

JAN COUCKE

Why is Azure Governance Crucial for the cloud – Part 2

WHY AZURE GOVERNANCE? RECAP PART 1

- Cloud adoption difficulties



WHY AZURE GOVERNANCE? RECAP PART 1

- What did happen before these sessions (real life stories!)

Unexpected high
billing

No audit trail

Data outside
accepted
jurisdiction

Unable to associate
cost with application
owner / business
division

Component
services
unavailable in
acceptable regions

Unsecured personal
data



WHY AZURE GOVERNANCE? RECAP PART 1



GOVERNANCE PROVIDES MECHANISMS AND PROCESSES TO MAINTAIN CONTROL OVER YOUR APPLICATIONS AND RESOURCES IN AZURE. IT INVOLVES PLANNING YOUR INITIATIVES AND SETTING STRATEGIC PRIORITIES.



NATIVE PLATFORM CAPABILITIES TO ENSURE COMPLIANCY



Policy

Real-time enforcement, compliance assessment and remediation

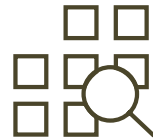
Control



Blueprints

Deploy and update cloud environments in a repeatable manner using composable artifacts

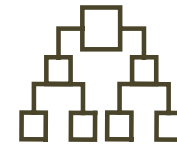
Environment



Resource Graph

Query, explore & analyze cloud resources at scale

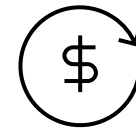
Visibility



Management Group

Define organizational hierarchy

Hierarchy



Cost

Monitor cloud spend and optimize resources

Consumption





AZURE POLICIES – ENFORCEMENT & COMPLIANCE

- **Policy definition**

- ▶ A lot of built-in policies are already available
 - Require minimum versions
 - Allowed resource types, locations, virtual machines, tags
 - ...

- **Effect types:**

- ▶ Append
- ▶ Deny
- ▶ Audit
- ▶ ...

- Periodic & on-demand compliance evaluation
- Real-time policy evaluation and remediation
- Combine a group of related policy definitions into ‘Policy Initiatives.’

```
"policyRule": {  
  "if": {  
    "not": {  
      "field": "location",  
      "in":  
        "[parameters('listOfAllowedLocations')]"  
    }  
  },  
  "then": {  
    "effect": "Deny"  
  }  
}
```

Resource Policy



RESOURCE POLICIES APPLIED AS PART OF THE DEVELOPMENT PROCESS

- Traditionally policies are applied in operate phase
- Shift left to deliver compliant code faster

