Firewalls

Compliance Program

- Microsoft Trust Center
- Service Trust Platform
- Compliance Manager

DDoS Mitigation

- Azure DDoS Protection
- Azure Traffic Manager
- Autoscaling
- Azure CDN
- Azure Load Balancers
- Fabric level edge protection

Pen Testing

- Per AUP
- Per TOS
- No contact required

Encryption

- Azure Key Vault (no dedicated option, though)
- Azure client-side encryption library
- Azure Storage Service Encryption
- SQL Transparent Data Encryption
- SQL Always Encrypted
- SQL Cell/Column Level Encryption
- Azure Cosmo DB encrypt by default
- Azure Data Lake encrypt by default
- VPN protocol encryption (ssl/ipsec)
- SMB 3.0 wire encryption

Identity and Access Management

- Azure Active Directory
- Azure Active Directory for Devs
- Azure Active Directory B2C
- Active Directory Domain Services
- Azure Active Directory MFA
- Conditional Access
- Azure Active Directory Identity Protection
- Azure Active Directory Privileged Identity Management
- Azure Active Directory App Proxy
- Azure Active Directory Connect
- Azure RBAC
- Azure Active Directory Access Reviews

Security Docs Site

- Azure Security Information site on Azure.com

Infrastructure Security

- Comes with Azure Data Centers

Config & Management

- Azure Security Center
- Azure Resource Manager
- Azure Automation
- Azure Advisor

Data Loss Prevention

- Cloud App Discovery
- Azure Information Protection

Monitoring and Logging

- Azure Log Analytics
- Azure Monitor
- Azure Application Insights

*Level2-moderate depth analysis

Penetration Testing Matrix for Microsoft-based products

Attacks/Testing	Product	Detection/Protection	Comments	Cloud	On-premise
Credential theft. Attacks on directory systems. Brute force attacks. Unauthorized access of sensitive data.	Azure Active Directory, Azure Information Protection	Azure Active Directory Premium	AAD Plan 2 Includes Identity protection: Privileged Identity Management, access reviews, vulnerabilities and risky accounts detection. Azure information protection included in P1 and P2	✓	✓
Credential theft. Attacks on directory systems. Brute force attacks.	Azure Active Directory	Microsoft Defender for Identity		✓	✓
Unauthorized access of sensitive data. Data leak		Advanced Threat Analytics	Advanced Threat Analytics		
Social engineering attacks, Phishing, malware, virus, spam	Office 365	Microsoft Defender for Office 365	Advanced threat protection included in Office 365 Plan 2. Phishing campaigns only included in Office defender P2	✓	✓
Credential, secrets and key leaks and/or theft	Key vault, Storage	Azure Key Vault	Credential, secrets and key leaks and/or theft	✓	
DDoS attacks	IaaS, PaaS	Azure DDoS (D/P) Sentinel (D)	DDoS attacks. Port scanning	✓	
Network penetration. Firewall bypass. Network vulnerabilities	Servers, App services, Azure SQL DB	Azure Firewall (D/P) Azure WAF (D/P) Sentinel (D)	Network penetration. Firewall bypass. Network vulnerabilities		
Vulnerability assessment	Servers, App services, SQL DB, Storage, Kubernetes	Azure Security Center (D)		✓	✓
Advanced persistent threats.	Servers, App services, SQL DB, Storage, Kubernetes	Azure Defender (P)		✓	
Active and passive reconnaissance for storage services	Storage	Azure Storage Service Encryption, Azure Storage Shared Access Signatures, Azure Storage Account Keys, Azure Key Vault		✓	

