



HYB20

Securing your Azure Environment

Michael Bender – Cloud Advocate
Microsoft

ITOpsTalk.com | #AZOps | @MichaelBender



Michael Bender

@MichaelBender

Cloud Advocate @Microsoft / #AzOps / #TheKrewe / Teacher / #PowerShell / People Connector / Lifelong Learner / DMs are Open / I tweet what I want

📍 Sun Prairie, WI 🌐 itsallgeek2mike.com 📅 Joined April 2008

834 Following 3,526 Followers

@MichaelBender on Twitter

Helping IT Pros



Cloud Advocacy focused
on Operations



In This Session

- Assessing and remediating subscription security configuration with [Azure Security Center](#)
- Introduction to [Azure Sentinel](#)
- Securing Azure Administrative Access
- Ensuring that VM workloads are kept current with patches using [Azure Update](#)

Cloud security is a shared responsibility

"Through 2020, 95 percent of cloud security failures will be the customer's fault" - Gartner







Security concerns are still the biggest reason organizations avoid the public cloud

Only a small percentage of security incidents impacting enterprises were the fault of the cloud platform

Cloud platform providers must take steps to help customers know the right measures to take to secure their deployments

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

Cloud security is a shared responsibility

Shared responsibility model for cloud security	
Microsoft's commitment	Joint responsibility
Secure foundation <hr/>  Physical assets <hr/>  Datacenter operations <hr/>  Cloud infrastructure	Microsoft provides built-in controls <hr/>  Virtual machines and networks <hr/>  Apps and workloads <hr/>  Data

Hybrid cloud requires new approach to security

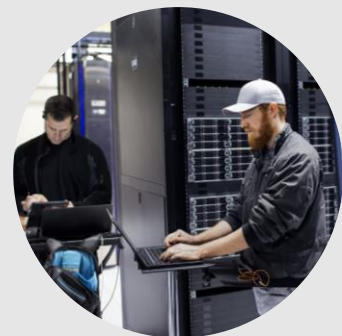
Infrastructure increasingly distributed across public clouds and on-premises datacenter



Rapidly changing
resources



Increasingly
sophisticated attacks



Security skills are in
short supply



Improving security across hybrid cloud environments



Azure Security Center



Strengthen security posture

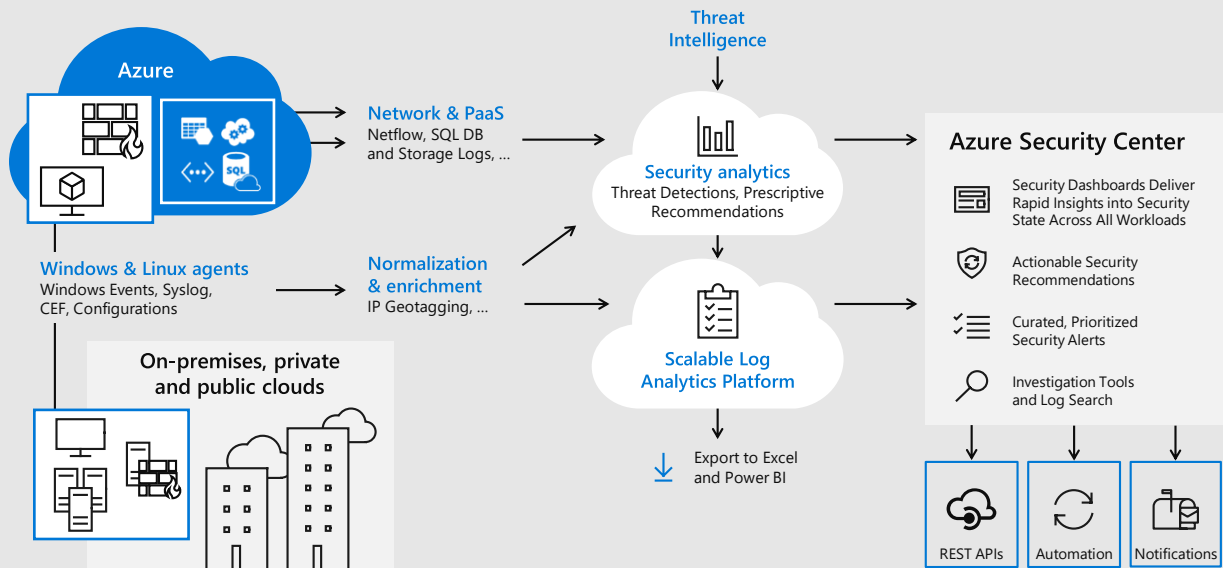


Protect against threats

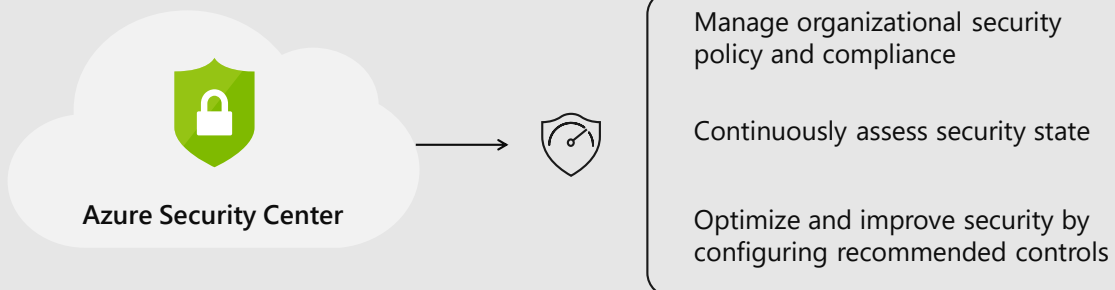


Get secure faster

What Azure Security Center Report On?



