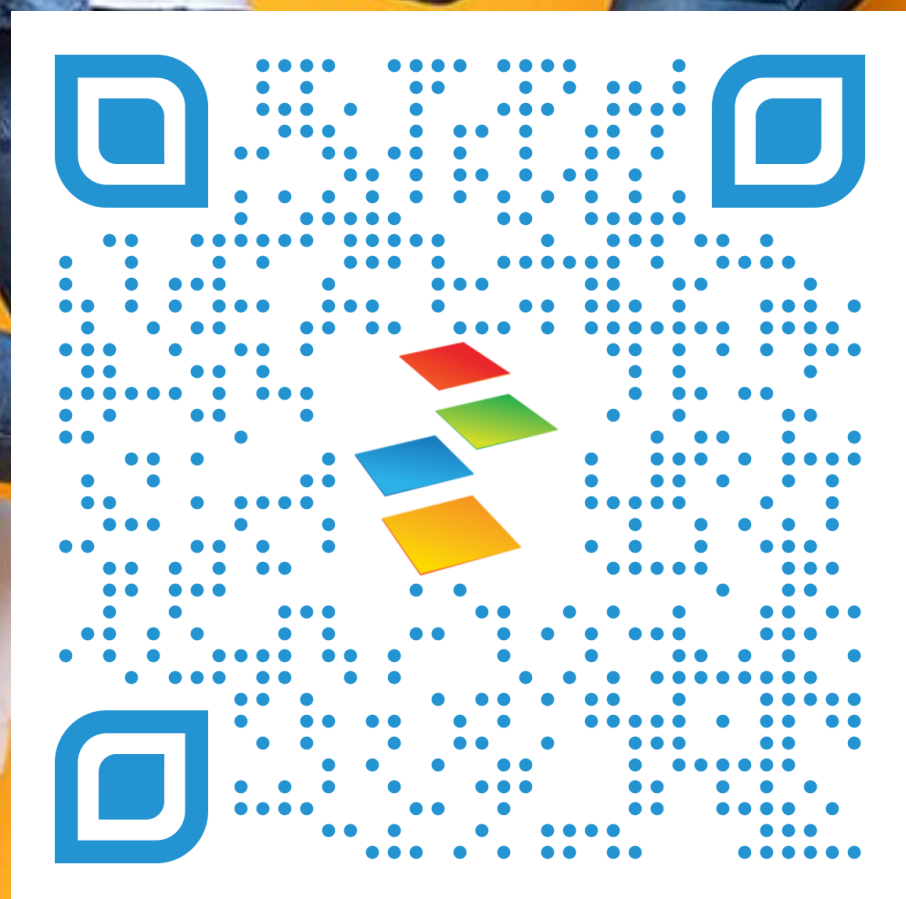




Lock and Roll with Microsoft 365 Security

A Zero Trust Adventure for Boosting Security
Swagger





Housekeeping

- Please silence your phones. If you need to take a call, feel free to step outside and come back in.
- Sessions are being recorded and will be available after.
- Please use this QR code to take the session survey before heading to the next session.
- Survey responses get you more entries into the raffle at the end of the day. (prizes included surface headphones, Smart Ray Bans, RayBan Meta Smart Bluetooth Glasses, and lots more).
- Wifi Info: BusinessTechnologySummit
Password: journeyteam!

How many of you...

- Have experienced a security breach
- Do not know how the attacker got in
- Are not entirely sure how to stop it from happening again
- Are using less effective MFA Methods (SMS & Voice), or are not using MFA
- Have service accounts that are sign in enabled but not registered or protected by MFA
- Have a 90 day password reset policy
- Require users to remember many different passwords for multiple applications
- Have permanently assigned admin roles in your tenant
- Have looked at Microsoft's Secure Score recommendations and wondered where to begin
- Are missing out on useful technology included in your M365 licensing that hasn't been implemented yet.