Penetration Testing Matrix for Microsoft-based products

Attacks/Testing	Product	Detection/Protection	Comments	Cloud	On-premise
SQL injection, Cross site scripting, Code execution, defacement	Web applications	Azure WAF (D/P) Azure Sentinel (D)		✓	✓
SQL Dictionary Attack, enumeration, SQL injection, SQL exploits	SQL DBs	Azure SQL Firewall, Azure Firewall (D/P) Azure Sentinel (D)		✓	
Advanced persistent threats. Brute force attacks	Servers, App services, SQL DB, Storage, Kubernetes	Azure Defender (D/P)		✓	
Network penetration. Firewall bypass. Network vulnerabilities	Servers, App services, Azure SQL DB	Azure Firewall (P) Azure Sentinel		✓	✓
DNS Queries, Security Tokens, User Enumeration @AD	Azure Active Directory	Microsoft Defender for Identity (D) Azure Sentinel (D)	Enumerate all user accounts & admin group membership. Password Spraying	✓	
Phishing Office365 accounts	Office 365	Office 365 ATP (D/P)			
Unpatched OS, Purposedly Infected devices	Endpoint Threat protection	Microsoft Defender for Endpoint (D/S)	Included in M365 E5		✓
Data exfiltration	Bitlocker	Microsoft Intune Microsoft Defender for Identity (D)			✓
Anonymization, credential theft, data exfiltration	SaaS	MCAS	Included in M365 E5	✓	

Building Environment and Tools

Rules of Penetration Testing

Prohibited	Encouraged
▪ 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.	▪ Create multiple test or trial accounts to test cross-account access vulnerabilities. However, using these test accounts to access other customer's data is prohibited. ▪ Running vulnerability scanning tools, port scan, or fuzz on your virtual machine. ▪ Testing your account by generating traffic which 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. ▪ Test Microsoft Intune to ensure all restrictions function as expected.

Building Environment

Azure Tenant

- Ensure Azure admin account is created to install scripts and tools for testing

Pentest VM

- Use ARM to deploy Windows Server (Save time) OR Use your favorite VM
- Having Windows Server with Linux capability will be a good start

Install Pentest Tools

- Standard sysadmin/networking tools (curl, httpx, wget, curl, PowerShell, jq, etc.)
- Standard Pentest tools (nmap, Metasploit, OpenWAS, BurpSuite, DNS uitilities, hydra, etc.)
- Azure specific pentest tools (https://github.com/Kyuu-Ji/Awesome-Azure-Pentest)

General Pentest Scope

External

Black Box Testing

Read-Only Configuration Review

Internal Network Scanning

Architecture Review

Attack Surface Analysis (Technical Scope)

External Black-Box Pentest

IP Address →
- Standard 65535 Port Scan
- Service Scan
- Vulnerable Service Exploitation
- Brute force user account credentials

Domain →
- Domain health checks
- DNS records checks
- Subdomain enumerations
- Subdomain takeovers

Web App →
- OWASP Top 10 web app attacks
- SANS Top 25 controls
- Abandoned/Unmaintained assets
- Business logic flaws

