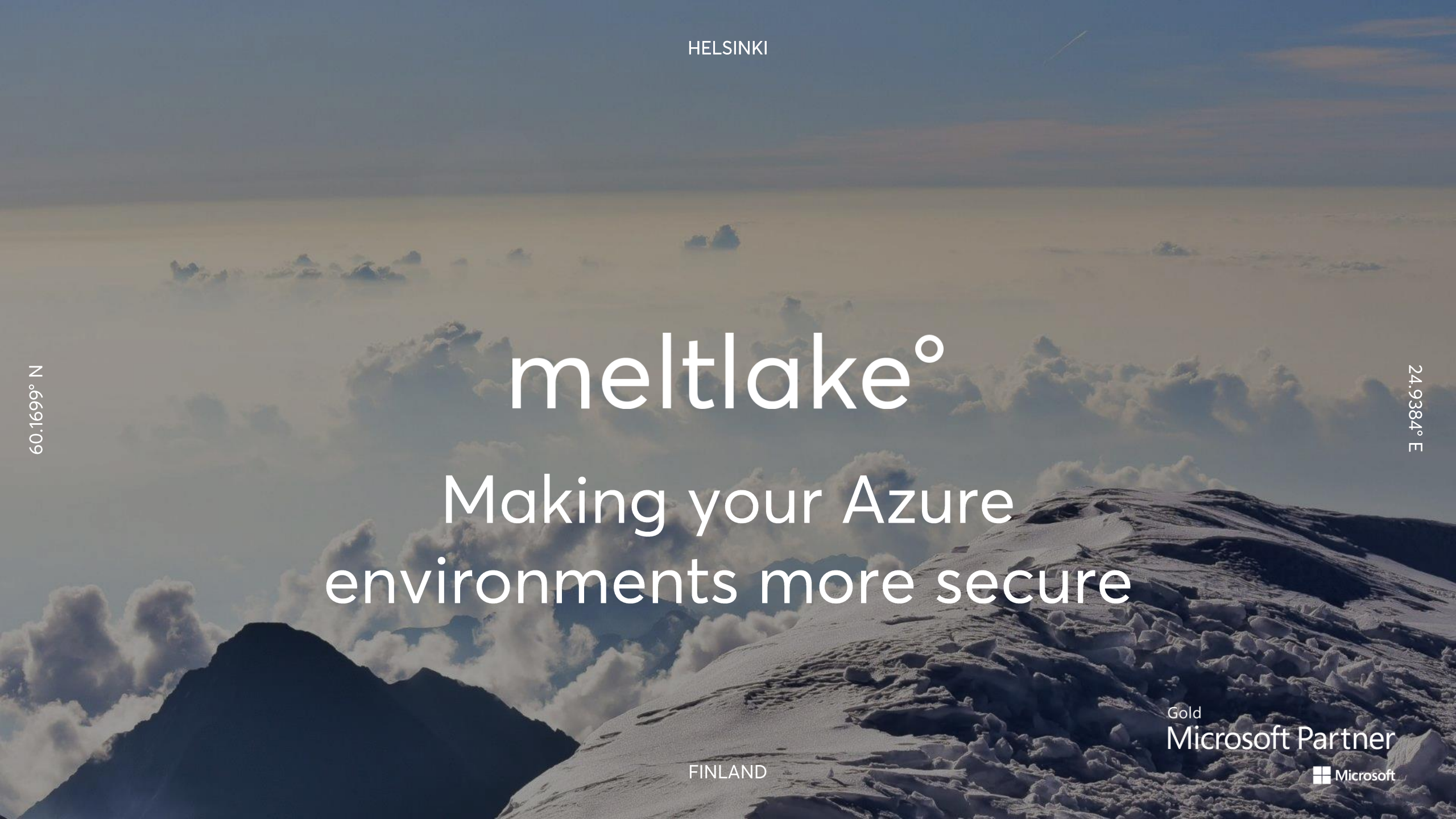

HELSINKI
60.1699° N
24.9384° E
meltlake°
Making your Azure environments more secure
FINLAND
Gold
Microsoft Partner
Microsoft

