



CLOUD DAY 2020

29 OTTOBRE • #CLOUDDAY2020

PROTEGGERE UNA WEB APP
SU AZURE:
LA MIGLIOR DIFESA È L'ATTACCO!

LORENZO BARBIERI
<https://publicspeaking.dev>



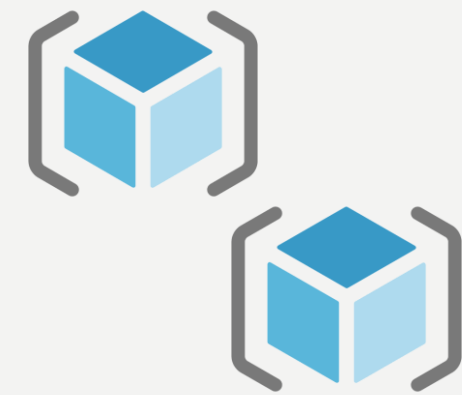
Kudos



managed/designs



EVERYTHING STARTS WITH A “GOOD” ARCHITECTURE



RG for
- Dev-Test
- Production



Web UI



RAW Photos
Thumbnails



Watermarking

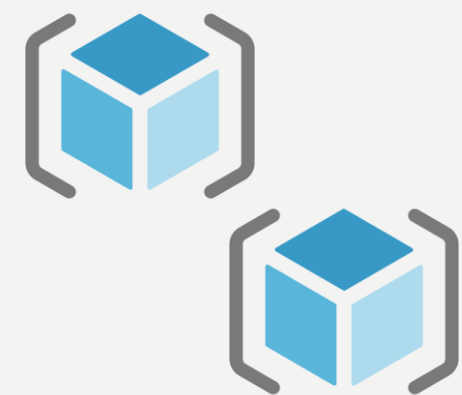


Users
Photos URLs



Photo resize





RG for
- Dev-Test
- Production



Web UI



Users
Photos URLs



RAW Photos
Thumbnails



Watermarking

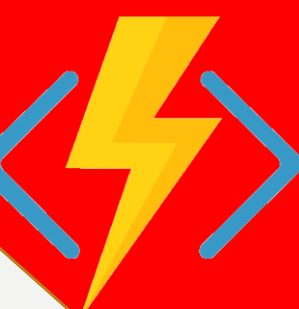


Photo resize

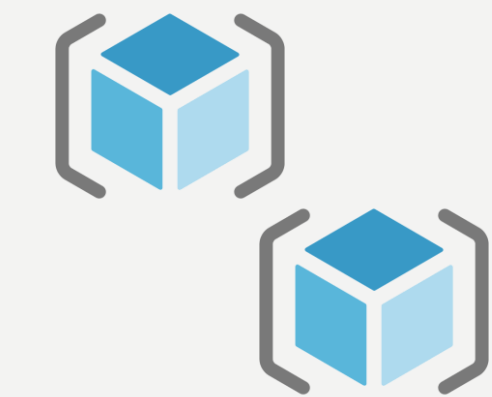
Attack
one!

Destroy
'em all!

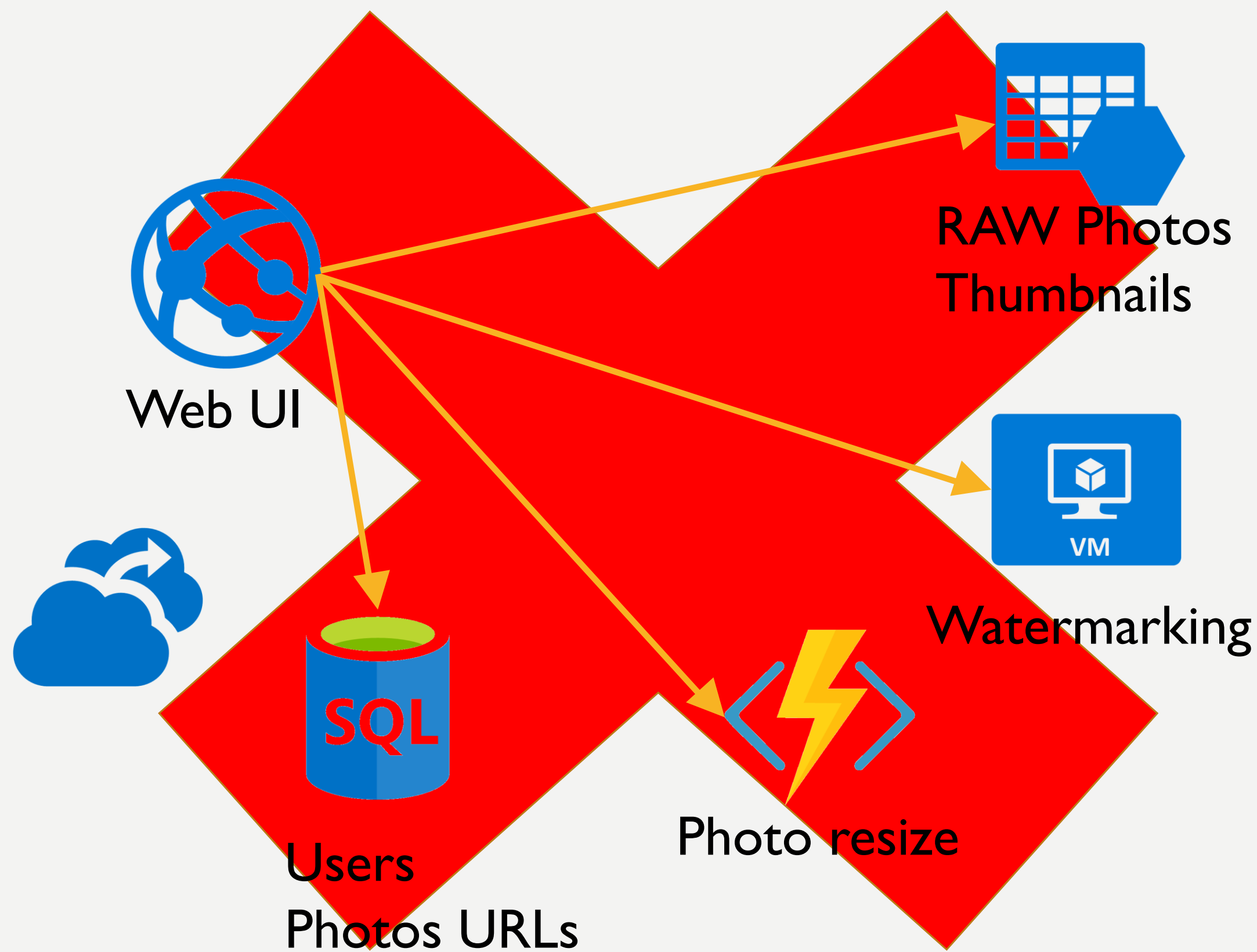


1ST STRIKE

The case of
disappearing
resources



RG for
- Dev-Test
- Production



MITIGATION

Infrastructure as Code:

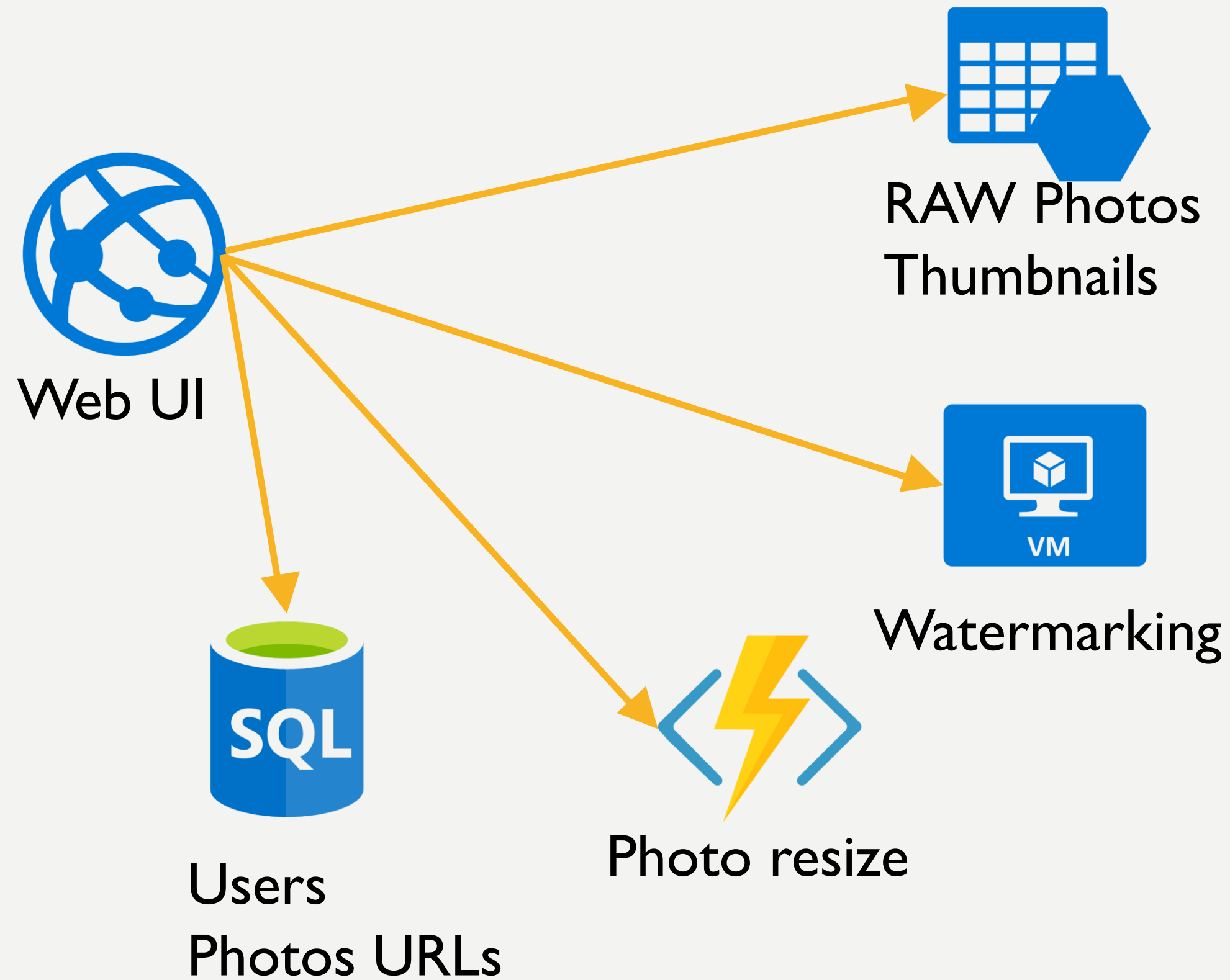
- Script & Backup everything
- ARM & Azure Policy