Strengthen security posture

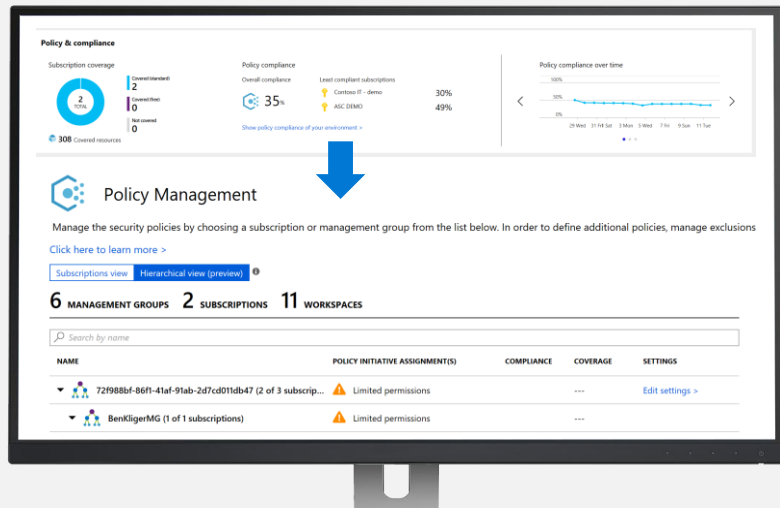


Manage organizational security policy and compliance

Review coverage for Azure Security Center across different subscriptions

Easily set centralized security policies across multiple subscriptions

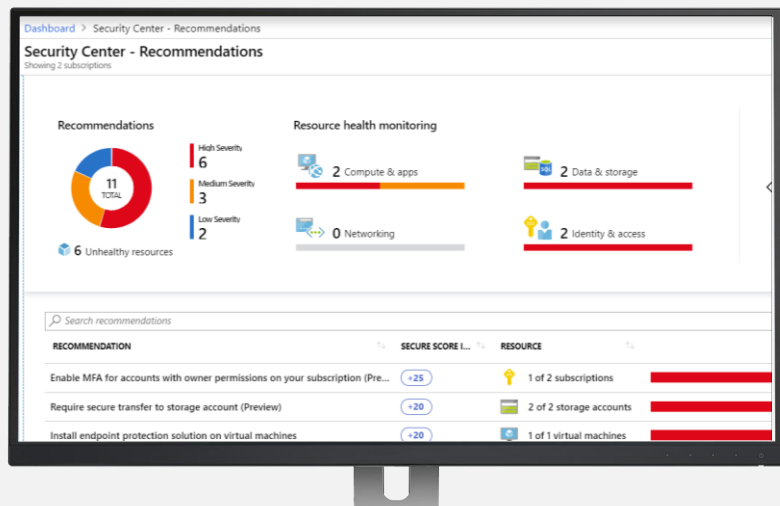
Track and review policy compliance and governance over time



Continuously assess and optimize with Secure Score

Get insights on the security state across your infrastructure

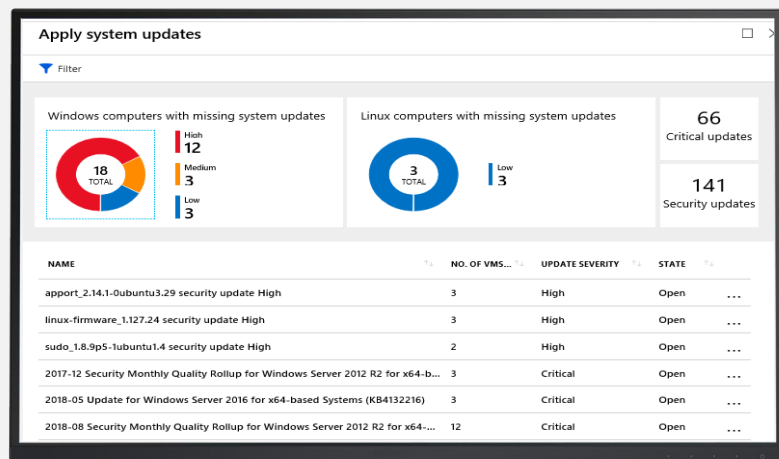
Prioritized recommendations with a security score



Optimize and improve security by configuring recommended controls

Apply a secure configuration standard with built-in recommendations

Reduce attack surface by applying proactive hygiene measures



Demo

Secure Score and Applying Recommendation

Protect against threats



Detect and block advanced malware and threats for servers

Detect threats across IaaS and PaaS services using advanced analytics

Reduce exposure to brute force attacks

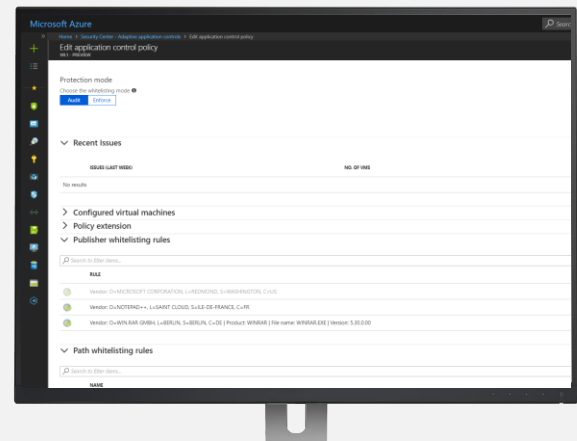
Protect data services against malicious attacks

Adaptive application controls

Control which applications can run on your VMs located in Azure

Adaptive whitelisting learns application patterns

Simplify management with recommended whitelists

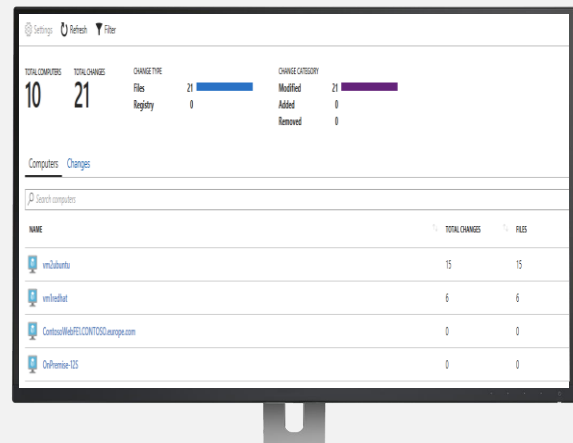


File integrity monitoring

Examines files and registries of the operating system, application software, and others for changes that might indicate an attack

Validates the integrity of Windows files, Windows registry, and Linux files.

