



Thank you to our host:



Using the Software You Own to Secure Office 365

Ed Higgins
Director of Security and Compliance



2019 Partner of the Year Winner
PowerApps Award
2019 Partner of the Year Finalist
Modern Desktop Award
Power BI Award

2019 MSUS Partner
Award Winner
Modern Workplace –
Security and Compliance



Who am I?

Security and Compliance Challenges

80%

of security incidents occur from within

62%

of cloud adopters nervous about cloud security

63%

of businesses are understaffed in security expertise

50%

of business cloud adoption is led by Shadow IT

\$7B

global damage caused by ransomware

51%

can't find and keep the needed skillsets

93%

of cyber attacks target user identity

\$4M

average cost of a successful security breach

Imagine if...

Our Collective Why



Sensitive data could be automatically encrypted

Compliance gaps between IT and Audit could be eliminated

You could be notified if SSN is posted in a document

Employee couldn't forward secure documents

Users could classify sensitive emails or documents

Cloud could be more secure than anything on-prem

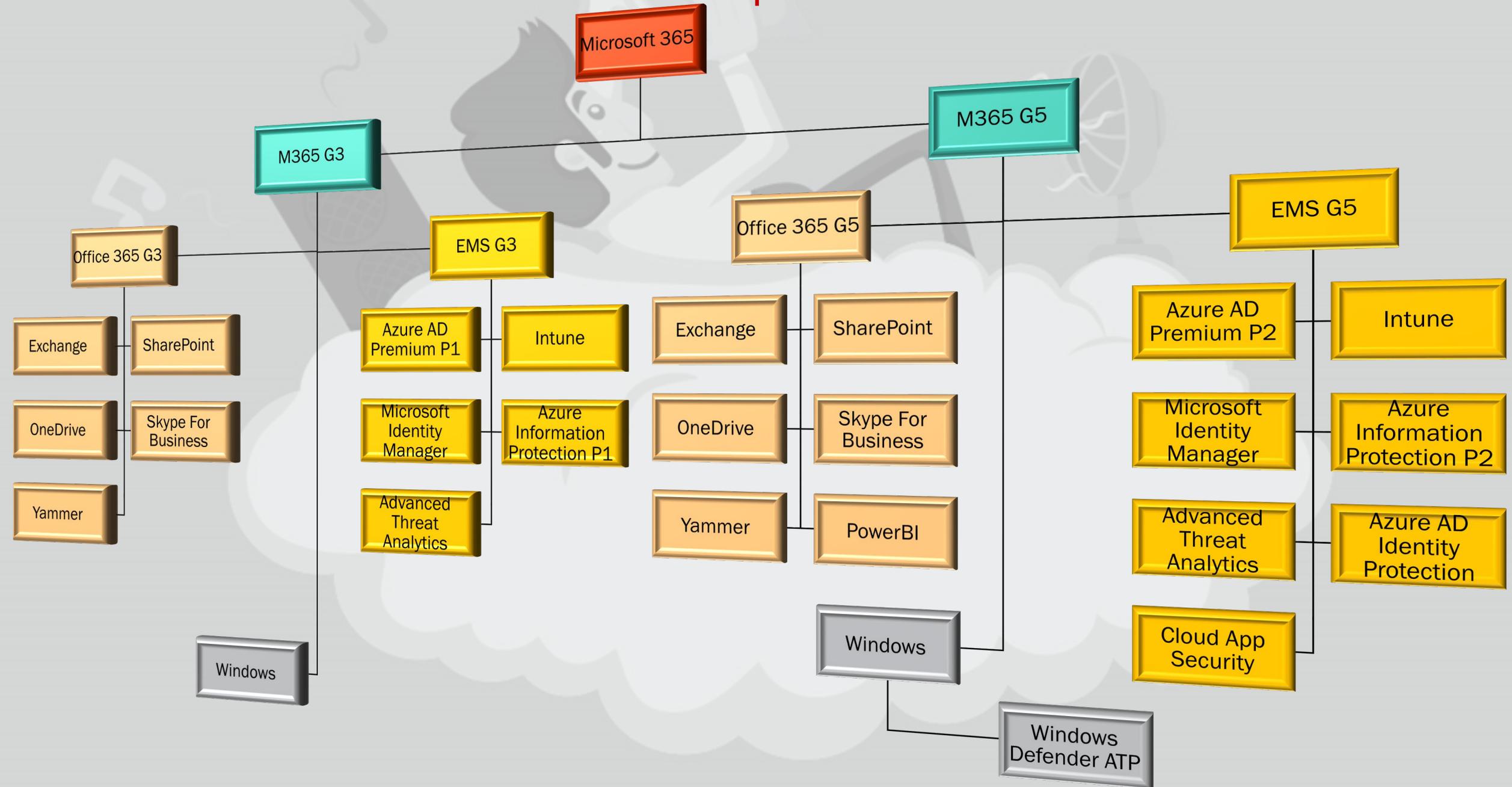
You could detect users logging in from improbable locations

Phishing success could be reduced to nearly zero

Employees could work securely from anywhere, anytime

Mobile devices could be more secure

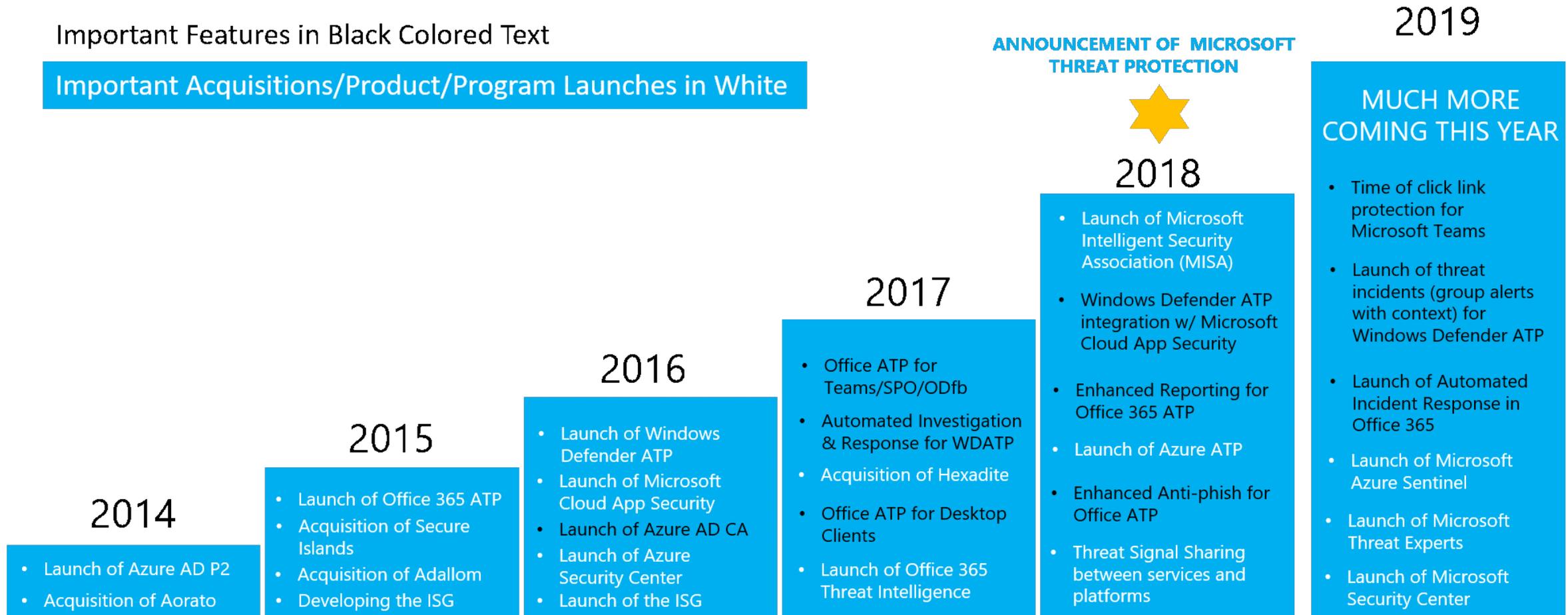
Let's Face It - Microsoft 365 is Complex