PaaS safeguards:

- Azure Web App Undelete
- SQL Point in time restore
- Blob Storage restore

Azure DevOps or GitHub





REMEDIATION

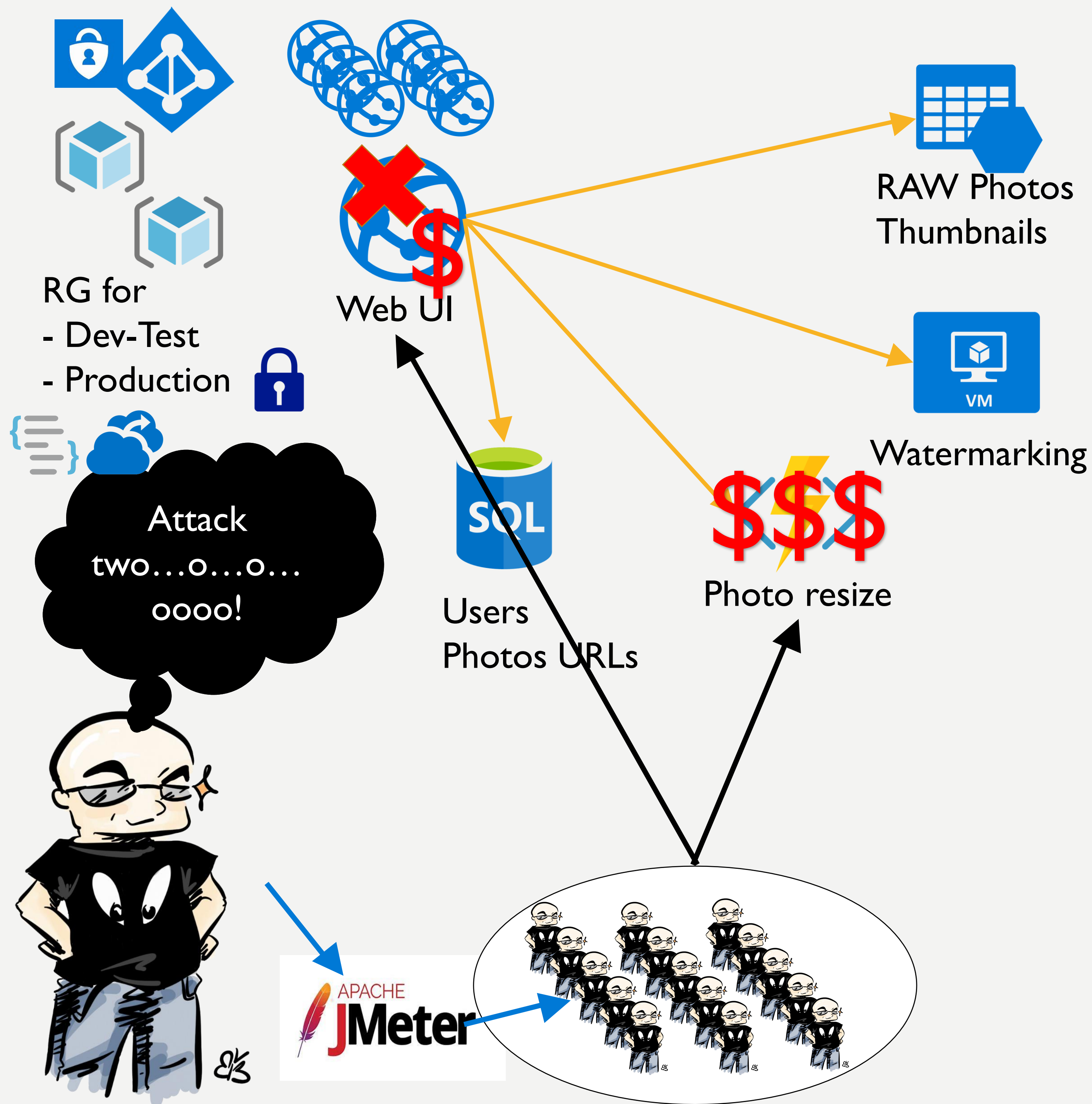
Subscription role
protection

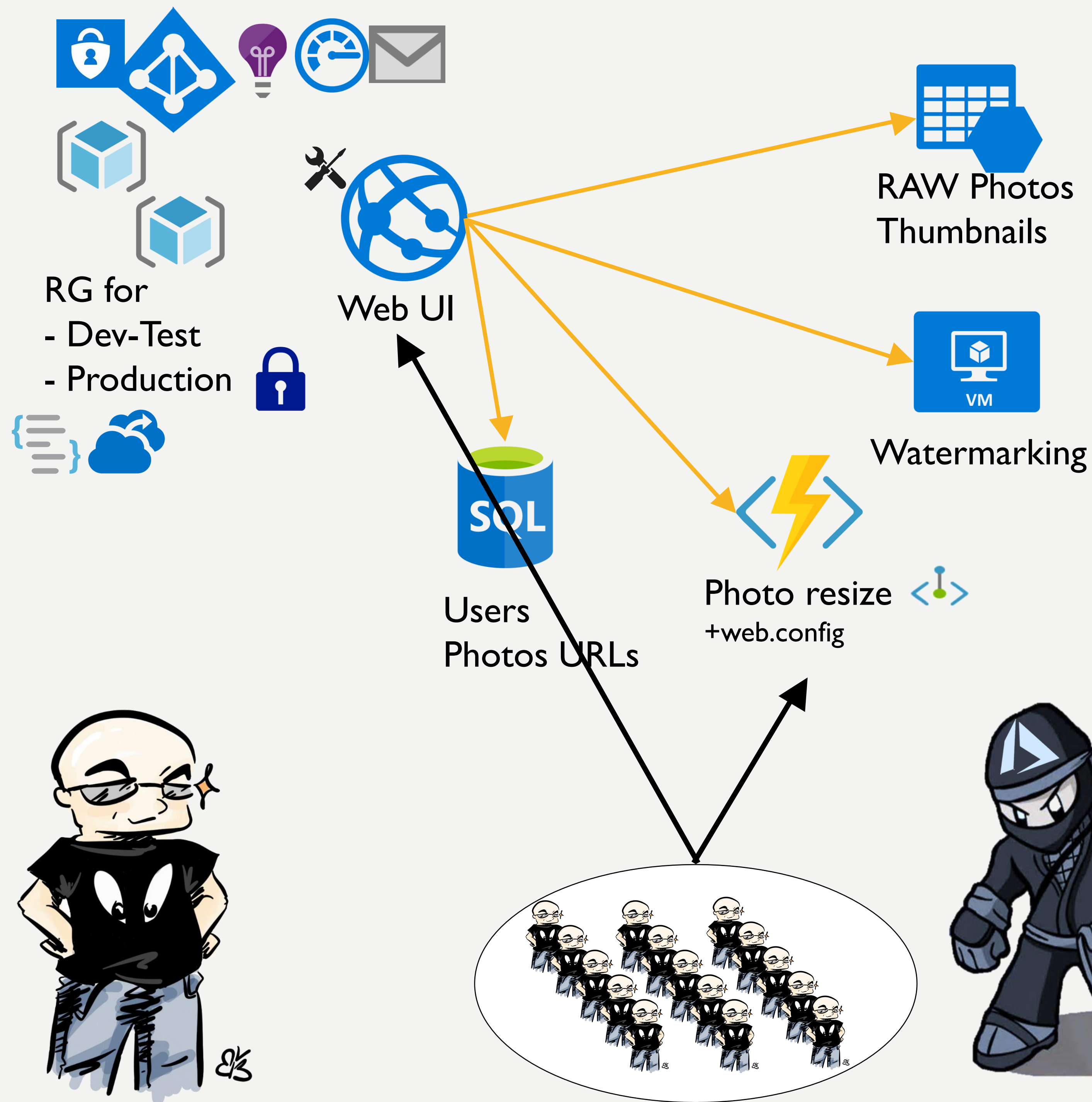
- RBAC

Azure AD could be
protected with MFA