Code

Build/Test

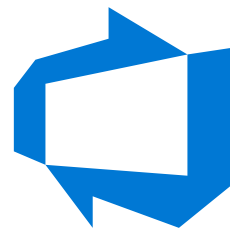
Deploy

Operate

 Monitoring

 Security

 Policy



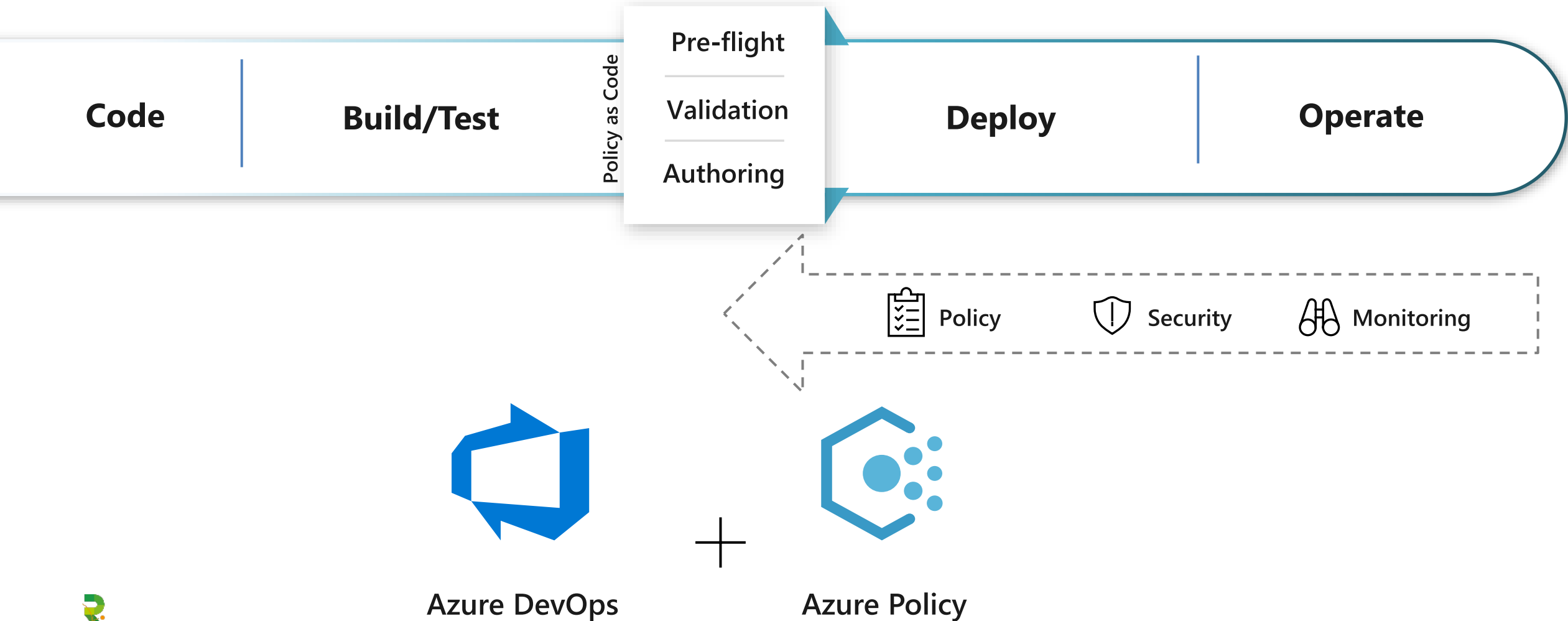
Azure DevOps





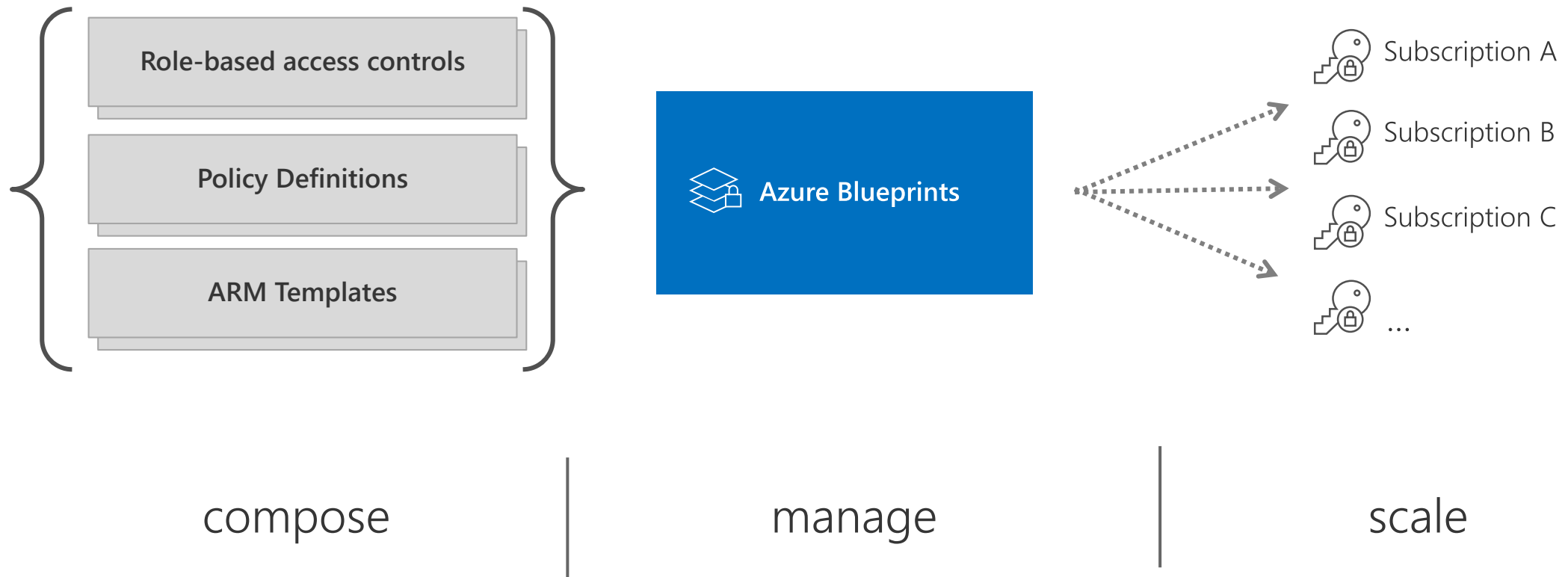
RESOURCE POLICIES APPLIED AS PART OF THE DEVELOPMENT PROCESS

- Built-in into your CI/CD Pipeline





AZURE BLUEPRINTS





AZURE BLUEPRINTS

- Deploy and update cloud environments in a repeatable manner using composable **artifacts**
 - Use Cases
 - Software as a Service Provider
 - IT Integrator
 - DTAP
- Publishing and assigning Blueprints
 - Definition located at Management Group / Subscription Level
 - Created in Draft mode
 - Publishing required before assignment
 - Temporary owner permissions will be granted to the Blueprint Managed Identity / User Identity
 - Versioning





AZURE BLUEPRINTS ~ SAMPLES ~ COMPLIANCY FRAMEWORKS



Blank Blueprint

An empty blueprint with no initial properties or artifacts.

[Start with blank blueprint](#)

Other Samples



Common Policies

A set of popular policies to apply to a subscription

[Use this sample](#)



Basic Networking (VNET)

Configures a virtual network with a subnet and an NSG.

[Use this sample](#)



Resource Groups with RBAC

Sets up two resource groups and configures a role assignment for each. [Learn More.](#)

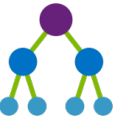
[Use this sample](#)