Storage Accounts →
- Azure Blob Storage (like open S3 buckets) anonymous access

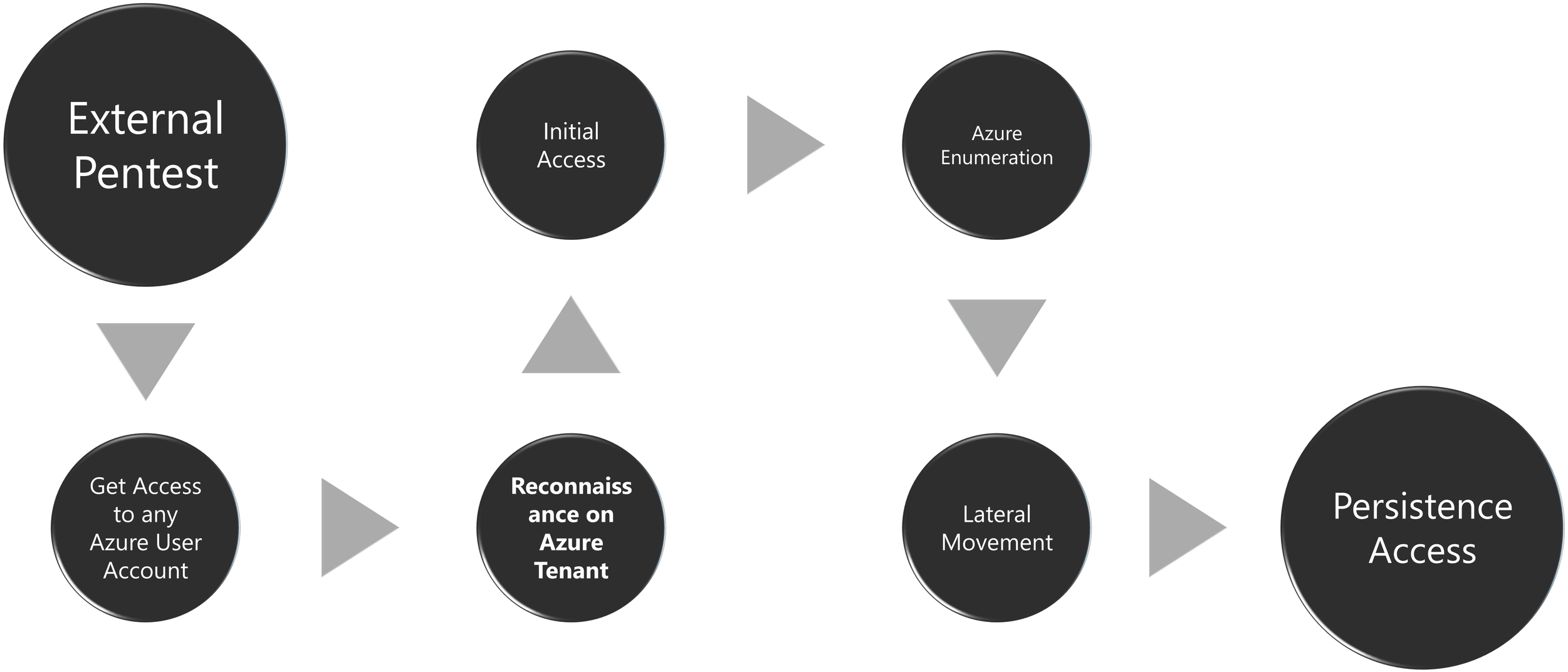
Internal Pentest (Based on Access Control)

Reader Access →
- Enumerate inventory of resources
- Enumerate Azure subscription information
- Enumerate cleartext data stores (keys, secret, DB, configs etc.)
- Enumerate and exploit App service configurations
- Dynamic group membership exploitation
- Privilege Escalation to other access roles

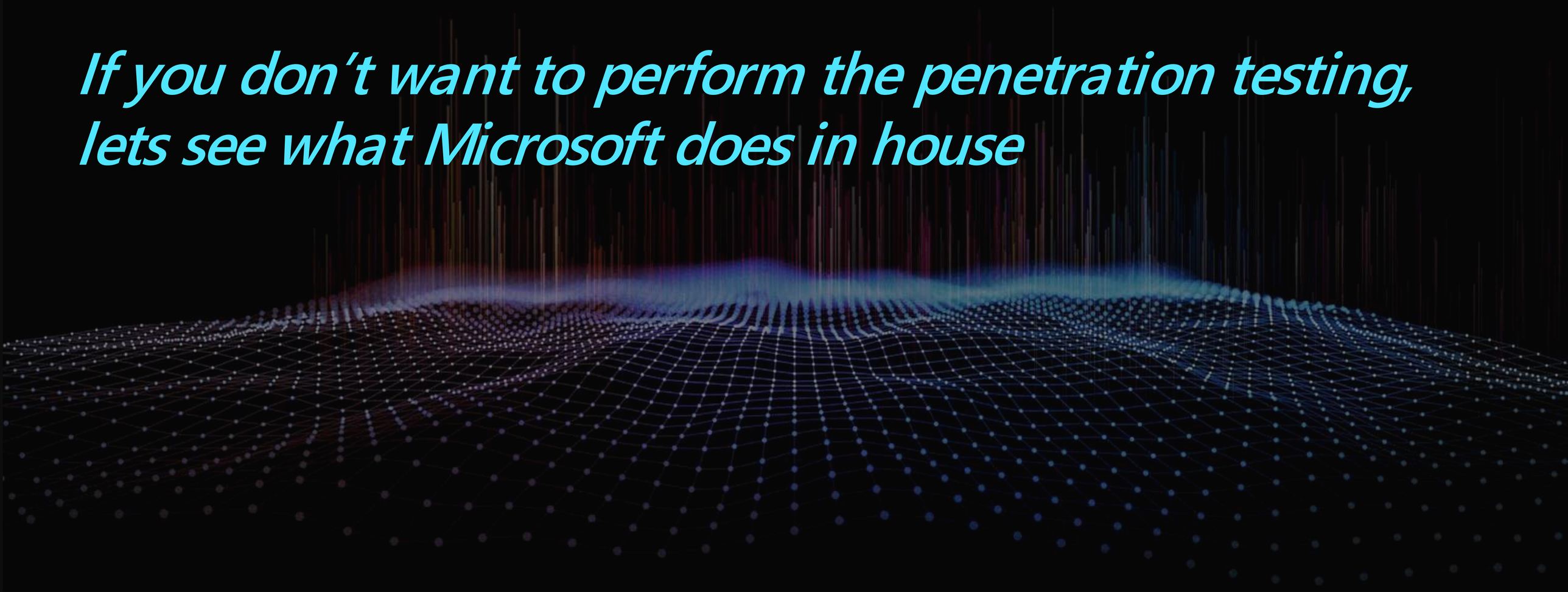
Contributor Access →
- Lateral movement
- Tenant credential dumping
- Local and Domain credential dumping
- Creds and sensitive data exfiltration
- Testing storage accounts, web apps

