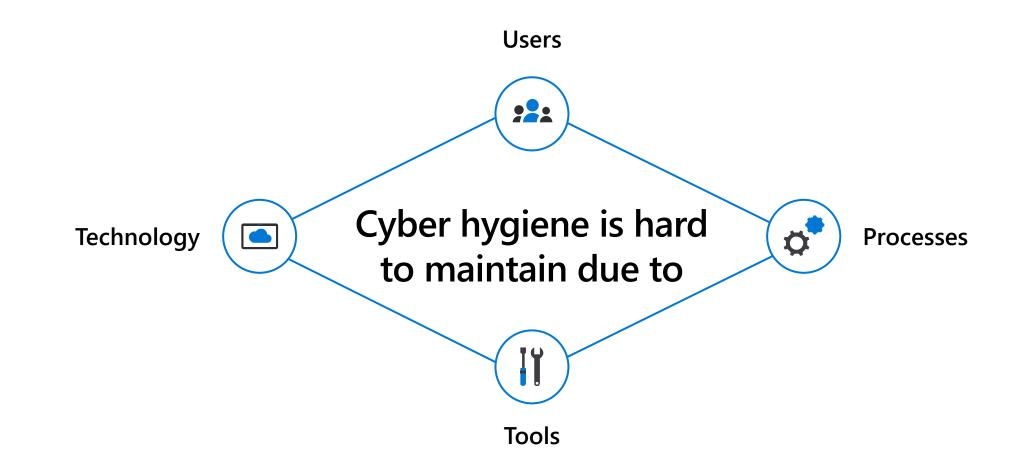


RAZOR TECHNOLOGY

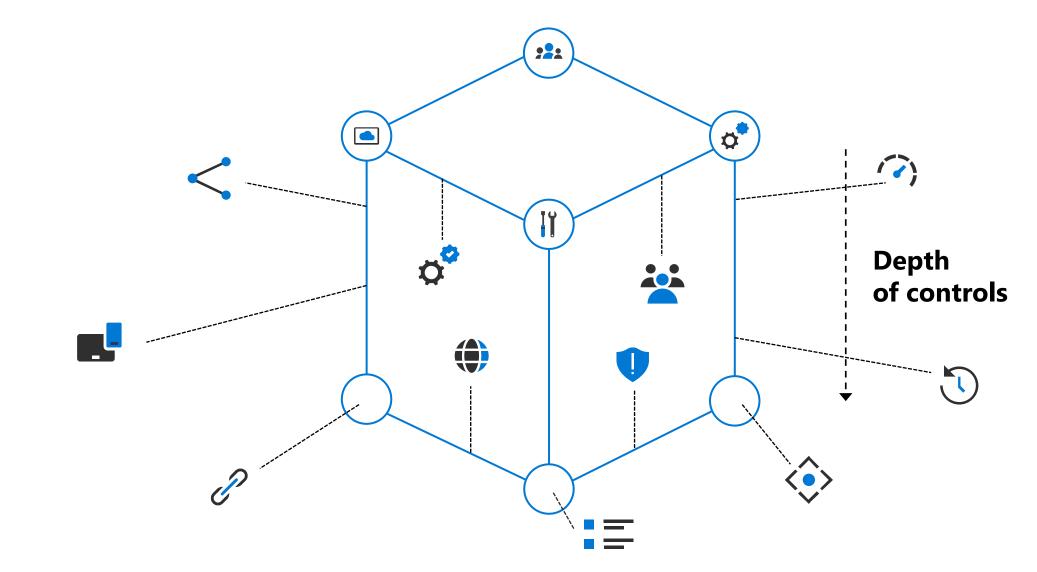
Identity Workshop Microsoft Secure Score Overview

