

Improve your security score with Azure Security Center



“Through 2020, 95 percent of cloud security failures will be the customer's fault” – Gartner

Source Gartner Reveals Top Predictions for IT Organizations and Users for 2016 and Beyond, October 2015,
<http://www.gartner.com/newsroom/id/3143718>

WHOAMI



Bart Verboven



Azure Technical consultant



bart.verboven@realdolmen.com



[bverboven](#)



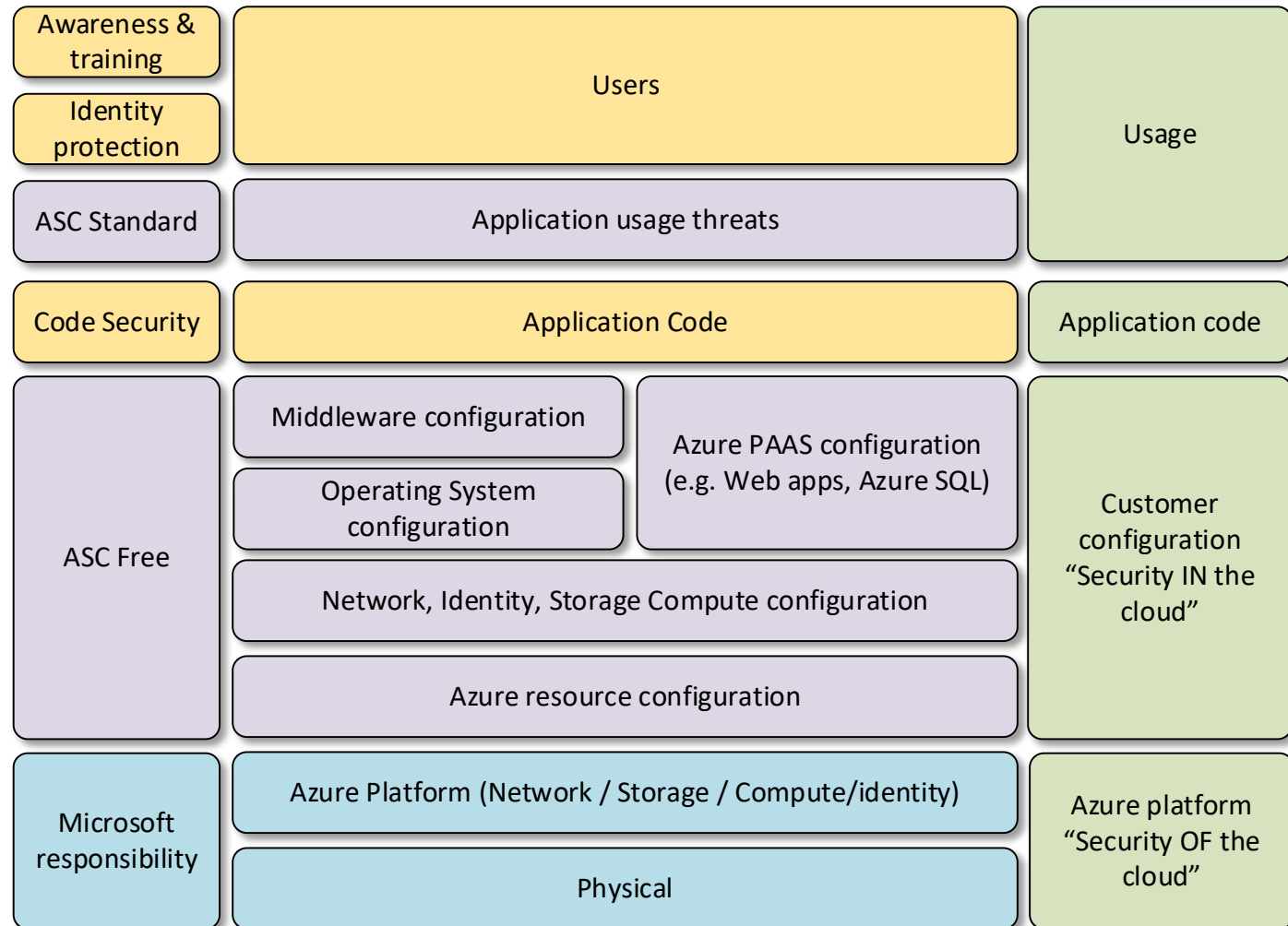
WHAT I AM GOING TO TALK ABOUT

- Setting the scene: Why should I care?
- Securing your configuration
- Azure policies as the cornerstone
- Adding intelligence into the mix
- Personal list of must have features
- Tips for successful implementation
- QnA



SETTING THE SCENE: WHY SHOULD I CARE?

- System of records & System of Intelligence
- Microsoft Monitoring Agent to gain OS insights
- Playbooks (logic apps) as remediation
- Regulatory compliance assistance



SECURING YOUR CONFIGURATION

- Good news: ASC has a free tier
- Even better news: it is enabled by default
- Configuration of Azure resources
- Configuration of the Operating Systems in Azure
- Identify possible missing security controls
- Tweakable to your personal needs
- Secure Score to reflect how you're doing