Presenters



REESE BRIGGS

MODERN WORK AND SECURITY
SOLUTION ARCHITECT

A DECADE OF EXPERIENCE TURNING ON MFA
AND TURNING OFF OLD SERVERS ... RIP SERVER 2012



CRAIG DUNN

MODERN WORK AND SECURITY
SOLUTION ARCHITECT

KNOWS A THING OR TWO
BECAUSE HE'S SEEN A BREACH OR TWO

44%

of people think an email is safe when it contains familiar branding



300-400K

telephone-oriented attack delivery attempts daily, with a peak of 600k per day in August 2022



can't define "malware," "phishing" and "ransomware"

Even basic concepts are misunderstood



ONLY 35% of organizations conduct phishing simulations

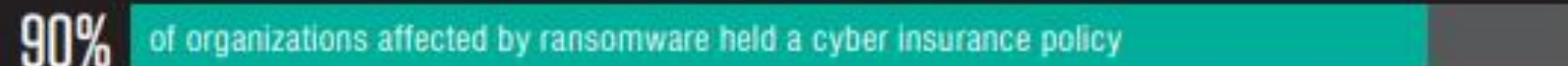
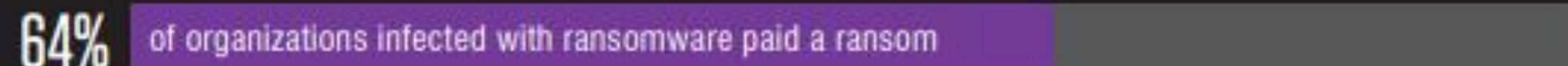
1/3



of people took a risky action (such as clicking links or downloading malware) when faced with an attack



Increase in direct financial loss from successful phishing



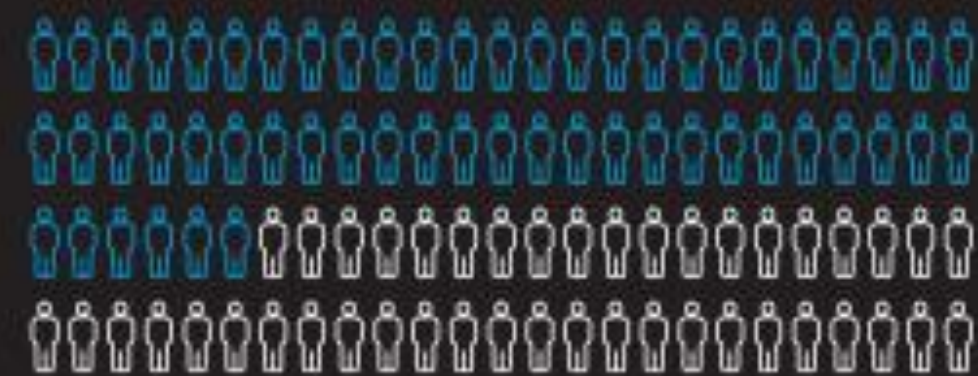
30 Million

malicious messages sent in 2022 involved Microsoft branding or products



> 1 in 10

threats were blocked as a result of user reporting



ONLY 56% of organizations with a security awareness program train all their employees



of security professionals consider security a top priority at their company

VS.



of employees say cybersecurity is not a top priority of theirs at work

Guiding Principals of Zero Trust

Verify Explicitly

- Always authenticate and authorize based on all available data points.

Use Least Privilege Access

Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.

Assume Breach

Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Visibility, Automation, Orchestration



