

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Stop Identity-Based Attacks and Enhance User Experience

Through Cisco Continuous Identity Security

Sheela Kishan, Solutions Engineer
sheelaknetwork (Linkedin)
BRKSEC-2233

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2233>





Are your password controls enough?

PASSWORD

Image(s) used under license from Shutterstock.com

RockYou2024: Massive Data Breach Exposes Nearly 10 Billion Passwords

Jul 9, 2024 News

The image is a screenshot of a forum post on a dark-themed website. The post title is "Rockyou2024 Password Compilation" with sub-labels "Cloud" and "Mix". It was posted "4 minutes ago". The main content of the post reads: "Hi, Xmas came early this year. I present you a new Rockyou24 Password Compilation with 9.8 billion passwords. I updated rockyou21 with collected new data from recent leaked databases in various forums over this and last years. Also cracked some old ones with my new 4090. This contains actual new real passwords from users." Below the text is a red warning: "You must either reply or click 'Like' to see the hidden information contained here." At the bottom, it says "Worked hard on this fellas, enjoy!" and has a "Report" button. A large, semi-transparent green "Rockyou2024" watermark is overlaid on the center of the image. On the left, a sidebar shows a user profile with a green-bordered icon, the name "ObamaCare", and a "Conversation" section with a list of items (5, 25, 32). At the bottom right of the post area are buttons for "Like!", "+Quote ObamaCare", and "Reply".



Are your MFA controls enough?



*Image(s) used under license from Shutterstock.com



Hi! I lost my phone.
I'm unable to
authenticate. Can you
add my new phone. I
need to meet a
customer in 10
minutes. It's urgent!!!

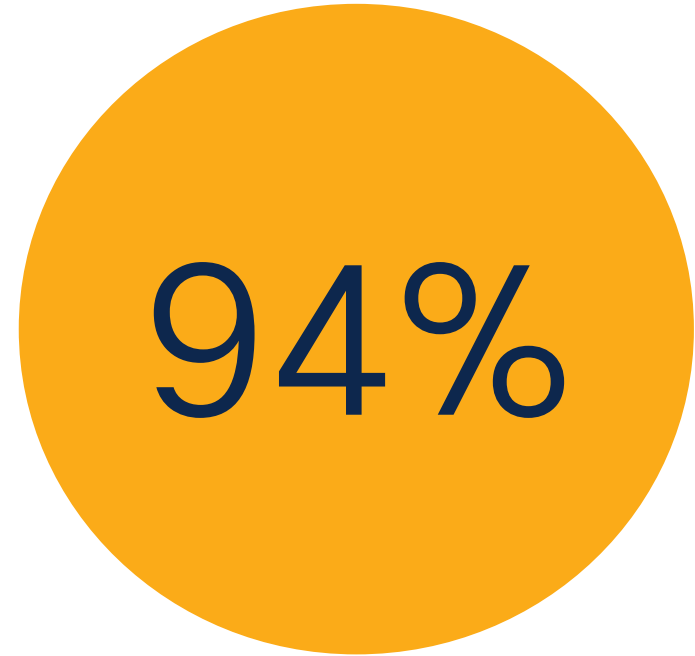
*Image(s) used under license from Shutterstock.com