Owner Access →
- Escalating from Azure AD to Azure RBAC roles
- Escalating from subscription Owner to Azure AD roles
- Attacking on-premises systems to escalate in Azure

High-level Pentest Workflow



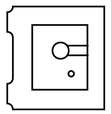
If you don't want to perform the penetration testing, lets see what Microsoft does in house



Security Tooling and Automation

Continuous scanning and detection of vulnerabilities

Millions of lines of code makes scale and coverage critical. Major investments into tools and automation - including static analysis, fuzzing, and attack surface detection



Ongoing code scanning

Tools to make penetration testing more effective

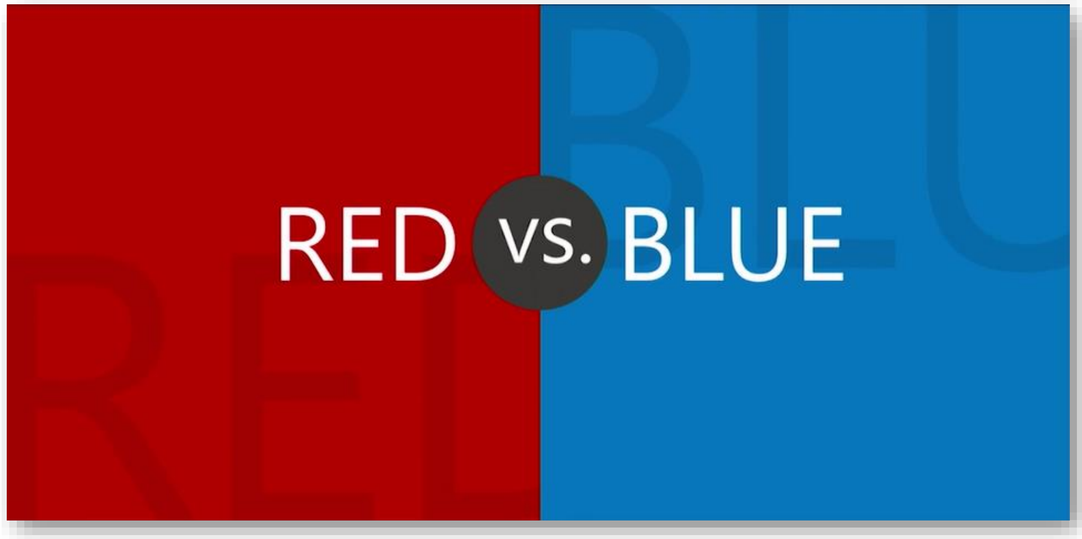
Mitigations

Self-Service developer tools

Penetration Testing

Internal Red – Blue Team Exercises

- Assume breach strategy



Red Team :
- FTEs tasked at attacking internal Azure infrastructure
- Gated by Rules of Engagement
- Simulate real world attacks
- Focused on Microsoft infrastructure and sites

Blue Team:
- Defense team, FTEs tasked at finding and preventing attacks
- Individuals are independent of Red Team and exercise real world response

https://learn.microsoft.com/en-gb/shows/azure-friday/red-vs-blue-internal-security-penetration-testing-of-microsoft-azure