Identity



Endpoints



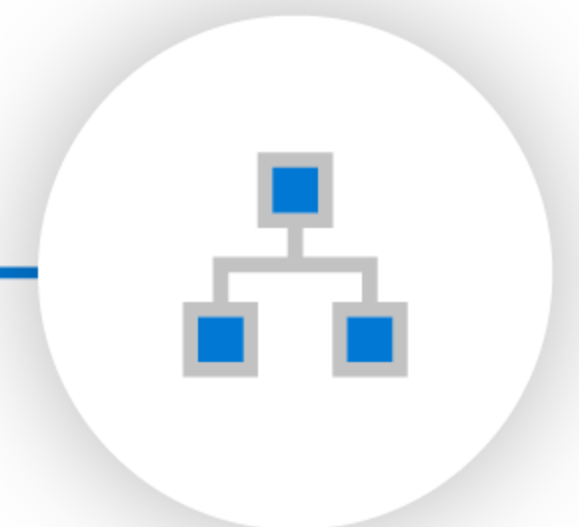
Data



Apps

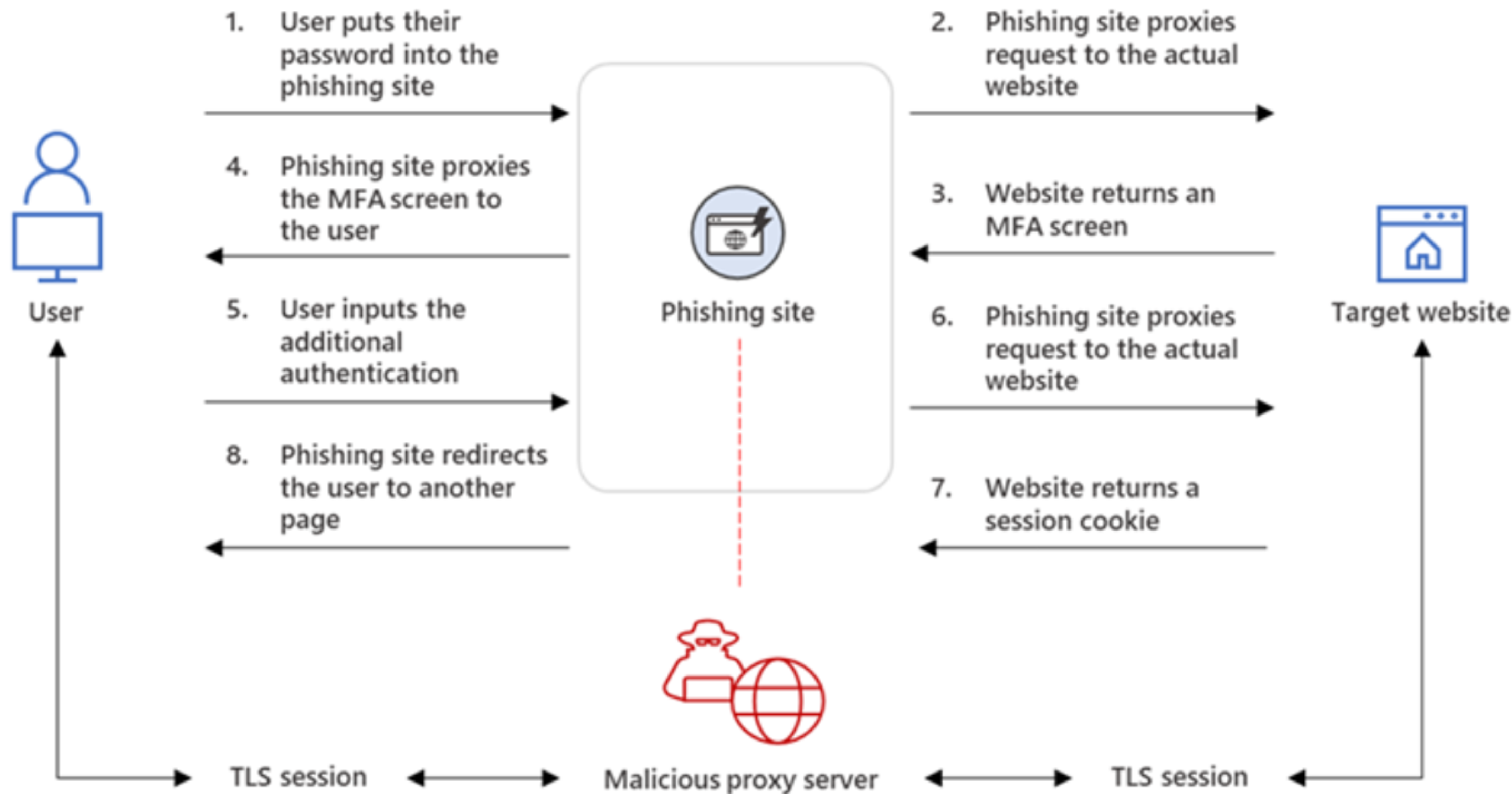


Infrastructure















Network

Man In The Middle Attack



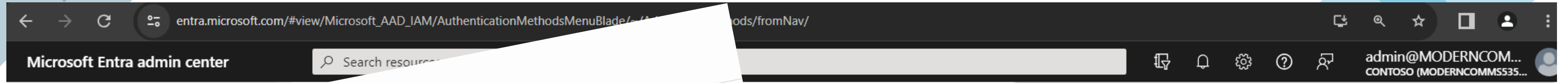
Authentication methods

Bad  Password (Only)	Good  Password +	Better  Password +	Best Passwordless 
123456 qwerty password Iloveyou Password1	 SMS  Voice	 Authenticator (Push notifications)  Software Tokens OTP  Hardware Tokens OTP (Preview)	 Windows Hello  Authenticator (Phone Sign-in)  FIDO2 security key