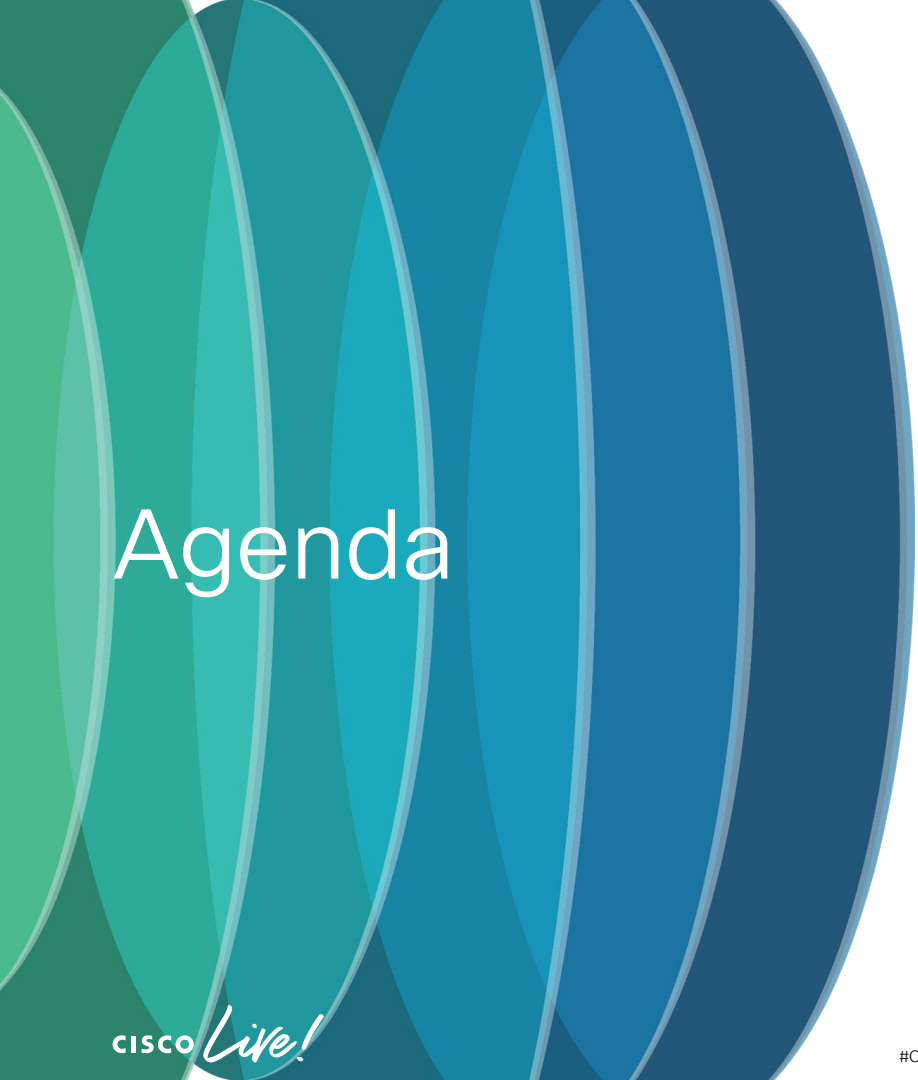


What is your employee ID?
What is your manager's email?
What is the name of your first pet?
What is the name of your first school?