Microsoft's Security Focus

Important Features in Black Colored Text

Important Acquisitions/Product/Program Launches in White

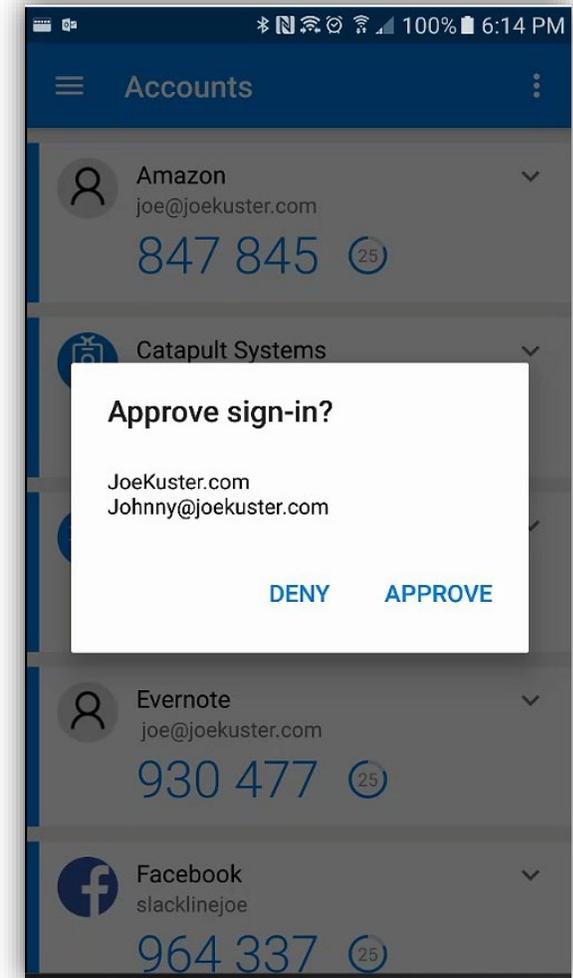
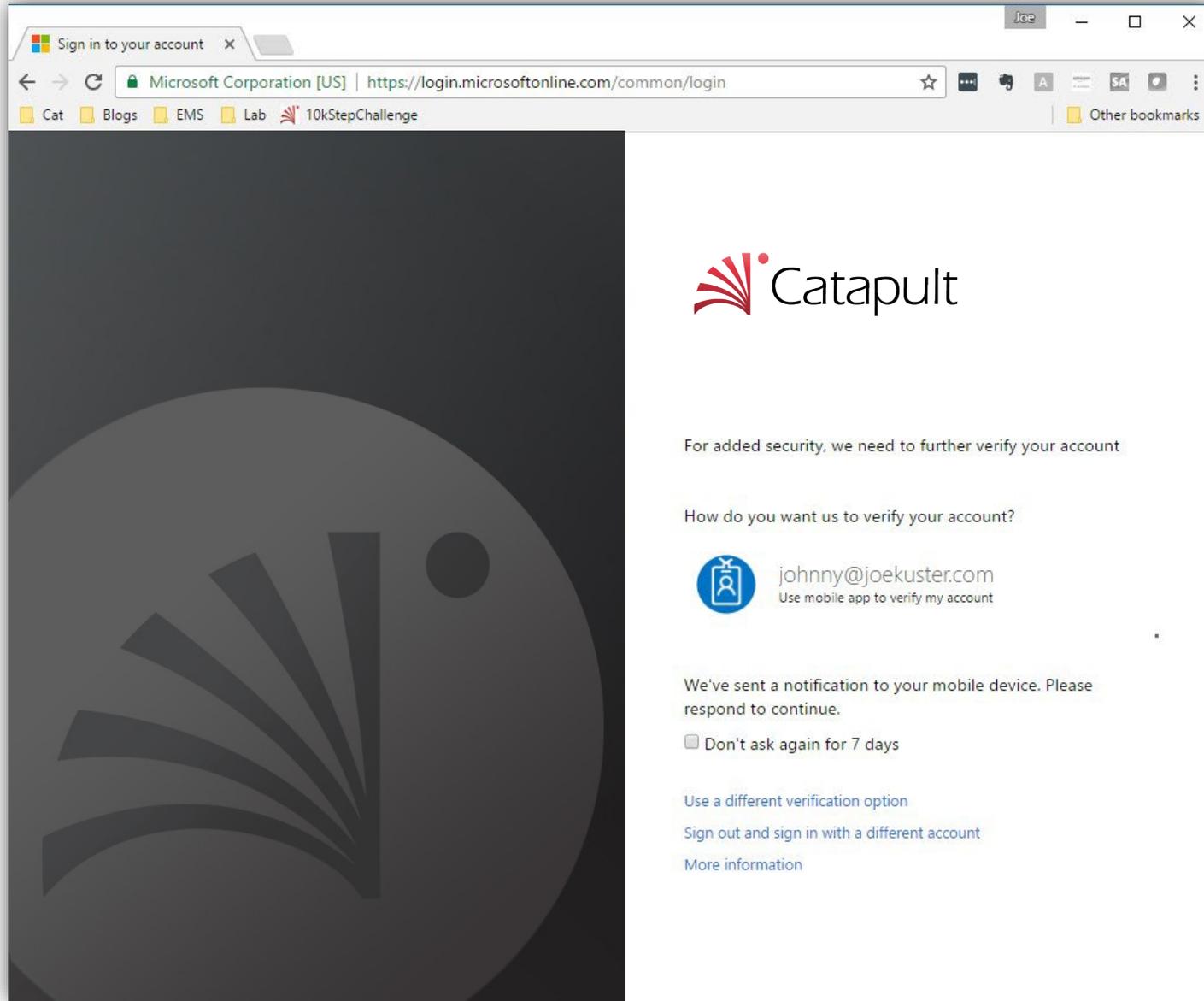


Hey, is this a sales pitch?