Red Teaming

Red Teaming

Model real-world attacks

- Model **emerging threats** & use **blended threats**
- **Pivot** laterally & penetrate deeper
- **Exfiltrate** & leverage compromised data
- **Escape & Evade / Persistence**

Identify gaps in security story

- **Measures Time to Compromise (MTTC) / Pwnage (MTTP)**
- **Highlight security monitoring & recovery gaps**
- **Improves incident response tools & process**

Demonstrable impact

- **Prove need for Assume Breach**
- **Enumerate business risks**
- **Justify resources, priorities, & investment needs**

Blue Teaming

Blue Teaming

Exercises ability to detect & respond

- **Detect** attack & penetration (MTTD)
- **Respond** & **recover** to attack & penetration (MTTR)
- **Practiced** incident response

Enhances situational awareness

- Produces **actionable intelligence**
- **Full visibility** into actual conditions within environment
- **Data analysis** & **forensics** for attack & breach indicators

Measures readiness & impact

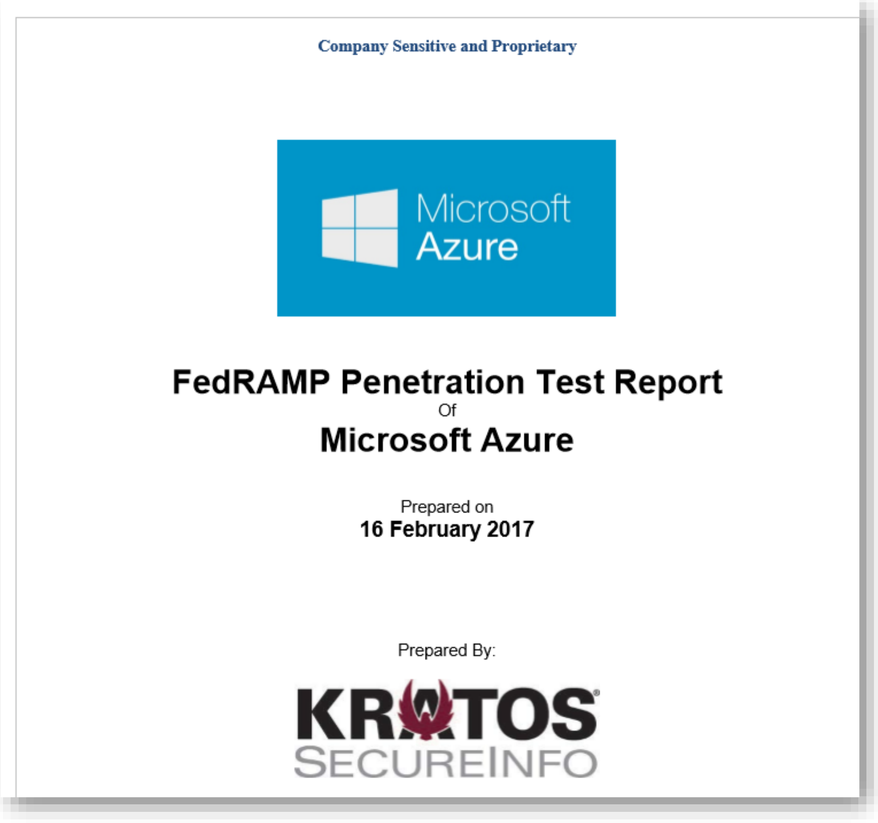
- **Accurately assesses** real-world attacks
- **Identifies** gaps & **investment needs**
- Focus on **slowing down attackers** & **speeding recovery**
- **Hardening** that prevents future attacks

External Independent Penetration Testing

External Pentest

- **Gated by Rules of Engagement**
- **Performed annually by independent entity**
  - Physical penetration constraints;
  - Incident Response Team or similar capability and the requirements for exercising the penetration test;
  - Acceptable social engineering pretext(s); etc.
  - Network, Web Application and Mobile Application penetration testing

All reports can be found at https://aka.ms/stp



Microsoft Bug Bounty Program

Bug Bounty

Leverage external research community to find and report bugs to Micrososft

Microsoft has multi-million dollar yearly bounty budget to drive external research and reporting of vulnerabilities

Bug Bounty Success

Our goal is for Microsoft to **earn customer trust.**

We do this through in several ways. Being transparent and working with the research community is one of those ways. Incentivizing the research community to responsibly detect potential vulnerabilities in our system helps us harden our securities and consistently improve the customer experience.