Delete Locks

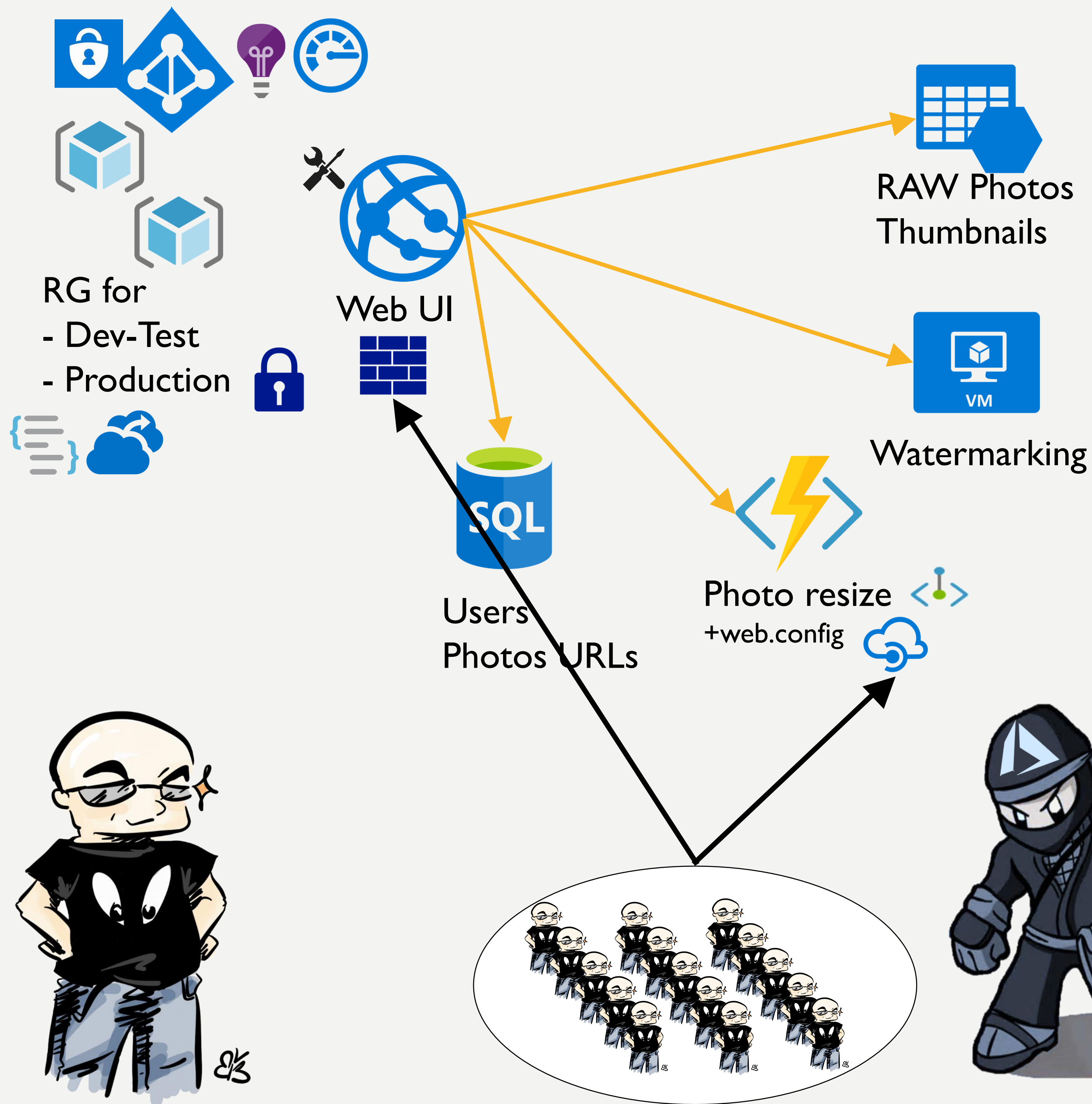






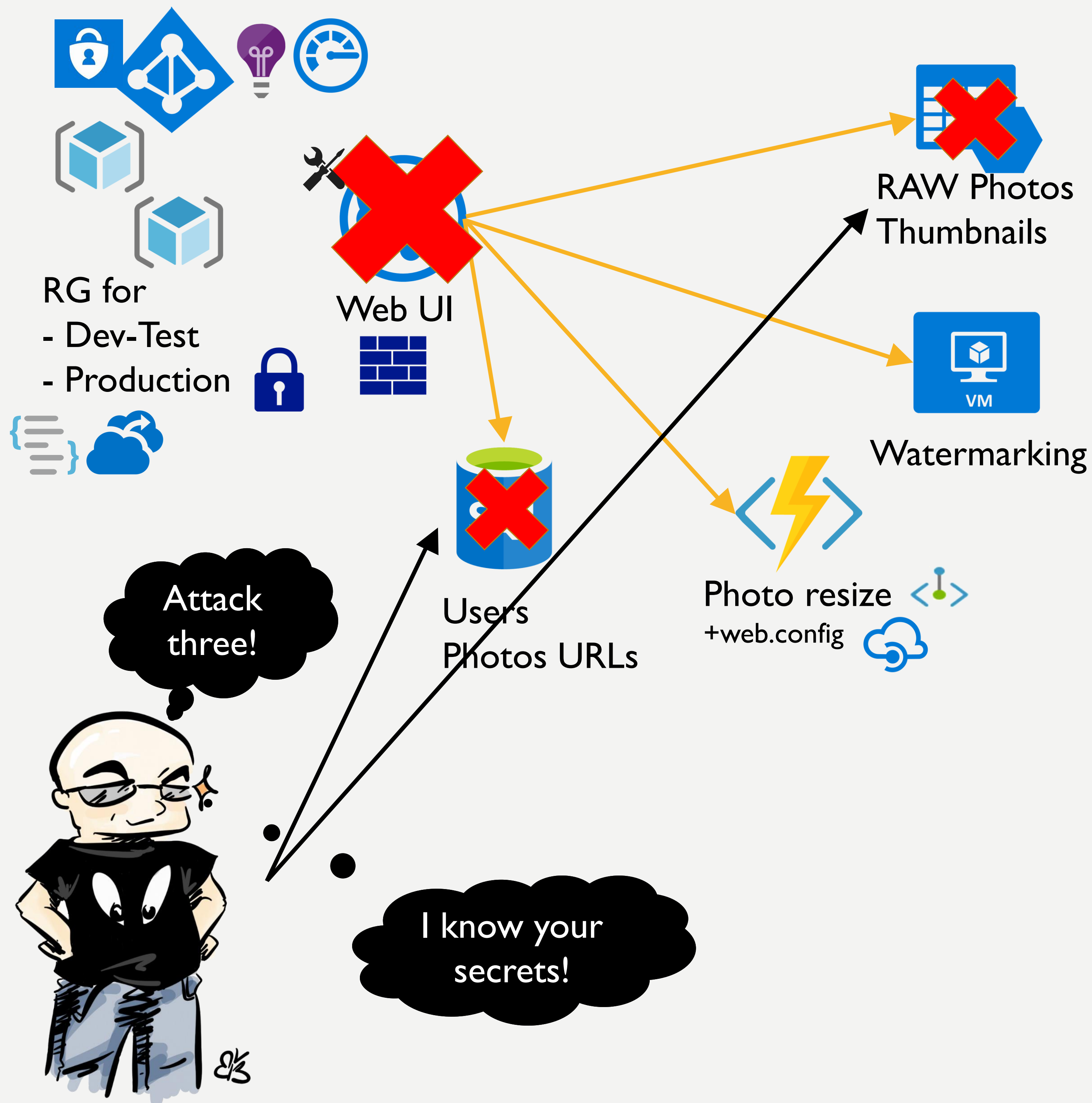
MITIGATION

- Alert rules and monitoring
- web.config based IP restriction OR Private Endpoint
- Functions in App Service Plan
- GB*s daily quota
- App Service Diagnostics