AZURE BLUEPRINTS

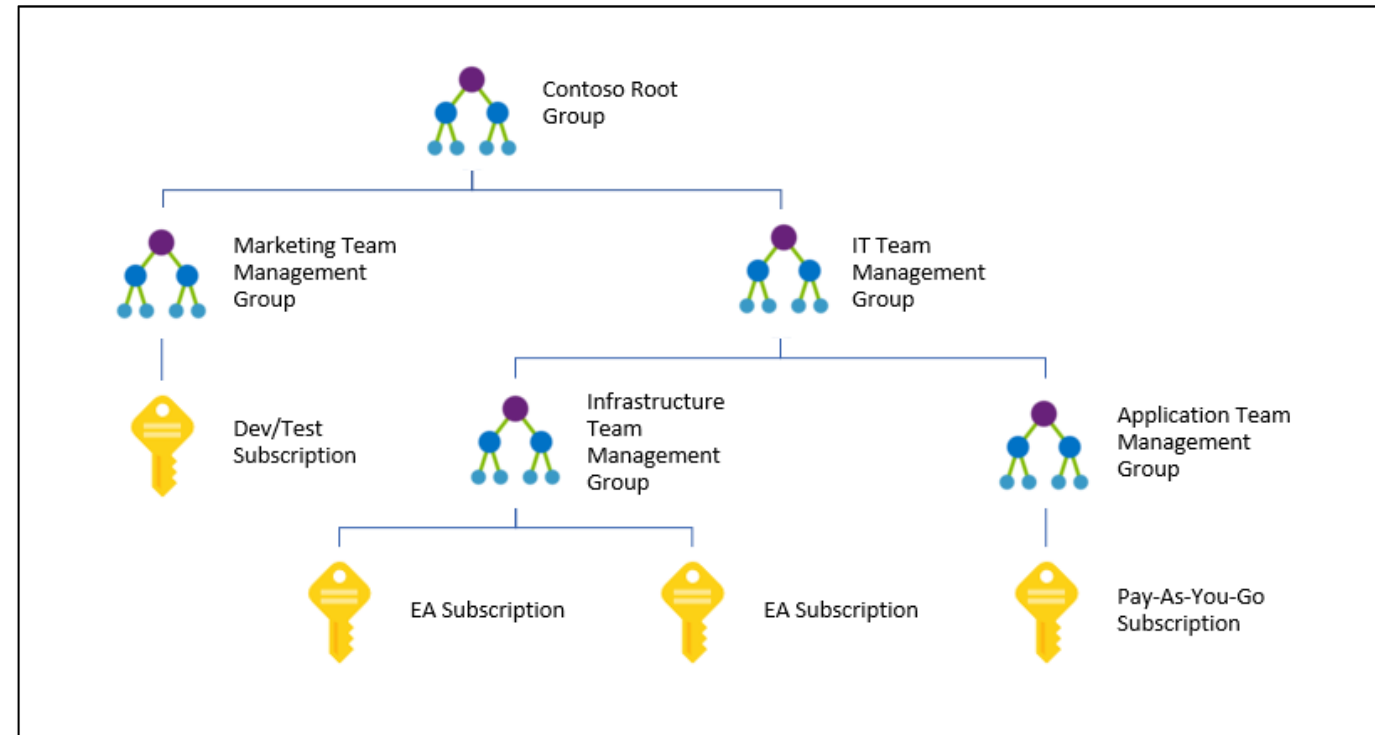
- Resource locking
 - ▶ ReadOnly
 - ▶ CannotDelete
- Additional settings within Blueprints:
 - ▶ Resources “Not Locked” by default.
 - ▶ Cannot Edit/Delete on resource group level
- Override locking
 - ▶ Not even for “Owners” through RBAC
 - ▶ You need to Update or delete your blueprint.





AZURE MANAGEMENT GROUPS

- Provides a level of scope above subscriptions
- Make environment management easier by grouping subscriptions together
- Create a hierarchy of management groups that fit your organization
- Apply governance controls with policies and access controls along with other Azure services such as:
 - Azure Policy
 - Role Based Access Control
 - Azure Cost Management
 - Azure Blueprints

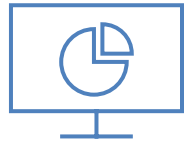




AZURE COST MANAGEMENT

- Comes in a variety of possibilities:

Cost Management
in Azure Portal



Ready to use*

Connectors
to PowerBI



Custom dashboards

Azure
APIs



Custom solutions





AZURE COST MANAGEMENT – PREVENT UNEXPECTED COSTS

- Forecast vs Actual spending

The screenshot shows the 'Pricing calculator' interface. At the top, it says 'Configure and estimate the costs for Azure products'. Below this, there's a 'Products' section with a search bar and a list of categories: Compute, Networking, Storage, Web + Mobile, Containers, Databases, and Data + Analytics. The 'Compute' category is selected, showing options for Virtual Machines, Virtual Machine Scale Sets, App Service, Functions, Batch, Service Fabric, and Cloud Services. A digital display at the top right shows the number '07734'.

Azure
Pricing Calculator

The screenshot shows the 'Choose a size' screen for creating a virtual machine. It lists two options: 'D1_V2 Standard' and 'D1 Standard'. The 'D1_V2 Standard' option is selected. The specifications for 'D1_V2 Standard' are: 1 Core, 3.5 GB memory, 2 Data disks, 2x500 Max IOPS, 50 GB Local SSD, and Load balancing. The estimated cost is 98.95 USD/MONTH. The 'D1 Standard' option has 1 Core, 3.5 GB memory, 2 Data disks, 2x500 Max IOPS, 50 GB Local SSD, and Load balancing, with an estimated cost of 104.16 USD/MONTH.

Azure
Estimated Costs

The screenshot shows the 'Realdolmen NV (79589097) - Cost analysis' dashboard. The total cost is €10,645. The dashboard includes a search bar, refresh, tour, and export buttons. The left sidebar lists various cost management features like Overview, Access control (IAM), Cost Management, Budgets, Billing, Usage + charges, Credits, Reservation transactions, Departments, Accounts, Subscriptions, and Settings. The main area features a line graph showing 'Accumulated cost' over time, with the y-axis ranging from €0 to €11K and the x-axis showing dates from Mar 1 to Mar 15. The cost starts at €0 and increases steadily to €10,645 by Mar 13.

