Uw datacenter in de public cloud: veiliger of net niet?

Bart Verboven, Inetum-Realdolmen

Bart Verboven

Cloud Security Architect

Consultant since 2007
Working with Azure since 2015

Bart.verboven@inetum-realdolmen.world

Security principals

Security is a shared responsibility (and a team sport)

- Between vendor and tenant
- Between teams

Shift-left

- Security by design
- Don’t just build it and throw a firewall in afterwards

Defense in-depth

- There is no silver bullet

Good agreements make good friends (and also good security)

Rules of the game: Azure Governance (cloud adoption framework)

- Decide on responsibilities
- No hard line between apps and infra
- Ongoing process

Be a team player: Trust no one

- Technically enforce (Azure policies) (deny or auto remediate)
- Follow up in compliance center

Examples

- Enforce locations
- Deny public IP addresses on VMs
- Enforce encryption

Encryption

Microsoft Managed Keys

Customer managed keys

External HSM

Encryption at rest

- Server side encryption
- More and more bring your own key options
- Attention to IaaS disks!
- Azure Disk Encryption (ADE) bitlocker / dmcrypt
- Side note: data remains in chosen Azure Region

Secret management: secrets, keys, certificates : Key Vault

- Full API support, you can stop mailing PFX files
- Secrets in code are a big no

Encryption in transit / processing

- Confidential compute
- On the network: HTTPS exists since 1994, about time you use it.

Network Security

Think in layers

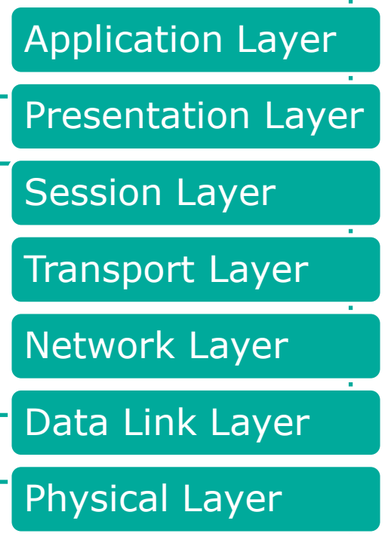
- The higher in the stack the better
- Microsoft takes care of the lowest levels
- Most components have built-in capabilities, use them!

Limit attack surface

- Private endpoints
- Service endpoints
- Access control lists

“classic” concepts remain valid

- Reverse proxy (application gateway)
- Network segmentation
- Next generation firewall



Authentication

Use modern protocols

- Azure AD
- Extend them with best practices like MFA
- Be wary of exposing basic authentication
- PaaS uses modern protocols
- You are responsible for the protocols in use on your Virtual Machines

Grant people access to Azure resources

- Just enough: Role based access
- Just in time: Privileged Identity Management
- Multifactor
- Conditional access is also possible for the Azure Management pane

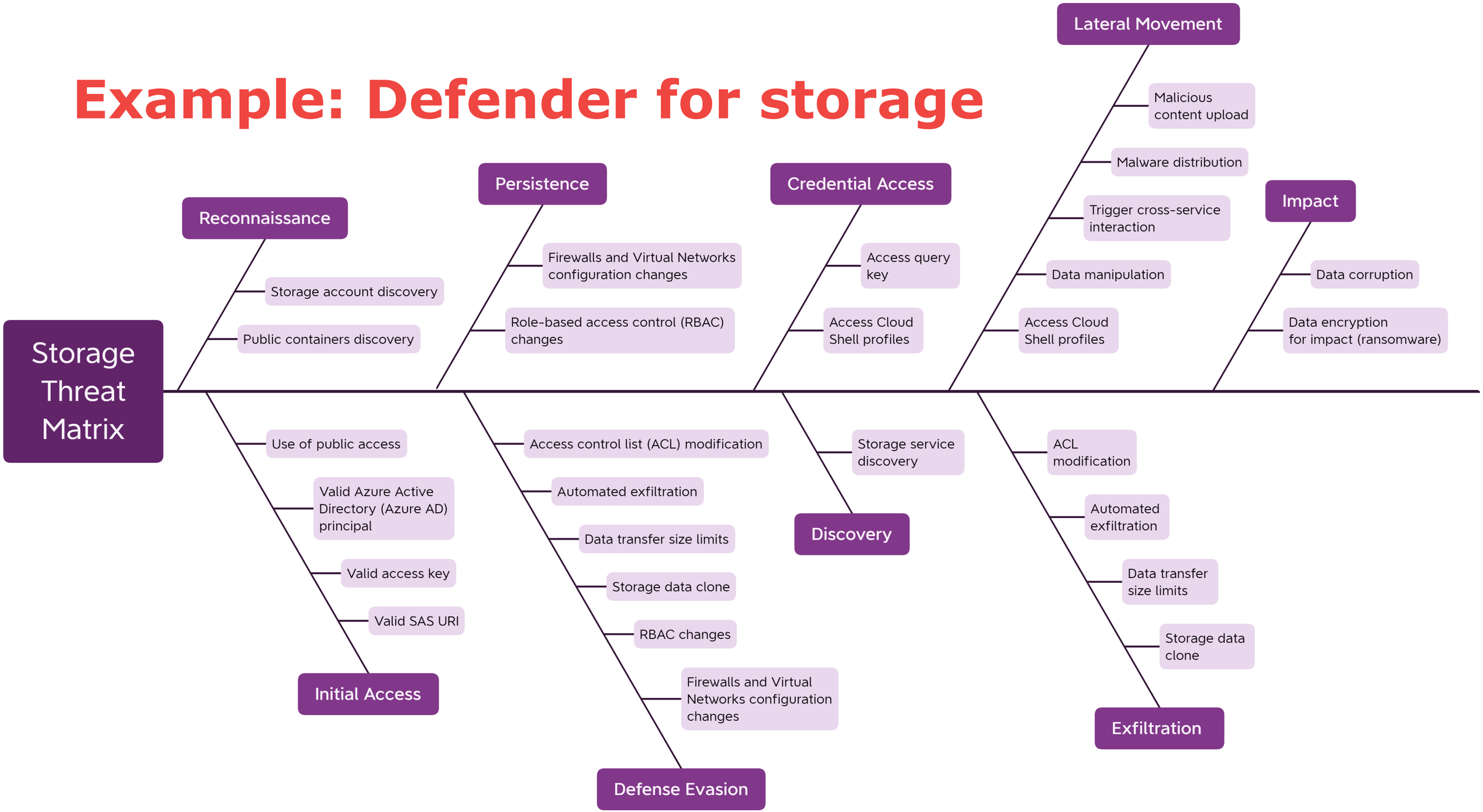
Grant applications access your resources