*Image(s) used under license from Shutterstock.com

Identity breaches





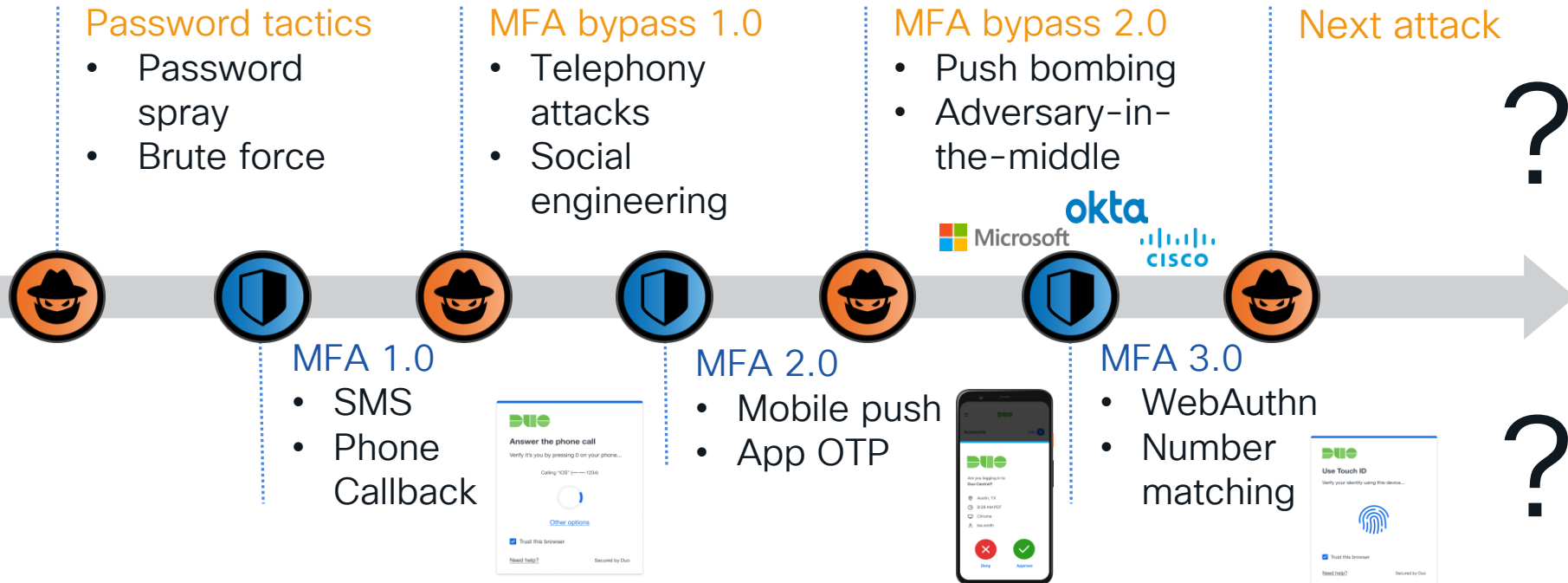
Agenda

- Challenges in Securing Identity
- Common Identity Attack Techniques
- Continuous Identity Security
- Key Takeaways