Secure score



423 OF 730





Demo

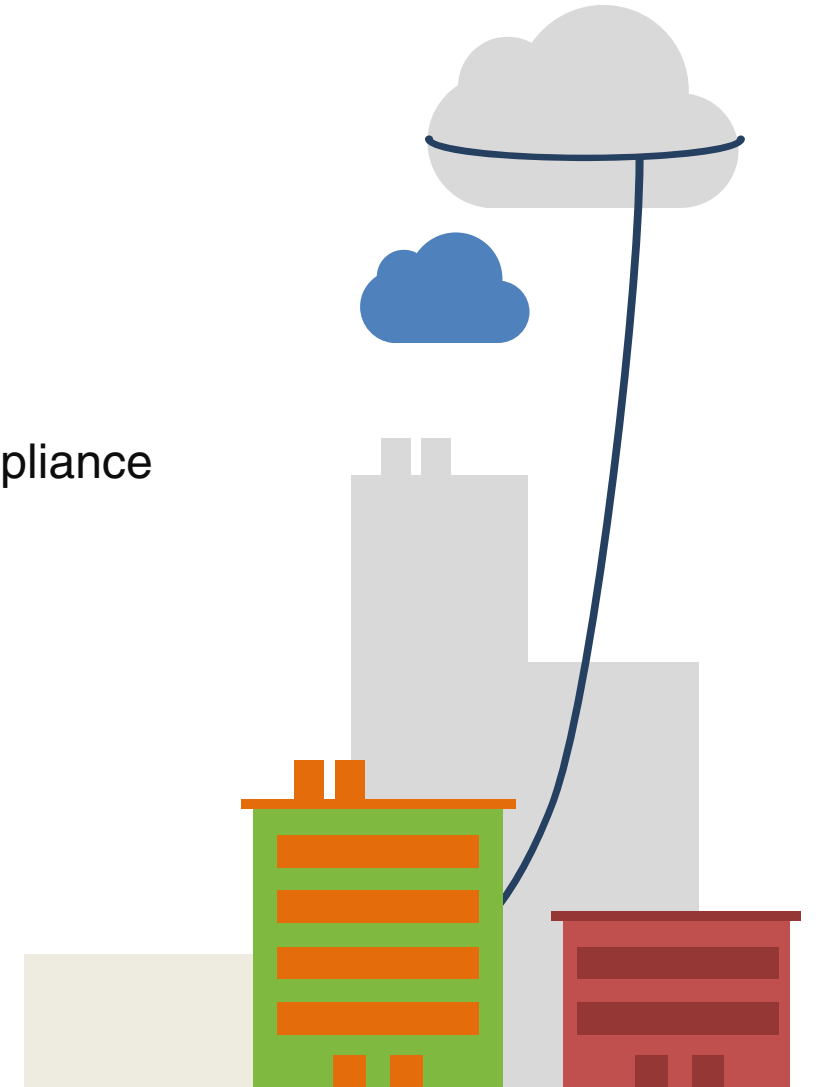
AZURE POLICIES AS THE CORNERSTONE

- Control at deployment: Deny / Audit / Append
- Control at operate: Audit or autofix
- Lots of built-in policies out of the box
- Not just Azure only: Guest OS configuration capabilities

- Exception handling

- Not only for security configuration but also for company policy compliance
 - ▣ Eg tagging, resource location

- Baseline & remediation





Demo

ADDING INTELLIGENCE IN THE MIX : ASC STANDARD




- Standard tier (€ per node/month) (vm / web app / Azure sql)
- Using ML & AI to identify active threats
- Extended Alerting capabilities
 - ▶ Handle them in the Azure portal or export them to a SIEM of your choice
 - ▶ ! New: Cloud based SIEM by Microsoft: Azure Sentinel (Preview)
- Log search possibility



ALERT EXAMPLE

- "Suspicious Download Then Run Activity"

^ General information

DESCRIPTION	Analysis of host data has detected a file being downloaded then run in the same command on GDCUWHPCW002. This is a common technique attackers use to get malicious files onto victim machines.
ACTIVITY TIME	Monday, January 14, 2019, 6:59:24 AM
SEVERITY	 Medium
STATE	Active
ATTACKED RESOURCE	GDCUWHPCW002
SUBSCRIPTION	PRD_Infra (ebe387b3-ef04-4d59-8986-f333cb3fbced)
DETECTED BY	 Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	 Virtual Machine
SUSPICIOUS PROCESS	/bin/busybox <code>/bin/sh -c "adduser -D -S -u 1001 -h /var/lib/varnish -s /sbin/nologin -G root varnish apk --update --no-cache -t .varnish-rundeps add make pwg certificates curl qzip tar unzip waet varnish="\\${VARNISH_VER ALPINE}" aotpl url="\`https://github.com/wodby/aotpl/releases/download/\\${GC</code>

Was this useful? Yes No



Investigation not available

[View playbooks](#)

ONE MORE ALERT EXAMPLE

		DESCRIPTION	↑↓	COUNT	↑↓	DETECTED BY	↑↓	ENVIRONMENT	↑↓	DATE	↑↓	STATE	↑↓	SEVERITY	↑↓
NEW	🛡️	EXE application control policy violation was audited		2		Microsoft		Azure		03/14/19		Active		⚠️ Medium	...
NEW	🛡️	PROTOCOL-ENFORCEMENT		42		Microsoft WAF		Azure		03/14/19		Active		⚠️ Medium	...
NEW	🛡️	BLOCKING-EVALUATION		2		Microsoft WAF		Azure		03/14/19		Active		⚠️ Medium	...
NEW	🛡️	APPLICATION-ATTACK-SQLI		2		Microsoft WAF		Azure		03/14/19		Active		⚠️ Medium	...
NEW	🛡️	EXE application control policy violation was audited		4		Microsoft		Azure		03/13/19		Active		⚠️ Medium	...
NEW	🛡️	PROTOCOL-ENFORCEMENT		61		Microsoft WAF		Azure		03/13/19		Active		⚠️ Medium	...
NEW	🛡️	Logon by an unfamiliar principal		2		Microsoft		Azure		03/12/19		Active		⚠️ Medium	...
NEW	🛡️	EXE application control policy violation was audited		4		Microsoft		Azure		03/12/19		Active		⚠️ Medium	...
NEW	🛡️	Suspicious authentication activity		1		Microsoft		Azure		03/12/19		Active		⚠️ Medium	...
NEW	🛡️	PROTOCOL-ENFORCEMENT		64		Microsoft WAF		Azure		03/12/19		Active		⚠️ Medium	...
NEW	🛡️	APPLICATION-ATTACK-SQLI		2		Microsoft WAF		Azure		03/12/19		Active		⚠️ Medium	...
NEW	🛡️	BLOCKING-EVALUATION		2		Microsoft WAF		Azure		03/12/19		Active		⚠️ Medium	...
	🛡️	EXE application control policy violation was audited		4		Microsoft		Azure		03/11/19		Active		⚠️ Medium	...
	🛡️	PROTOCOL-ENFORCEMENT		66		Microsoft WAF		Azure		03/11/19		Active		⚠️ Medium	...
	🛡️	APPLICATION-ATTACK-SQLI		6		Microsoft WAF		Azure		03/11/19		Active		⚠️ Medium	...
	🛡️	BLOCKING-EVALUATION		6		Microsoft WAF		Azure		03/11/19		Active		⚠️ Medium	...