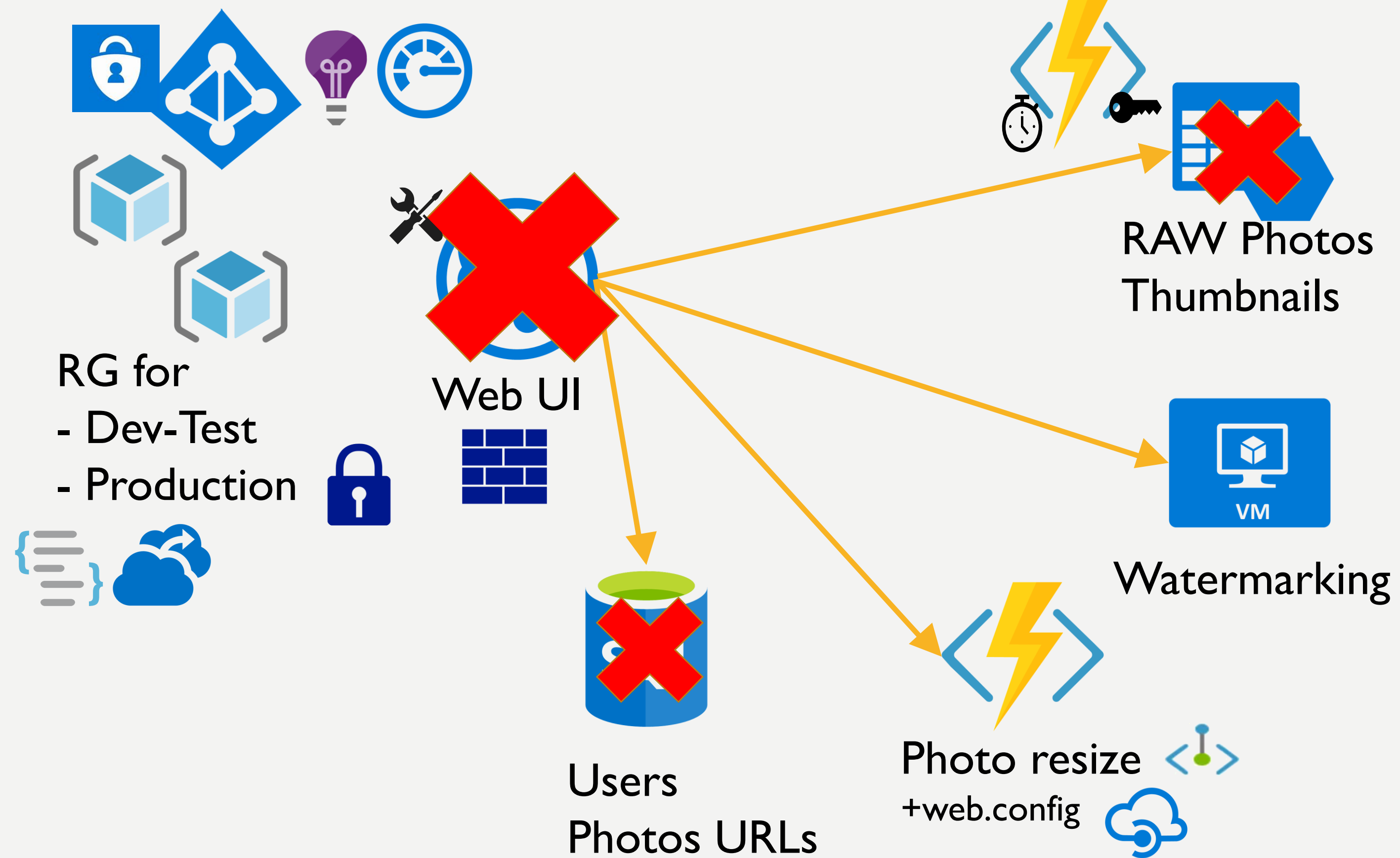
REMEDIATION

- Web App
Firewall/Azure
Firewall/Application
Gateway/3rd party
- API Management
- Azure DDOS
Protections for VNET



3RD STRIKE

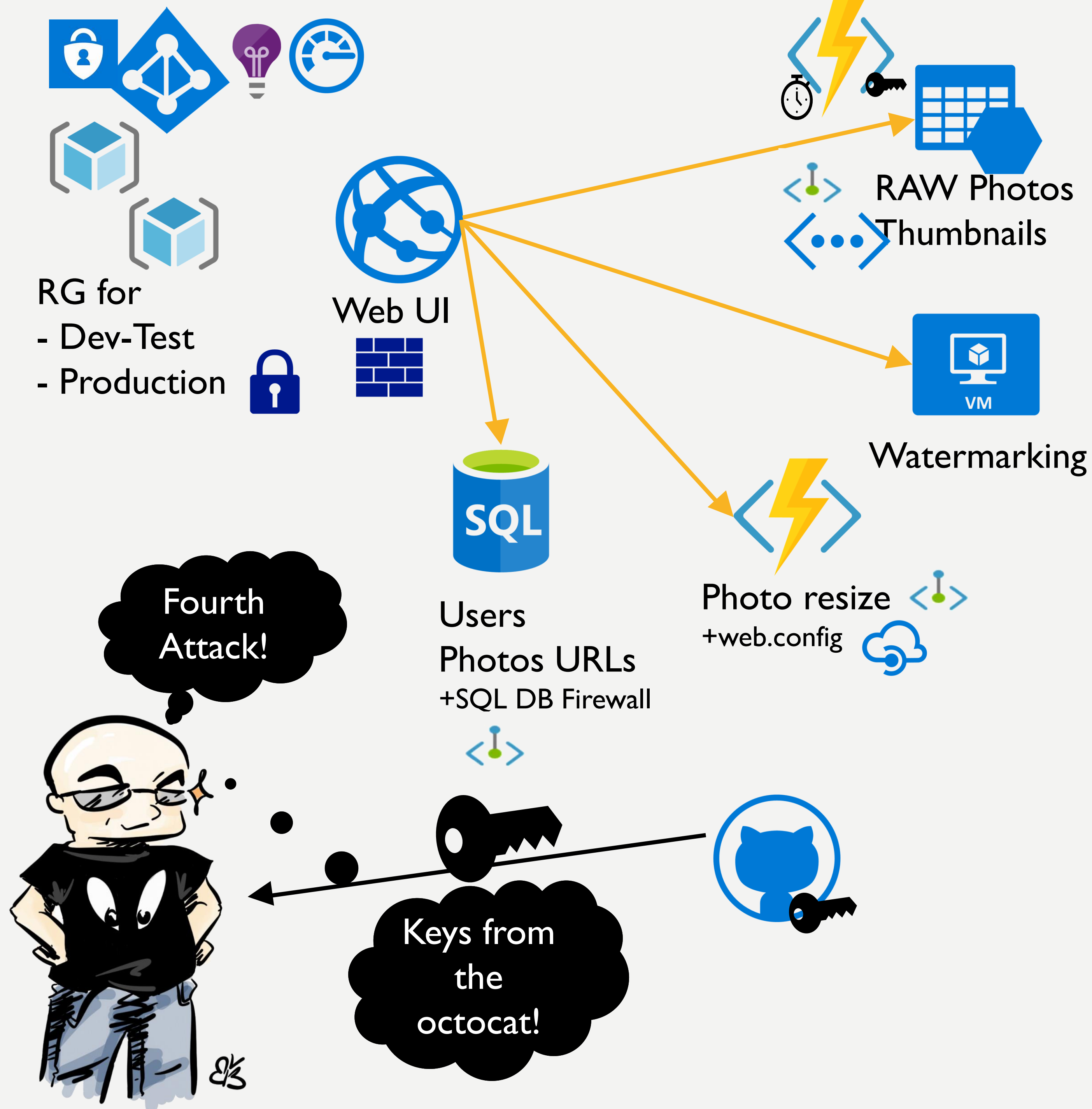
The case of
data and
storage loss



MITIGATION

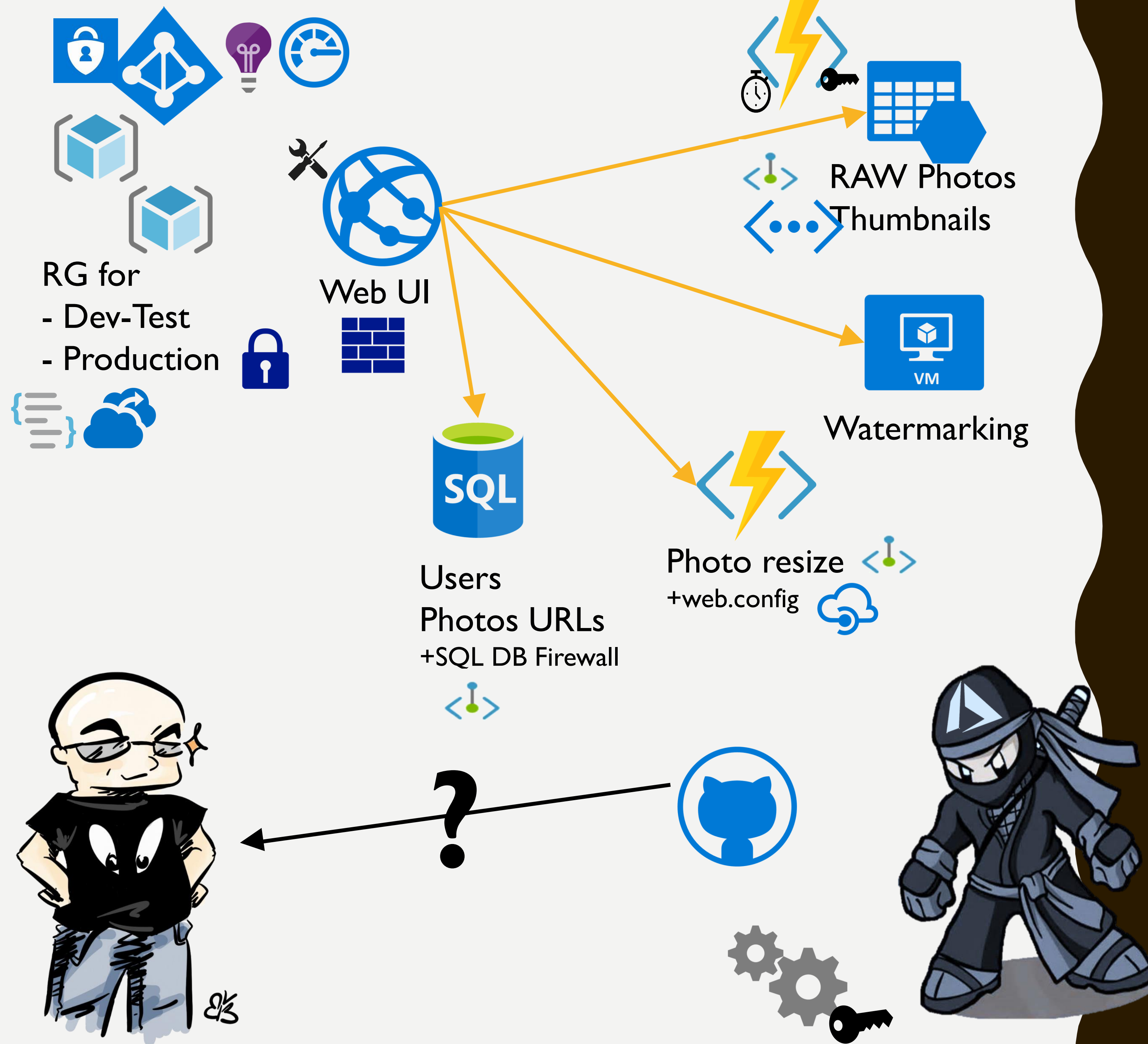
- Key rotation
- Least user privilege (DB)
- Alert