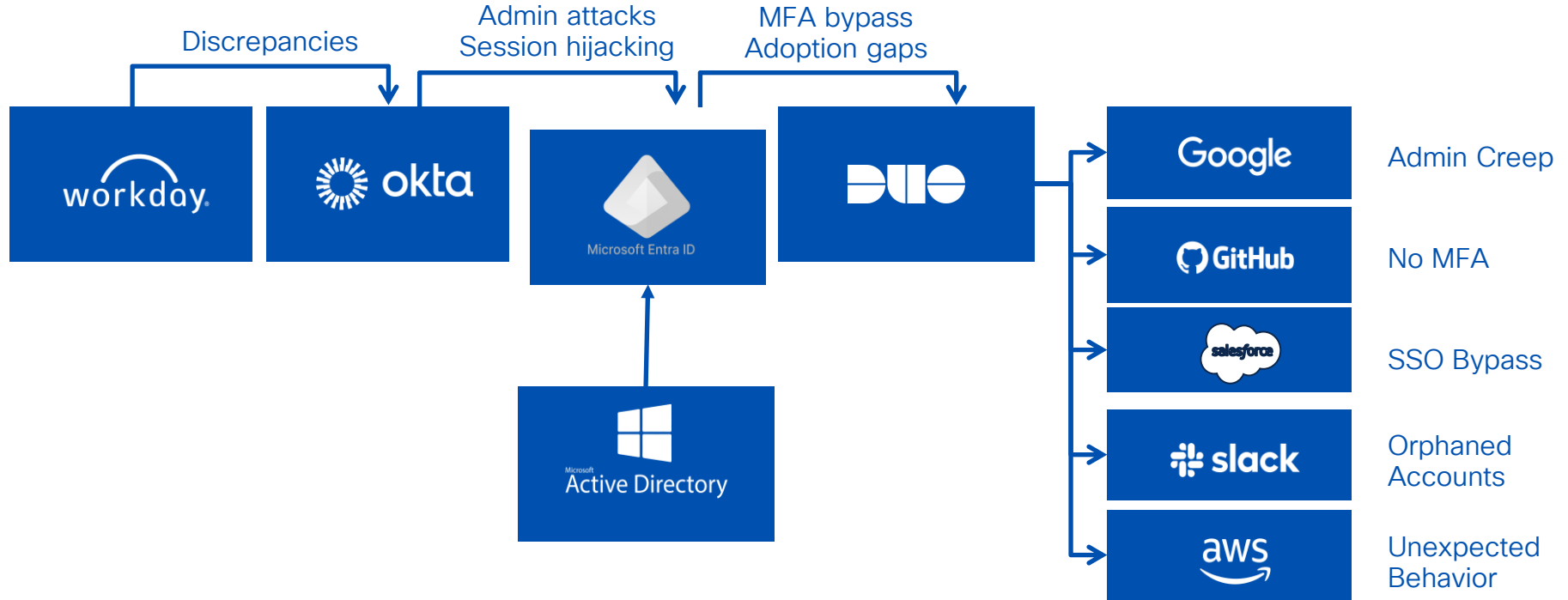
Challenges in Security Identity



Evolution of authentication and attack tactics



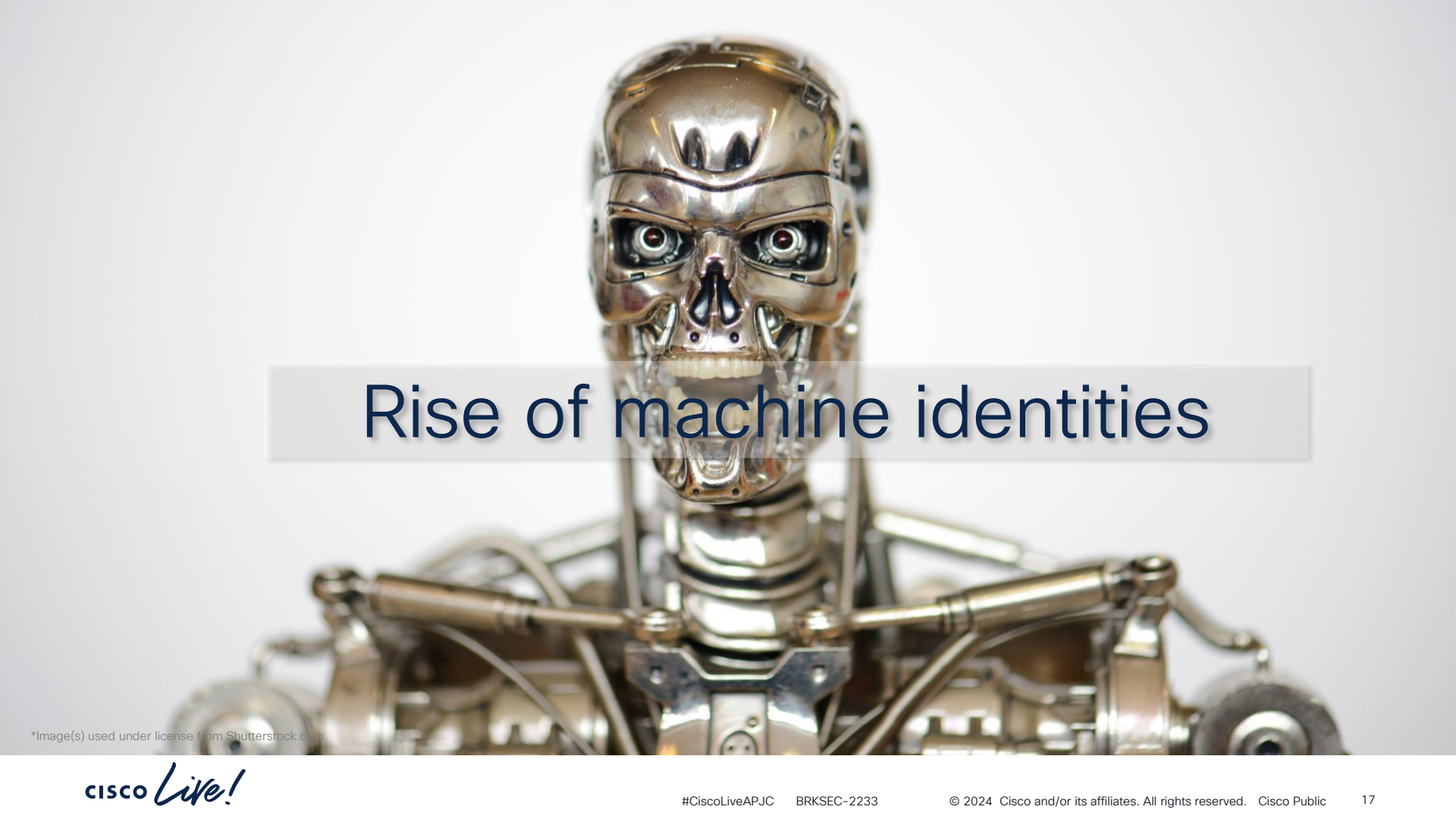
Fragmented identity ecosystem





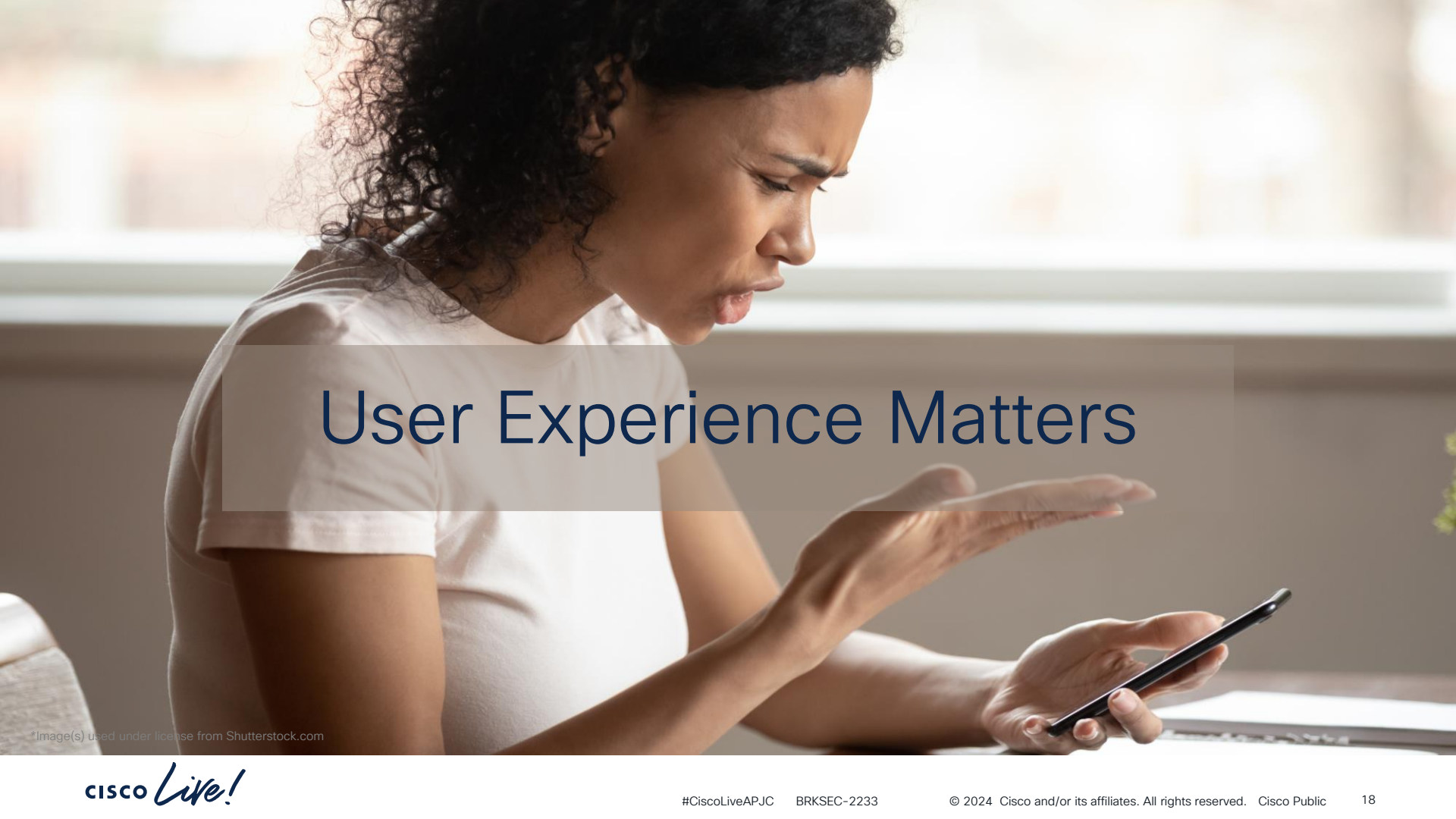
One user -> many identities

*Image(s) used under license from Shutterstock.com



Rise of machine identities

*Image(s) used under license from Shutterstock.com