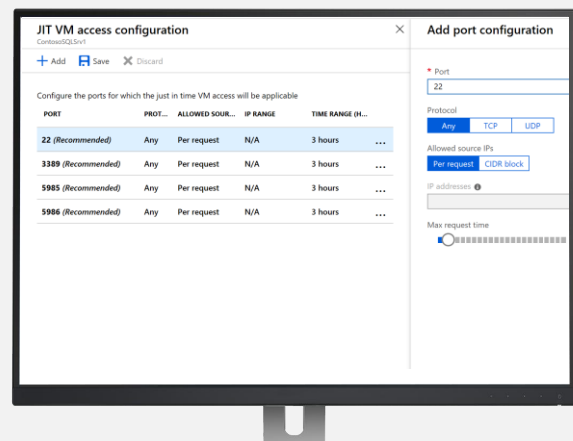
Select the files that you want to be monitored by enabling File Integration Monitoring (FIM)



Limit exposure to brute force attacks

Reduce access to VM ports only when it is needed with Just-in-Time VM Access

Access automatically granted for selected ports, and for limited time, approved users and source IPs



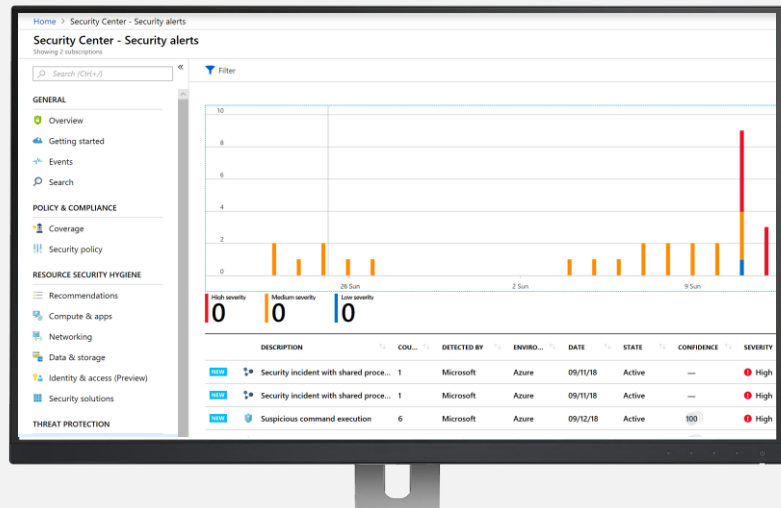
Detect threats across services using advanced analytics

Threat intelligence: looks for known malicious actors

Behavioral analytics: looks for known patterns and malicious behaviors

Anomaly detection: uses statistical profiling to build historical baselines

Fusion: combines events and alerts from across the kill chain to map an attack campaign



Demo

Securing RDP with Just-In-Time Access

Get secure faster

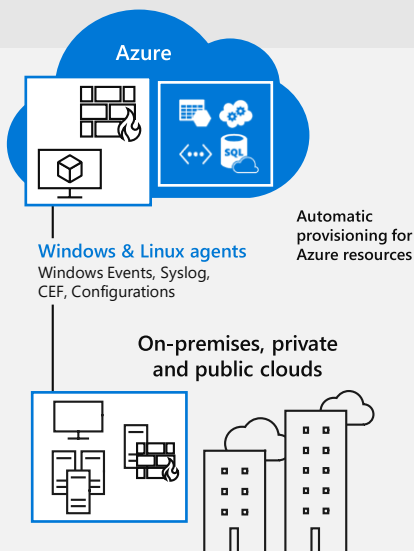


Automatically discover and onboard Azure resources

Extend to server workloads running in other clouds and on-premises datacenter

Integrate with existing workflows and tools (SIEM, NG Firewall..)

Automatic onboarding & extending to hybrid cloud



Seamless Azure integration

Automatically discovers and monitors security of Azure resources

Extensive log collection

Protect servers running on other clouds and on-premises

Adding Computers On-Premises or in Other Clouds

Home > Security Center > Getting started > Onboard servers to Security Center > Direct Agent

Security Center

...e data or use one of the workspaces listed below.

...s for which you have permission. To get tenant-wide visibility follow these [instructions](#).

...space's pricing tier to Standard and start your free 30-day trial. [Learn more](#)

...ow to install the Microsoft Monitoring Agent. [Learn more](#)

...ines under [Compute and apps](#)

COVERAGE	VMS & SERVERS	SUBSCRIPTION	
Standard	0	CDA Global Demos	+ Add Servers
c-a608-83...	Free	4	Upgrade
Standard	2	Ignite the Tour	+ Add Servers
Free	4	CDA Global Demos	Upgrade

/node/month. [Pricing details](#)

Direct Agent

Download an agent for your operating system, then install and configure it using the keys for your workspace ID.