PRICING MODEL

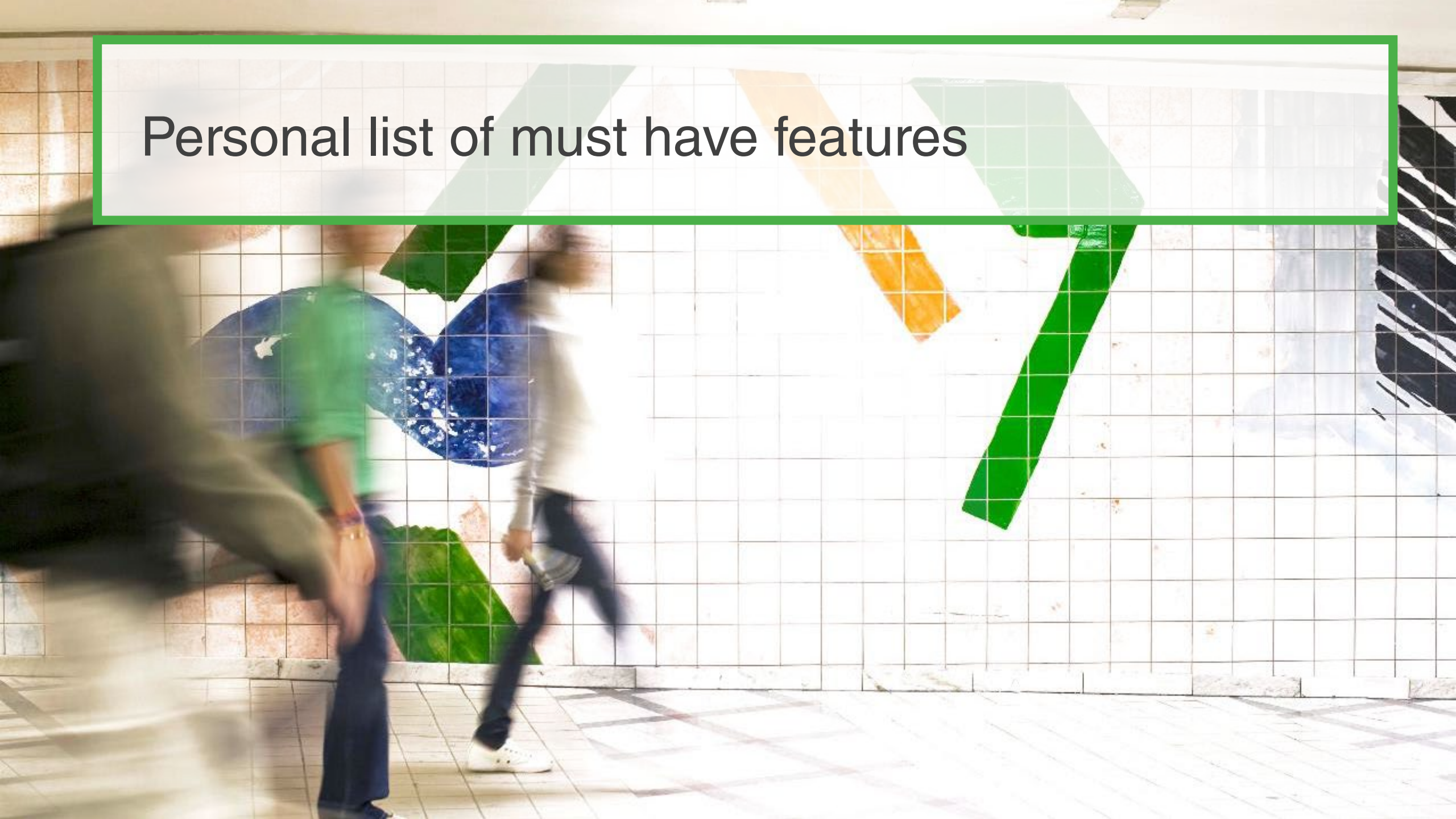
FEATURES	FREE (AZURE RESOURCES ONLY)	STANDARD (HYBRID INCL. AZURE)
Security policy, assessment, and recommendations	✓	✓
Connected partner solutions	✓	✓
Security event collection and search	--	✓
Just-in-time VM Access	--	✓
Adaptive application controls	--	✓
Advanced threat detection for networks, VMs/servers, and Azure services	--	✓
Built-in and custom alerts	--	✓
Threat intelligence	--	✓
Included data	Not applicable	500 MB per day ¹
Price	Free	\$15 / node / month

¹The daily included data allocation is pooled across nodes. For example, if there are 10 nodes connected to the service, then the total 'included data' allocation is 5,000 MB per day.