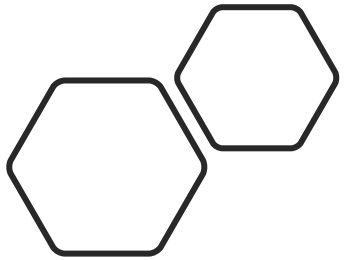
Antti Arnell

Cloud and Data Lead | Azure Advisor

antti.arnell@meltlake.com

https://www.linkedin.com/in/arnell

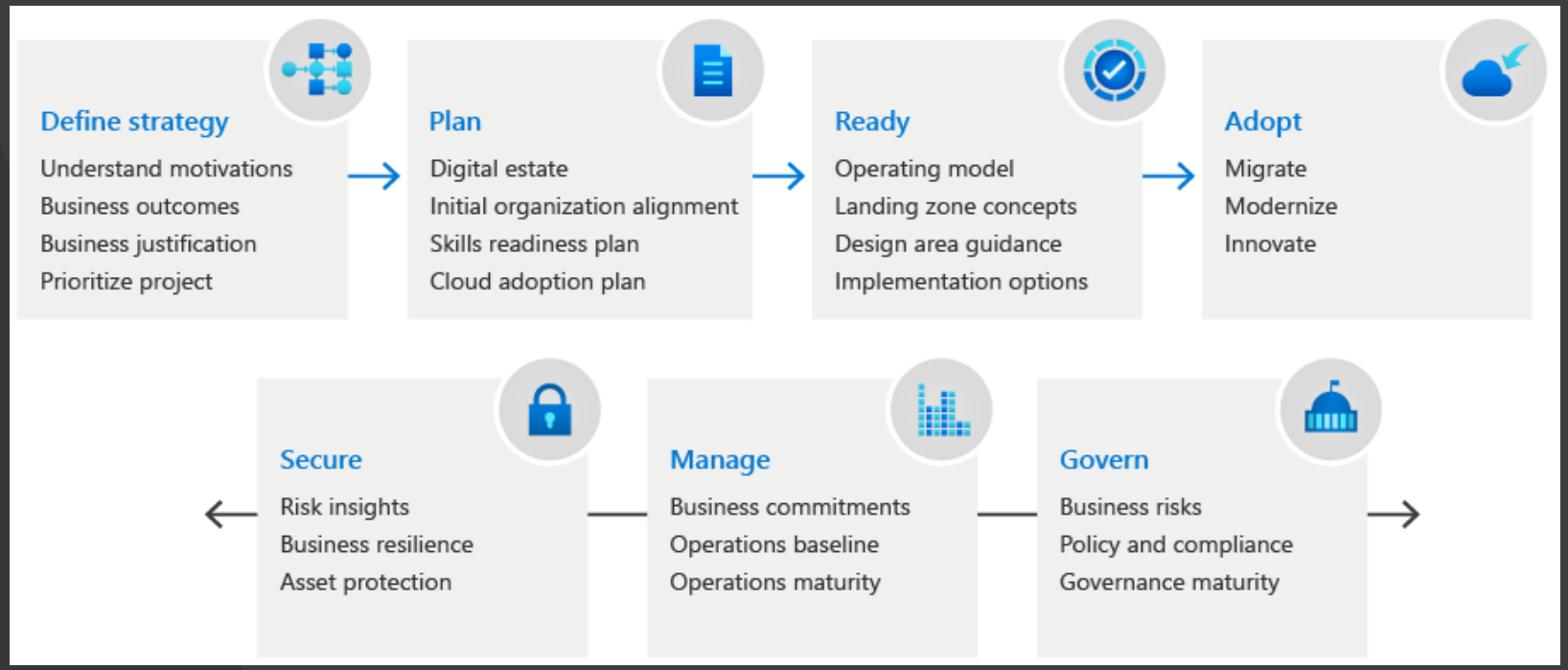
A bit of theory on cloud security



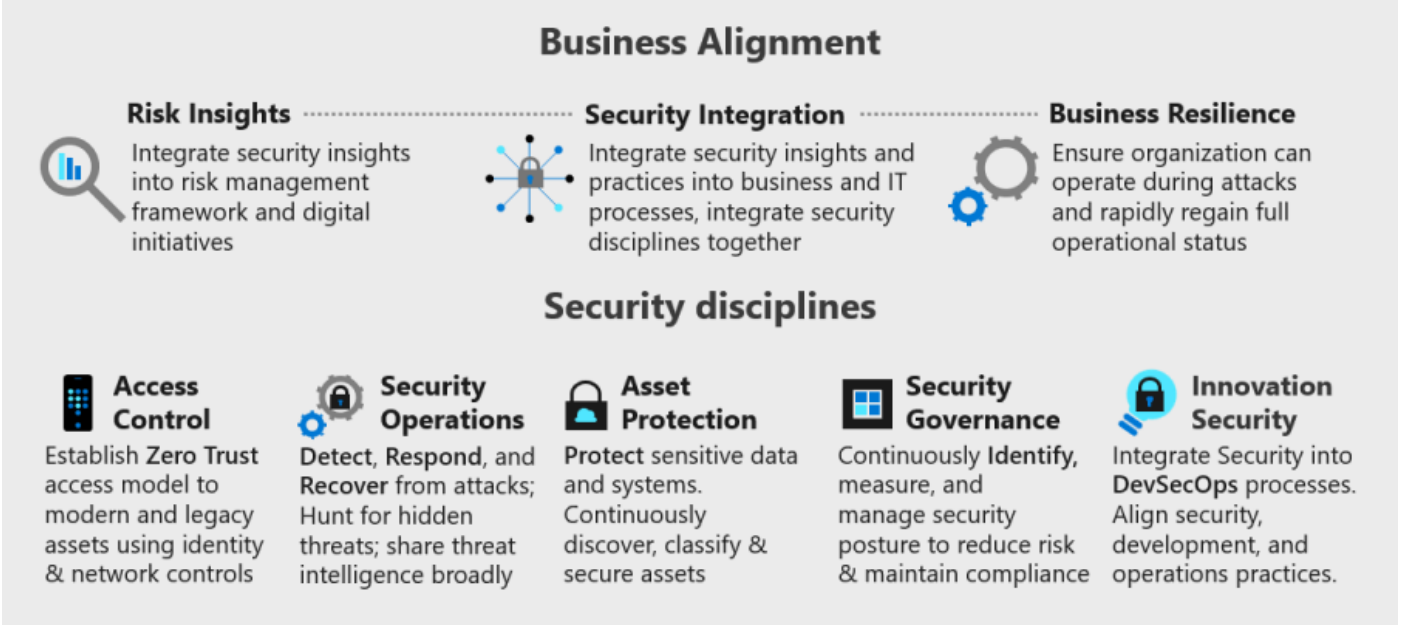
How would I know that I'm doing correct things?