Azure
Cost Management



AZURE COST MANAGEMENT ~ BREAKDOWN – MONITOR BURN RATE



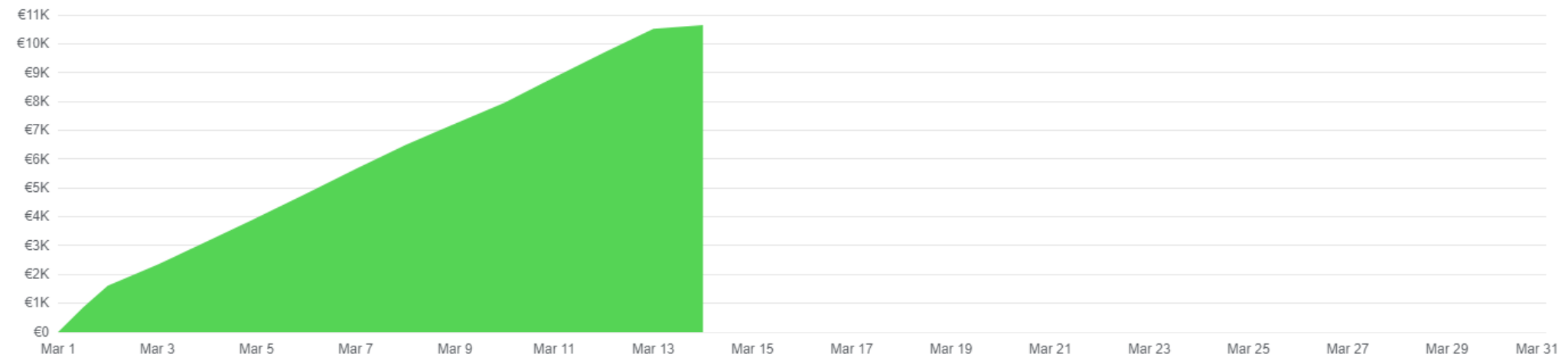
Search (Ctrl+)

Refresh Tour Export

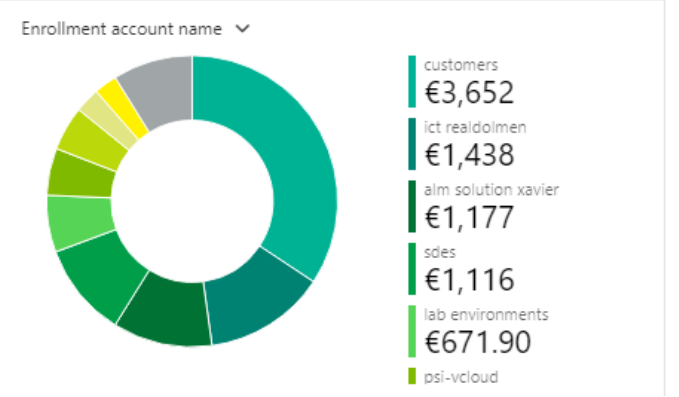
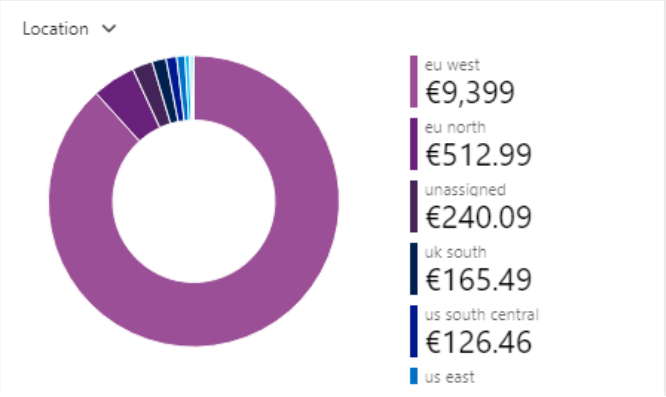
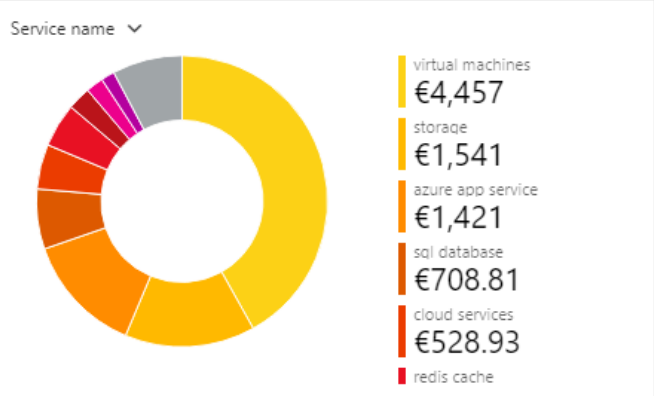
- Overview
- Access control (IAM)
- Cost Management
 - Cost analysis
 - Budgets
- Billing
 - Usage + charges
 - Credits
 - Reservation transactions
 - Departments
 - Accounts
 - Subscriptions
- Settings
 - Properties
 - Notifications
 - Policies

Scope: Realdoim... Accumulated costs Mar 2019 Granularity: Accumulated Group by: None Add filter