Demo

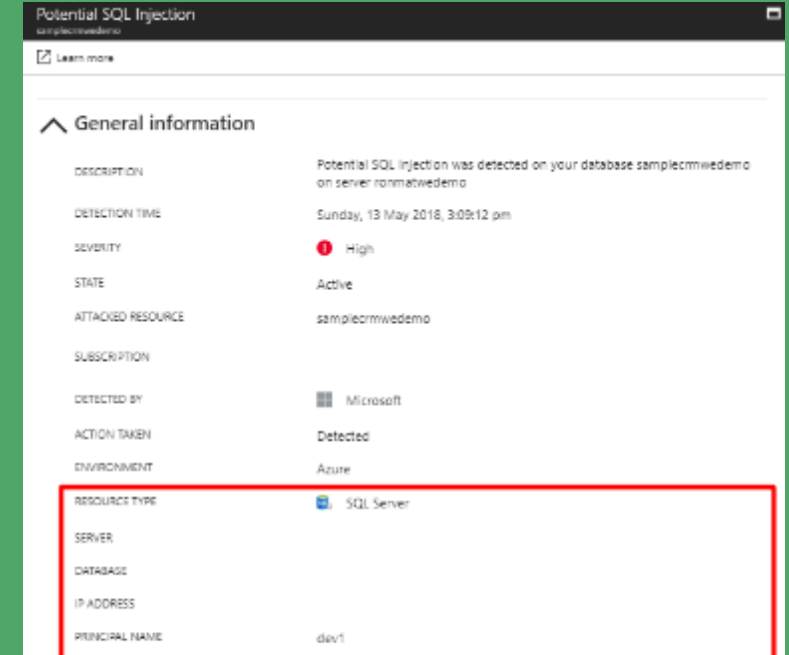
Personal list of must have features



PROTECT ACCESS TO YOUR AZURE SQL DATA

- Azure SQL Data protection
- SQL injection detection
- Unusual access
 - ▶ Location
 - ▶ Principal
- Brute force attempts

- Part of the advanced data security offering
 - ▶ Also offers data discovery
 - ▶ Data classification
 - ▶ Vulnerability reports

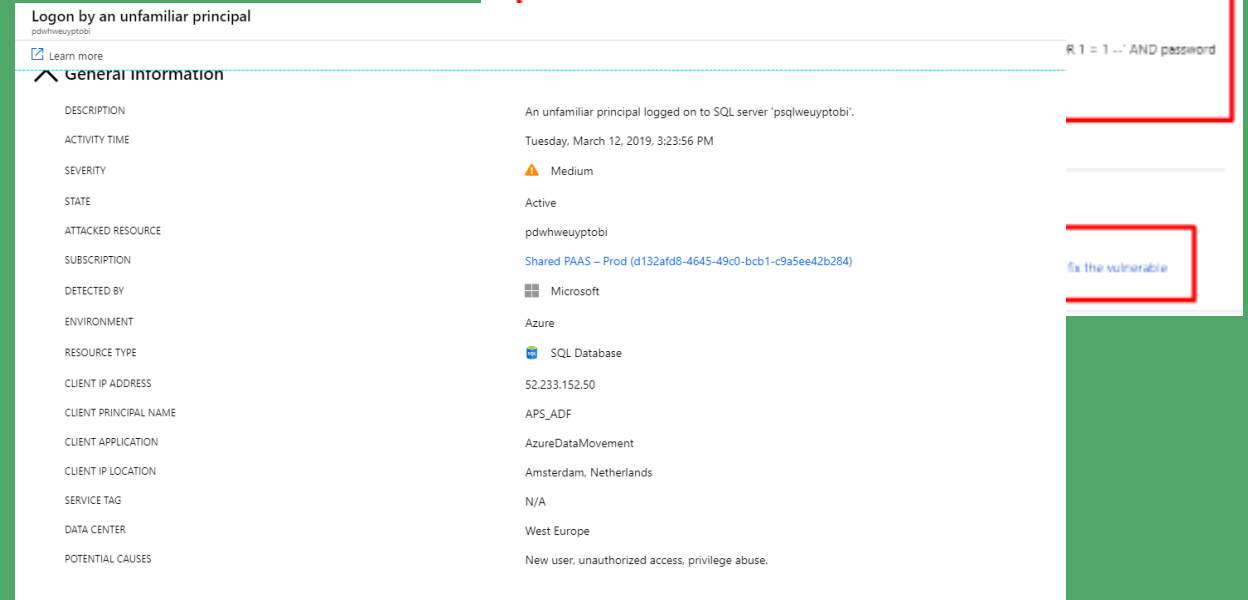


Potential SQL Injection
samplecmwedemo

Learn more

General information

DESCRIPTION	Potential SQL injection was detected on your database samplecmwedemo on server ronmatwedemo
DETECTION TIME	Sunday, 13 May 2018, 3:09:12 pm
SEVERITY	High
STATE	Active
ATTACHED RESOURCE	samplecmwedemo
SUBSCRIPTION	
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	SQL Server
SERVER	
DATABASE	
IP ADDRESS	
PRINCIPAL NAME	dev1



Logon by an unfamiliar principal
pdwhweuyptobi

Learn more

R.1 = 1 --' AND password

General information

DESCRIPTION	An unfamiliar principal logged on to SQL server 'psqlweuyptobi'.
ACTIVITY TIME	Tuesday, March 12, 2019, 3:23:56 PM
SEVERITY	Medium
STATE	Active
ATTACHED RESOURCE	pdwhweuyptobi
SUBSCRIPTION	Shared PAAS - Prod (d132afd8-4645-49c0-bcb1-c9a5ee42b284)
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	SQL Database
CLIENT IP ADDRESS	52.233.152.50
CLIENT PRINCIPAL NAME	APS_ADF
CLIENT APPLICATION	AzureDataMovement
CLIENT IP LOCATION	Amsterdam, Netherlands
SERVICE TAG	N/A
DATA CENTER	West Europe
POTENTIAL CAUSES	New user, unauthorized access, privilege abuse.