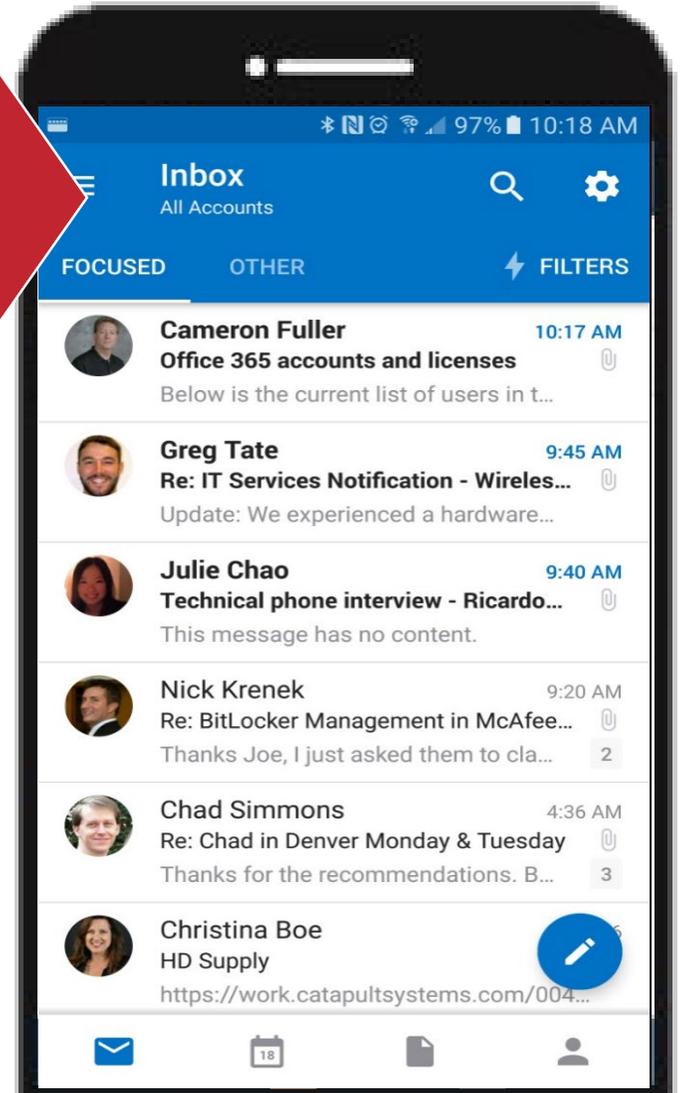
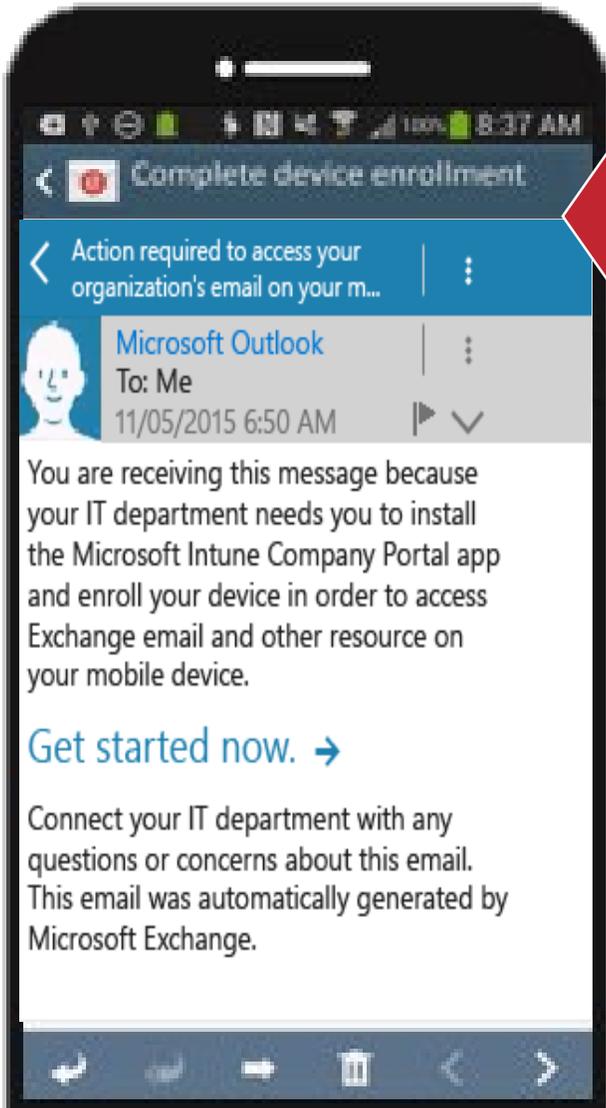
- Not at all.
- Microsoft has created some great security tools and features that you already own.
- Knowing where these are, how to use them, how they impact your security posture
- Tools and threat-landscape is always advancing – hard to keep up. That's my point.



Login Protection – Priv-users or All users



Conditional Access



Secured Emails (Content, Classification, Automated)

Classify to your Policy

Tooltips warn user on content

Action based on content/class

Automatically detect sensitive info

The screenshot shows the Microsoft Word interface for editing an email. The title bar reads "Sensitive Email Test - Message (HTML)". The ribbon includes "File", "Message", "Insert", "Options", "Format Text", and "Review". The "Message" ribbon is active, showing options like "Message Fields", "Basic Text", "Names", "Include", and "Protection".

Information Classification: **Confidential (Lock it Down) \ Do Not Forward** | Public (Wide Open) | Sensitive (General Business) | Confidential (Highly Confidential)

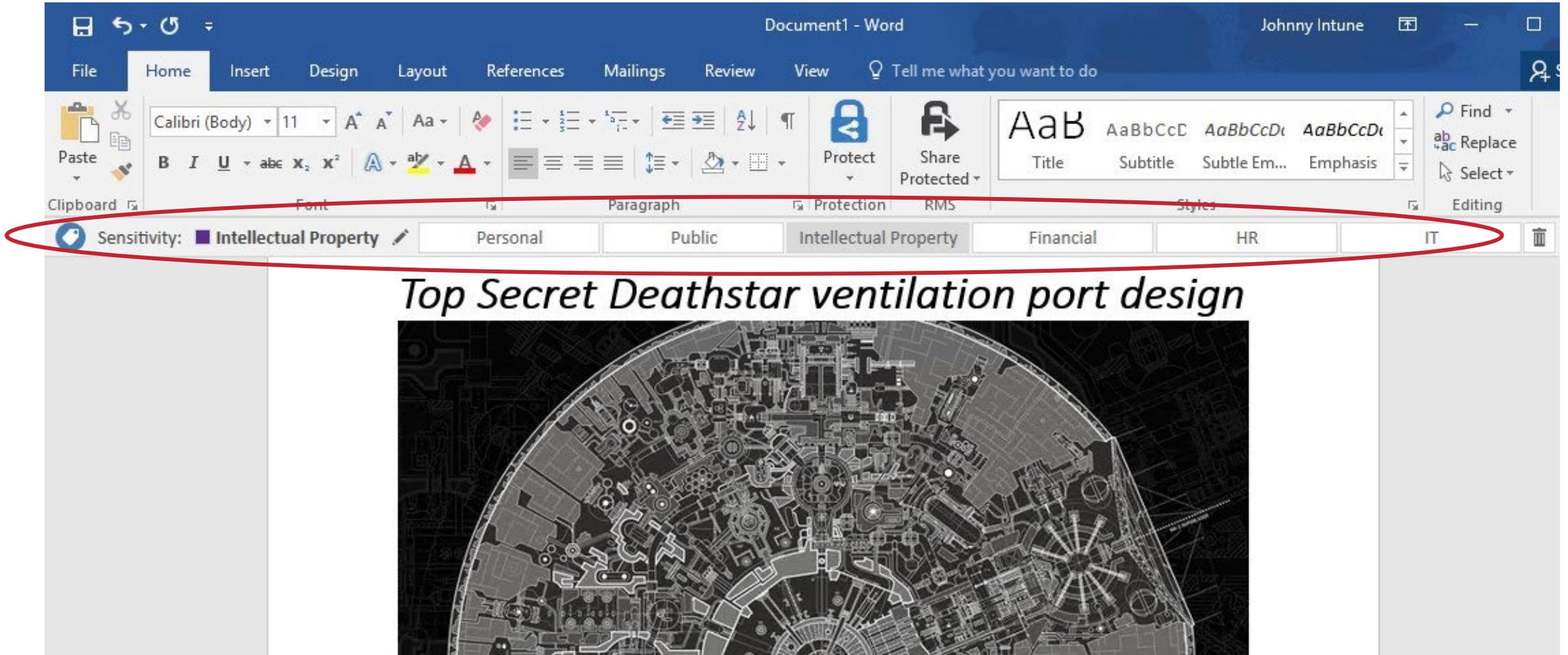
Policy Tip: This message appears to contain sensitive information. Make sure all recipients are authorized to receive it.