Cloud Adoption Framework

Microsoft has collected best practices from themselves, partners, and customers. This is called Cloud Adoption Framework. It follows full lifecycle of cloud adoption.



CAF has a security component that takes business requirements and matches to security methods.

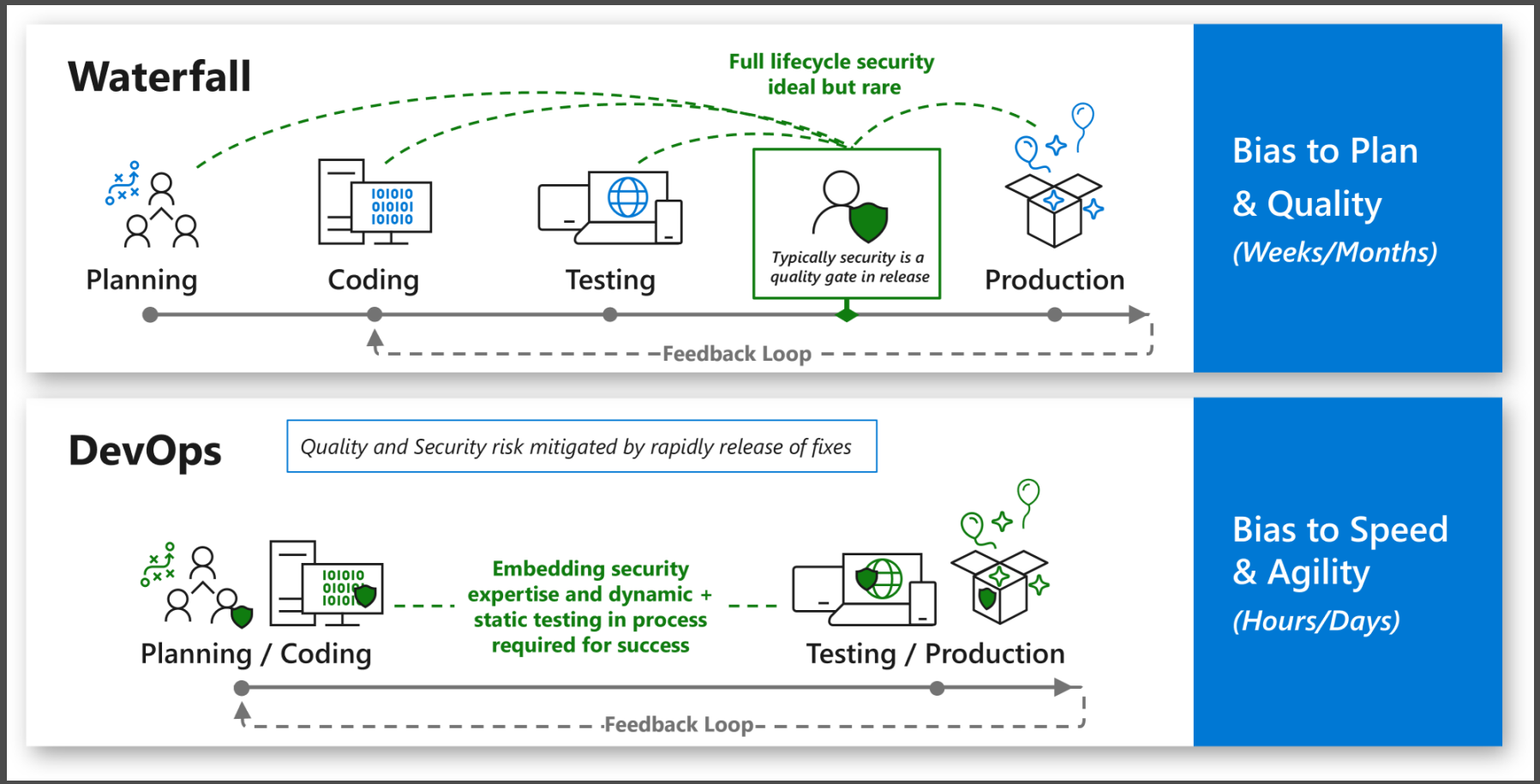


Well Architected Framework

Another important framework is Well Architected. It has guiding themes to improve quality of a solution.

Pillar	Description
Reliability	The ability of a system to recover from failures and continue to function.
Security	Protecting applications and data from threats.
Cost Optimization	Managing costs to maximize the value delivered.
Operational Excellence	Operations processes that keep a system running in production.
Performance Efficiency	The ability of a system to adapt to changes in load.

Well Architected Framework security pillar



DevSecOps

Brings security into development process if you start to make solutions secure by design and "shifting left".