TOTAL €10,645 BUDGET: NONE --



Accumulated cost

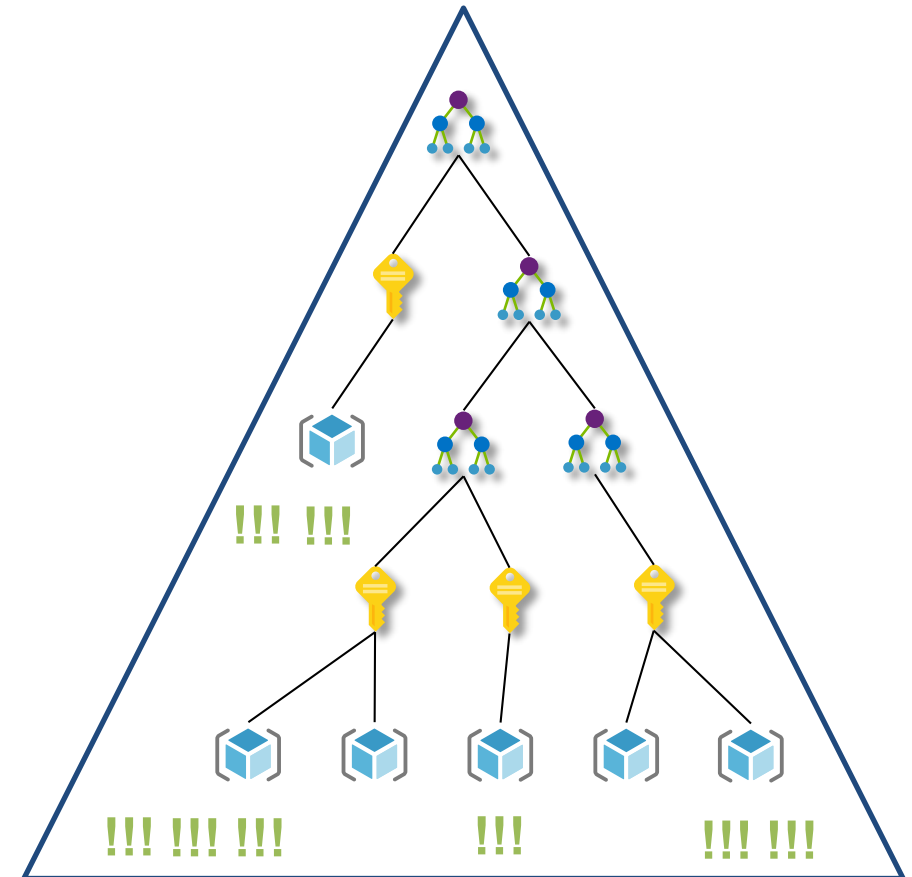




AZURE COST MANAGEMENT – COST ANALYSIS

Resource TAGS add context for cost analysis

- Finance codes
 - CostCenter tag, etc.
- Application context
 - AppService tag, etc.
- Deployment context
 - Environment tag, etc.
- Who is accountable
 - BusinessOwner tag, etc.
- Tags should be enforced by configuration policies.
 - Enforce that tags exists
 - Set default value for tags
 - Audit if tags are missing



AZURE COST MANAGEMENT – BUDGETS

- Set an Azure spending budget
 - ▶ Scope-based
 - Subscription / Resource Group
 - ▶ Notifications
 - ▶ Actions
- Action Types
 - ▶ Email / SMS / Push / Voice
 - ▶ Azure Function
 - ▶ LogicApp
 - ▶ Webhook
 - ▶ ITSM
 - ▶ Automation Runbook

Create budget

Budget



Manage action groups Help

* Name
JanShouldNotGoOverBudget

* Amount * Resets

* Start date

* Expiration date

Alerts

Configure alert conditions and send email notifications based on your spend.

* Alert conditions

Delete

<input checked="" type="checkbox"/>	% OF BUD...	AMOUNT	ACTION GROUP	ACTION GROUP TYPE
<input type="checkbox"/>	75	75	ag-budgets-mail	1 Email
<input checked="" type="checkbox"/>	100 <input checked="" type="checkbox"/>	100	ag-budgets-shutd... <input type="checkbox"/>	1 Automation Runb...
<input type="checkbox"/>	<input type="text"/>		None <input type="checkbox"/>	

* Alert recipients (email)

Delete

ALERT RECIPIENTS (EMAIL)



AZURE COST MANAGEMENT ~COST OPTIMIZATION

- Azure Advisor Recommendations
 - ▶ Capacity management ~ VM Size considerations
 - ▶ Orphaned artifacts
 - Managed Disks
 - ▶ Unused Virtual network gateways
- Azure offering can make a huge difference
 - ▶ Subscription Contract
 - Enterprise Agreement / Cloud Solution Provider / Pay-As-You-Go / ...
 - ▶ Reserved Instances
 - ▶ Hybrid Use Benefits

➔ Follow the webinar “Options to buy Azure” by Rik Delva.