Authentication Methods Migration – Complete by Sept 30, 2025

Authentication methods



Password reset | Authentication methods

Authentication Methods for SSPR and Signin can now be managed in one converged policy. [Learn more](#)

Number of methods required to reset: **2**

Methods available to users:

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

- Hardware OATH tokens (Pre)
- Third-party software OATH
- Voice call
- Email OTP
- Certificate-based authentication

multi-factor authentication service settings

Allow users to create app passwords to sign in to non-browser apps

trusted ips

- Skip multi-factor authentication for requests from federated users on my intranet
- Skip multi-factor authentication for requests from following range of IP address subnets

verification options

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

remember multi-factor authentication on trusted device

Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)

Number of days users can trust devices for: **90**

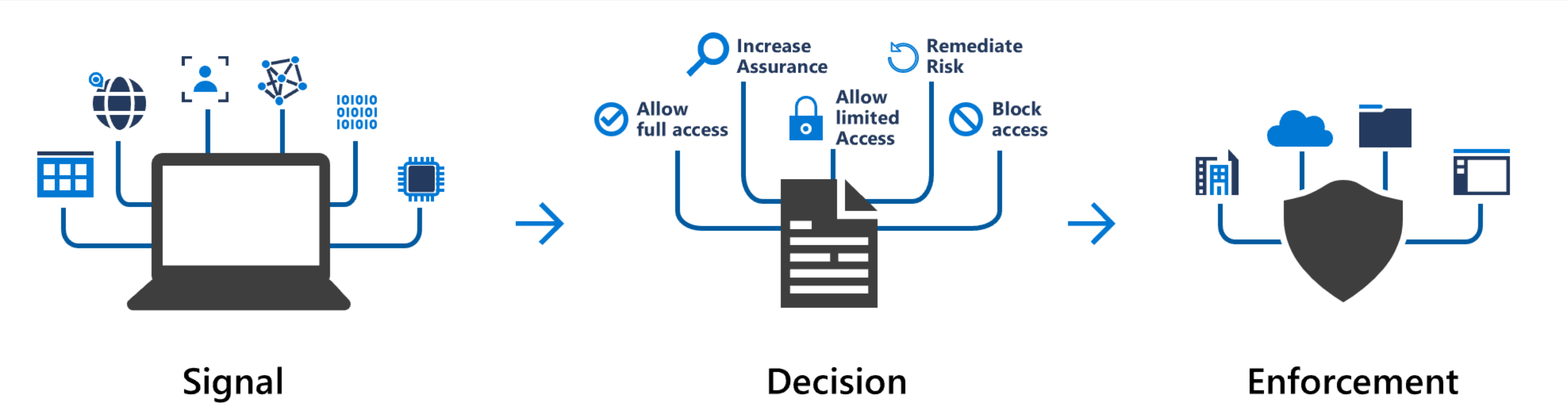
NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' be sure to extend the duration to 90 or more days. [Learn more about reauthentication prompts.](#)

save



Authentication Methods Migration – Complete by Sept 30, 2025

Conditional Access





76% Trust in the News

Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN
2 minute read · Published 2:31 AM EST, Sun February 4, 2024



Cloud security breaches surge on a wave of stolen credentials

News
ITPro. By Steve Ranger published about 23 hours ago

Cloud security attacks are growing in both scale and intensity, according to new research from CrowdStrike, with threat actors leveraging stolen credentials to devastating effect