Microsoft Zero Trust Principles

Verify explicitly

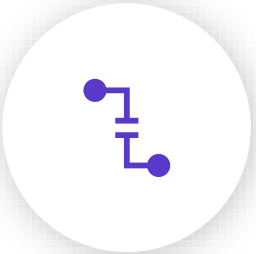
Always validate all available data points including

- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies

Use least privilege access

To help secure both data and productivity, limit user access using

- Just-in-**time** (JIT)
- Just-**enough**-access (JEA)
- Risk-based **adaptive** polices
- Data protection against **out of band** vectors



Assume breach

Minimize blast radius for breaches and prevent lateral movement by

- **Segmenting access** by network, user, devices, and app awareness.
- **Encrypting** all sessions end to end.
- **Use analytics** for threat detection, posture visibility and improving defenses

Securing your cloud

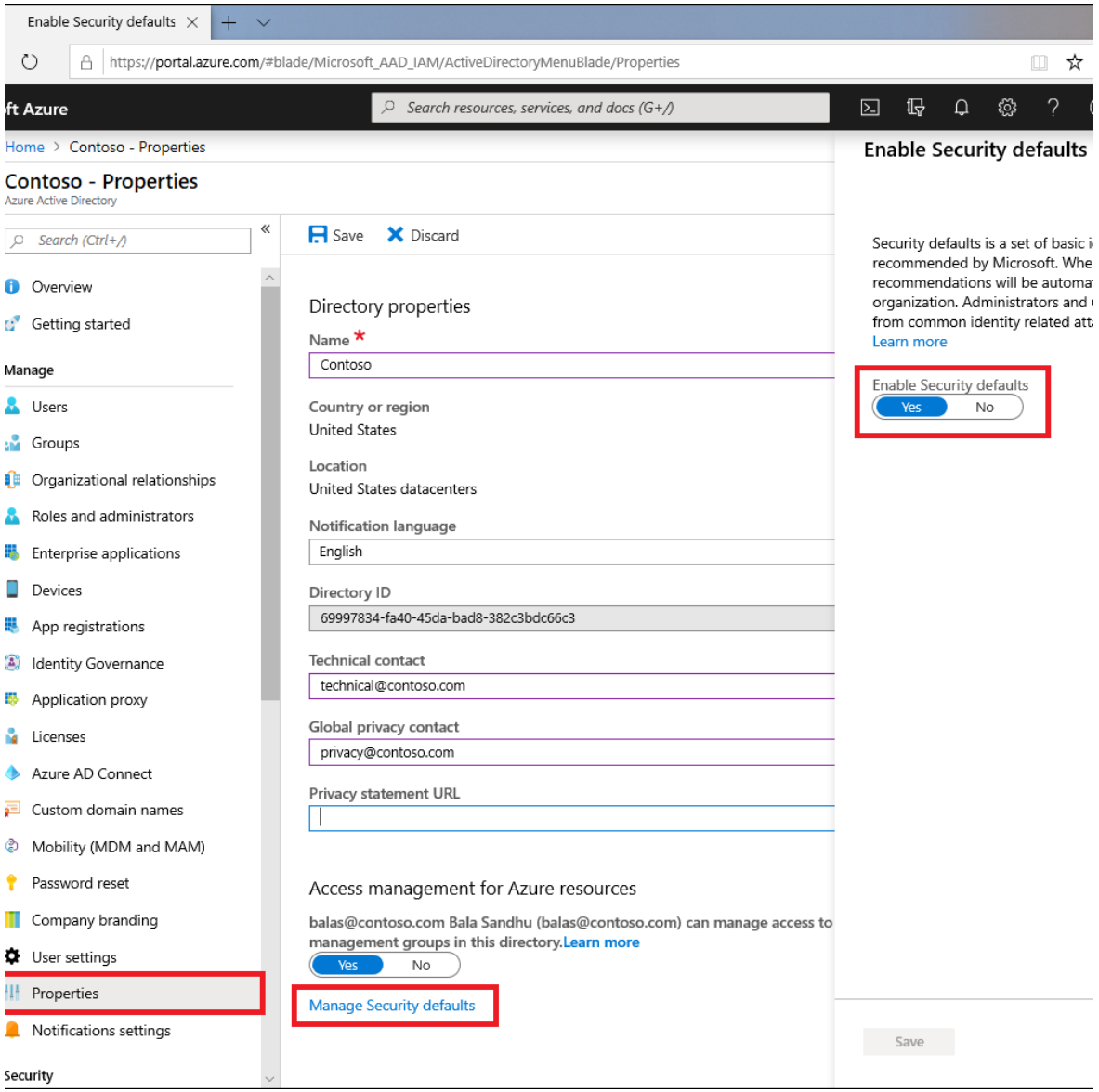
Or what to look out for and think about

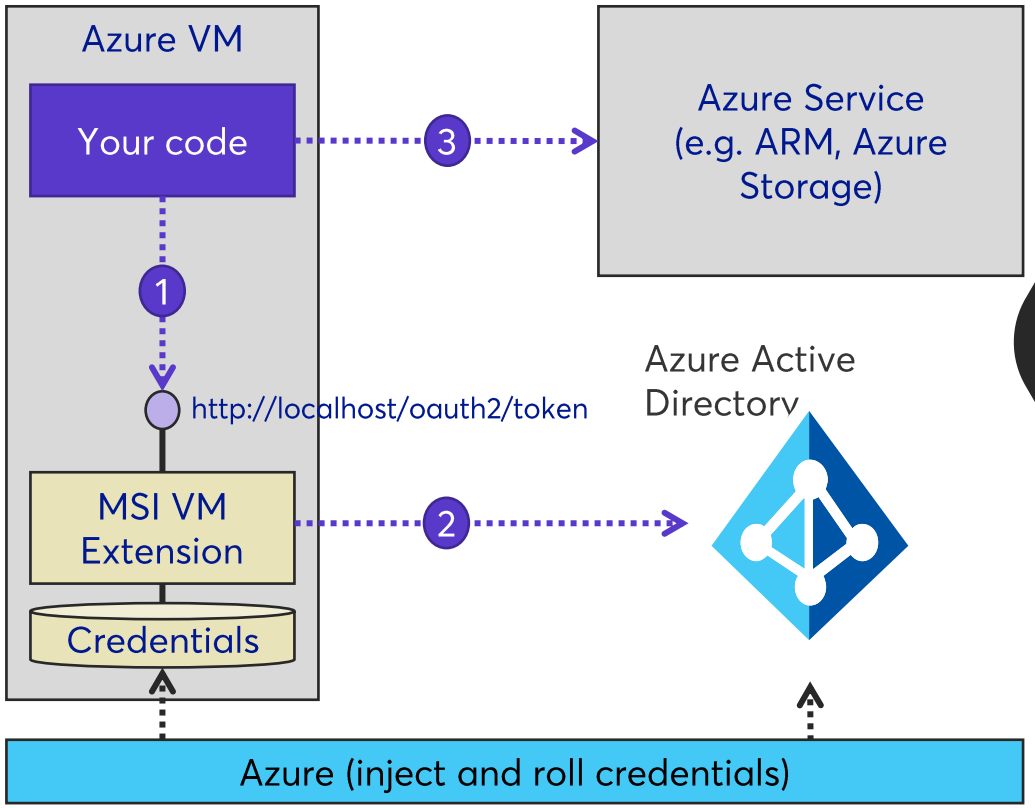
Identity & environment

Basically, just protect your accounts

- Separate your admin accounts
- MFA at the minimum
- Conditional access if you can

*Check out “Security defaults” if no licenses



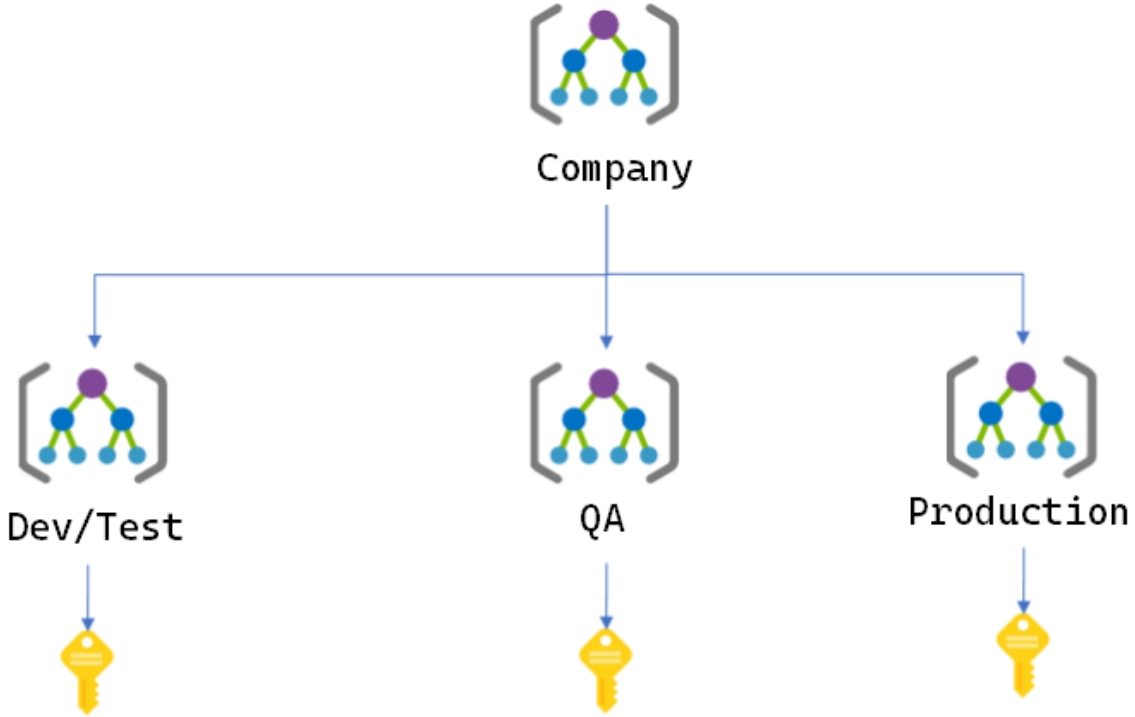


Managed identities for Azure resources

- Simplifies authentication/security for developers (vs. service principals)
- Authenticate to services without inserting credentials into code
- E.g., Allow (code running on) a specific VM to access Azure Key Vault, Storage Account, Azure SQL, etc.