As a part of our bug bounty program, we encourage researchers to be transparent with the information they discover. You may see Microsoft mentioned in blogs more than others due to our transparent approach to working with researchers. Working collaboratively makes us better for you.

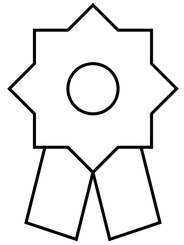
Microsoft Bug Bounty Program

Mission

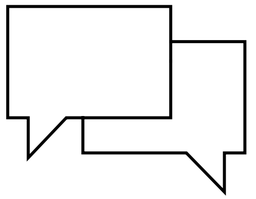
Protect customers through partnership with the global security research community

Awards to incentivize researchers to find and confidentially report high-impact security vulnerabilities in Microsoft products and services

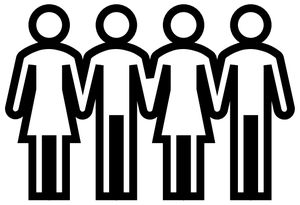
Key numbers Jul 2020 – Jun 2021



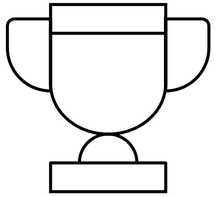
$13.6M
in bounty awards



1,261
Eligible reports



341
Researchers awarded from +60 countries



$200K
Biggest reward

Make money and get famous with Microsoft Bounty

Cloud Programs

Program Name	Start date	Last Updated	End date	Eligible entries	Bounty Range
Microsoft Azure	2014-09-23	2021-10-18	Ongoing	Vulnerability reports on Microsoft Azure cloud services	Up to $60,000 USD
Microsoft Identity	2018-07-17	2019-10-23	Ongoing	Vulnerability reports on Identity services, including Microsoft Account, Azure Active Directory, or select OpenID standards.	Up to $100,000 USD
Xbox	2020-01-30	2020-01-30	Ongoing	Vulnerability reports on the Xbox Live network and services	Up to $20,000 USD
M365	2014-09-23	2019-08-05	Ongoing	Vulnerability reports on applicable Microsoft cloud services, including Office 365	Up to $20,000 USD
Microsoft Azure DevOps Services	2019-01-17	2019-01-17	Ongoing	Vulnerability reports on applicable Microsoft Azure DevOps Services	Up to $20,000 USD
Microsoft Dynamics 365 and Power Platform	2019-07-17	2022-04-14	Ongoing	Vulnerability reports on applicable Microsoft Dynamics 365 and Power Platform applications	Up to $20,000 USD
Microsoft .NET	2016-09-01	2020-11-20	Ongoing	Vulnerability reports on .NET Core and ASP.NET Core RTM and future builds (see link for program details)	Up to $15,000 USD

https://www.microsoft.com/en-us/msrc/bounty

How to secure your Azure Cloud

Native Security for Azure

End-to-End capabilities that apply Zero Trust principles to Infrastructure & Platform as a Service (IaaS & PaaS)

Azure Cloud Adoption Framework (CAF)
Guidance on security strategy, planning, roles and responsibilities https://aka.ms/CAF

Management Plane Security
Platform provided security guardrails, governance, policy, and more

- Azure Blueprints
- Management Groups
- Azure Lighthouse
- Azure Policy
- Role Based Access Control (RBAC)
- Azure Security Center
- Azure Backup
- Resource Locks
- Azure Backup & Site Recovery
- •••

Data Plane Security
Per-Application/Workload Controls

Enable Zero Trust Networking & Secure Access Service Edge (SASE)

Azure Well Architected Framework (WAF)

Internal Communications (East/West)
- Network/App Security Groups
- PrivateLink & Service Endpoints

External Communications (North/South)
- API Management Gateway
- Azure DDoS and Web Application Firewall (WAF)

- Encryption & Azure Key Vault, Application RBAC Model
- Azure Firewall and Firewall Management
- Azure DevOps Security
- GitHub Advanced Security