CLOUD LIFECYCLE MANAGEMENT

- Optimization is the path to success
 - Cost efficiency
 - business growth
- Optimization is not a one-time effort
 - Cloud services are growing at an enormous pace
 - Microsoft provides roadmaps
 - Transform from IaaS to native PaaS Services
 - Common business cases:
 - Business reporting / datawarehouse
 - Archiving / storage
 - EDI scripts



CLOUD LIFE CYCLE MANAGEMENT IN FUNCTION OF COST MANAGEMENT

- Upgrade to newer Azure Artifacts versions
 - ▣ Virtual Machine Example:

The screenshot displays the Azure Virtual Machine configuration interface. It shows a sequence of three overlapping panels, each representing a different configuration state. The final configuration is selected, showing the following details:

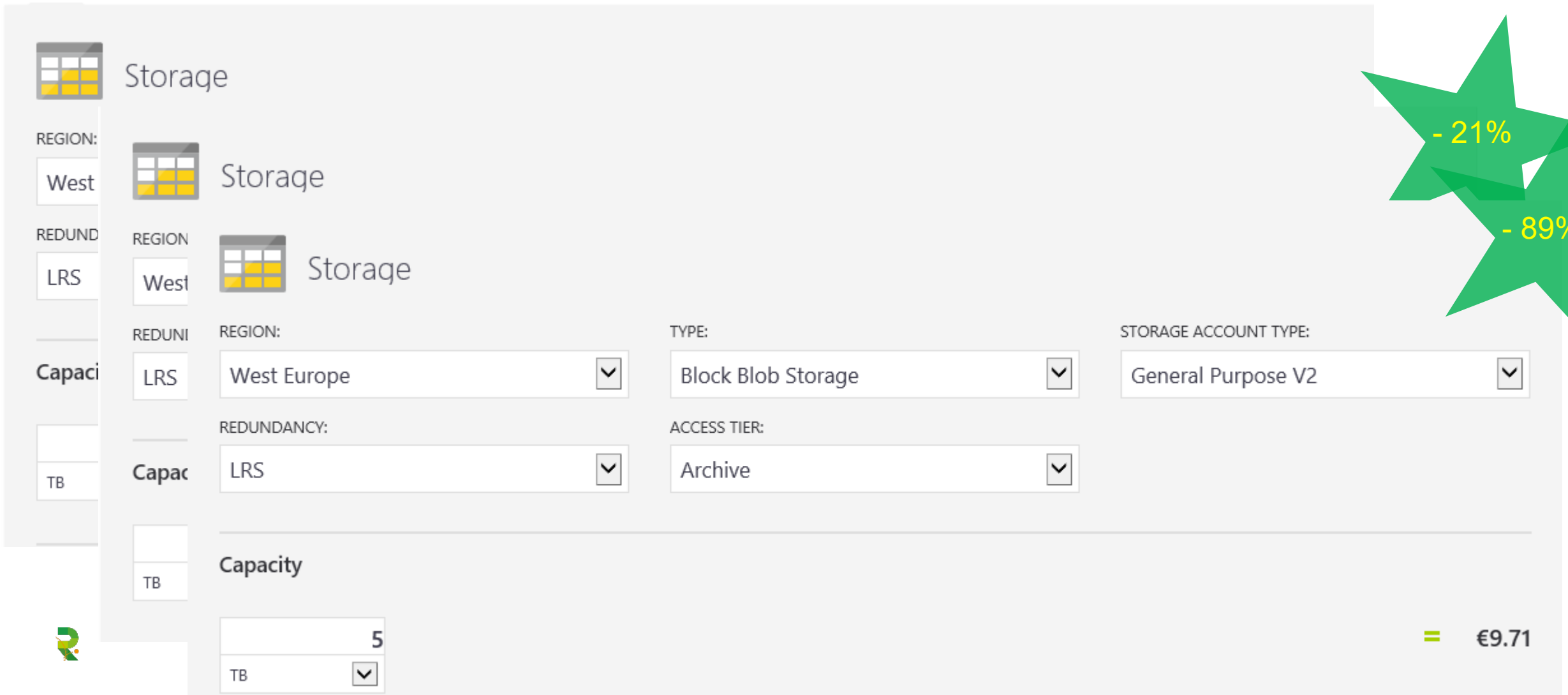
- REGION: West Europe
- TIER: Standard
- OPERATING SYSTEM: Windows
- TYPE: (OS Only)
- TIER: Standard
- INSTANCE: D2 v3: 2 vCPU(s), 8 GB RAM, 50 GB Temporary storage, €0.1421/hour

At the bottom, the configuration is summarized as 1 Virtual machine for 730 Hours, resulting in a total cost of €130.51 Per month. Two green starburst callouts on the right indicate cost reductions: -10% and -29%.



CLOUD LIFE CYCLE MANAGEMENT IN FUNCTION OF COST MANAGEMENT

- Upgrade to newer Azure Artifacts versions



The image shows a screenshot of the Azure Storage configuration interface. On the right side, there are two green starburst callouts indicating cost savings: -21% and -89%. The interface includes several configuration options:

- REGION:** West
- REDUNDANCY:** LRS
- REGION:** West
- REDUNDANCY:** LRS
- REGION:** West Europe
- TYPE:** Block Blob Storage
- STORAGE ACCOUNT TYPE:** General Purpose V2
- REDUNDANCY:** LRS
- ACCESS TIER:** Archive
- Capacity:** 5 TB

The total cost is displayed as **€9.71**.

OTHER SUPPORTING TOOLS THAT CAN HELP IN YOUR GOVERNANCE JOURNEY



Security Center

Strengthens the security posture and provides advanced threat protection across your hybrid workloads in the cloud.



Advisor

Cloud consultant that helps you follow best practices to optimize your Azure deployments



SECURITY CENTER ~ OVERVIEW



Security Center - Overview

Showing 2 subscriptions

Search (Ctrl+)

GENERAL

Overview

Getting started

Events

Search

POLICY & COMPLIANCE

Coverage

Secure score

Security policy

Regulatory compliance (Prev...