Environment segmentation

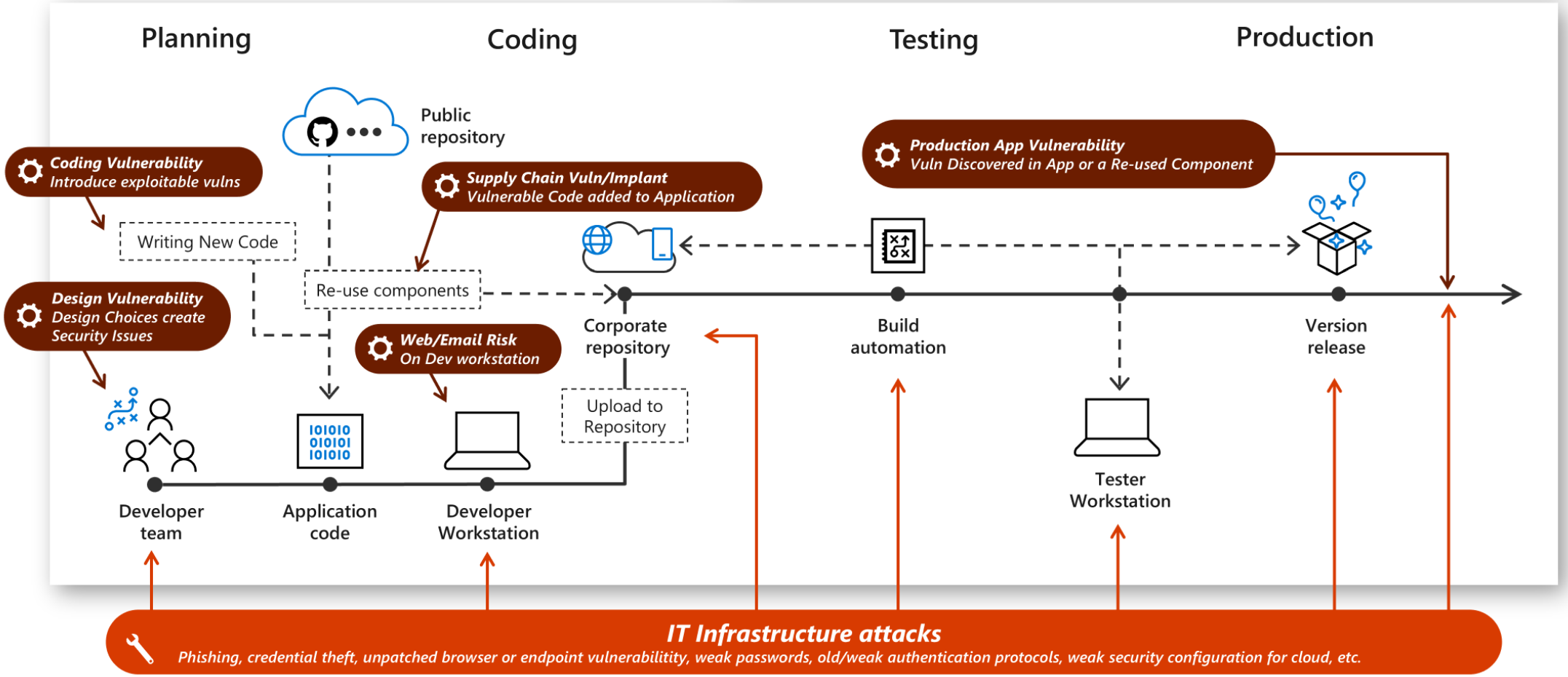
Consider splitting your development stages into separate segments with proper access strategy.




Code
security

Attacker Opportunities

Note: Attackers may conduct a multi-stage attack that increases their illicit access with stolen credentials, stolen keys, implanting malware, implanting backdoors in code, and more



Secure development

Attackers have plenty of vectors available to them.

Code review and add code analysis to continuous integration.