Is the vulnerable






PROTECT ACCESS TO YOUR AZURE SQL DATA

Logon by an unfamiliar principal

pdwhweuyptobi

[Learn more](#)

General information

DESCRIPTION	An unfamiliar principal logged on to SQL server 'psqlweuyptobi'.
ACTIVITY TIME	Tuesday, March 12, 2019, 3:23:56 PM
SEVERITY	 Medium
STATE	Active
ATTACKED RESOURCE	pdwhweuyptobi
SUBSCRIPTION	Shared PAAS – Prod (d132afd8-4645-49c0-bcb1-c9a5ee42b284)
DETECTED BY	 Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	 SQL Database
CLIENT IP ADDRESS	52.233.152.50
CLIENT PRINCIPAL NAME	APS_ADF
CLIENT APPLICATION	AzureDataMovement
CLIENT IP LOCATION	Amsterdam, Netherlands
SERVICE TAG	N/A
DATA CENTER	West Europe
POTENTIAL CAUSES	New user, unauthorized access, privilege abuse.





PROTECT ACCESS TO YOUR AZURE SQL DATA

Potential SQL Injection
samplecrmwedemo

[Learn more](#)

General information

DESCRIPTION	Potential SQL Injection was detected on your database samplecrmwedemo on server ronmatwedemo
DETECTION TIME	Sunday, 13 May 2018, 3:09:12 pm
SEVERITY	! High
STATE	Active
ATTACKED RESOURCE	samplecrmwedemo
SUBSCRIPTION	
DETECTED BY	 Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	 SQL Server
SERVER	
DATABASE	
IP ADDRESS	
PRINCIPAL NAME	dev1
APPLICATION	.Net SqlClient Data Provider
VULNERABLE STATEMENT	SELECT * FROM sqll_users WHERE username = 'OR 1 = 1 --' AND password = 'dfdfdfdf'
THREAT ID	1

Remediation steps

INVESTIGATION STEPS	View the vulnerable SQL statement
REMEDATION STEPS	Read more about SQL Injection threat and how to fix the vulnerable application code.



THREAT DETECTION ON APP SERVICE

- Analyzes traffic patterns
- Usage patterns (e.g. Bitcoin mining)
- Leverages visibility of Microsoft as cloud provider
- Transparent for your application

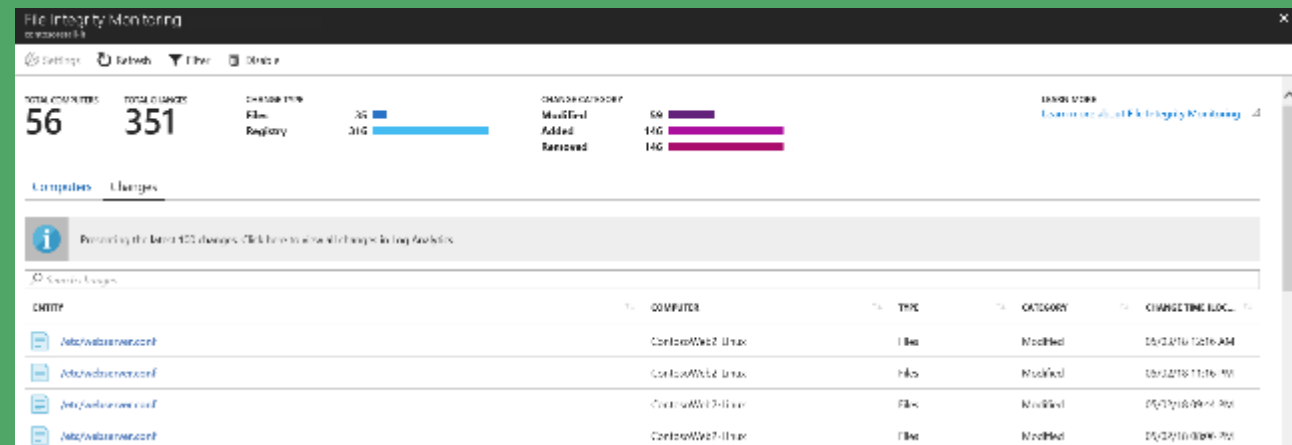


KEEP AN EYE ON IMPORTANT FILES AND SETTINGS

- File Integrity Monitoring
- File & registry creation & removal
- Exclusions possible
- Linux support



PROPERTY	VALUE BEFORE	VALUE AFTER
Ads	[["Name": "owner" "Value": "NT AUTHORITY\SYSTEM"]] ..	[["Name": "owner" "Value": "NT AUTHORITY\SYSTEM"]] ..
ValueData	C:\Windows\System32\WINTRUST.DLL	C:\Windows\SysWOW64\WINTRUST.DLL
▼ Unchanged prop...		
SourceComput...	cda27197-3886-4fb6-8720-112304d1ae1d	No Change
RegistryKey	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptograph...	No Change
Hive	HKEY_LOCAL_MACHINE	No Change
ValueName	Dll	No Change
ValueType	REG_SZ	No Change
Size	32	No Change
SourceSystem	OpsManager	No Change
MG	00000000-0000-0000-0000-000000000001	No Change
ManagementG...	AD1-5bc7c24b-ad6c-4f7f-905c-3ac3f3259938	No Change
TenantId	5bc7c24b-ad6c-4f7f-905c-3ac3f3259938	No Change
VMUID	c14ded1b-054b-4403-9f01-1629eb76c406	No Change



File Integrity Monitoring

Settings | Refresh | Filter | On/Off

total monitors: 56 **total changes: 351**

File: 25 Registry: 316

Changes: 59

Added: 146 Removed: 146

Learn more about File Integrity Monitoring

Computers | Changes

Powered by the latest 100 changes. Click for more details on top priorities.