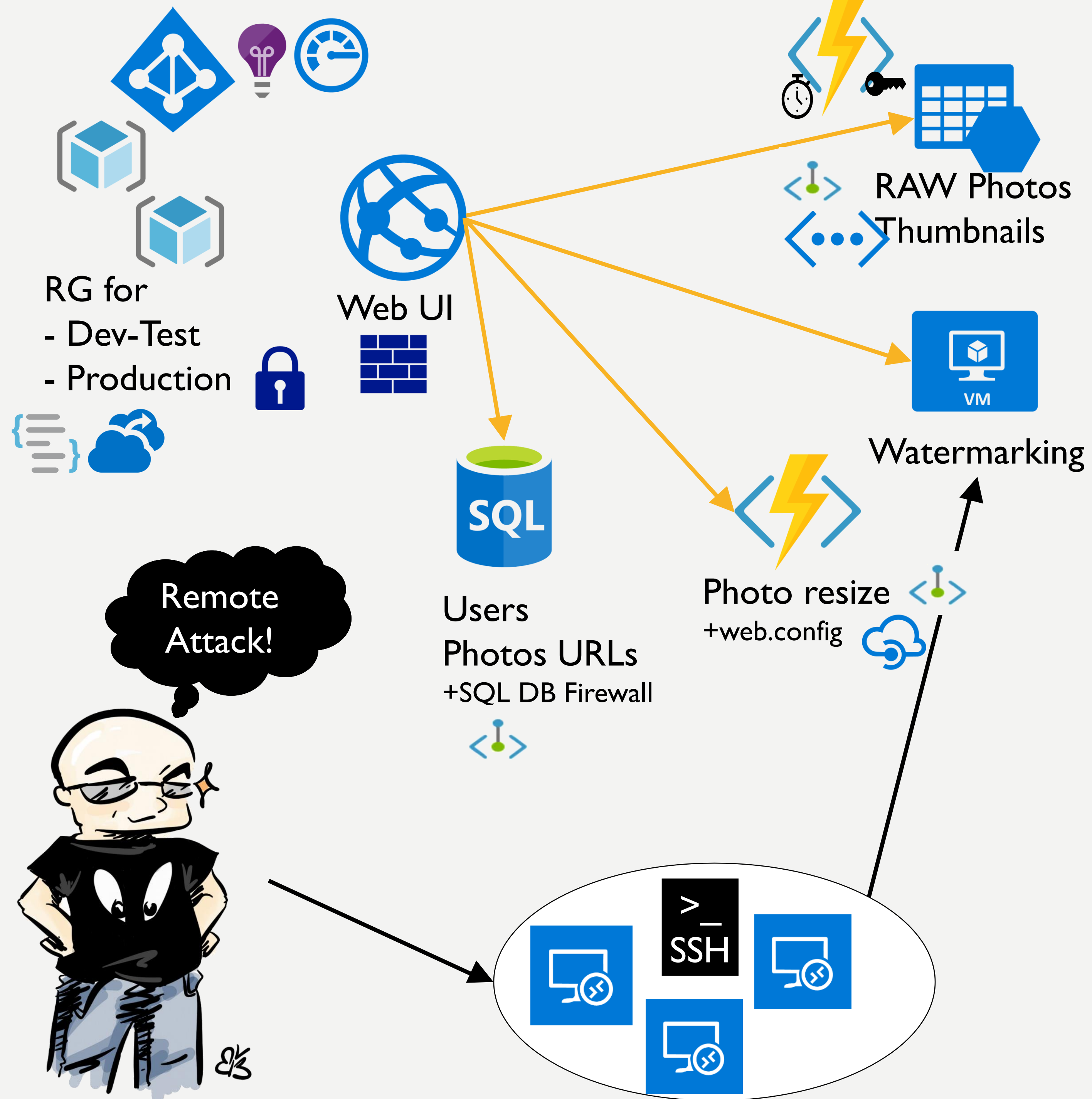
4TH STRIKE

The case of
being Gitted



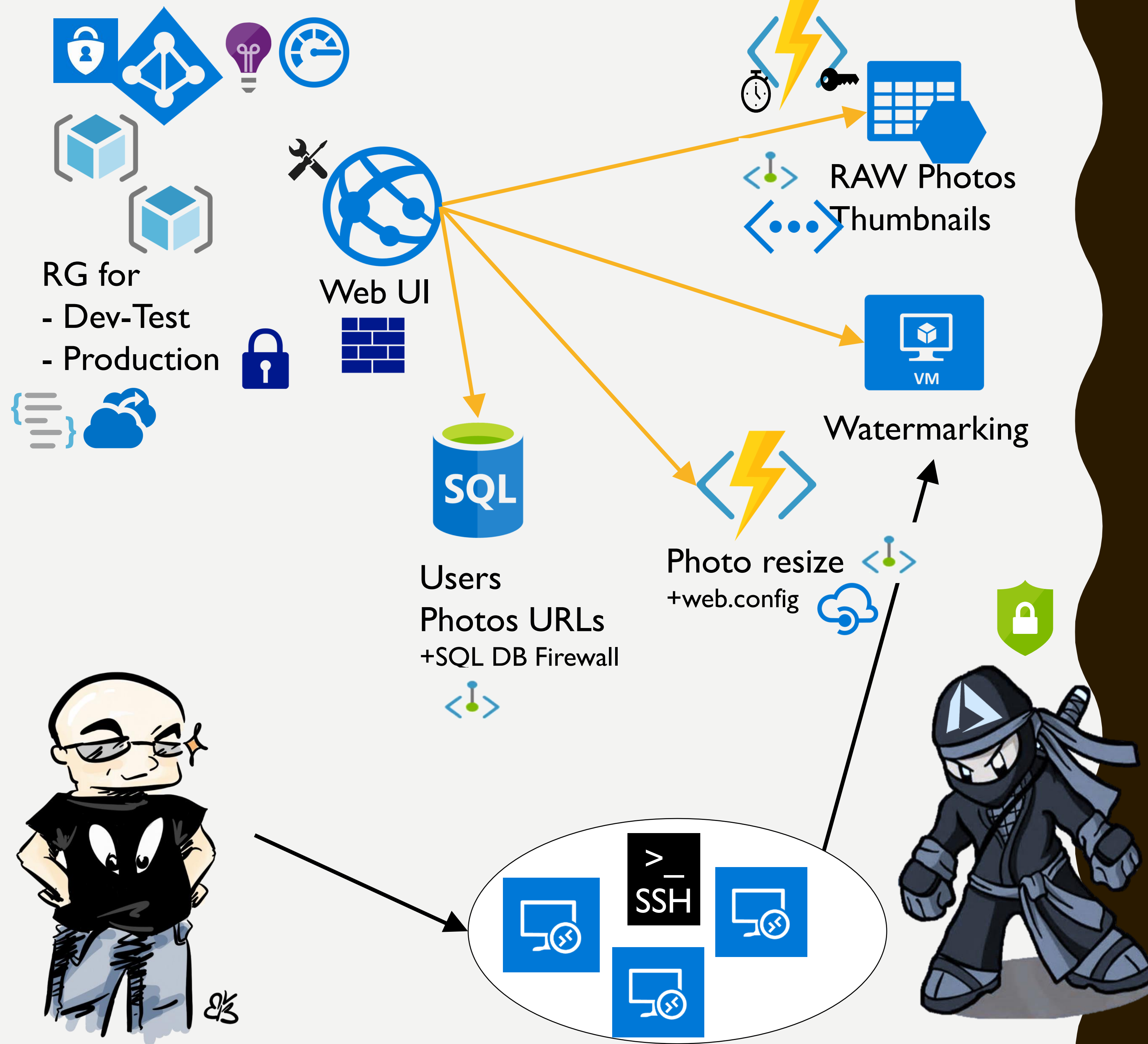
REMEDIATION

- Move all the keys to a secure path
- Use Azure Pipelines or GitHub Actions to set them before deployment
- Azure Key Vault
- Managed Service Identity