Do Not Forward - Recipients can read this message, but cannot forward, print, or copy content. The conversation owner has full permission to their message and attachments.
Permission granted by: Ed.Higgins@catapultsystems.com

To... 'ed.higgins@gmail.com';
Cc...
Subject Sensitive Email Test

Hi Ed,
Your social security number is: **013-32-2390**

Azure Information Protection – Secured Documents



What is Azure Sentinel and Why You Need It

Sentinel is Microsoft's Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR)

SIEM solutions aggregate events and alerts from numerous solutions to correlate intelligence. The consolidated view streamlines threat hunting as well as allows for automated remediations, or assisted investigations.

SOAR solutions are a stack of compatible software programs that allow an organization to collect data about security threats from multiple sources and respond to low-level security events without human assistance.

Azure Sentinel

SIEM and SOAR

Security Information and Event Management

- Advanced alerting
- Threat hunting
- Threat queries

Security Operations and Automated Remediation

- Hunted threats – leads to automation remediation.
- Reduce recurring threats, build automated remediations.



The screenshot displays the Azure Sentinel interface. At the top, it shows 24 Connectors, 10 Connected, and 1 Coming soon. The main content area is titled "Azure Active Directory" and shows a list of connectors. The "Azure Active Directory" connector is highlighted, showing it is connected and last received data on 07/24/19 at 06:26 PM. The right-hand panel provides details for this connector, including a description, last data received, related content (2 Dashboards, 2 Queries), and a data received chart. The chart shows a significant spike in data received on July 21st, reaching 8.75K SigninLogs and 229 AuditLogs. A button at the bottom right says "Open connector page".

STATUS	CONNECTOR NAME	PROVIDER	LAST LOG RECEIVED
---	Amazon Web Services Amazon	---	---
Connected	Azure Active Directory Microsoft	Microsoft	Last log received: 07/24/19, 06:26 PM
---	Azure Active Directory Identity Protection Microsoft	Microsoft	Last log received
---	Azure Advanced Threat Protection Microsoft	---	---
---	Azure Information Protection Microsoft	---	---
---	Azure Security Center Microsoft	---	---
---	AzureActivity Microsoft	Microsoft	Last log received: 07/24/19, 06:22 PM
---	Barracuda Web Application Firewall Barracuda	---	---
---	Check Point CheckPoint	---	---
---	Cisco ASA Cisco	---	---
---	Common Event Format (CEF) Any	---	---
---	CyberArk CyberArk	---	---
---	DNS Microsoft	---	---
---	F5 F5	---	---

DATA RECEIVED

DATE	SIGNINLOGS	AUDITLOGS
June 30	~0K	~0K
July 7	~0K	~0K
July 14	~0K	~0K
July 21	8.75K	229

Where is SecureScore?

- Administrators can access protection.office.com as:
 - Global Administrator,
 - Security Administrator, or
 - Security Reader
- Once logged in, your SecureScore summary is available for you in the center-right of the Home/Dashboard.

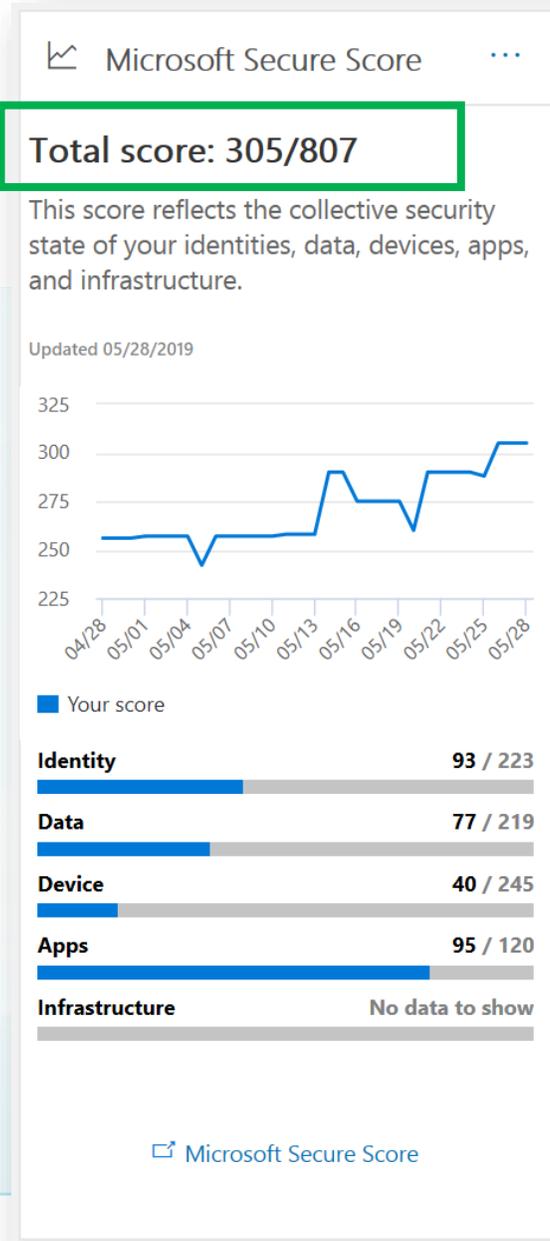
The screenshot shows the 'Home' dashboard with a 'Customize' button. It features three main sections: 'We're committed to helping on your GDPR journey', 'Data governance', and 'Threat management'. Each section includes a brief description and a 'Go to the dashboard' link.

The screenshot shows the 'Microsoft Secure Score' summary card. It displays a total score of 305/807, updated on 05/28/2019. A line graph shows the score's history from 04/28 to 05/28. Below the graph, a bar chart breaks down the score by category: Identity (93/223), Data (77/219), Device (40/245), Apps (95/120), and Infrastructure (No data to show). A 'Microsoft Secure Score' link is at the bottom.

Category	Score	Max Possible
Identity	93	223
Data	77	219
Device	40	245
Apps	95	120
Infrastructure	No data to show	

How it's calculated

- Your Score is calculated based on the controls you can configure versus what you have configured
- Total Score is 305 out of 807



The Numerator

- The numerator (framed in the green box) is the sum of the security controls that you fully or partially meet
- Already you see a useful reporting metric. You have increased your score by total 49 points over past 30 days (framed in blue box)

Microsoft Secure Score

Overview Improvement actions History

Your secure score

Total score: 305 / 807

Microsoft Secure Score analyzes the protection state of your identities, data, devices, apps, and infrastructure.