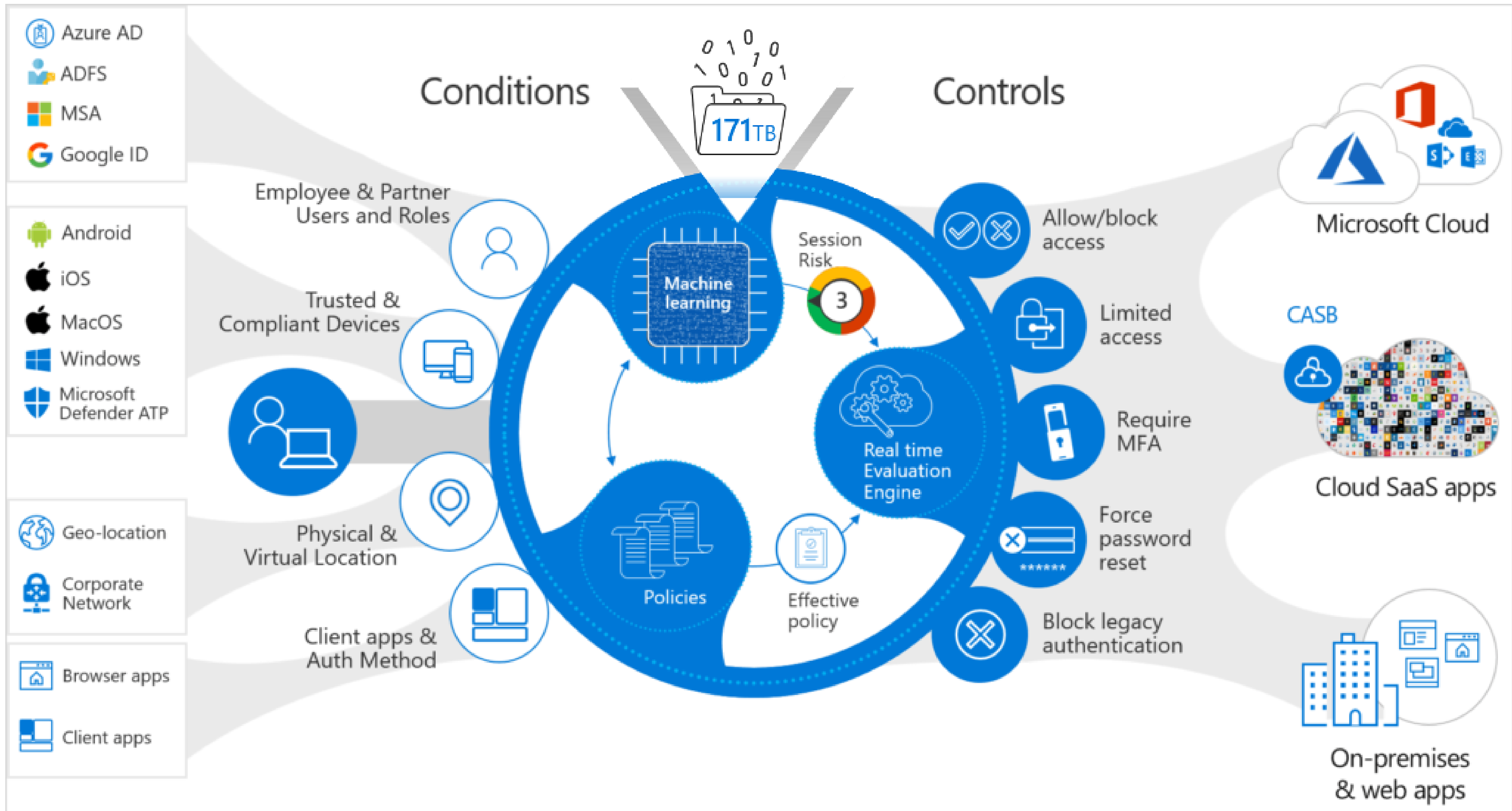
Second accidental data leak in four months 'regrettable', finance department says

Incident comes as data shows government sector breaches mostly caused by human error, not criminal acts

Tory Shepherd
Thu 22 Feb 2024 02:49 EST



Estimated Financial Impact: \$100,000,000+



As difficult as possible for an attacker As frictionless as possible for an employee

WOODGROVE
samlburton@woodgrove.net

Your account is blocked

We've detected suspicious activity on your account.

Sorry, the organization you are trying to access restricts at-risk users. Please contact your Woodgrove admin. [Learn more](#)

[Sign out and sign in with a different account](#)