User Experience Matters

*Image(s) used under license from Shutterstock.com

Common Identity Attack Techniques





*Image(s) used under license from Shutterstock.com

Scattered Spider* Attack Technique

Social
engineering

Gain
credentials /
MFA code

Privilege
escalation

Gains access
to data

* Cybercriminal group responsible for MGM breach

Reference: https://www.cisa.gov/sites/default/files/2023-11/aa23-320a-scattered_spider_0.pdf

*Image(s) used under license from Shutterstock.com

LAPSUS\$* attack technique

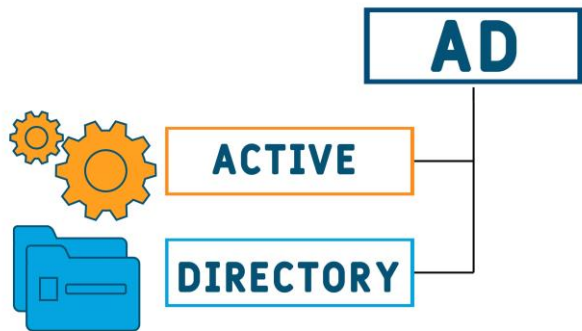
Compromised
credentials

Vishing/push
bombing

Register own
MFA device

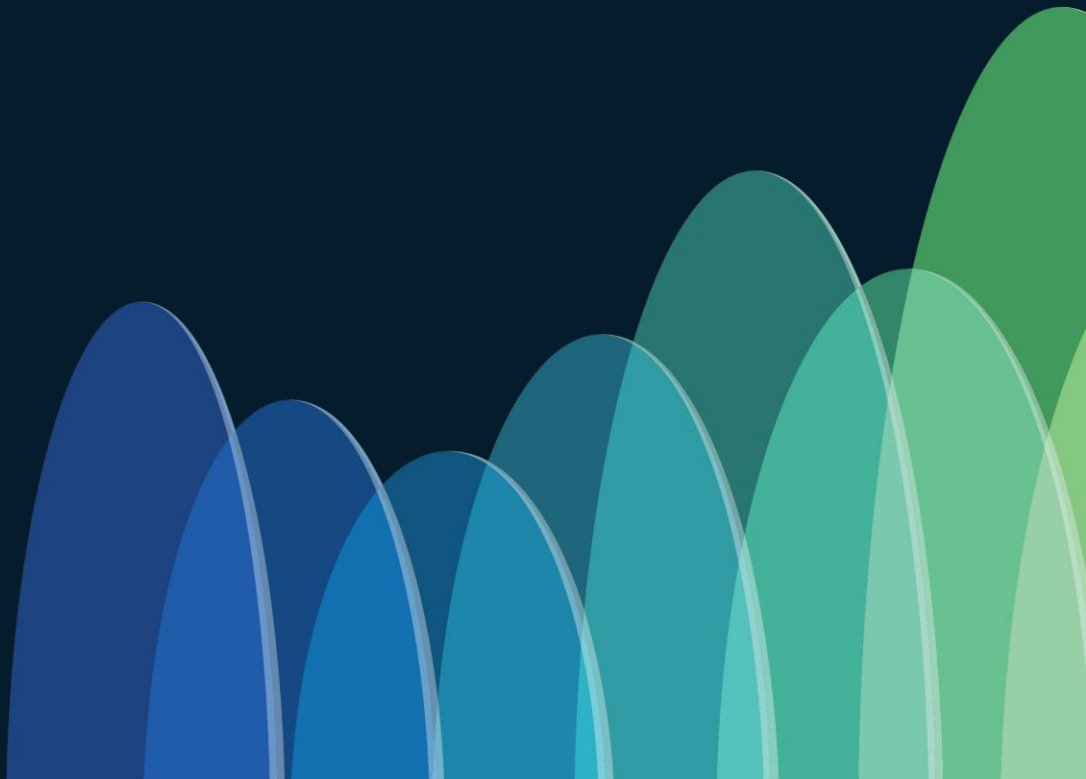
Privilege
escalation

* Cybercriminal group responsible for Cisco breach
Reference: <https://blog.talosintelligence.com/recent-cyber-attack>