Identity 93 / 223

Protection state of your Azure AD accounts and roles

Data 77 / 219

Protection state of your Office 365 documents

Device 40 / 245

Protection state of your devices

Apps 95 / 120

Protection state of your email and cloud apps

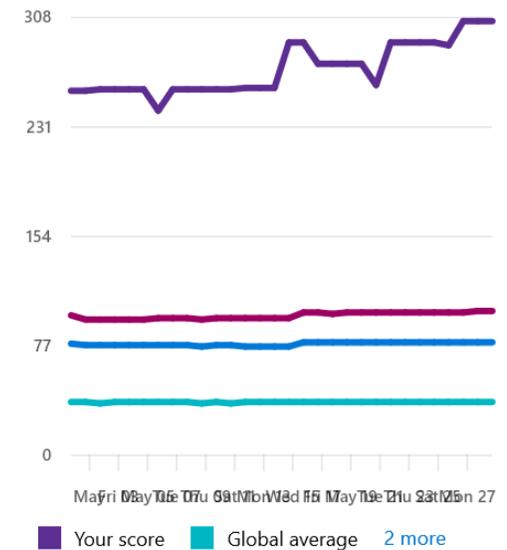
Infrastructure No data to show

Protection state of your Azure resources

History

▲ 49 points in 30 days

Your secure score over time and how you compare to other organizations.



The Denominator

- The denominator (framed in the green box) represents the number of points you can earn given the set of features you have available

Microsoft Secure Score

Overview Improvement actions History

Your secure score

Total score: 305 / 807

Microsoft Secure Score analyzes the protection state of your identities, data, devices, apps, and infrastructure.

Identity 93 / 223

Protection state of your Azure AD accounts and roles

Data 77 / 219

Protection state of your Office 365 documents

Device 40 / 245

Protection state of your devices

Apps 95 / 120

Protection state of your email and cloud apps

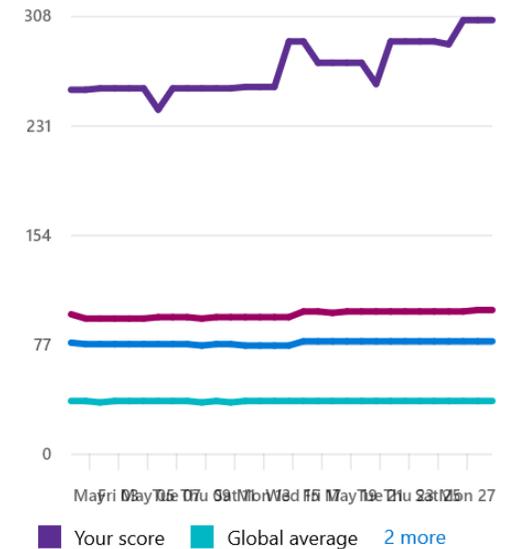
Infrastructure No data to show

Protection state of your Azure resources

History

▲ 49 points in 30 days

Your secure score over time and how you compare to other organizations. Total score ▾



Improvement Actions

Microsoft Secure Score

Overview **Improvement actions** History

Actions you can take to improve your Microsoft Secure Score. Points r

↓ Export

Improvement action	Rank	Score	Category
✓ Require MFA for Azure AD privileg...	1	18/50	Identity
Require MFA for all users	2	0/30	Identity
Turn on audit data recording [Not S...	3	15/15	Data
Block Client Forwarding Rules [Not ...	4	0/20	Data
Set outbound spam notifications [N...	7	0/15	Data
Turn on mailbox auditing for all use...	8	0/10	Data
Enable Password Hash Sync if hybrid	9	10/10	Identity
Register all users for multi-factor au...	12	5/20	Identity
Store user documents in OneDrive f...	14	10/10	Data
Review permissions & block risky O...	15	15/15	Apps

Require MFA for Azure AD privileged roles

18/50 points

Status

- Not completed

Description

Requiring multi-factor authentication (MFA) for all Azure Active Directory accounts with privileged roles makes it harder for attackers to access accounts. Privileged roles have higher permissions than typical users, and include all admin roles such as global admin, SharePoint admin, or Exchange admin. If any of those accounts are compromised, critical devices and data will be open to attacks.

You have 7 of 11 accounts with privileged roles that don't use MFA.

Category
Identity

Protects against
Password Cracking
Account Breach
Elevation of Privilege

User impact
Low

Complexity
Low

Next steps

Turn on **Baseline policy: Require MFA for Admins** through the conditional access portal in Azure AD. Select the policy to view all the roles that will be required to use MFA. You can also choose users to exempt from the policy. To enable the policy and require MFA for admins, select **Use policy immediately** and **Save**. Optionally, you can setup your own conditional access policy requiring MFA for the same set of privileged roles described in Baseline policy: Require MFA for Admins. See the improvement action titled "Require MFA for all users" for the correct way to set up your own conditional access policy and earn full points.

How will this affect my users?

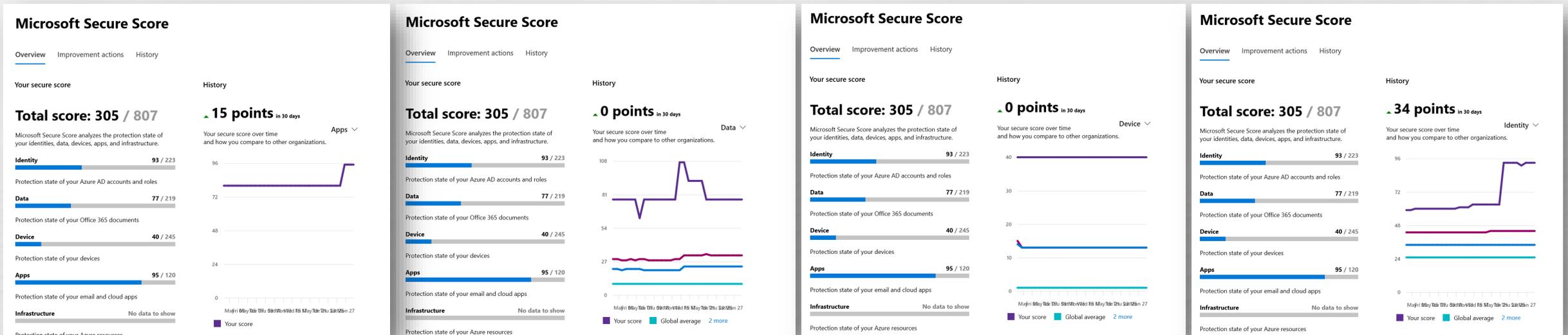
When you require MFA for your privileged roles, they will need to authenticate using at least two methods when accessing the privileged account.