David J. Rosenthal VP & GM, Digital Business September 17, 2020

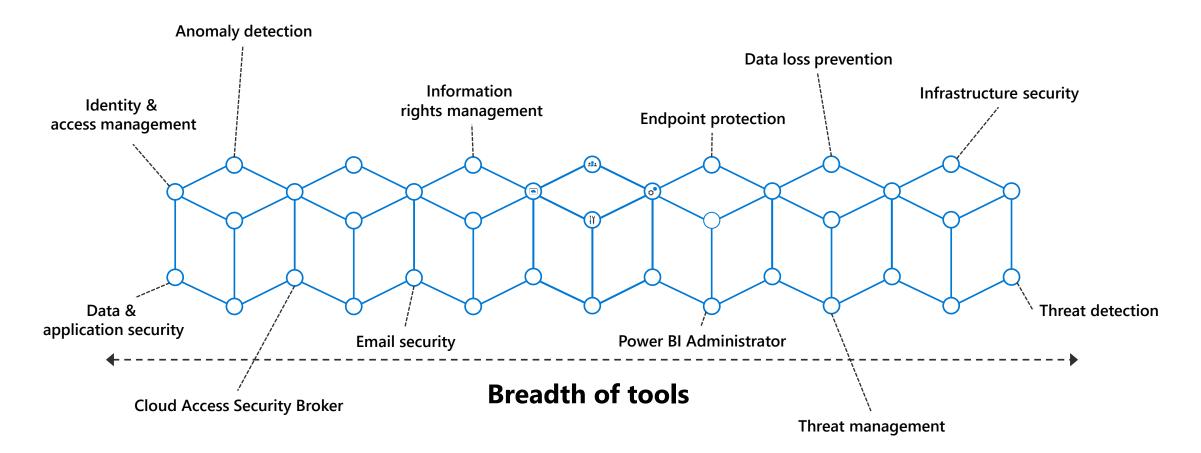




Cyber hygiene is hard to maintain due to

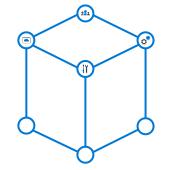


Cyber hygiene is hard to maintain due to



Cyber hygiene is hard to maintain due to

1000s of security controls



~100 security apps and tools



Microsoft Secure Score Vision

Empower every organization to achieve their most secure, most productive security posture.

One number for org-wide posture; Higher number indicating lower risk

Absolute true posture

Built-in and integrated

Heterogenous environment

	Microsoft 365 security					
=						
ଜ ୫ ଅ	Microsoft Secure Score (preview) This service is currently in preview and is subject to the terms and conditions in the Online Services Terms. Overview Improvement actions History Metrics & trends Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.					
0 	Your secure score Inclu Secure Score: 44% 798/7/B13 Points achieved	ude \vee	Actions to review Regressed ^① To address Planned Risk accepted 3 81 11 4	Recently added ⁽¹⁾ 3	Recently updated ^①	
م ن	50%		Top improvement actions			
<u> </u>	25%		Improvement action	Score impact	Status	Category
5	مرین مان طور علی قان این شان مان می شود این مان می شود می می شود می	6 tol 10 120 P2	Require MFA for Azure AD privileged roles Update Microsoft Defender Antivirus definitions	+10%	 To address To address 	Identity Device
5	Breakdown points by: Category 🗸		Restrict unauthorized network access to Azure resources	+9%	 To address 	Device
5	Identity	60%	Discover trends in shadow IT application usage	+9%	 To address 	Apps
0	Data	27%	Turn on Microsoft Defender ATP sensor	+9%	 To address 	Device
	Device	46%	Set up Office 365 ATP Safe Links policies to verify URLs	+9%	 To address 	Data
	Apps 33% Infrastructure 28% Points achieved Opportunity		Turn on customer lockbox feature	+8%	 To address 	Data
			Allow anonymous guest sharing links for sites and docs	+8%	 To address 	Data
			Enable 'Local Security Authority (LSA) protection' View all	+8%	 To address 	Device
	History			Messages from Microsoft		
	October 24, 2019 11:33 AM	n creating child processes		10/16/2019 Top 6 email security best practices to pro email compromise https://www.microsoft.com/security/blc exploiting-the-winrar-cve-2018-20250-1		
	October 23, 2019 5:00 PM • 8% regressed for Turn on Microsoft Defender /					
	October 23, 2019 5:00 PM Security Admin marked Designate more than one global admin as risk accepted				09/26/2019	2210-20200-
	October 23, 2019 12:02 PM • -1% score change because Microsoft added Apply Data Loss Prevention Policies			Multi-stage, fileless Noder	sok campaign	