Windows Computers

[Download Windows Agent \(64 bit\)](#)

[Download Windows Agent \(32 bit\)](#)

Linux Computers

[Agent for Linux](#)

DOWNLOAD AND ONBOARD AGENT FOR LINUX

[wget https://raw.githubusercontent.com/...](#)

Workspace ID and Keys

WORKSPACE ID

7b55f52b-10f8-42f6-bd38-9b0037a...

PRIMARY KEY

IC23Dw3PnkV4BF1QeEtJUNICA8g...

SECONDARY KEY

zTIZR9-U2XPPiD9GwJtfk413VM...

OMS Gateway

If you have machines with no internet connectivity to Log Analytics, download the OMS Gateway to act as a proxy. [Learn more](#)

Video on Azure Sentinel

<https://aka.ms/AzureSentinel>

Azure Sentinel

Intelligent security analytics for your entire enterprise.



Collect data at cloud scale—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.



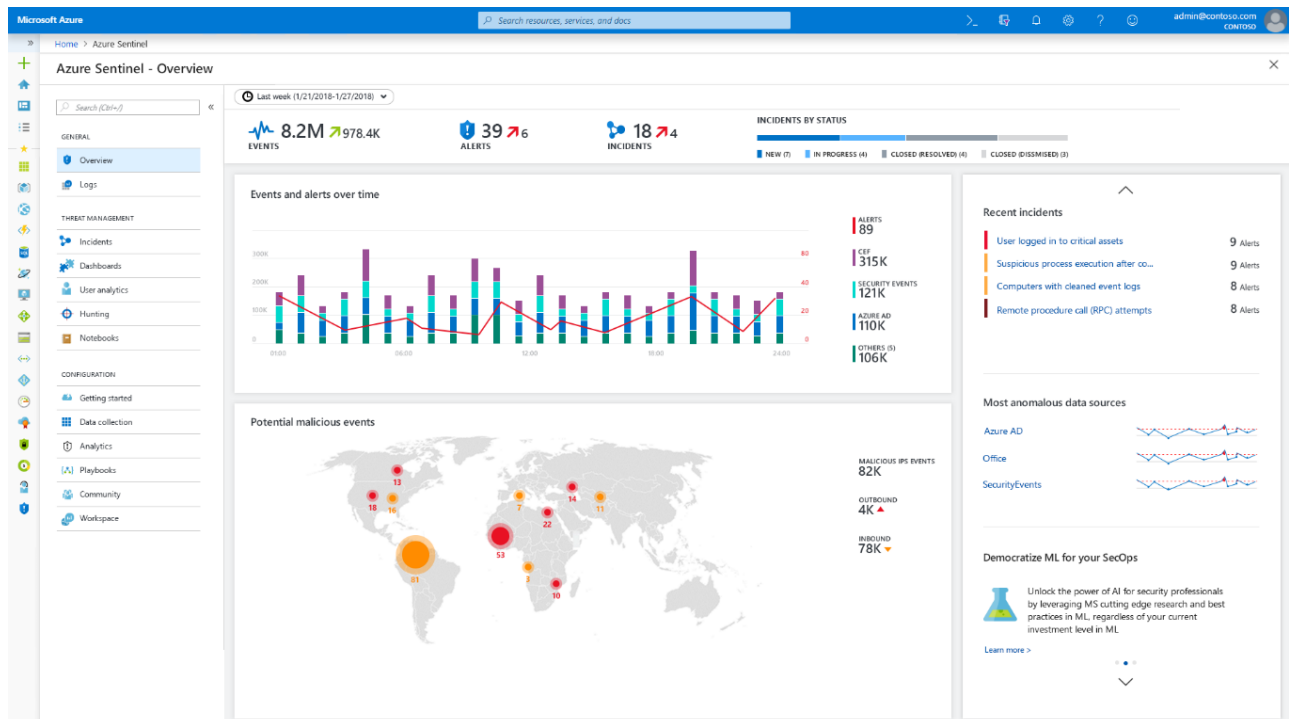
Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence.