Compliance Controls

[View settings](#) [Resolved through third-party](#) [Ignore](#)

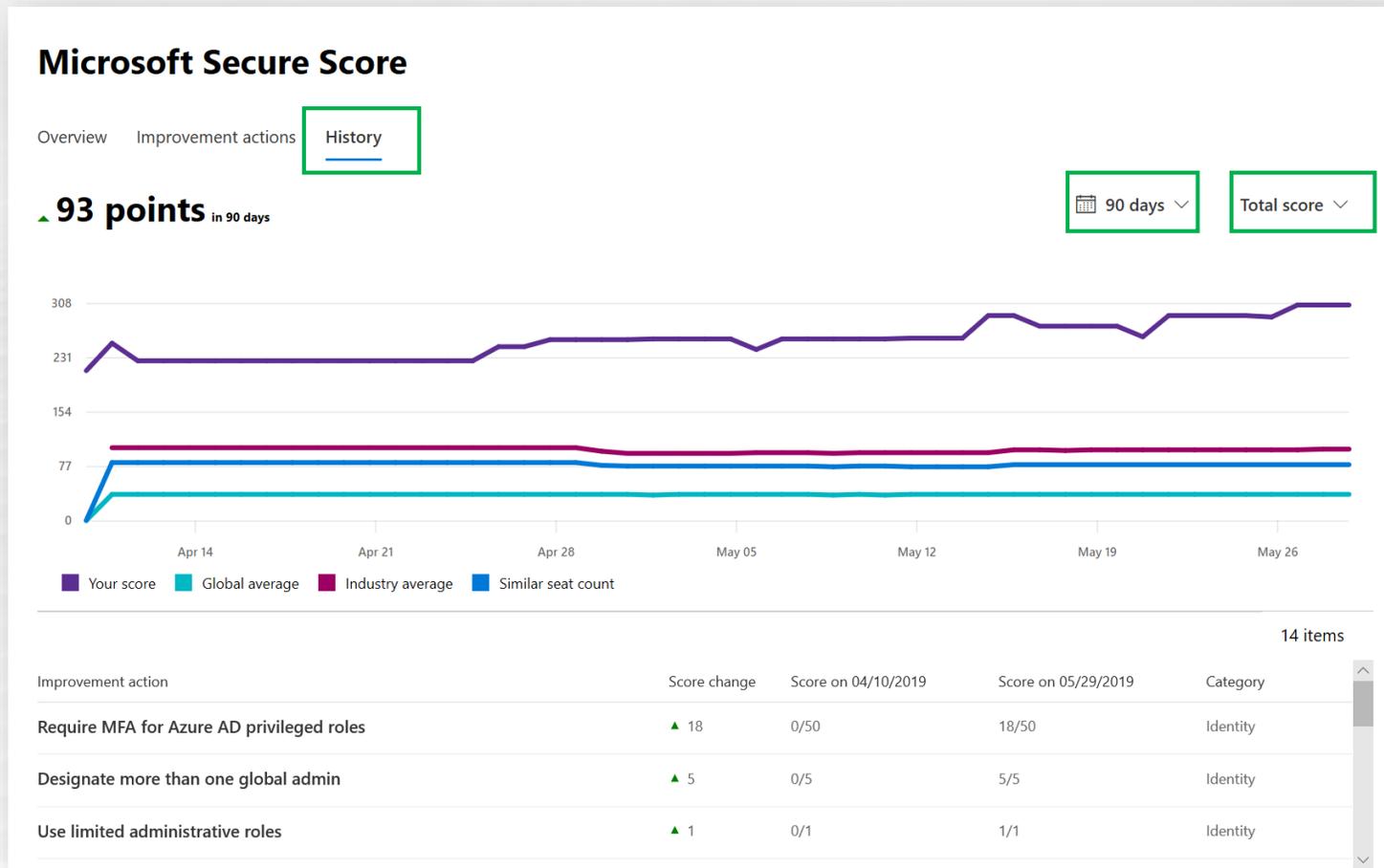
- **View settings** – shows you what/who's impacted, and advice for user impact.
- **Resolved thru 3rd party** – helpful if you use RSA for MFA.
- **Ignore** – your business makes the decision that the Improvement Action item is not suitable for your environment.

View Historic Improvements by area: Apps, Data, Device & Identity



This illustrates gained improvements (or lapses) over time by category area. If you want to focus your efforts on Data, you can.

Historic Trends – Useful Info



- History – changes view to illustrate graph and Improvement Actions performed (with gained points). Partial points are sometimes given...
- Choose the period you are looking for (back to 90 days).
- Choose view perspective (Total Score, or by App, Data, Device, Identity).

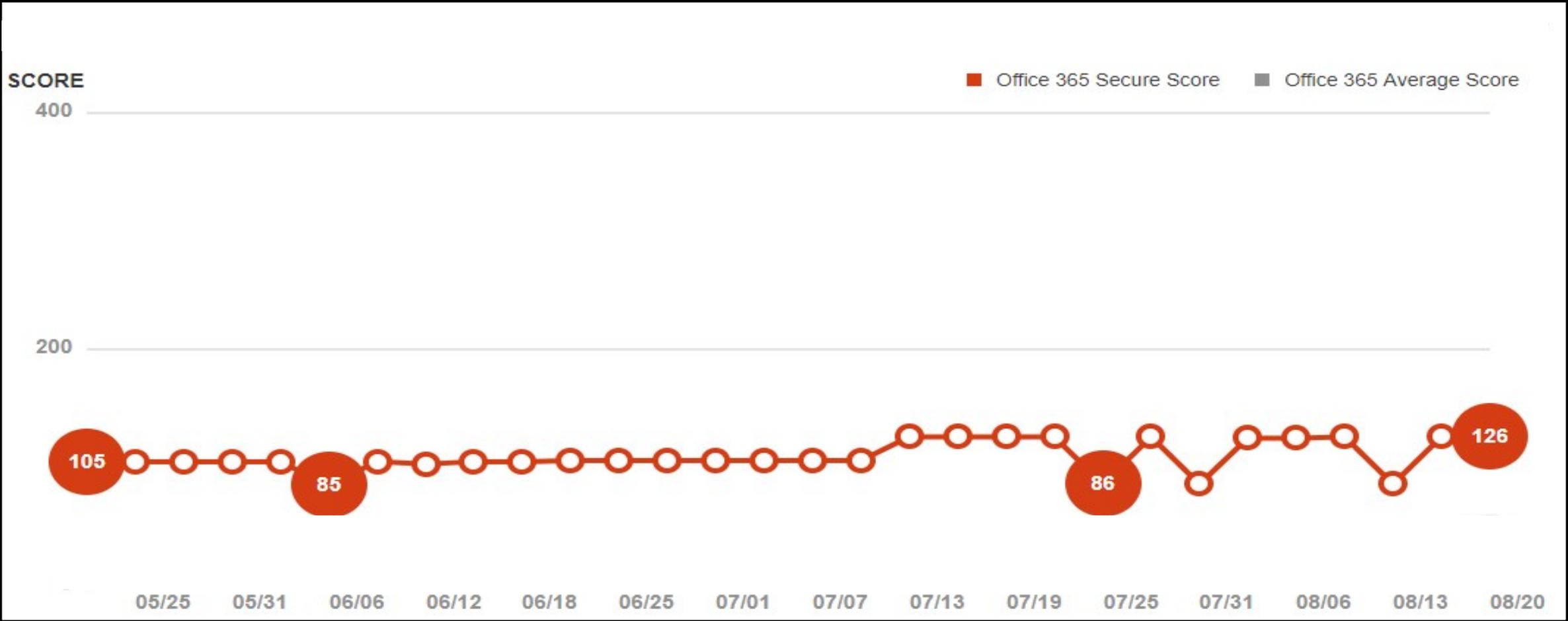
Setting your Goal – Catapult’s Recommended Best-Practice

- Regulated Records = 550+
 - FERPA, CUI, CJIS, HIPAA, PCI
- Sensitive Records = 450+
 - PII, Bank Accounts, Tax Information
- Non-Sensitive Records (General Best-Practice) = 350+
 - Non-sensitive information, Internal-Only