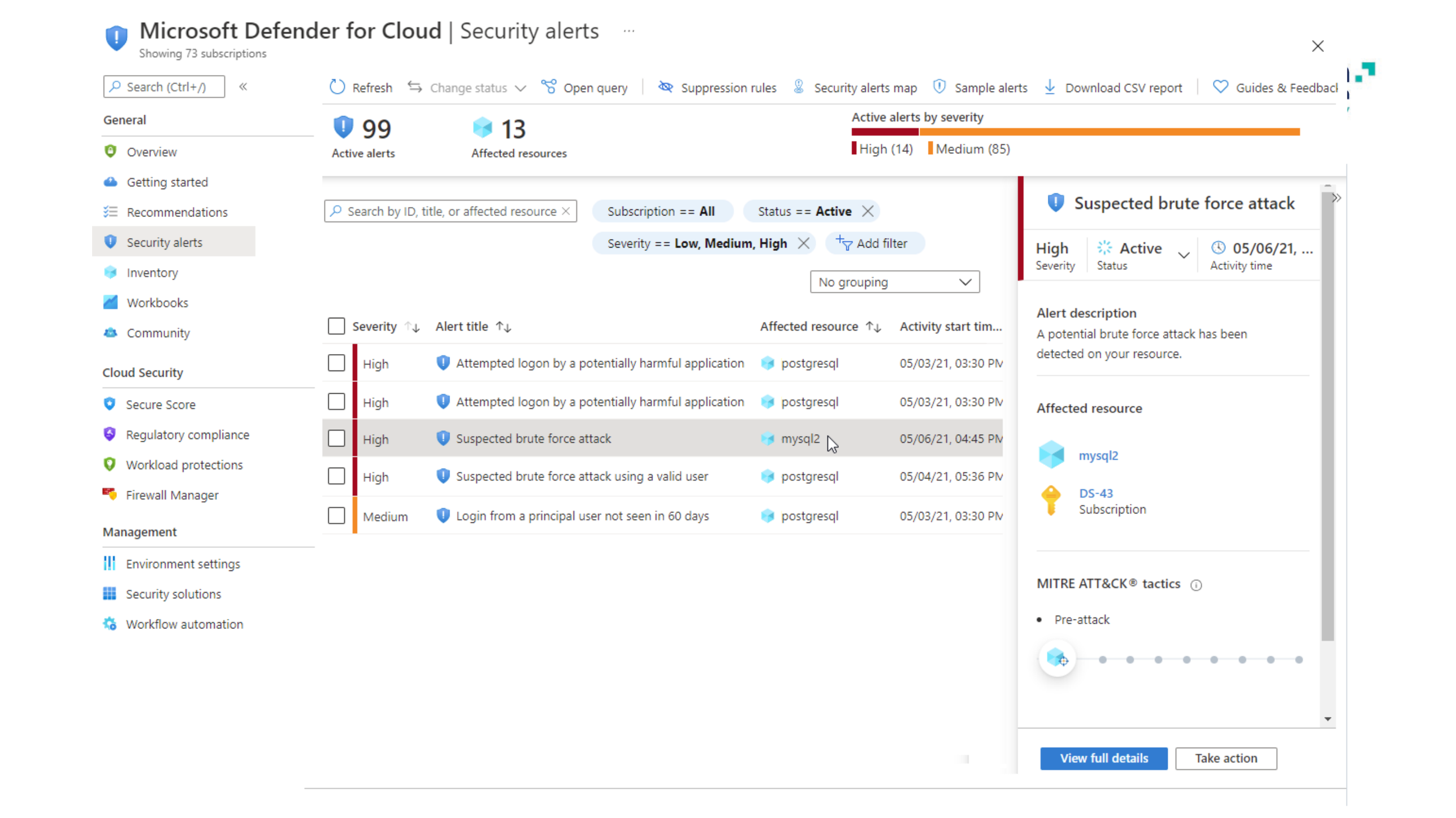
- Service principals
- Managed identities