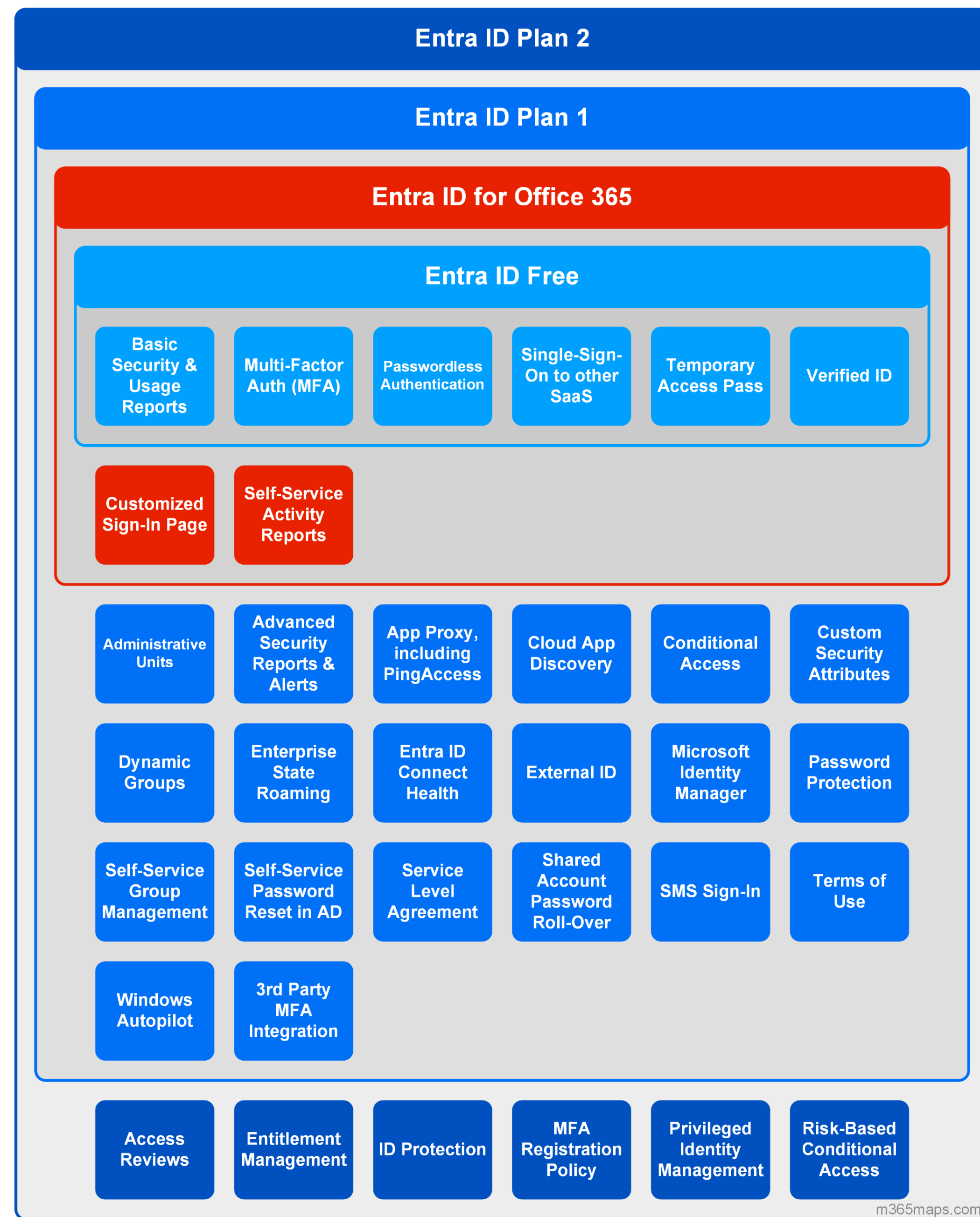
[More details](#)

Hate typing your password? Go passwordless today
aka.ms/passwordless [Need Support? Email Woodgrove Support](#)



Gold Standard in 2024

- Consistent and Consolidated Identity Verification
- Phishing Resistant MFA
- All Accounts are MFA Capable
- Defender Everywhere
- Least Privileged + Just in Time (PIM)
- Restrict Service Account Access to IP Ranges
- User Risk & Sign In Risk Evaluations



m365maps.com



Call to Action

- JourneyTEAM offers a simple \$3,000 "**Foundational Identity Assessment**" of your environment.
- Helps you see where you are at today and what areas you can adopt and improve on in this journey.
- BTS participants will get 2 FREE FIDO2 Security keys when you commit to our Foundational Identity Assessment by end of day Friday March 1st.
 - Request through feedback survey:



4. What session did you attend during this block? *

End-to-End Efficiency: Migrating to Cloud ERP for Comprehensive Process Improvement with Cecilee Nelson

Cutting Costs by Moving Your Data Platform to Microsoft with Preston Reynolds and Jason Fife

Lock and Roll with Microsoft 365 Security: A Zero Trust Adventure for Boosting Security Swagger with Reese Briggs and Craig Dunn

Experlogix: Empower Sales with Technology for Enhanced Customer Experiences with Gwyn Golden and Jim Meyer