5TH STRIKE

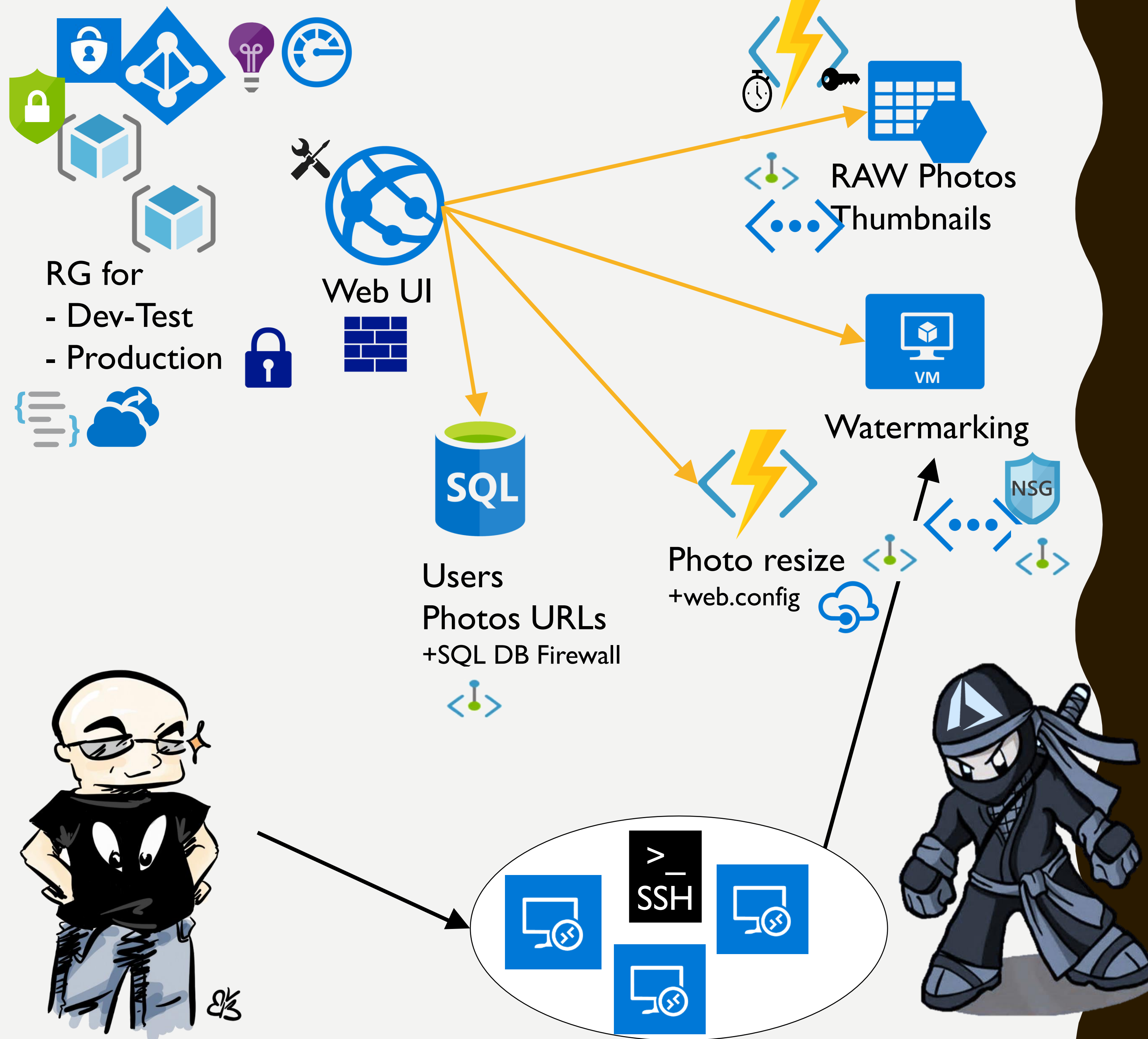
The case of
remote
connections



MITIGATION

- Patching and security policies
- Azure Security Center

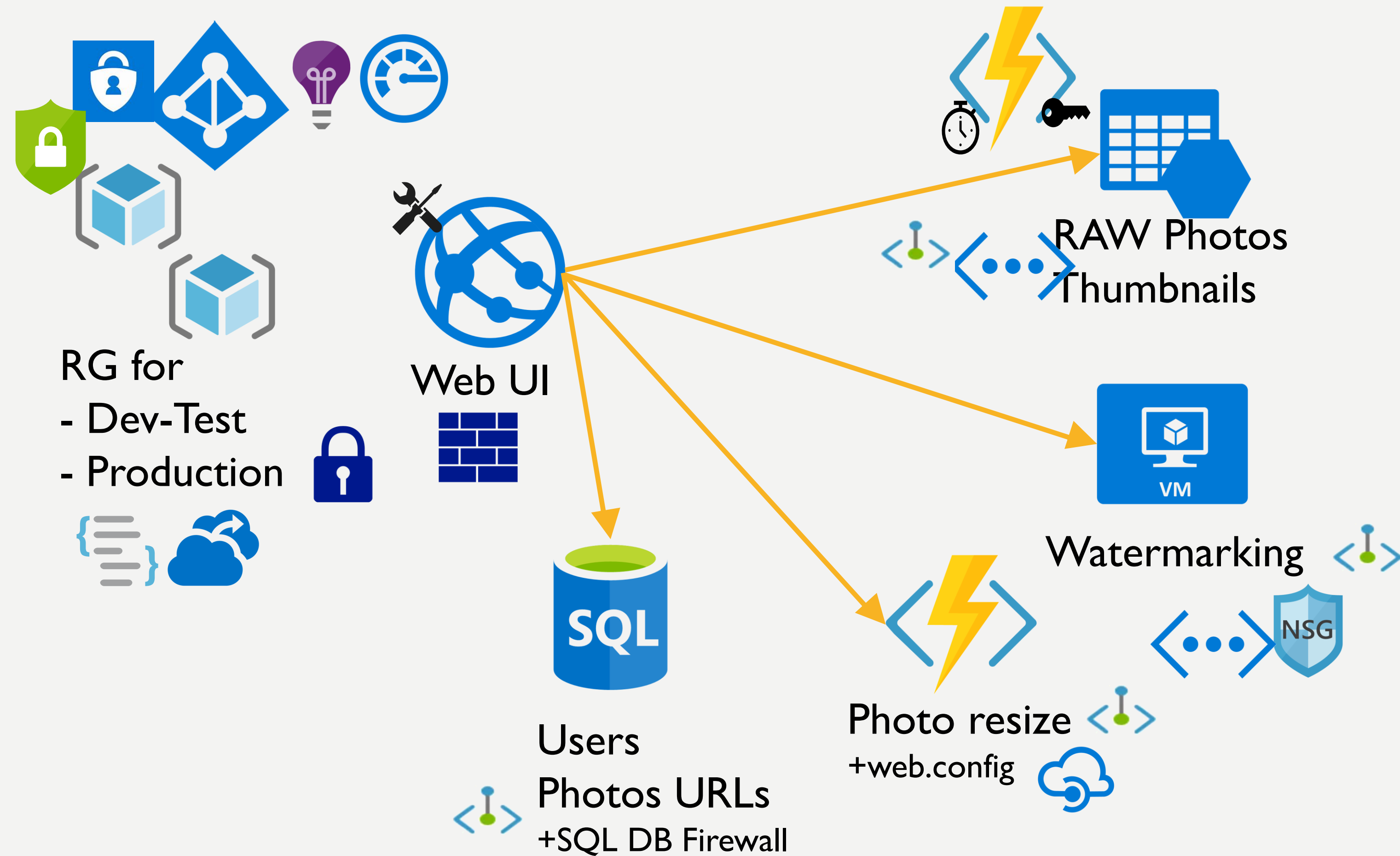
Not only for VMs, could check networks, App Services, Blob Storage, SQL, etc...














REMEDIATION

- Network Security Groups
- VNET
- Private Endpoint

A BETTER ARCHITECTURE



RECAP – THE 7 GOLDEN RULES

- Script everything 
- Backup everything 
- Least user privilege    
- Trust no one 
- Monitor everything  
- Assume cloud failure 
- Protect your secrets 





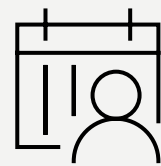
**WHAT IS DOING
MICROSOFT TO
SECURE AZURE?**

PHYSICAL DATACENTER SECURITY

Access approval

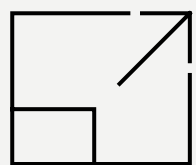


Background check

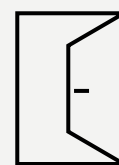


System check

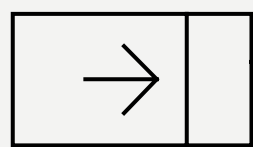
Perimeter



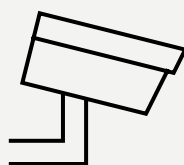
Perimeter fencing



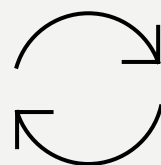
Front entrance gate



1 defined access point



Video coverage

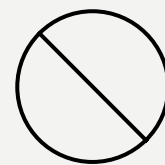


Ongoing roaming patrols

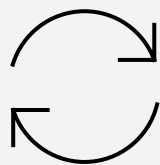
Building



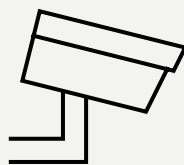
Two-factor authentication with biometrics



