

# Securing Resource Endpoints

---



**John Savill**

TECHNICAL ARCHITECT

@ntfaqguy <https://savilltech.com>

# Module Overview



**Public Endpoint Overview**

**Firewall and IP Restrictions**

**Microsoft Peering**

**Threat Detection**

# Public Endpoints

Nearly all Azure services have a public endpoint

Some dedicated services are private IP focused but may have the option of adding a public IP, i.e. endpoint

Remember the defense in depth, use authentication to control who may access the service, at what scope and what actions can be done

Additionally network controls can be leveraged

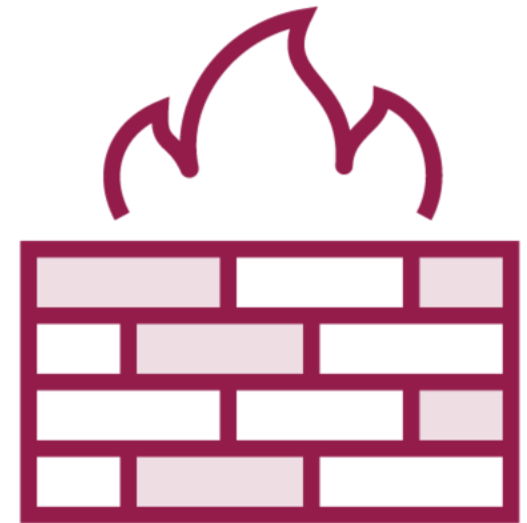
# Firewall and IP Restrictions

**Data services have a common Firewall capability**

**This enables access to be controlled based on:**

- Virtual networks (specific subnets using service endpoints)
- IP ranges
- Trusted Microsoft services

**Limit to only those that require access**



# Microsoft Peering



ExpressRoute provides a private link between customer networks and the Microsoft WAN



Microsoft peering allows for PaaS services to be advertised using BGP via the ExpressRoute link based on BGP communities



Connectivity to public endpoints will traverse via the private connection instead of the Internet



Additionally customer provided IPs provide the NAT from the internal on-premises IP space enabling those NAT IPs to be configured on Azure service firewalls

# Threat Detection

- Azure provides many types of protection for all services, for example DDoS
- Additional types of threat detection are available for some services, for example Advanced Threat Protection for Azure SQL Database and Azure Storage
- Utilize Vulnerability Assessment services when available
- Azure Security Center is also a good resource to utilize

# Module Overview



**Public endpoint overview**

**Firewall and IP restrictions**

**Microsoft peering**

**Threat detection**

THANK YOU!