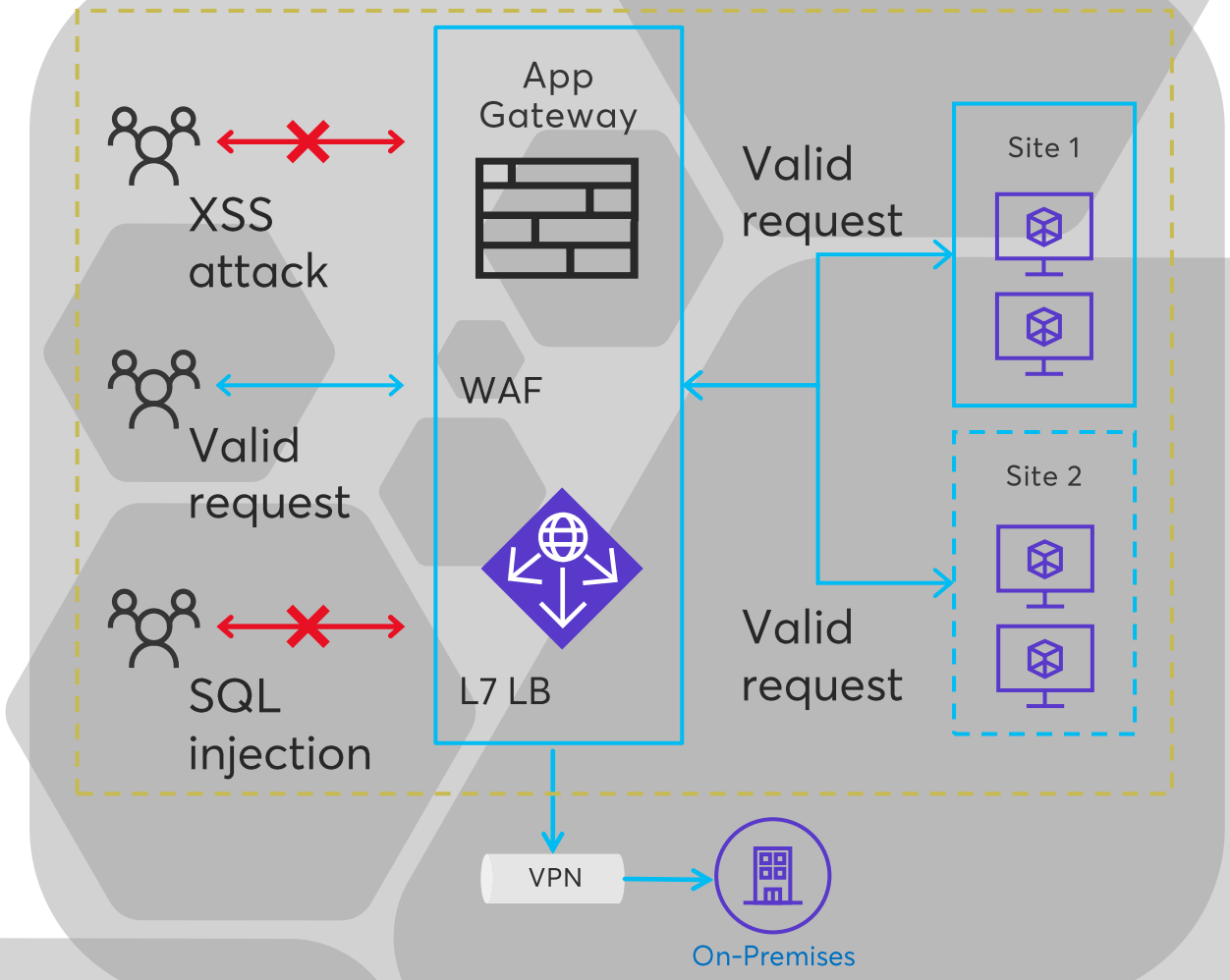
For example, SonarCloud that contains multiple static application security testing (SAST).

Also gate approvals in process

Pipeline secrets management & Key Vault

- Sounds stupid but a lot of people have secrets in their code. Just don't do it.
- Key Vault is a secret store: it's a centralized cloud service for storing application secrets.
- Key Vault keeps your confidential data safe by keeping application secrets in a single, central location and providing secure access, permissions control, and access logging.
- Always put your keys, certificates, secrets, and connection strings in a Key Vault

Network security

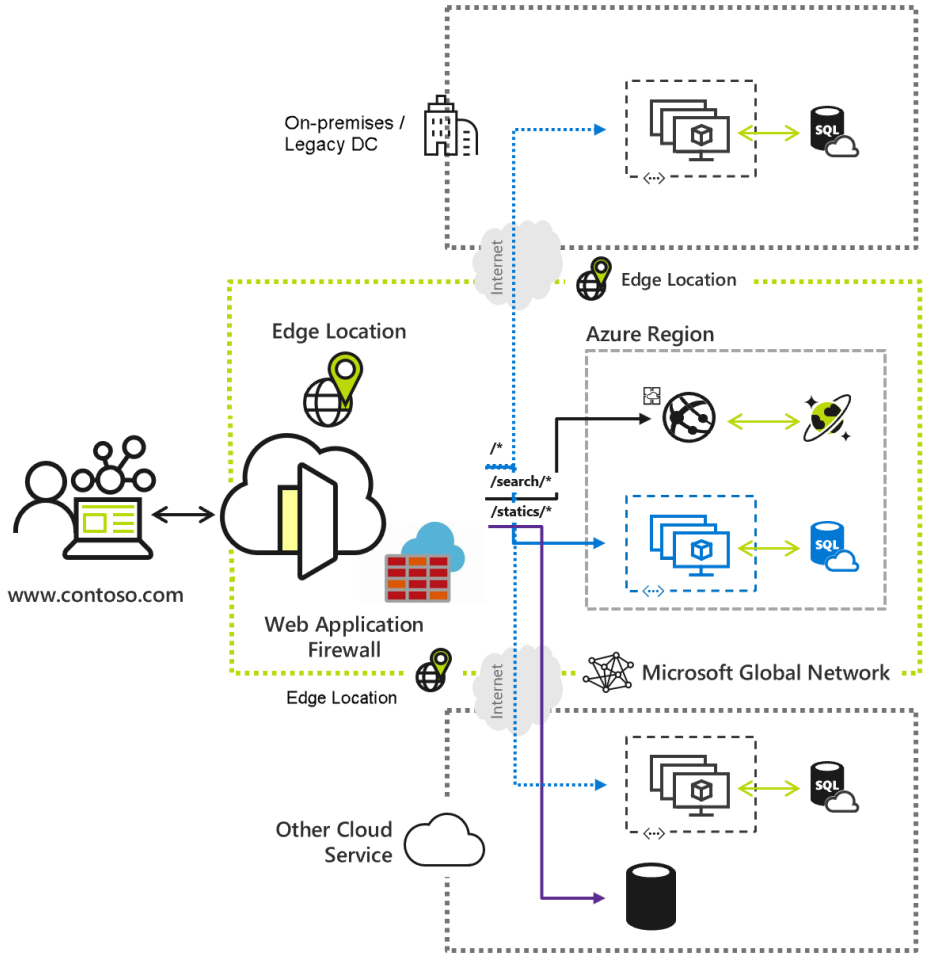


Web Application Firewall

- Protects your application against prevalent X-Site Scripting and SQL Injection attacks
- Blocks threats based on OWASP core rule sets
- Bot protection
- Custom rules like geo-block
- Integrated with Azure Security Center
- Real-time logging with Azure Monitor

Azure Front Door

Content Delivery Network (CDN) that provides fast, reliable, and secure access between your users and your applications' static and dynamic web content.