RESOURCE SECURITY HYGIENE

Recommendations

Compute & apps

Networking

Data & storage

Identity & access (Preview)

Security solutions

Subscriptions

Policy & compliance

Secure score



416 OF 780

Secure score impact changed. [Learn more](#)

[Review your secure score](#)

Least compliant regulatory standards

SOC TSP 1 of 13 passed controls

ISO 27001 3 of 21 passed controls

PCI DSS 3.2 6 of 33 passed controls

Subscription coverage



76 Covered resources

Fully covered 0
Partially covered 2
Not covered 0

Make alert data available to your SIEM



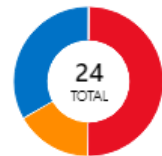
You can make Security Center alerts available to a SIEM connector



[Set up SIEM connector](#)

Resource security hygiene

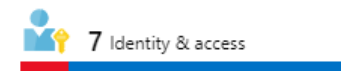
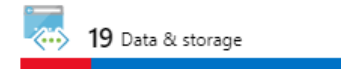
Recommendations



51 Unhealthy resources

High Severity 12
Medium Severity 4
Low Severity 8

Resource health monitoring



Top recommendations by secure score impact

- [Enable MFA for accounts with owner permissions on...](#) +50
- [Enable Network Security Groups on virtual machines](#) +30
- [Apply a Just-In-Time network access control](#) +30

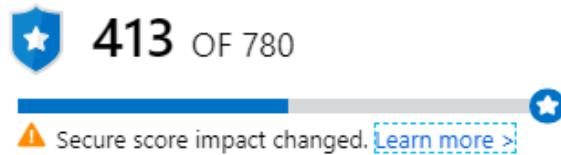




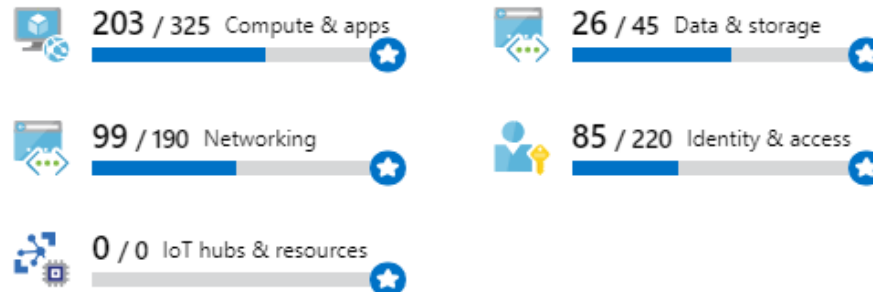
SECURITY CENTER – SECURE SCORE

- Security center mimics the work of a security analyst
 - Can be linked to an existing SIEM solution or Azure Sentinel (preview)
- Constantly reviews your active recommendations & calculates your secure score.

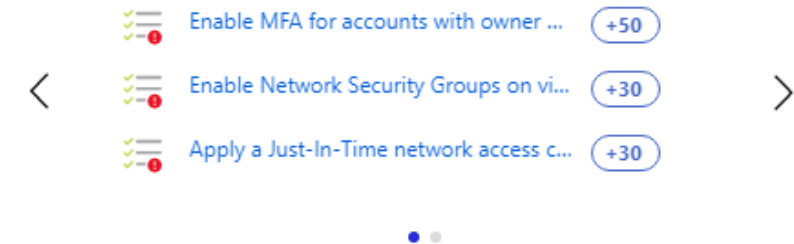
Overall secure score



Secure score by category



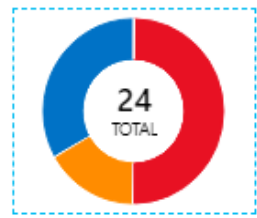
Top recommendations by secure score impact





SECURITY CENTER ~ RESOURCE SECURITY HYGIENE ~ RECOMMENDATIONS

Recommendations



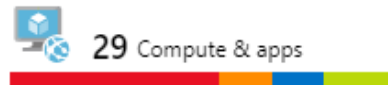
High Severity
12

Medium Severity
4

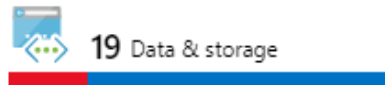
Low Severity
8

51 Unhealthy resources

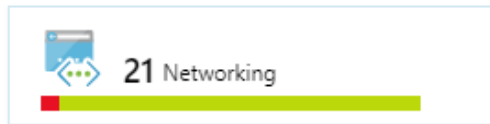
Resource health monitoring



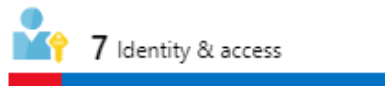
29 Compute & apps



19 Data & storage



21 Networking



7 Identity & access

Top recommendations by secure score impact

- Enable MFA for accounts with owner permissions **+50**
- Enable Network Security Groups on virtual machines **+30**
- Apply a Just-In-Time network access control **+30**

RECOMMENDATION	SECURE SCORE IMP...	FAILED RESOURCES	
Enable MFA for accounts with owner permissions on your subscription (Preview)	+50	1 of 1 subscriptions	
Apply a Just-In-Time network access control	+30	8 of 8 virtual machines	
Enable Network Security Groups on virtual machines	+30	8 of 8 virtual machines	
Remove external accounts with owner permissions from your subscription (Preview)	+30	1 of 1 subscriptions	
Restrict access to App Services	+20	8 of 8 web applications	
Resolve endpoint protection health issues on your machines	+15	5 of 8 virtual machines	
Enable DDoS Protection Standard	+10	1 of 1 virtual networks	