No building signage



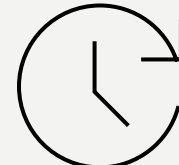
Ongoing roaming patrols



Video coverage

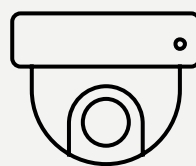


Verified single person entry

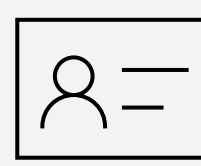


24x7x365 security operations

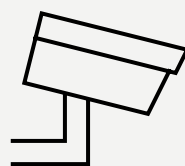
Server environment



Video coverage rack front & back



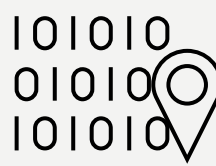
Employee & contractor vetting



Video coverage



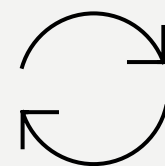
Metal detectors



Inability to identify location of specific customer data



Two-factor authentication with biometrics



Ongoing roaming patrols



Secure destruction bins

PROTECT DATA AND COMMUNICATIONS

Enable built-in encryption across resources

Azure Storage Service Encryption

Azure Disk Encryption

SQL TDE/Always Encrypted

Encrypt data while in use

Azure confidential computing

Use delegated access to storage objects

Shared Access Signature enables more granular access control

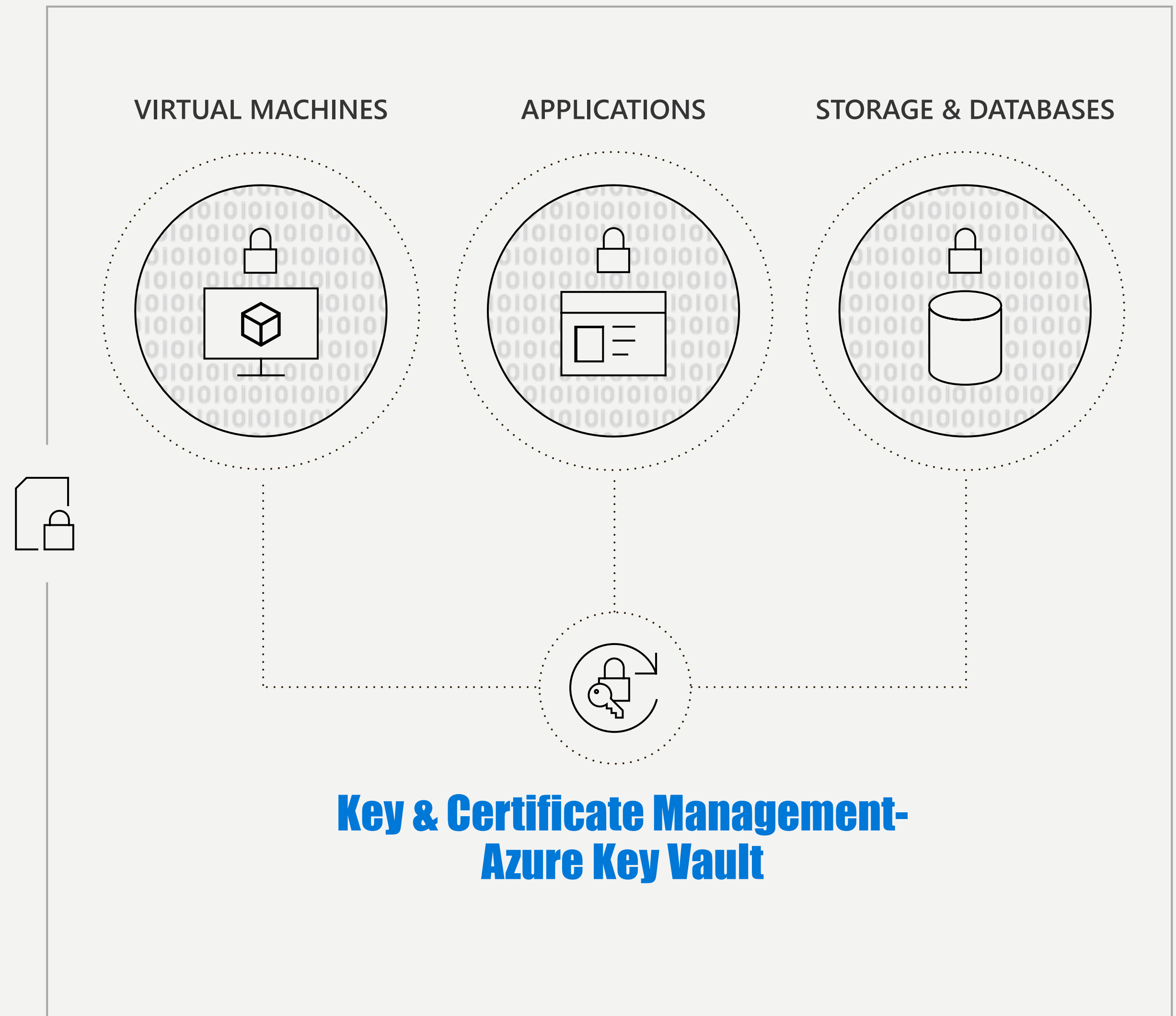
Use a key management system

Keep keys in a hardware HSM/don't store key in apps/GitHub

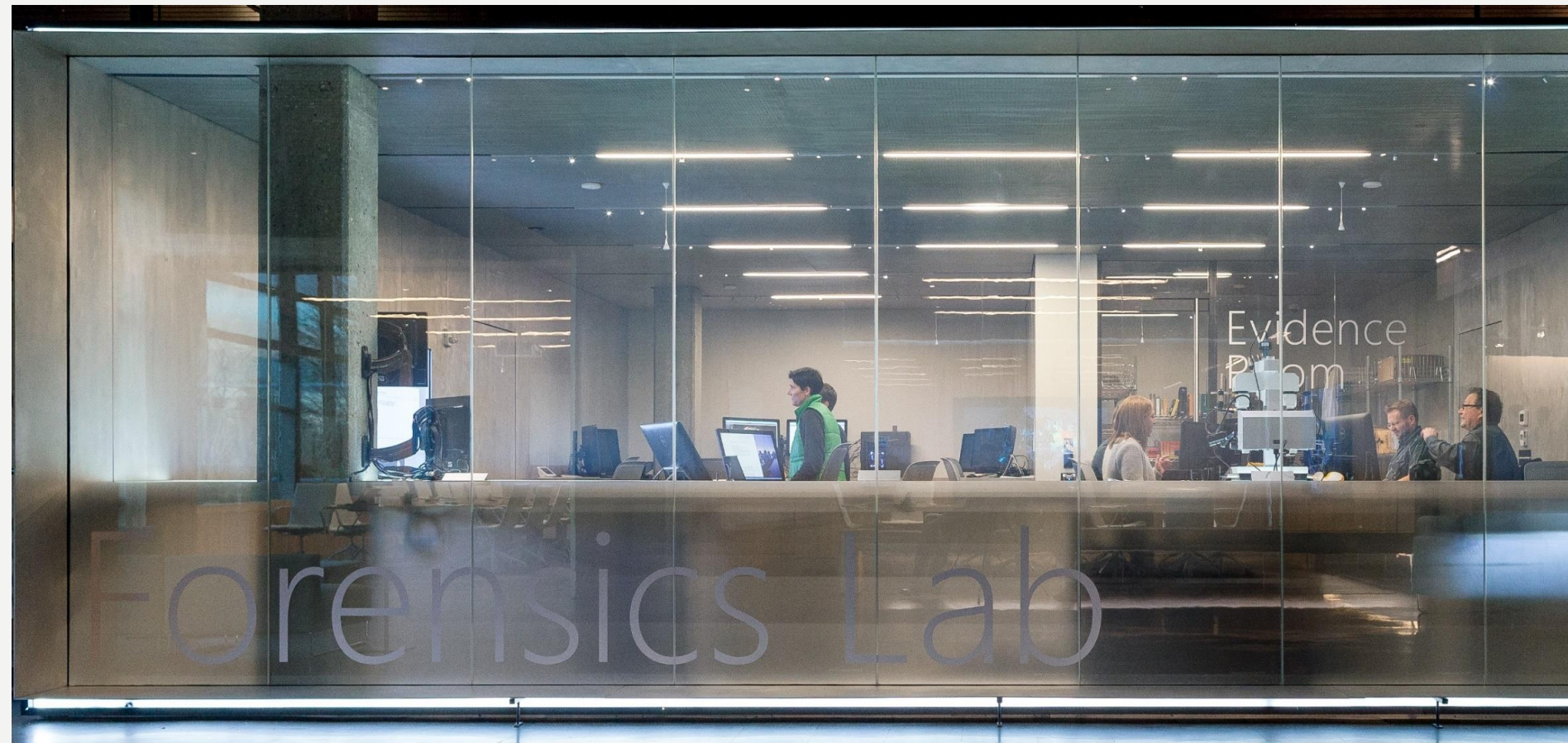
Use one Key Vault per security boundary/per app/per region

Monitor/audit key usage-pipe information into SIEM for analysis/threat detection

Use Key Vault to enroll and automatically renew certificates



TAKE A LOOK AT AZURE SECURITY CENTER



GENERAL

- Overview
- Getting started
- Events
- Search

POLICY & COMPLIANCE

- Coverage
- Security policy

RESOURCE SECURITY HYGIENE

- Recommendations
- Compute & apps
- Networking
- Data & storage
- Identity & access (Preview)
- Security solutions

THREAT PROTECTION

Connected solutions (3)

View all security solutions currently connected to Azure Security Center, monitor the health of solutions, and access the solutions' management tools for advanced

 **QualysVa1**
QUALYS, INC.
Vulnerability Assessment

Healthy

[VIEW](#)

 **CheckPoint-Firewall-Cen...**
CHECK POINT
Next Generation Firewall

Healthy

[VIEW](#)


 **QualysVaContoso**
QUALYS, INC.
Vulnerability Assessment

Healthy

[VIEW](#)

Discovered solutions (1)

Connect your security solution to Azure Security Center. View, monitor and get notified on solution health and security alerts.