Azure Security Benchmarks (ASB)
Prescriptive Best Practices and Controls

Control

Governance & Policy Enforcement

Preventive Controls

Azure AD Identity Governance
- Automated User Provisioning
- Entitlement Management
- Access Reviews
- Privileged Identity Management (PIM)
- Terms of Use

Microsoft Endpoint Manager
- Intune
- Configuration Manager

- Azure Bastion
- Microsoft 365 Defender

Zero Trust Access Control
Explicit trust validation for users and devices before allowing access

MFA and Passwordless
- Azure AD MFA
- Windows Hello
- Existing MFA

- Azure AD Privileged Identity Management (PIM)
- Azure AD Identity Protection
- Azure AD Conditional Access

Privileged Access Workstation (PAW)

Microsoft Cloud App Security

Full Time Employees, Partners, and/or outsourced providers

- Business Users
- Developers
- Administrators
- App/Service and Automation

Azure Active Directory (AD) and B2B

Active Directory

- Access Applications
- CI/CD Pipeline
- Azure Resource Management (ARM)
  - Azure Portal
  - Command Line Interface (CLI)
  - Automation/API

- On-Premises & Other Cloud Resources/Data
- On-Premises & Other Cloud Resources/Data

Azure AD B2C

- Application
- API

Customers (and 'External' Partners)

- Azure IoT Hub
- Azure Sphere
- Existing/Other

Internet of Things (IoT) Devices

'Internal' Access — Workstations — Accounts — **Identity** — Access and Privileges — Interface — **Infrastructure** — Resource — Network & 'External' Access

Visibility

Risk Factors & Governance

Threat Detection

Raw Logs and Signal for Investigation & Hunting

Microsoft Secure Score

Microsoft 365 Defender
- Microsoft Defender for Endpoint
- Azure AD Identity Protection
- Microsoft Defender for Identity

Azure Sentinel
Threat detection, investigation, remediation, and hunting

- Security Incident & Event Management (SIEM)
- Security Orchestration, Automation, and Remediation (SOAR)
- Unified Entity Behavioral Analytics (UEBA)
- Machine Learning (ML) & Artificial Intelligence (AI)
- Security Data Lake

- Endpoint logs
- Azure AD logs, access logs, alerts, risk scoring
- PIM Logs

Azure Security Center (ASC) - Risk & Regulatory Compliance Reporting

Azure Policy (audit) & Azure resource graph API

Microsoft Cloud App Security (MCAS)
- MCAS Alerts
- MCAS Logs

Azure Defender - Detections across assets and tenants
- VMs & Tenants (Azure, On-prem, 3rd party clouds)
- Containers and Kubernetes
- IoT and Legacy OT Devices (SCADA, ICS, etc.)
- Azure SQL & Cosmos DB
- Azure Storage Accounts
- And More...

- Azure WAF Alerts
- Azure Firewall Alerts
- Azure DDOS Alerts

- Application Logs
- Network Watcher – IP Flow logs, Packet Capture, Virtual TAP
- Azure activity log
- Azure Service Diagnostic Logs & Metrics

Azure Security Benchmarks

- Provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure. Includes:
  - **Cloud Adoption Framework** – Guidance on security, including strategy, roles and responsibilities, Azure Top 10 Security Best Practices, and reference implementation.
  - **Azure Well-Architected Framework** – Guidance on securing your workloads on Azure.
  - **Microsoft Security Best Practices** – recommendations with examples on Azure
- These controls are consistent with well-known security benchmarks, such as those described by the Center for Internet Security (CIS) Controls and (NIST) SP800-53.
- All the controls are available in a downloadable format:
  - https://github.com/MicrosoftDocs/SecurityBenchmarks/find/master

- ✓ Network security
- ✓ Identity management
- ✓ Privileged access
- ✓ Data protection
- ✓ Asset management
- ✓ Logging and threat detection
- ✓ Incident response
- ✓ Posture and vulnerability management
- ✓ Endpoint security
- ✓ Backup and recovery
- ✓ Governance and Strategy

Thank You !

Abbas Kudrati
APAC Chief Cybersecurity Advisor
Abbas.Kudrati@Microsoft.com
@askudrati
https://aka.ms/abbas