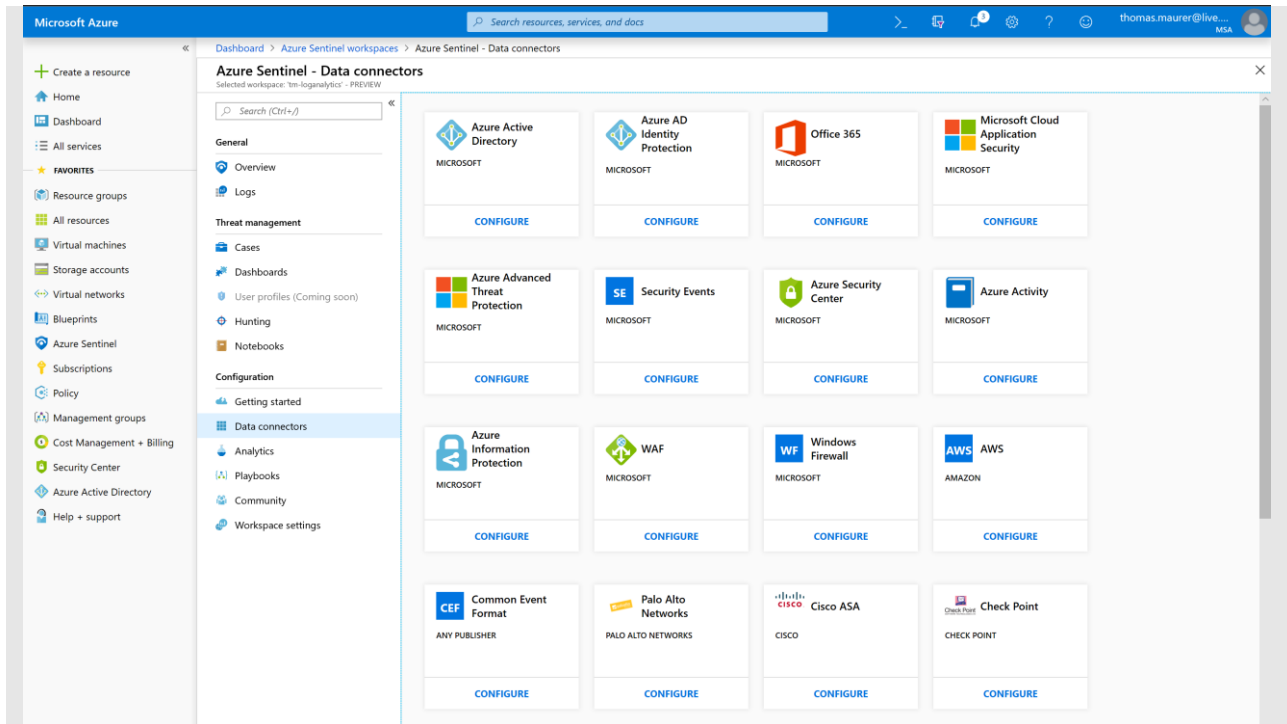


Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.




Respond to incidents rapidly with built-in orchestration and automation of common tasks.





Want More on Azure Sentinel?

- More Information at <https://aka.ms/AzureSentinel>
- Preview Docs: <https://aka.ms/AzSentinelDocs>



What steps can be taken to improve the security of Azure administrative identities and reduce the chance that an account is hijacked and used to impact the subscription?

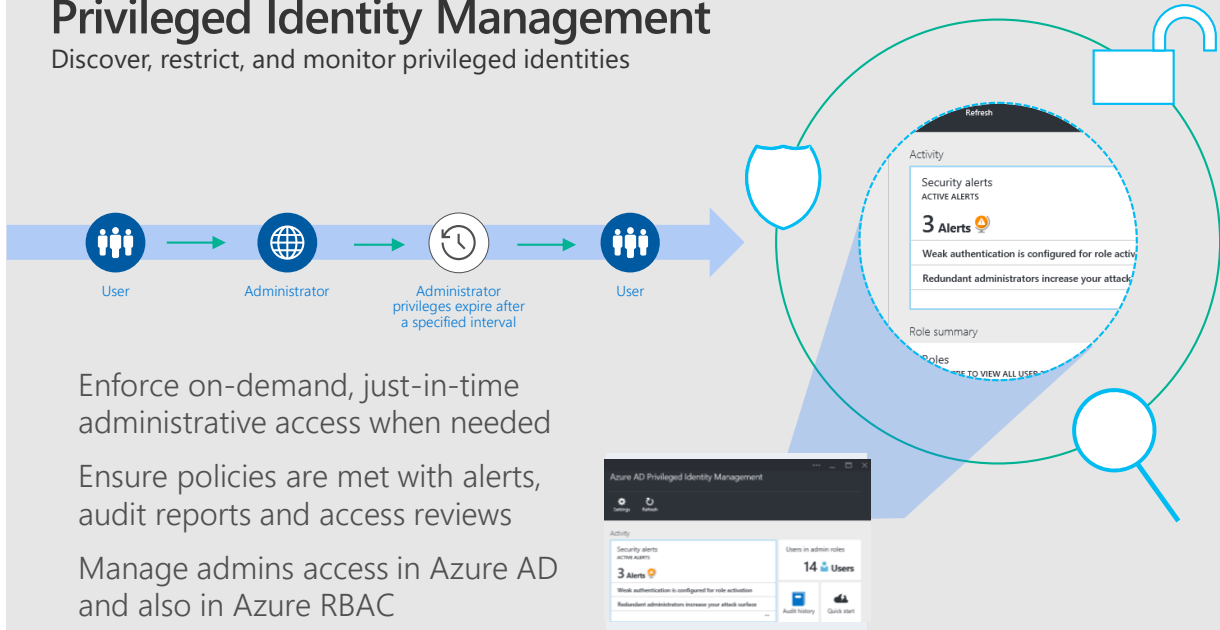
Privileged Accounts are the Keys to the Kingdom



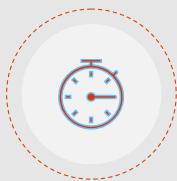
This Photo by Unknown Author is licensed under [CC BY-NC-ND](#)

Privileged Identity Management

Discover, restrict, and monitor privileged identities



Azure AD Privileged Identity Management



Just in Time
Access



Just Enough
Access



Privileged Admin
Workflow



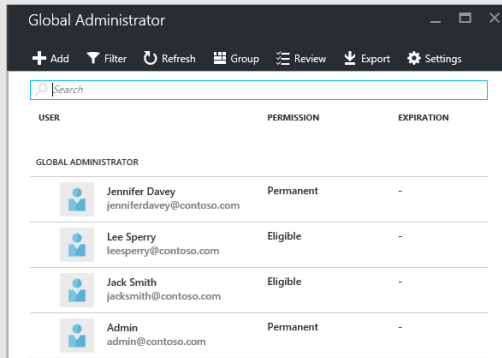
Audit-ready

Protect and control privileged access to your organization

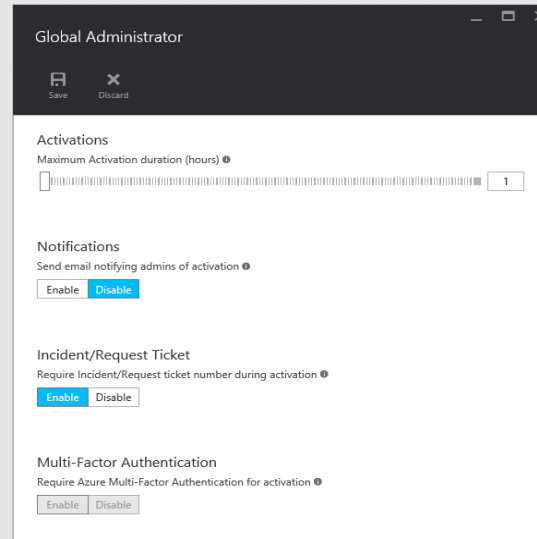
Requires Azure AD P2

Azure PIM role management

Manage the administrators by adding or removing permanent or eligible administrators to each role:



USER	PERMISSION	EXPIRATION
GLOBAL ADMINISTRATOR		
Jennifer Davey jenniferdavey@contoso.com	Permanent	-
Lee Sperry leesperry@contoso.com	Eligible	-
Jack Smith jacksmith@contoso.com	Eligible	-
Admin admin@contoso.com	Permanent	-



Global Administrator

Save Discard

Activations

Maximum Activation duration (hours) 1

Notifications

Send email notifying admins of activation

Enable Disable

Incident/Request Ticket

Require Incident/Request ticket number during activation

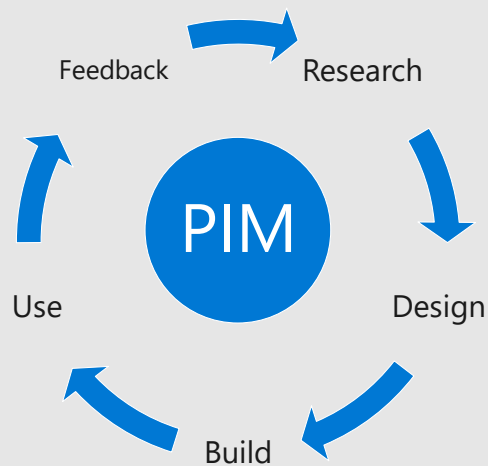
Enable Disable

Multi-Factor Authentication

Require Azure Multi-Factor Authentication for activation

Enable Disable

Planning & Implementing PIM

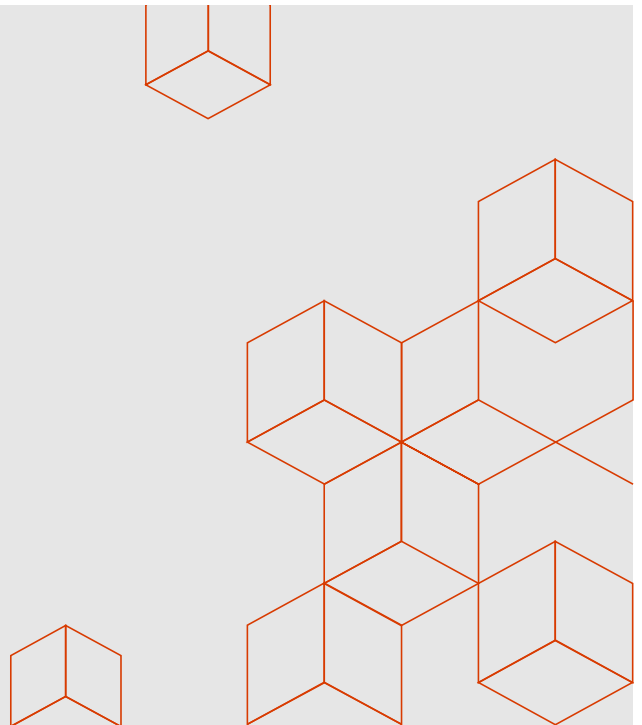


Tailwind Traders management wants to ensure that anyone performing privileged Azure administrative actions verifies their identity and that access to especially sensitive roles requires approval

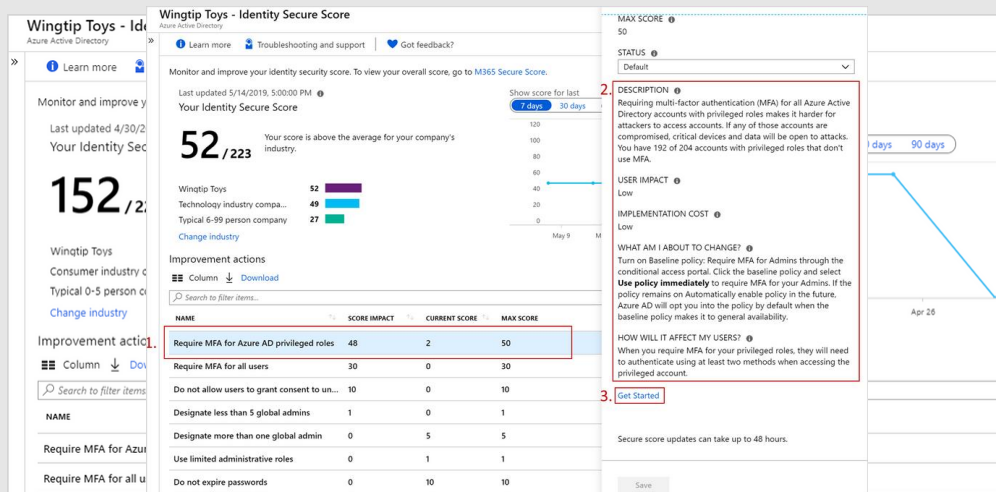


Demo

Privileged Identity Management



Identity Secure Score - Preview



More Information : <https://aka.ms/AA564lb>

If you do one thing, Please Secure Your Privileged Accounts!!!