System Changes

CHITF	COMPUTER	TYPE	CATEGORY	CHANGETIME LOG
Atc/wabswmverconf	ControlWeb2-Ulxax	File	Modified	10/22/16 12:06:34M
Atc/wabswmverconf	ControlWeb2-Ulxax	File	Modified	10/22/16 11:06:30M
Atc/wabswmverconf	ControlWeb2-Ulxax	File	Modified	10/22/16 09:04:30M
Atc/wabswmverconf	ControlWeb2-Ulxax	File	Modified	10/22/16 08:06:30M



KEEP AN EYE ON IMPORTANT FILES AND SETTINGS

File Integrity Monitoring

contosoetail-it

Settings Refresh Filter Disable

TOTAL COMPUTERS

56

TOTAL CHANGES

351

CHANGE TYPE

Files
Registry

35

316

CHANGE CATEGORY

Modified
Added
Removed

59

146

146

LEARN MORE

[Learn more about File Integrity Monitoring](#)

Computers Changes



Presenting the latest 100 changes. Click here to view all changes in Log Analytics.

Search changes

ENTITY	COMPUTER	TYPE	CATEGORY	CHANGE TIME [LOC...]
/etc/webserver.conf	ContosoWeb2-Linux	Files	Modified	05/03/18 12:16 AM
/etc/webserver.conf	ContosoWeb2-Linux	Files	Modified	05/02/18 11:16 PM
/etc/webserver.conf	ContosoWeb2-Linux	Files	Modified	05/02/18 09:44 PM
/etc/webserver.conf	ContosoWeb2-Linux	Files	Modified	05/02/18 08:06 PM



KEEP AN EYE ON IMPORTANT FILES AND SETTINGS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllRemoveS... X
Change details

PROPERTY	VALUE BEFORE	VALUE AFTER
Acls	[{"Name": "owner" "Value": "NT AUTHORITY\\SYSTEM" } { "...	[{"Name": "owner" "Value": "NT AUTHORITY\\SYSTEM" } { "...
ValueData	C:\Windows\System32\WINTRUST.DLL	C:\Windows\SysWOW64\WINTRUST.DLL
▼ Unchanged prope...		
SourceComput...	cda27197-3886-4fbb-8720-1f2304d1ae1d	No Change
RegistryKey	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptograph...	No Change
Hive	HKEY_LOCAL_MACHINE	No Change
ValueName	Dll	No Change
ValueType	REG_SZ	No Change
Size	32	No Change
SourceSystem	OpsManager	No Change
MG	00000000-0000-0000-0000-000000000001	No Change
ManagementG...	AOI-5bc7c24b-ad6c-4f7f-905c-3ac3f3259938	No Change
TenantId	5bc7c24b-ad6c-4f7f-905c-3ac3f3259938	No Change
VMUUID	c14ded1b-054b-4483-9fd1-1829eb76c406	No Change



BLOCK MALWARE AND OTHER UNWANTED APPLICATIONS

- Adaptive Application Control
- Recommended whitelists
- Applocker technology
- Linux support

PROPERTY	VALUE
DESCRIPTION	The below user ran executables that are violating the application control policy of your organization on this machine. It can possibly expose the machine to malware or application vulnerabilities.
ACTIVITY TIME	Wednesday, March 13, 2019, 9:29:47 PM
SEVERITY	Medium
STATE	Active
ATTACKED RESOURCE	tvmaweudslabw
SUBSCRIPTION	Shared PAAS - Test (f836570e-0b34-4af7-96ca-30426fa0dd1)
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
SIGNATURE	-
TARGETUSER	NT AUTHORITY\SYSTEM
HIT COUNT	1
PATH	%OSDRIVE%\WINDOWS\AZURE\SECAGENT\WASECAGENTPROV.EXE



BLOCK MALWARE AND OTHER UNWANTED APPLICATIONS

Description

The steps below will guide you through the process of creating the rules that are unique to this specific resource group.

▼ Select VMs

<input checked="" type="checkbox"/>	VIRTUAL MACHINE	STATE	SEVERITY
<input checked="" type="checkbox"/>	vm2	Open	
<input checked="" type="checkbox"/>	vm1	Open	
<input checked="" type="checkbox"/>	vm3	Open	

▼ Select processes for whitelisting rules

<input checked="" type="checkbox"/>	NAME	PROCESSES	COMMON	EXPLOITABLE
<input checked="" type="checkbox"/>	▶ C:\Windows	134	false	
<input checked="" type="checkbox"/>	▶ C:\Packages\Plugins	27	false	
<input checked="" type="checkbox"/>	▶ C:\WindowsAzure\GuestAgent_2.7.1198.822	6	false	
<input checked="" type="checkbox"/>	▶ C:\Program Files	13	false	
<input checked="" type="checkbox"/>	C:\Program Files (x86)\Qualys\QualysAgent...	1	false	



BLOCK MALWARE AND OTHER UNWANTED APPLICATIONS

EXE application control policy violation was audited

tvmaweudslabw

[Learn more](#)

General information

DESCRIPTION

The below user ran executables that are violating the application control policy of your organization on this machine. It can possibly expose the machine to malware or application vulnerabilities.