Practicable Best-Practice



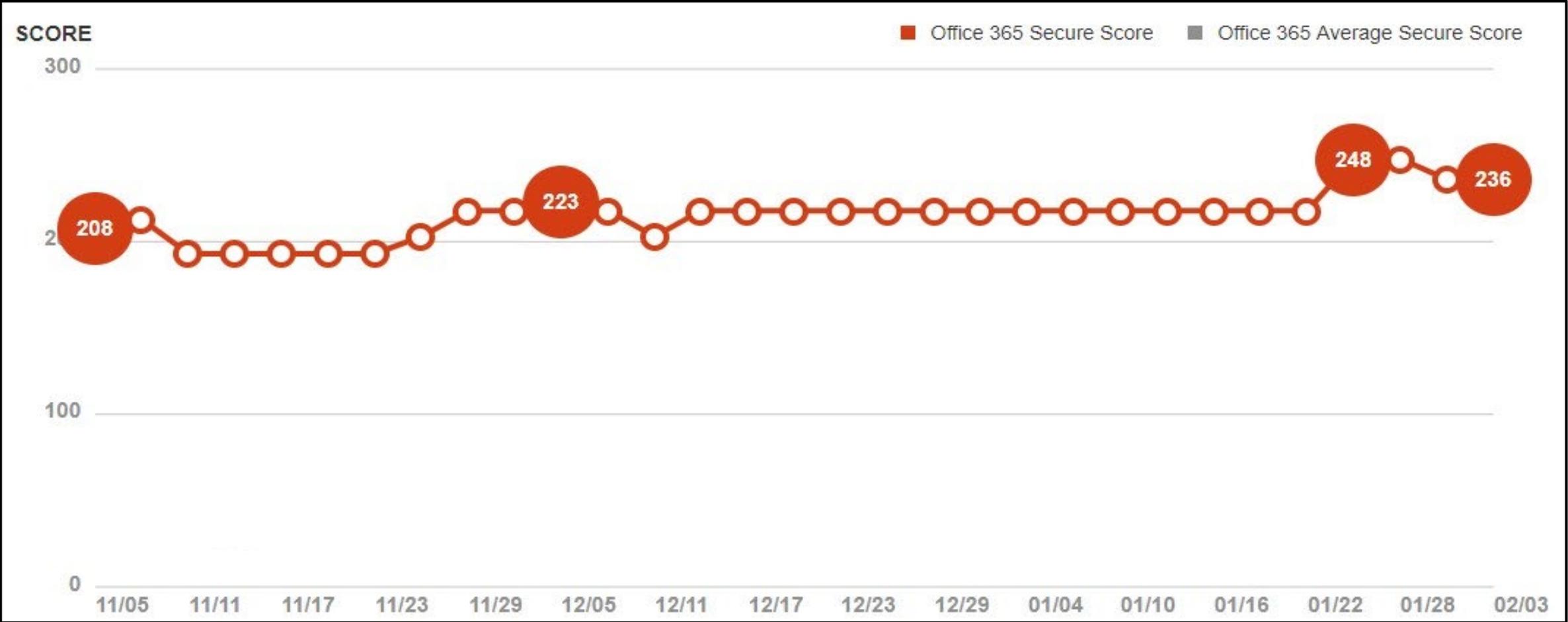
Secure Score May 2018 through Aug 2018



Helps to Quickly Validate your Roadmap Impact (example)

- Use existing security service to increase score to 230+ by January 2019
 - Implement moderate impact controls based on best practices and user adoption
1. Assign EM+S E5 License to Admins & Sensitive Users
 2. Implement MFA for all Global Admins, utilize lower permissions where possible
 3. Deploy Privileged Identity Management & Cloud App Discovery
 4. End-user data handling training for email content
 5. DLP/Encryption and user notification tool-tips for sensitive data
 6. Conditional Access policy enforcement to prevent anomalous access, impossible travel, reduce MFA prompts on trusted scenarios
 7. User password testing (Attack Simulator)
 8. Disable legacy authorization and unapproved Oauth Trusts by users

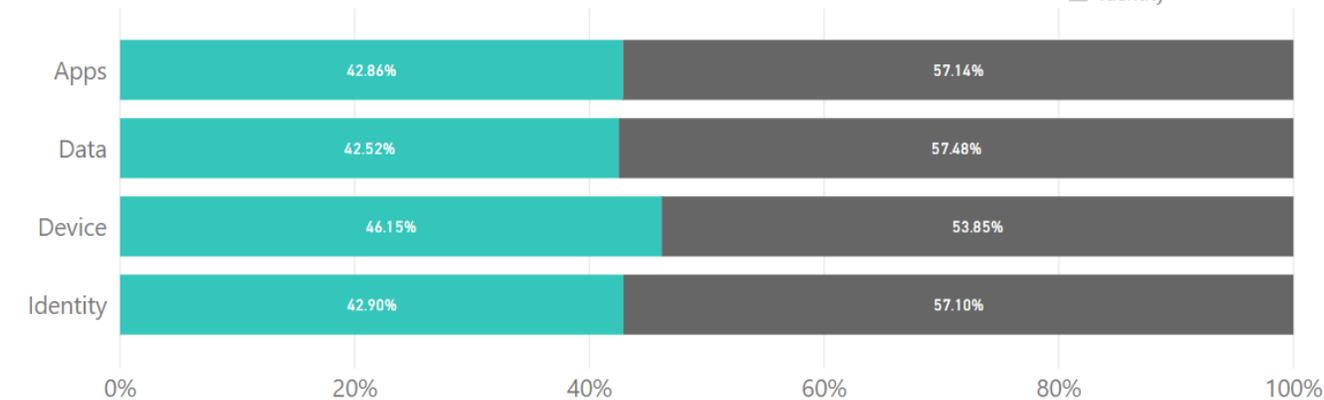
SecureScore Nov 2018 through Jan 2019



Spyglass Office 365 Report Card

● Complete ● In Progress

- ▢ Apps
- ▢ Data
- ▢ Device
- ▢ Identity



Client Information

Client: Acme Corporation ▾

Category	Grade	Total Possible	Completed
Device	B	245	210
App	C	120	90
Data	C	219	162
Identity	C	193	145

Action Category	Name	Possible Score	Completed	User Impact	Description	Special Notes
Identity	Require MFA for all users	30	30	Moderate	Requiring multi-factor authentication (MFA) for all user accounts helps protect devices and data that are accessible to these users. Adding more authentication methods, such as a phone token or a badge, increases the level of protection in the the event that one factor is compromised.	
Identity	Turn on sign-in risk policy	30	30	Moderate	Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multi-factor authentication.	
Identity	Turn on user risk policy	30	0	Moderate	With the user risk policy turned on, Azure AD detects the probability that a user account has been compromised. As an administrator, you can configure a user risk conditional access policy to automatically respond to a specific user risk level. For examplbe, you can block access to your resources or require a password change to get a user account back into a clean state.	
Apps	Discover risky and non-compliant shadow IT applications	20	20	Low	Cloud App Security Discovery analyzes firewall traffic logs to provide visibility into cloud application usage and overall security posture. By setting up Cloud Discovery, you can discover shadow IT applications in your organization that run without official approval.	
Apps	Set automated notifications for new OAuth applications connected to your corporate	20	20	Moderate	With app permission policies, you can discover Open Authorization (OAuth) abuse in the organization by identifying trending applications based on usage & permissions granted.	

Spyglass Chatter

Bluekeep Vulnerability Now Compounded by NLA client-side attacker bypass bug...