Microsoft Defender for cloud

Continuously Assess	Secure	Defend
- Secure score - Vulnerability Assessments - Asset inventory - Regulatory compliance - File integrity monitoring	- Security recommendations - Just-in-time VM access - Adaptive network hardening - Adaptive application control	- Microsoft Defender - Security alerts - Integration with Sentinel and other SIEMs

Example: Defender for storage




Microsoft Defender for Cloud | Security alerts
Showing 73 subscriptions
Search (Ctrl+/)
General
Overview
Getting started
Recommendations
Security alerts
Inventory
Workbooks
Community
Cloud Security
Secure Score
Regulatory compliance
Workload protections
Firewall Manager
Management
Environment settings
Security solutions
Workflow automation
Refresh
Change status
Open query
Suppression rules
Security alerts map
Sample alerts
Download CSV report
Guides & Feedback
99
Active alerts
13
Affected resources
Active alerts by severity
High (14)
Medium (85)
Search by ID, title, or affected resource
Subscription == All
Status == Active
Severity == Low, Medium, High
Add filter
No grouping
Severity
Alert title
Affected resource
Activity start tim...
High
Attempted logon by a potentially harmful application
postgresql
05/03/21, 03:30 PM
High
Attempted logon by a potentially harmful application
postgresql
05/03/21, 03:30 PM
High
Suspected brute force attack
mysql2
05/06/21, 04:45 PM
High
Suspected brute force attack using a valid user
postgresql
05/04/21, 05:36 PM
Medium
Login from a principal user not seen in 60 days
postgresql
05/03/21, 03:30 PM
Suspected brute force attack
High
Severity
Active
Status
05/06/21, ...
Activity time
Alert description
A potential brute force attack has been detected on your resource.
Affected resource
mysql2
DS-43
Subscription
MITRE ATT&CK® tactics
Pre-attack
View full details
Take action

Monitoring and visibility

Log Analytics

- Big data store
- Audit trail and diagnostics
- Built-in query language (KQL)

Ingest Data

- Enforce Audit settings (Azure policy)
- All subscription / AAD activity
- Not just for Azure resources only (Azure Arc)

Gain insights

- Visualize
- Application insights
- The more data, the more you can correlate
- Integrate with a SIEM (e.g. Sentinel)

Create Tangible actions

Proactive

- Azure workbooks (e.g. Zero trust workbook)
- Posture management
- Regulatory compliance

Reactive

- Defender alerts
- Check where a SIEM/SOAR can assist you (e.g. Sentinel)

Compliance regulatory standards	Passed controls	Passed controls %	7-day change	30-day change
ISO-27001:2013	3/207	1,45%	-0,48%	-22%
Azure-CIS-1.3.0	33/105	31,4%	0,95%	-22%
Microsoft-cloud-security-benchmark	32/59	54,2%	-10%	N/A

Recommendations

Search

RecommendationDisplayName	Total
Audit diagnostic setting	369
Only approved VM extensions should be installed	361
Vulnerabilities in security configuration on your Windows...	104
Machines should have a vulnerability assessment solution	96
Storage accounts should be migrated to new Azure Res...	94
Storage accounts should allow access from trusted Micr...	94
Secure transfer to storage accounts should be enabled	94
Storage account public access should be disallowed	94
Access to storage accounts with firewall and virtual netw...	94
Storage account should use a private link connection	94

Recommendations by Control Family

Search

ControlFamily	Total
Universal Security Capabilities	2532
Data Protection	849
Intrusion Detection	415
Web	354
Networking	349
Unified Communications & Collaboration	218
Files	199
Resiliency	68
Email	67
Enterprise	23

So to answer the question…

Your datacenter in public cloud: Safe or not?

Cloud brings the tools within reach to make your environment more secure than ever before.

A lot of responsibilities are already handled by a mature hyperscale cloud provider

Thank you!