Azure DDOS Protection

- Tuned to your apps
- Logging, alerting and telemetry via Azure Monitor
- L7 Protection via Web App Firewall (WAF)
- Availability Guarantee and Rapid Response Support

Always on L3/L4 attack protection

Deployed today in all Azure regions

No additional charge and available to all Azure Customers

Vnets are so legacy… but secure your service access

Private Endpoints

Network interface for your service with private ip in your subnet

Service Endpoints (Service Tunnel)

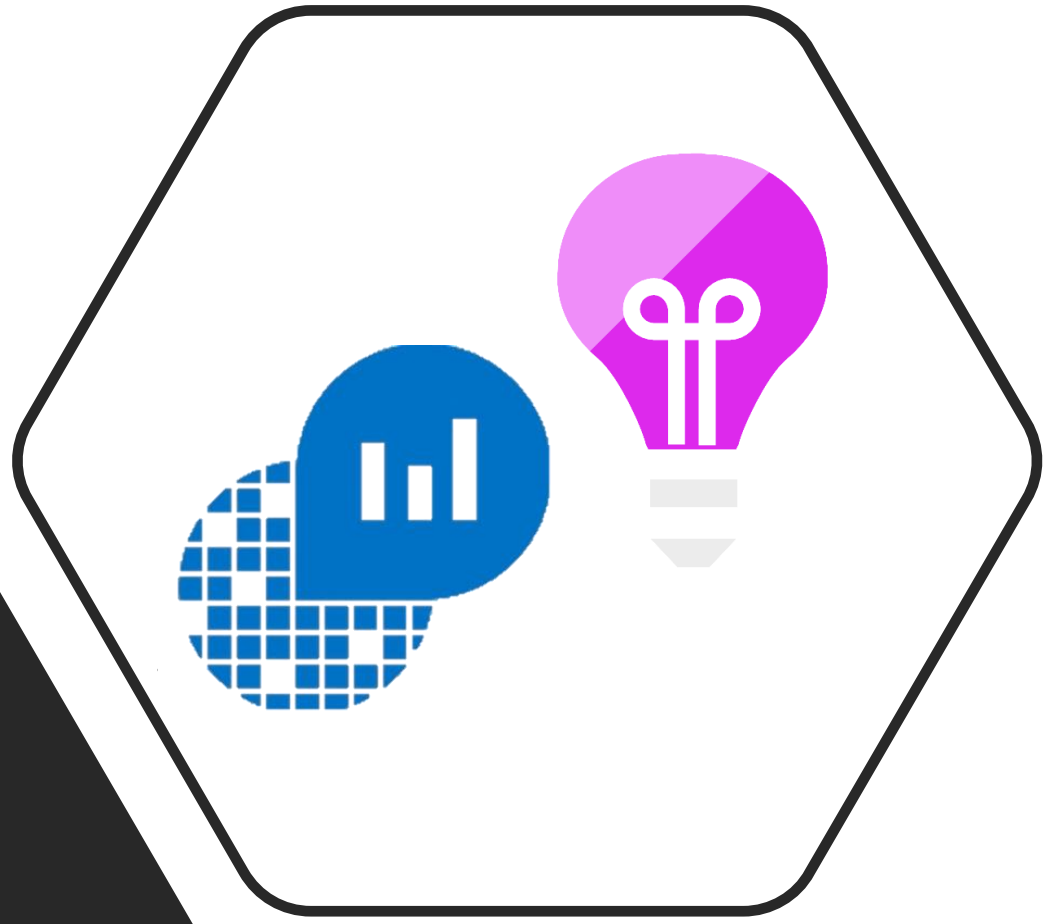
Additional path of availability of service into your subnet

VNet Service Injections

Private dedicated instance available only via private IP addresses within your subnet

Logging & Monitoring

Monitor the shit out of your environment



Critical Logs

- Azure Activity
- Azure AD Activities
- Azure AD Identity Protection alerts
- NSG Logs (deny rule violations)
- Azure Key Vault
- Application Gateway / Front Door
- Business Critical Applications

Azure Sentinel

Collect

Microsoft Services

Apps, users, infrastructure

Public Clouds

Security solutions

Analyze & detect threats

Machine learning, UEBA

Investigate & hunt suspicious activities

Interactive Attack Visualization, Azure Notebooks

Automate & orchestrate response

Playbooks

Enrichment with Intelligence (Geo location, IP Reputation)

Data Ingestion

Data Repository

Data Search

Azure Monitor (log analytics)

Integrate

ServiceNow

Other tools

Community

Thank You

meltlake°