Provides security administrators with

- Discoverability
- Guidance

Microsoft 365 security

Top improvement actions

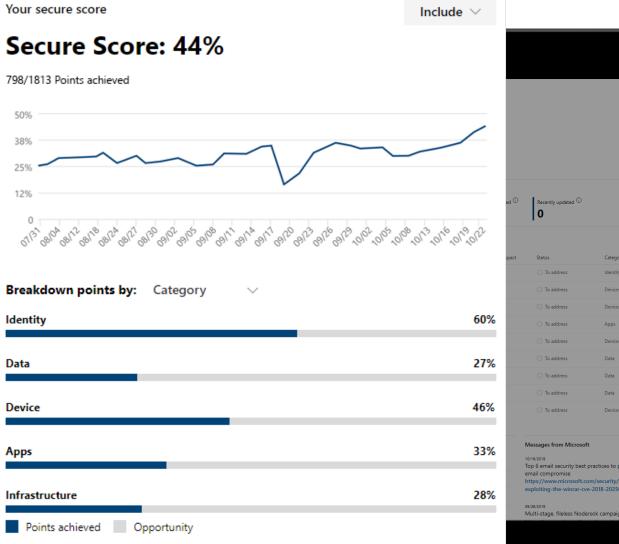
Improvement action	Score impact	Status	Category
Require MFA for Azure AD privileged roles	+10%	 To address 	Identity
Update Microsoft Defender Antivirus definitions	+9%	 To address 	Device
Restrict unauthorized network access to Azure resources	+9%	 To address 	Device
Discover trends in shadow IT application usage	+9%	 To address 	Apps
Turn on Microsoft Defender ATP sensor	+9%	 To address 	Device
Set up Office 365 ATP Safe Links policies to verify URLs	+9%	O To address	Data
Turn on customer lockbox feature	+8%	O To address	Data
Allow anonymous guest sharing links for sites and docs	+8%	O To address	Data
Enable 'Local Security Authority (LSA) protection' View all	+8%	O To address	Device

October 23, 2019 12:02 PM	 -1% score change because Microsoft added Apply Data Loss Prevention Policies 	09/26/2019 Multi-stage, fileless Nodersok campaign
October 23, 2019 5:00 PM	Security Admin marked Designate more than one global admin as risk accepted	exploiting-the-winrar-cve-2018-20250-v
October 23, 2019 5:00 PM	8% regressed for Turn on Microsoft Defender ATP	email compromise https://www.microsoft.com/security/blo
October 24, 2019 11:33 AM	 1% gained by completing Block all Office applications from creating child processes 	Top 6 email security best practices to pro

What is my security posture?

Enables organizations to assess

- Org wide security posture
- Broken down by category, product, security solution



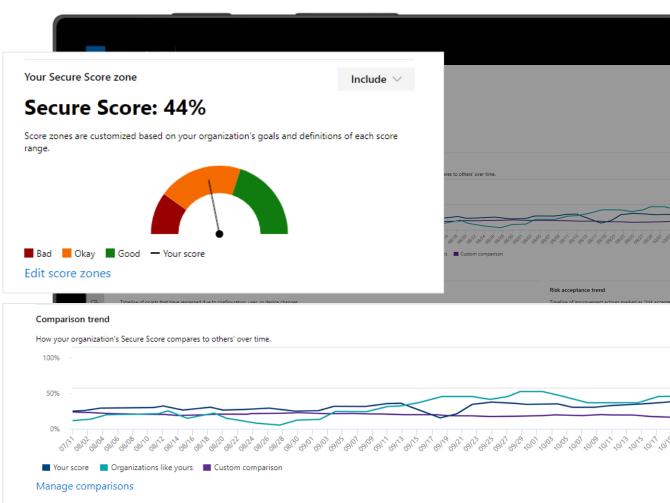
How do I take action
 In-built experiences to plan Integration with workload portals and IT-BPOS systems
and monitor control effectiveness?
Real-time monitoring