ACTIVITY TIME

Wednesday, March 13, 2019, 9:29:47 PM

SEVERITY

 Medium

STATE

Active

ATTACKED RESOURCE

[tvmaweudslabw](#)

SUBSCRIPTION

[Shared PAAS – Test \(f836570e-0b34-4af7-96ca-30426dfa0dd1\)](#)


DETECTED BY

 Microsoft

ENVIRONMENT

Azure

RESOURCE TYPE

 Virtual Machine

SIGNATURE

-

TARGETUSER

NT AUTHORITY\SYSTEM

HIT COUNT

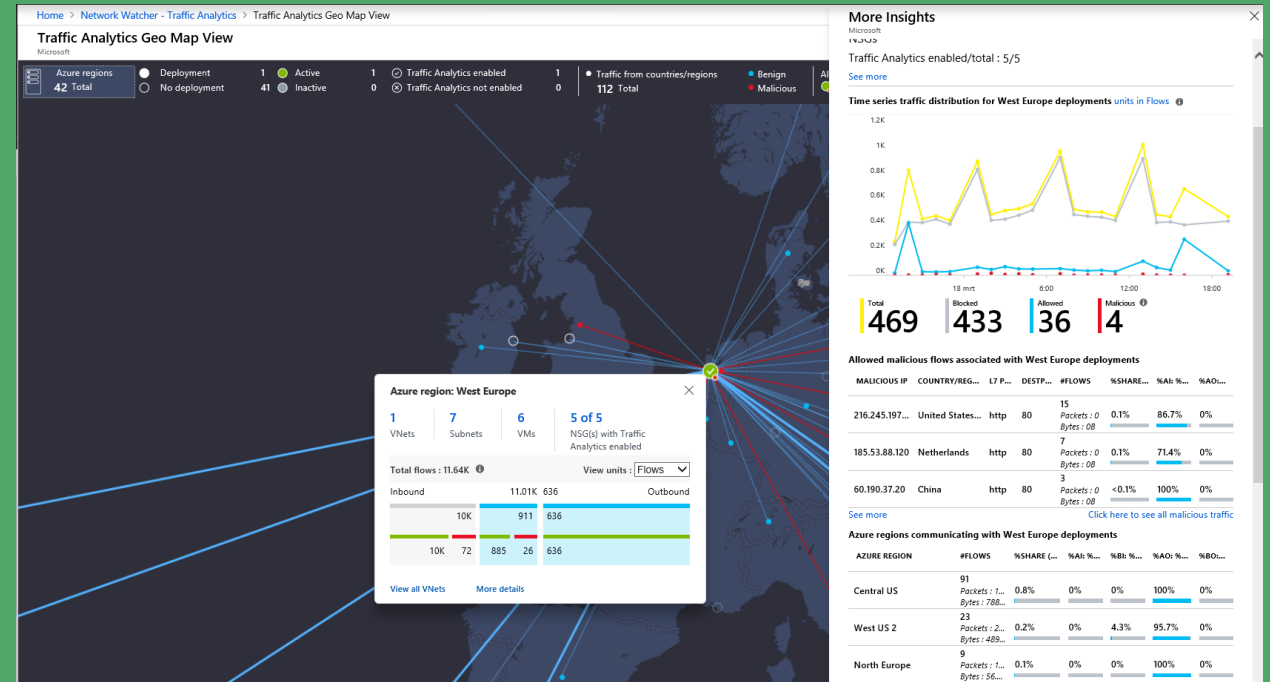
1

PATH

No Signature
%OSDRIVE%\WINDOWS\AZURE\SECAGENT\WASECAGENTPROV.EXE

BE ON TOP OF YOUR NETWORK

- NSG Flow Logs & Traffic Analytics
- Traffic insights



BE ON TOP OF YOUR NETWORK

Home > Network Watcher - Traffic Analytics > Traffic Analytics Geo Map View

Traffic Analytics Geo Map View

Microsoft

Azure regions: 42 Total

Deployment: 1 Active, 41 Inactive, 0 No deployment

Traffic Analytics: 1 enabled, 0 not enabled

Traffic from countries/regions: 112 Total

Benign: 0, Malicious: 0

Azure region: West Europe

1 VNets | 7 Subnets | 6 VMs | 5 of 5 NSG(s) with Traffic Analytics enabled

Total flows: 11.64K

View units: FLOWS

Inbound		Outbound	
10K	911	636	636
10K	72	885	26

[View all VNets](#) [More details](#)

More Insights

Traffic Analytics enabled/total : 5/5

[See more](#)

Time series traffic distribution for West Europe deployments units in Flows

Total: 469 | Blocked: 433 | Allowed: 36 | Malicious: 4

Allowed malicious flows associated with West Europe deployments

MALICIOUS IP	COUNTRY/REG...	L7 P...	DESTP...	#FLOWS	%SHARE...	%AI: %...	%AO:...
216.245.197...	United States...	http	80	15	Packets : 0 Bytes : 0B	0.1%	86.7%
185.53.88.120	Netherlands	http	80	7	Packets : 0 Bytes : 0B	0.1%	71.4%
60.190.37.20	China	http	80	3	Packets : 0 Bytes : 0B	<0.1%	100%

[See more](#) [Click here to see all malicious traffic](#)

Azure regions communicating with West Europe deployments

AZURE REGION	#FLOWS	%SHARE (...)	%AI: %...	%BI: %...	%AO: %...	%BO:...
Central US	91	Packets : 1... Bytes : 788...	0.8%	0%	0%	100%
West US 2	23	Packets : 2... Bytes : 489...	0.2%	0%	4.3%	95.7%
North Europe	9	Packets : 1... Bytes : 56...	0.1%	0%	0%	100%



ASSISTANCE ON THE PATH TO CERTIFICATIONS

- Regulatory Compliance
- Preview
- More checks and certifications incoming
- Automatically generate a report

ASSESSMENT	RESOURCE TYPE	FAILED RESOURCES
[CCE-37659-0] Allow log on locally (Windows Server 2012 R2 Standard)	VMs & computers	1 of 5
[CCE-37659-0] Enable network access protection (Windows Server 2012 R2 Standard)	VMs & computers	1 of 5

Download report

Expand all compliance controls

A5. Information security policies

A6. Organization of information security

A6.1. Internal organization

A6.1.1. Information security roles and responsibilities

A6.1.2. Segregation of duties

ASSESSMENT	RESOURCE TYPE	FAILED RESOURCES
Designate more than one owner on your subscription (Preview)	Subscriptions	0 of 1