SECURITY CENTER ~ STRENGTHEN SECURITY POSTURE



Compute

+ Add Computers

Navigation menu with icons and labels:

- Overview (Active)
- VMs and Computers
- VM scale sets
- Cloud services
- App services
- Containers (Preview)
- Compute resources (Preview)

Search recommendations

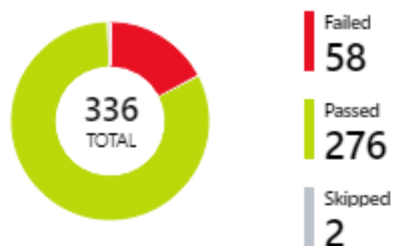
RECOMMENDATION	SECURE SCORE IMPACT	FAILED RESOURCES	
Resolve endpoint protection health issues on your machines	+15	5 of 8 virtual machines	
Enable Adaptive Application Controls on virtual machines	+9	3 of 8 virtual machines	
Apply disk encryption on your virtual machines	+6	5 of 8 virtual machines	
Install endpoint protection solution on virtual machines	+4	2 of 8 virtual machines	
Install a vulnerability assessment solution on your virtual machines	+30	4 of 8 virtual machines	
Web Application should only be accessible over HTTPS	+6	2 of 7 web applications	
CORS should not allow every resource to access your Web Application	+6	2 of 7 web applications	
Remediate vulnerabilities in security configuration on your machines	+30	5 of 8 virtual machines	
Troubleshoot missing scan data on your machines	+11	5 of 8 virtual machines	
Enable diagnostics logs in Service Bus (Preview)	+5	4 of 4 service buses	



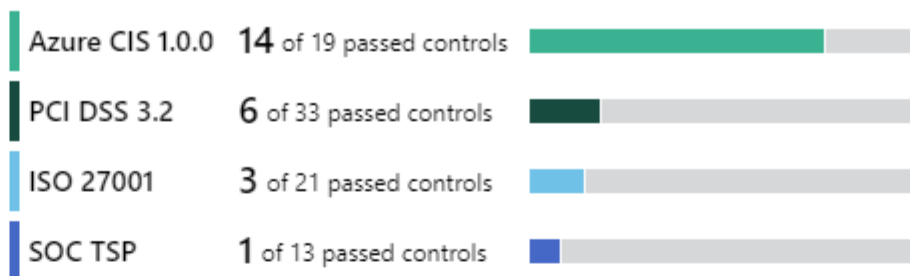


SECURITY CENTER ~ REGULATORY STANDARDS COMPLIANCE

Regulatory compliance assessment



Regulatory standards compliance status



[Azure CIS 1.0.0](#) [PCI DSS 3.2](#) [ISO 27001](#) [SOC TSP](#) [All](#)

Under each applicable compliance control is the set of assessments run by Security Center that are associated with that control. If they are all green, it means those assessments for any particular regulation are covered by Security Center assessments, and therefore this report is only a partial view of your overall compliance status.

Expand all compliance controls

∨ **1. Identity and Access Management**


∨ **2. Security Center**

∨ **3. Storage Accounts**


∨ **4. SQL Services**

∨ **5. Logging and Monitoring**

AZURE ADVISOR


 High Availability

6 Recommendations




0 High impact 5 Medium impact 1 Low impact

14 Impacted resources


 Security

23 Recommendations




23 High impact 0 Medium impact 0 Low impact

46 Impacted resources


 Performance


1 Recommendation



1 High impact 0 Medium impact 0 Low impact

11 Impacted resources

 Cost



You are following all of our cost recommendations

[See list of cost recommendations](#)



TOO LATE? TIME TO RETAKE CONTROL!



HOW TO TAKE BACK CONTROL?



HOW TO TAKE BACK CONTROL?

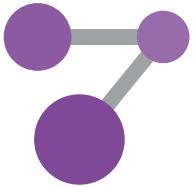
Review



How much are we burning?



What artifacts are we spending it on?



Are we out of compliance?

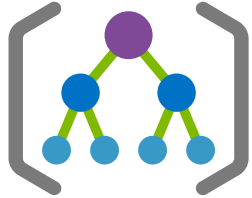


Where should our effort go first?

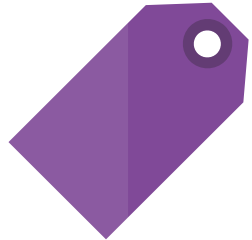


HOW TO TAKE BACK CONTROL? ORGANISE

Organise



Create a subscription hierarchy



Classify Subscriptions and Resources



Apply access rights consistently



HOW TO TAKE BACK CONTROL?



Develop Policies



Apply Budgets



Audit the impact of these policies



Get ready for enforcement

HOW TO TAKE BACK CONTROL?

Enforce



Change policies to enforcement



Add remediation actions



Enforce Budgets



Create new subscriptions already compliant



AZURE WITHOUT GOVERNANCE IS LIKE
SLOWLY DRIVING YOUR CAR INTO AN
ACCIDENT.

DON'T BE THAT DRIVER. ACT NOW!

WHAT'S NEXT ?

	Technical Track	Services & Management Track
12:30-13:30	Lunch	
13:30-14:15	Your data platform in the cloud: strategy and options <i>Brecht Vuylsteke</i>	DNA and added value of a chatbot <i>Dirk Gepts</i>