Microsoft 365 Manage	security I순 Share	Edit status and notes	ivileged roles ** It harder for attackers to access accounts. Privileged roles have higher permissions than typical users, and include all admin stical devices and data will be open to attacks.	Points achieved Point of 0/10 0
At a Glanc Category: Ider Protects again	Mic	Actions to review	e to ServiceNow ×	Implementation
Compliance: CSA CCM301: (User impact: Lov	Si W	3	ire * ire MFA for Azure AD privileged roles	Prerequisites Vone Next steps Create a new policy throug 1. Select + New Policy 2. Go to Assignments > Us
Complexity: Low Source: Azure Active Direct Tags: Add tags	ory	Ac	<pre>_scription * equiring multi-factor authentication (MFA) for all Azure tive Directory accounts with privileged roles makes it irder for attackers to access accounts. // rity *</pre>	3. At a minimum, select the admin. Helpdek admin. Se 4. Go to Cloud apps or such southing slee) 5. Enable policy > On 7. Create You have 0 of 24 accounts Learn more How MRA works Plan for Asser MRA
			date	
			i Nov 15 2019	
Related reports <u>Risky use</u> <u>Risk even</u>		Designate fewer than 5 global admins Require MFA for all users Register all users for multi-factor authentication		

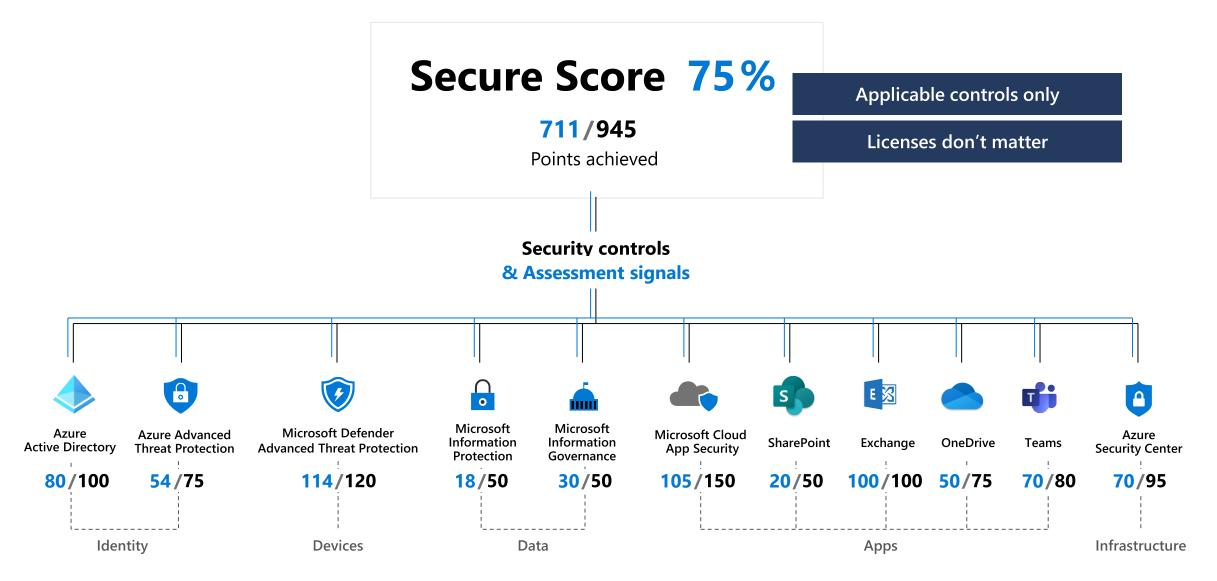
How can I report to my CISO?

Enables security teams to demonstrate

- Progress to CISO
- Benchmark



How does it work?



Questions & Answers



Thank you

© Copyright Microsoft Corporation. All rights reserved.