One of the remedies to the pre-auth RDP bug (pet-named Bluekeep) was to require users to enter RDP sessions with Network Level Authentication (NLA). Those that can't (or won't) patch their systems, ran to NLA as a way to mitigate the risk. Well, Not So Fast! Web application security test specialists published a report detailing a ... [Continue reading "Bluekeep Vulnerability Now Compounded by NLA client-side attacker bypass bug..."](#)

06-5-2019 16:18:22

Alert: Microsoft patches Windows XP, Server 2003 to try to head off 'wormable' flaw with massive potential

Important for EOSL Operating Systems older than Windows 8 and Windows Server 2008 The Situation Yesterday (May 14) Microsoft issued a global warning about a Monster Computer Bug. This article aims to get into some of the details about why this could be very important to your business and includes some steps you should take to ... [Continue reading "Alert: Microsoft patches Windows XP, Server 2003 to try to head off 'wormable' flaw with massive potential"](#)

05-14-2019 15:03:15

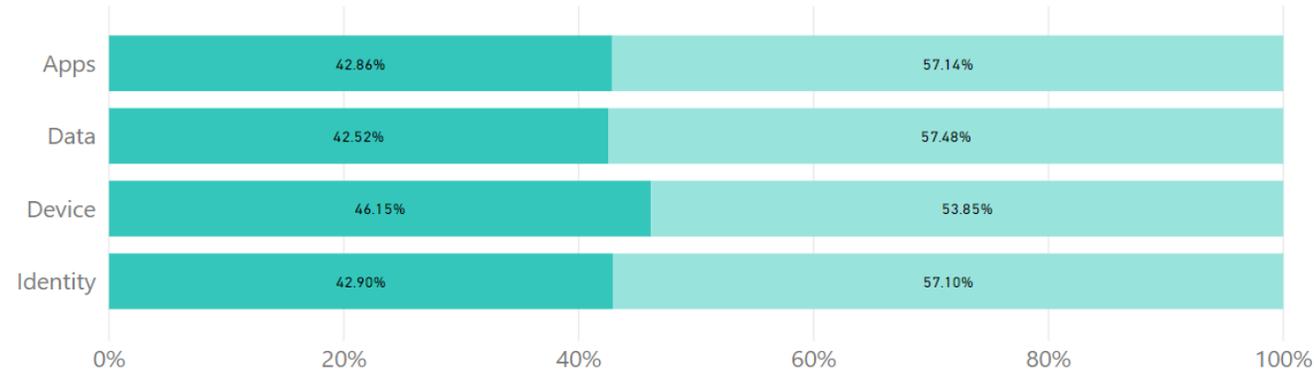
ALERT: RunC Vulnerability Gives Attackers Root Access on Docker, Kubernetes Hosts

This alert applies to anyone running CAS data collectors via containers. This does not apply to those specifically using Microsoft CAS. But, the Spyglass team is relaying this critical alert as a courtesy since a broad range of clients might be leveraging the vulnerable variety. A container breakout security flaw found in the runc container runtime ... [Continue reading "ALERT: RunC Vulnerability Gives Attackers Root Access on Docker, Kubernetes Hosts"](#)

02-11-2019 19:43:03

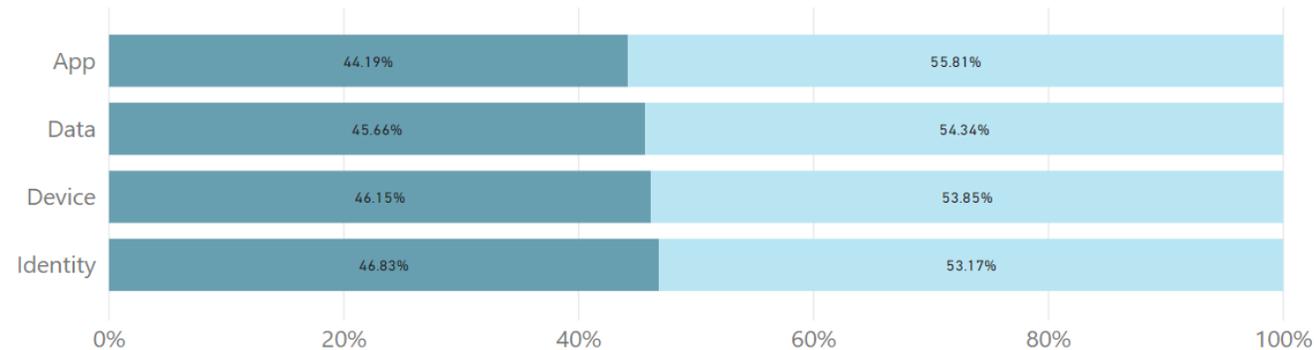
Spyglass Office 365 Report Card

● Complete ● In Progress



Median Score Across All Spyglass Clients

● Median Complete ● Median In Progress



Client Information

Client:



Your Score

Category	Grade	Total Possible	Completed
App	C	120	90
Data	C	219	162
Device	B	245	210
Identity	C	193	145

Median Score Across Spyglass Clients

Category	Grade	Total Possible	Low	High	Average
App	C	120	80	110	95
Data	B	219	150	218	184
Device	B	245	180	240	210
Identity	B	193	150	190	170

Spyglass Chatter

Bluekeep Vulnerability Now Compounded by NLA client-side attacker bypass bug...

One of the remedies to the pre-auth RDP bug (pet-named Bluekeep) was to require users to enter RDP sessions with Network Level Authentication (NLA). Those that can't (or won't) patch their systems, ran to NLA as a way to mitigate the risk. Well, Not So Fast! Web application security test specialists published a report detailing a ... [Continue reading "Bluekeep Vulnerability Now Compounded by NLA client-side attacker bypass bug..."](#)

06-5-2019 16:18:22

Alert: Microsoft patches Windows XP, Server 2003 to try to head off 'wormable' flaw with massive potential

Important for EOSL Operating Systems older than Windows 8 and Windows Server 2008 The Situation Yesterday (May 14) Microsoft issued a global warning about a Monster Computer Bug. This article aims to get into some of the details about why this could be very important to your business and includes some steps you should take to ... [Continue reading "Alert: Microsoft patches Windows XP, Server 2003 to try to head off 'wormable' flaw with massive potential"](#)

05-14-2019 15:03:15

ALERT: RunC Vulnerability Gives Attackers Root Access on Docker, Kubernetes Hosts

This alert applies to anyone running CAS data collectors via containers. This does not apply to those specifically using Microsoft CAS. But, the Spyglass team is relaying this critical alert as a courtesy since a broad range of clients might be leveraging the vulnerable variety. A container breakout security flaw found in the runc container runtime ... [Continue reading "ALERT: RunC Vulnerability Gives Attackers Root Access on Docker, Kubernetes Hosts"](#)

02-11-2019 19:43:03

SecureScore Summary

- Provides an objective target based on your identities, the types of data you hold, and tools you have enabled.
 - Remember the Spyglass recommended target scores.
- Compares metrics for industries like yours – be careful – the laggards are pulling down the industry averages. That’s why we built the Spyglass Report Card.
 - Don’t get a false sense of security when comparing your score against the laggards.
- Do the low-hanging fruit first.
 - Most are easy to achieve, provides sound advice, and has a direct impact on reducing attack surface.
- You can simplify your communications of important stuff to your Executives as well as non-technical personnel.
 - We have increased our score from 126 to over 230 in the last 6 months.
 - We did these “things” to reduce our risk and exposure.
 - Compared to environments our size, we are doing well but here’s where we need to focus.



Q & A



Ed Higgins, cissp, cism, cgeit
Security and Compliance Solutions
Catapult Systems
Ed.Higgins@catapultsystems.com