Michael Bender @MichaelBender

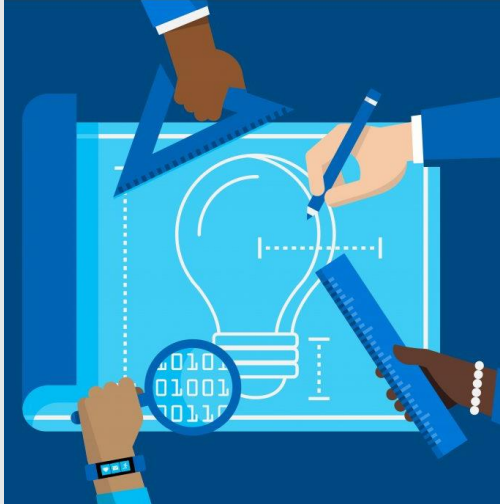
If you aren't looking are securing your Identities in #Azure, you really aren't serious about security. Take @markmorow's advice on this.

Mark Morowczynski @markmorow · May 21

Alright folks, take a look at this. A large portion of my conversations with customers can be eliminated if people would just follow this. We could talk about other things. Books you are reading. Why they shouldn't re-make Cowboy Bebop. Whatever you want. It would be great. twitter.com/Alex_A_Simons...

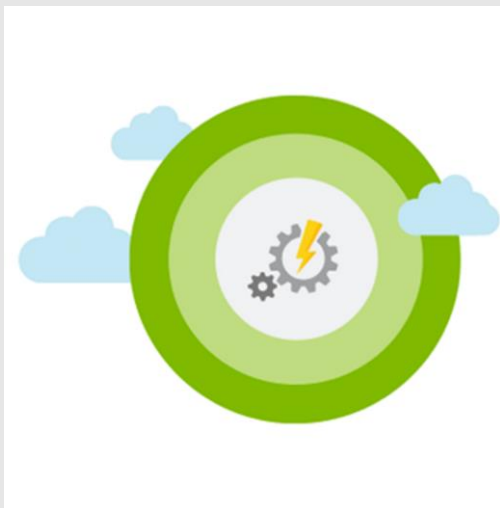
10:48 AM · May 22, 2019 · Twitter Web App

Software Update Management Challenge



- Both physical and virtual machines, both on-prem and IaaS, running Windows or Linux remain current with software updates
- Ability to determine update compliance of physical and virtual machines, both on-prem and IaaS, running Windows or Linux
- Centralize deployment of software updates to on-prem and IaaS Windows and Linux computers

Azure Software Update



- Checks update compliance of their Windows and Linux computers, both on-prem and in Azure IaaS
- Can deploy and install software updates to Windows and Linux computers, both on-prem and in Azure IaaS
- Avoids having to use different products depending on operating system or where the computer is located within the hybrid deployment

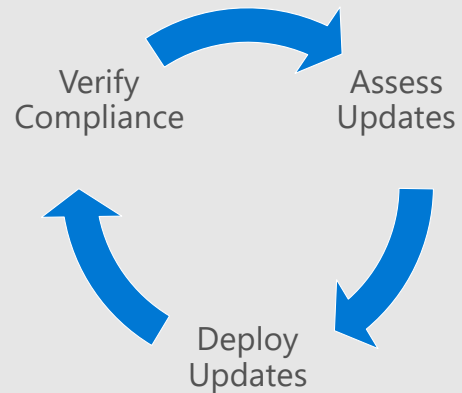
Azure Update Management

Assess update status of servers across your environment

- Windows, Linux
- Azure, other cloud, on-prem

Deploy updates

- Custom approval criteria
- Single pane of glass
- Automated periodic deployments



Azure Update Management

Compliance Scan:






- Windows: Every 12 hours
- Linux: Every 3 hours (every 15 minutes if MMA agent is deployed)

Update Deployment:

- Linux computers can check against a local repo or public repo
- Windows computers can check against MS Update or WSUS



Supported Operating Systems

				
Windows: Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019	Red Hat Enterprise Linux 6 (x86/x64) and 7 (x64)	SUSE Linux Enterprise Server 11 (x86/x64) and 12 (x64)	Ubuntu Server 14.04 LTS & 16.04 LTS	CentOS 6 (x86/x64) and 7 (x64)

Demo

Azure Software Updates

In this session we learned how you can:

- Improve the security configuration of workloads running in Azure by leveraging **Azure Security Center** recommendations and remediations
- Improve the security of Azure administrative accounts using **Privileged Identity Management**
- Ensure that IaaS VM operating systems can be kept current with the latest software updates using **Azure Software Update**

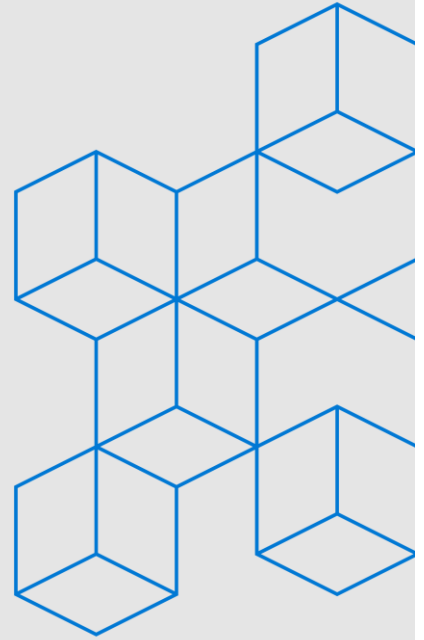
Watch the full Presentation from Microsoft Ignite | The Tour



- <https://youtu.be/aO9tMfGVuRI>

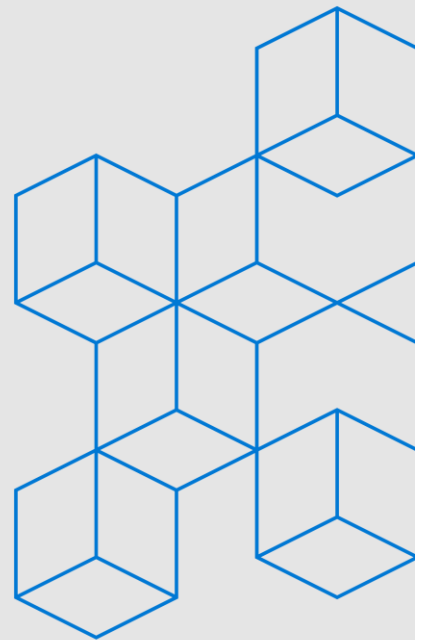


Want to learn more?