A6.1.3. Contact with authorities

A6.1.4. Contact with special interest groups

A6.1.5. Information security in project management

A6.2. Mobile devices and teleworking



ASSISTANCE ON THE PATH TO CERTIFICATIONS

[Download report](#)

Expand all compliance controls


▼ **A5. Information security policies**

▲ **A6. Organization of information security**

▲ **A6.1. Internal organization**

▼ A6.1.1. Information security roles and responsibilities

▲ **A6.1.2. Segregation of duties**

ASSESSMENT	RESOURCE TYPE	FAILED RESOURCES	
Designate more than one owner on your subscription (Preview)	 Subscriptions	0 of 1	<div style="width: 100%; height: 10px; background-color: #92d050;"></div>

▼ A6.1.3. Contact with authorities

▼ A6.1.4. Contact with special interest groups

▼ A6.1.5. Information security in project management

▼ **A6.2. Mobile devices and teleworking**

ASSISTANCE ON THE PATH TO CERTIFICATIONS

∨ **A6. Organization of information security**

∨ A7. Human resources security

∨ **A8. Asset management**

∧ **A9. Access control**

∧ **A9.1. Business requirement of access control**

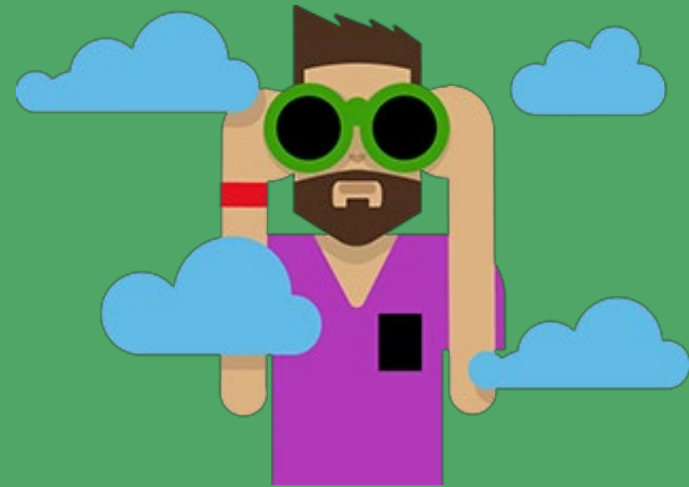
∨ A9.1.1. Access control policy

∧ **A9.1.2. Access to networks and network services**

ASSESSMENT	RESOURCE TYPE	FAILED RESOURCES
[CCE-37659-0] Allow log on locally (Windows Server 2012 R2 Standard)	VMs & computers	1 of 5
[CCE-36923-1] Deny log on as a batch job (Windows Server 2012 R2 Standard)	VMs & computers	1 of 5
[CCE-36877-9] Deny log on as a service (Windows Server 2012 R2 Standard)	VMs & computers	1 of 5
[CCE-37146-8] Deny log on locally (Windows Server 2012 R2 Standard)	VMs & computers	1 of 5
[CCE-36867-0] Deny log on through Remote Desktop Services (Windows Server 2012 R2 St	VMs & computers	1 of 5

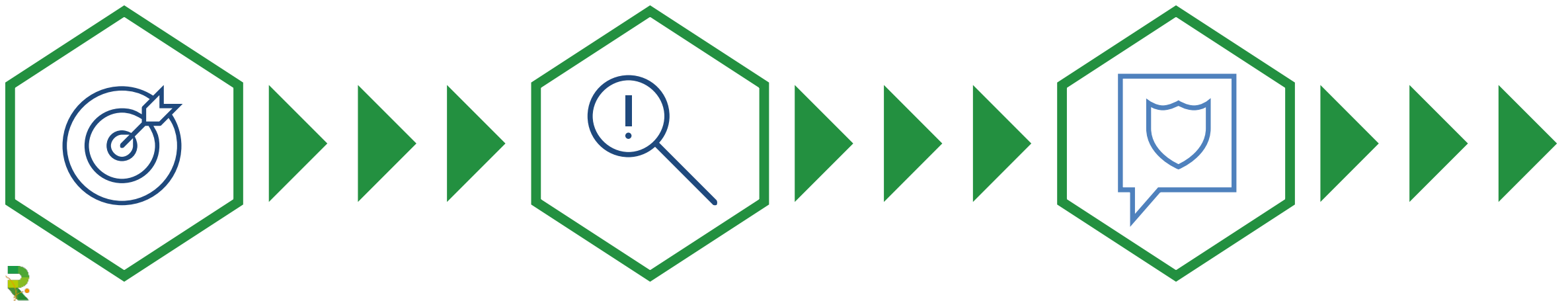
THINK OUTSIDE THE CLOUD

- Non-azure VMs
- CEF events
- SIEM integration
- NGFW connection
- Third party tool integration
- AAD Identity protection
- Advanced Threat analytics



TIPS FOR A SUCCESSFUL IMPLEMENTATION

- Quick win: Start with free (it's enabled by default)
 - Review your current setup
- Let ML do the work for you, no need in endless tweaking
- Define what you want to do with the intelligence
 - Processes
 - Responsibilities
 - Post Breach





QnA

WHAT'S NEXT ?

	Technical Track	Services & Management Track
16:15-17:00	<p>Identity-as-a-Service using Azure Active Directory</p> <p><i>Harold Baele</i></p>	<p>How to make your teams more productive with (Azure) Devops</p> <p><i>Vlad Tomsa, Microsoft</i></p>
17:00-18:30	Reception and Networking	

Thank you!

Reach out to me at:
bart.verboven@realdolmen.com
<https://www.linkedin.com/in/bverboven>