7. Are you interested in any of the following? (select all that apply)

Business Central Catalyst Packages

Migration Assessment

Data Strategy Roadmap

Power BI Tenant Health Check

Foundational Identity Analysis (2 FREE FIDO2 keys promotion)

Experlogix CPQ

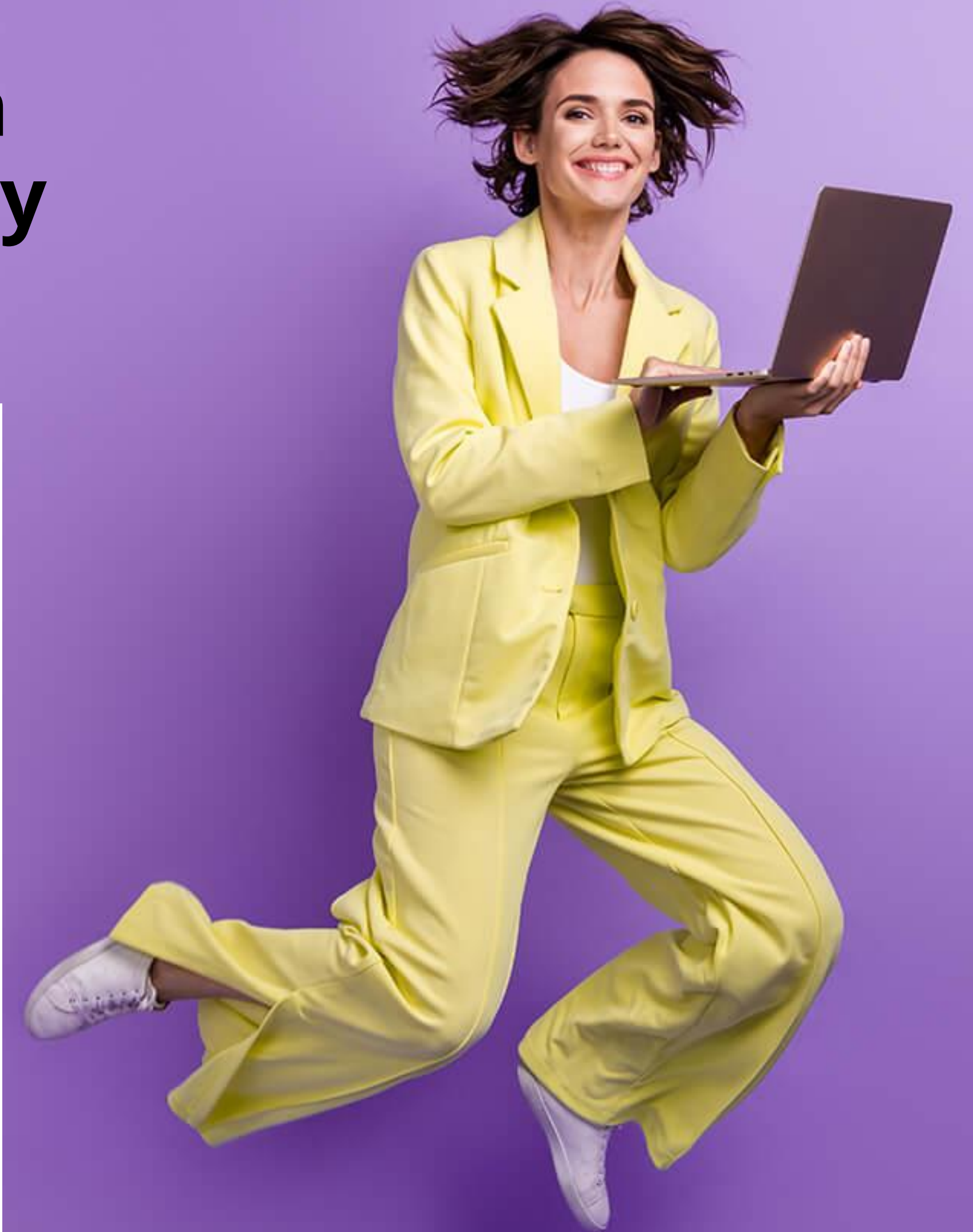
Other

Submit



QUESTIONS

We love feedback!
Please complete the session
survey for **an extra giveaway
raffle ticket!**





Thank You!

Let's Connect:

Reese Briggs
Craig Dunn

info@journeyteam.com



WHERE DO I GO NEXT?



Exhibit Hall

Customer Awards

Giveaways

Closing Note