 **Azure AD Identity Protec...**
MICROSOFT
Azure AD Identity Protection

Overview

Recommendations

17 Total

Partner solutions

2 Healthy

New alerts & incidents

1 0

Policy

Quickstart

Prevention

Compute

9 Total

Networking

8 Total

Storage & data

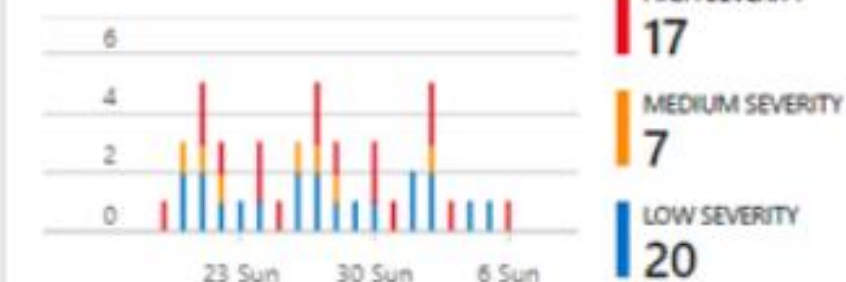
28 Total

Applications

4 Total

Detection

Security alerts



Most attacked resources

vm1	21 Alerts
vm3	9 Alerts
vm4	7 Alerts

Advanced cloud defense

Just in time VM access - last week







Application whitelisting

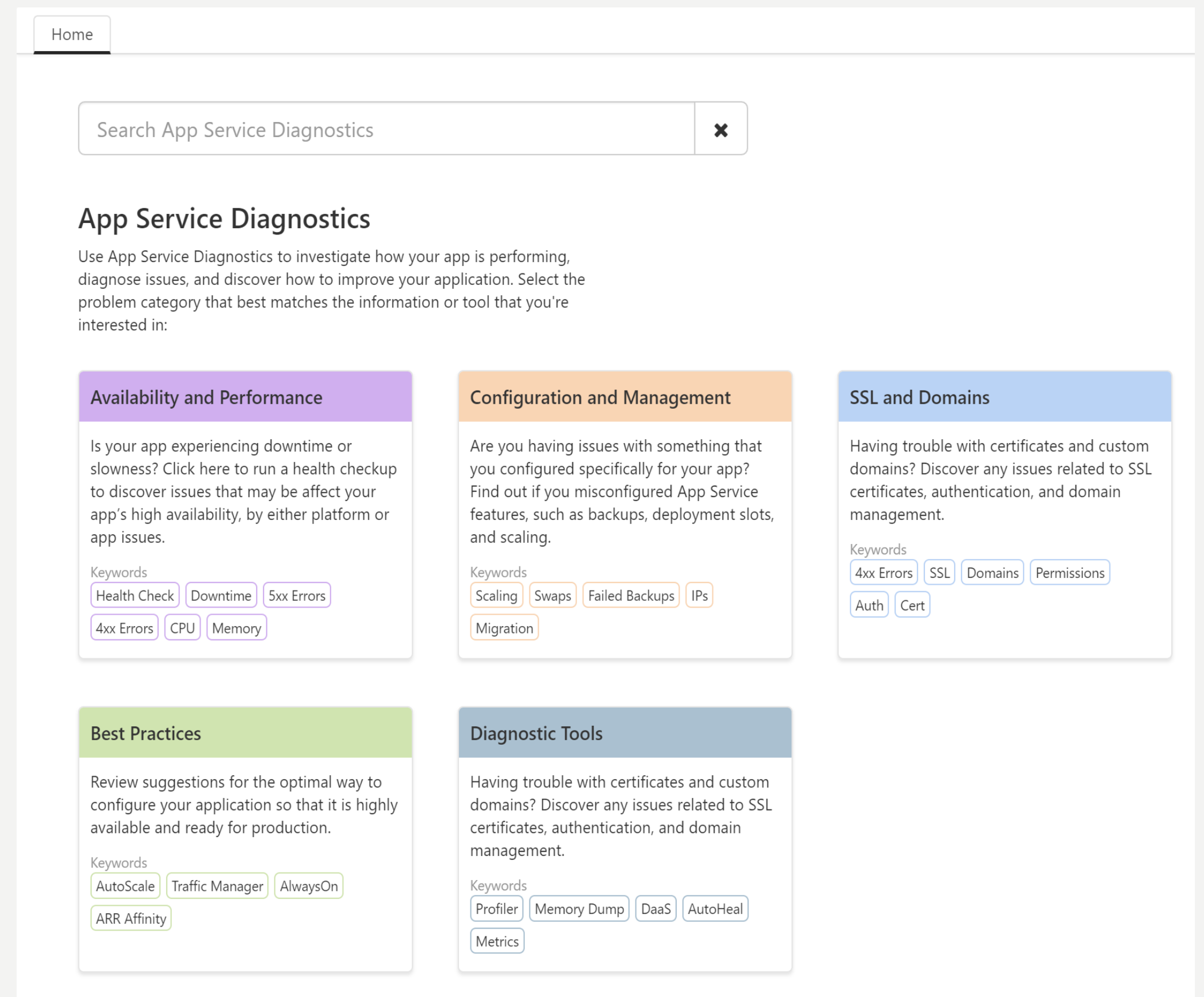
3 of 6 VMs configured

Violations Audited 1 VMs

Violated rules - changed manually 1 VMs

APP SERVICE DIAGNOSTICS

- An interactive and intelligent experience for self-troubleshooting your app issues
- What does that actually mean?
-  Diagnose and troubleshoot your app issues and learn about best practices
-  Use Genie to guide you through each problem category tile
-  Intelligent search capabilities
-  Straight out-of-the box, no extra configuration necessary



The screenshot displays the 'App Service Diagnostics' web application. At the top, there is a 'Home' tab and a search bar labeled 'Search App Service Diagnostics' with a close button. Below the search bar, the title 'App Service Diagnostics' is followed by a brief description: 'Use App Service Diagnostics to investigate how your app is performing, diagnose issues, and discover how to improve your application. Select the problem category that best matches the information or tool that you're interested in:'. The main content area features six category tiles arranged in a 2x3 grid. Each tile has a colored header, a description, and a list of keywords. The categories are: 'Availability and Performance' (purple header), 'Configuration and Management' (orange header), 'SSL and Domains' (blue header), 'Best Practices' (green header), and 'Diagnostic Tools' (blue header). The 'SSL and Domains' category is shown in two separate tiles. The keywords for each category are: Availability and Performance (Health Check, Downtime, 5xx Errors, 4xx Errors, CPU, Memory); Configuration and Management (Scaling, Swaps, Failed Backups, IPs, Migration); SSL and Domains (4xx Errors, SSL, Domains, Permissions, Auth, Cert); Best Practices (AutoScale, Traffic Manager, AlwaysOn, ARR Affinity); and Diagnostic Tools (Profiler, Memory Dump, DaaS, AutoHeal, Metrics).

Home

Search App Service Diagnostics

App Service Diagnostics

Use App Service Diagnostics to investigate how your app is performing, diagnose issues, and discover how to improve your application. Select the problem category that best matches the information or tool that you're interested in:

Availability and Performance

Is your app experiencing downtime or slowness? Click here to run a health checkup to discover issues that may be affect your app's high availability, by either platform or app issues.

Keywords

Health Check Downtime 5xx Errors

4xx Errors CPU Memory

Configuration and Management

Are you having issues with something that you configured specifically for your app? Find out if you misconfigured App Service features, such as backups, deployment slots, and scaling.

Keywords

Scaling Swaps Failed Backups IPs

Migration

SSL and Domains

Having trouble with certificates and custom domains? Discover any issues related to SSL certificates, authentication, and domain management.

Keywords

4xx Errors SSL Domains Permissions

Auth Cert

Best Practices

Review suggestions for the optimal way to configure your application so that it is highly available and ready for production.

Keywords

AutoScale Traffic Manager AlwaysOn

ARR Affinity

Diagnostic Tools

Having trouble with certificates and custom domains? Discover any issues related to SSL certificates, authentication, and domain management.

Keywords

Profiler Memory Dump DaaS AutoHeal

Metrics



publicspeaking.dev



lorenzo.barbieri@microsoft.com



@_geniodelmale

Thank you!

Feedbacks are important...

Tweet @_geniodelmale or send me an email 😊