Want to try Microsoft Azure?

More information on free trial at
<https://azure.microsoft.com/free/>



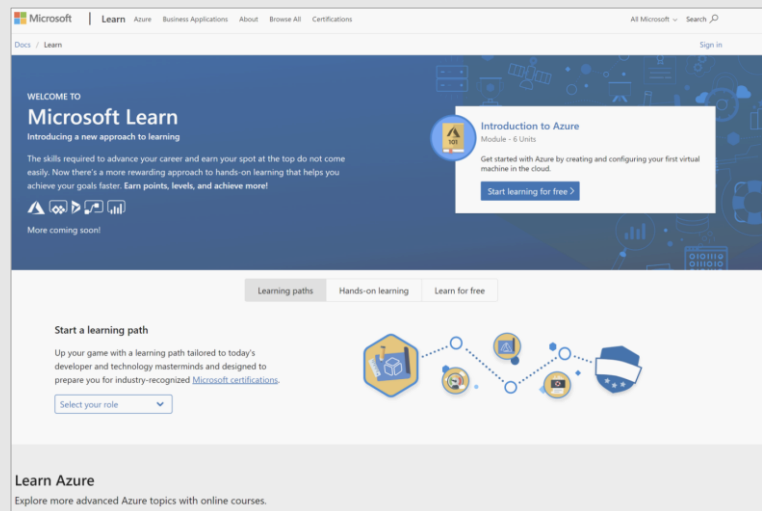
/Learn alert

Introduction to security in Azure

<https://aka.ms/AzureSecurityStarter>

Top 5 security items to consider before pushing to production

<https://aka.ms/AzureSecurityCenterLab>



/Docs alert

Azure Security Center

<https://aka.ms/ASCstarter>

Privileged Identity Management

<https://aka.ms/PIMDocs>

Azure Software Update

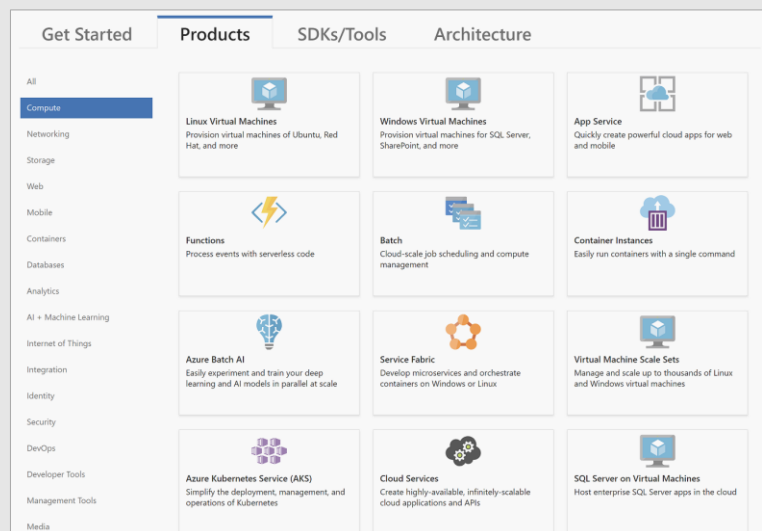
<https://aka.ms/ASUDocs>

Just In Time VM Access

<https://aka.ms/JITDocs>

Azure Sentinel

<https://aka.ms/AzSentinelDocs>



/Docs alert

Secure Score

<https://aka.ms/SecScoreDocs>

Security Center Policies

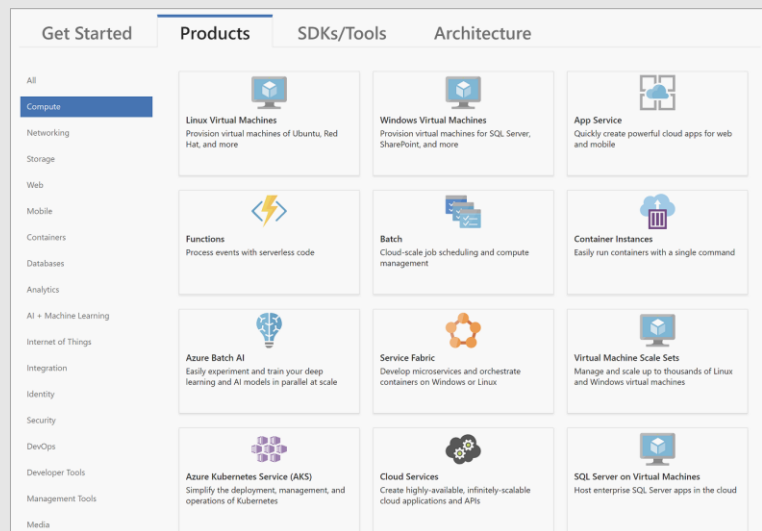
<https://aka.ms/SecPolicyDocs>

Conditional Access Azure Management

<https://aka.ms/CondAccessDocs>

Identity Secure Score

<https://aka.ms/AA5641b>



/Social alert

TechCommunity Blog

ITOpsTalk.com

Social

[#AZOps](https://twitter.com/MichaelBender)

@MichaelBender on Twitter





Thank You

© Copyright Microsoft Corporation. All rights reserved.