*Image(s) used under license from Shutterstock.com

Continuous Identity Security

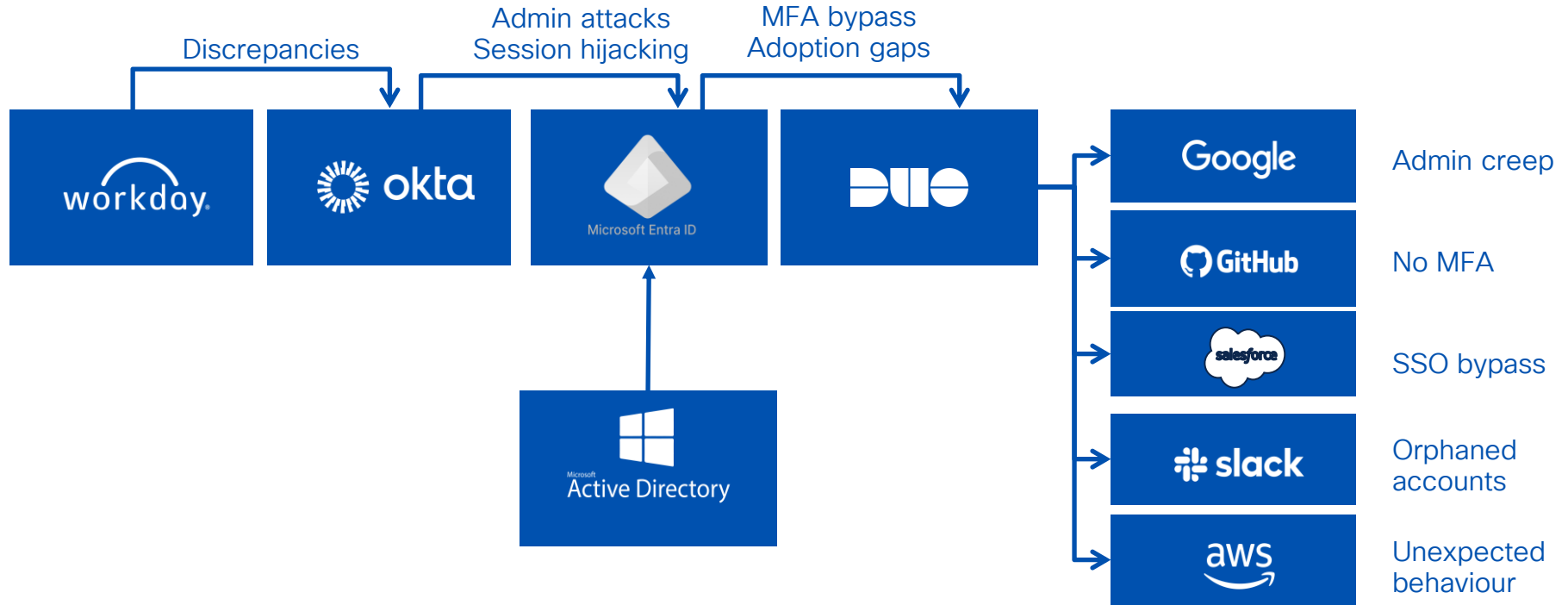


Cisco Identity Intelligence

CISCO *Live!*



Fragmented identity ecosystem



Analytics layer



Users



Machines



Services



Apps



Data



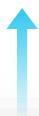
Behaviours



Auth0



Workday



Okta



GitHub



Amazon

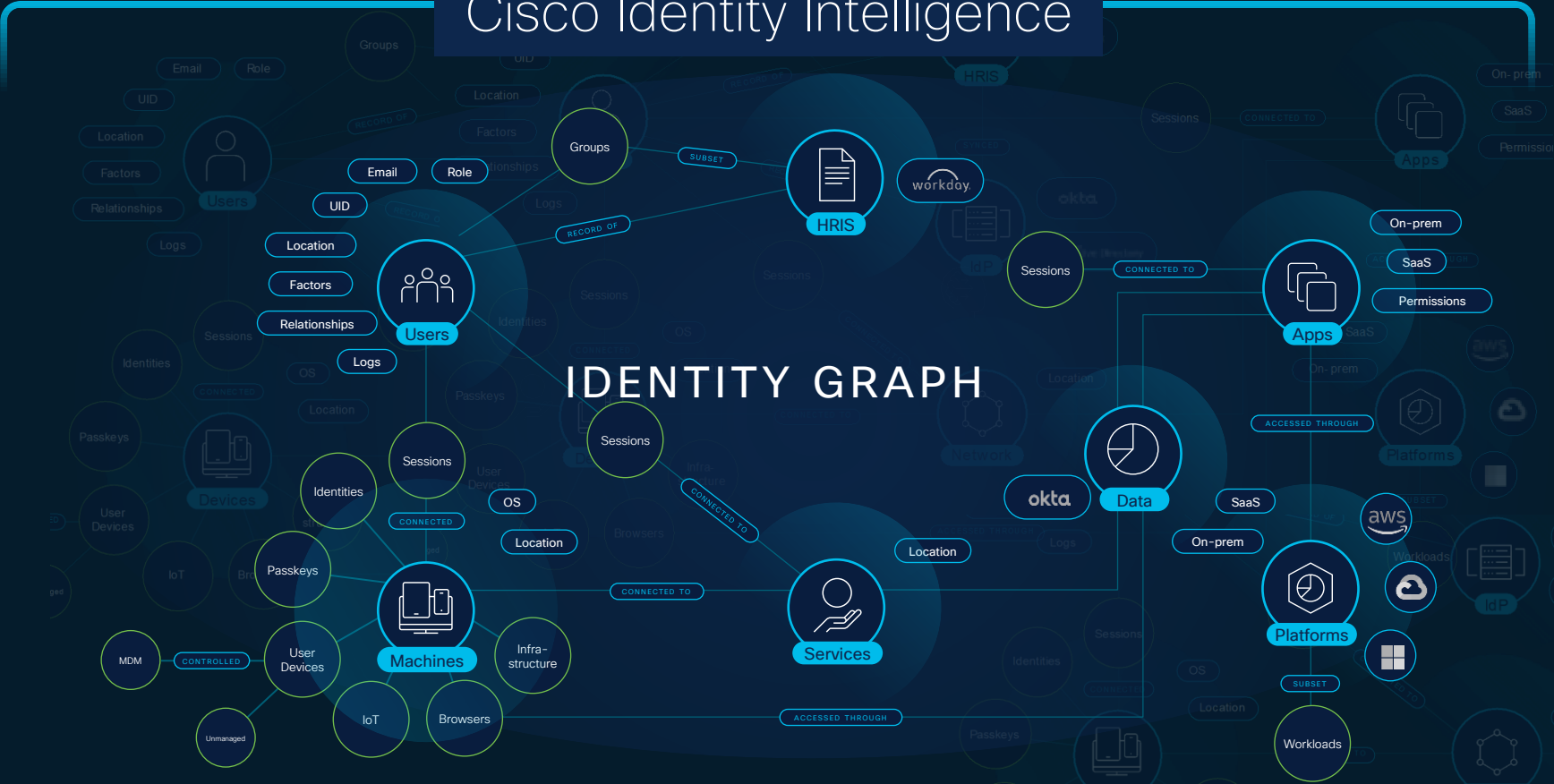


Ping



Microsoft

Cisco Identity Intelligence



User 360

Saved Filters
Default

Status

All

☐ Active 217

☒ Deleted

☒ Deprovisioned

☒ Disabled

☐ Inactive 13

☐ Inconsistent 7

Sources

All

☐ Demo Auth0 2

☐ Demo AWS 3

☐ Demo Azure AD 11

☐ Demo Duo 4

☐ Demo GitHub 8

☐ Demo GSuite 5

☐ Demo Okta 211

☐ Demo Salesforce 7

☐ Demo Workday 6

☐ Slack - oort-teamdata-testing 2

Trust Score

All

☐ Favorable 1

☐ Neutral 19

☐ Questionable 22

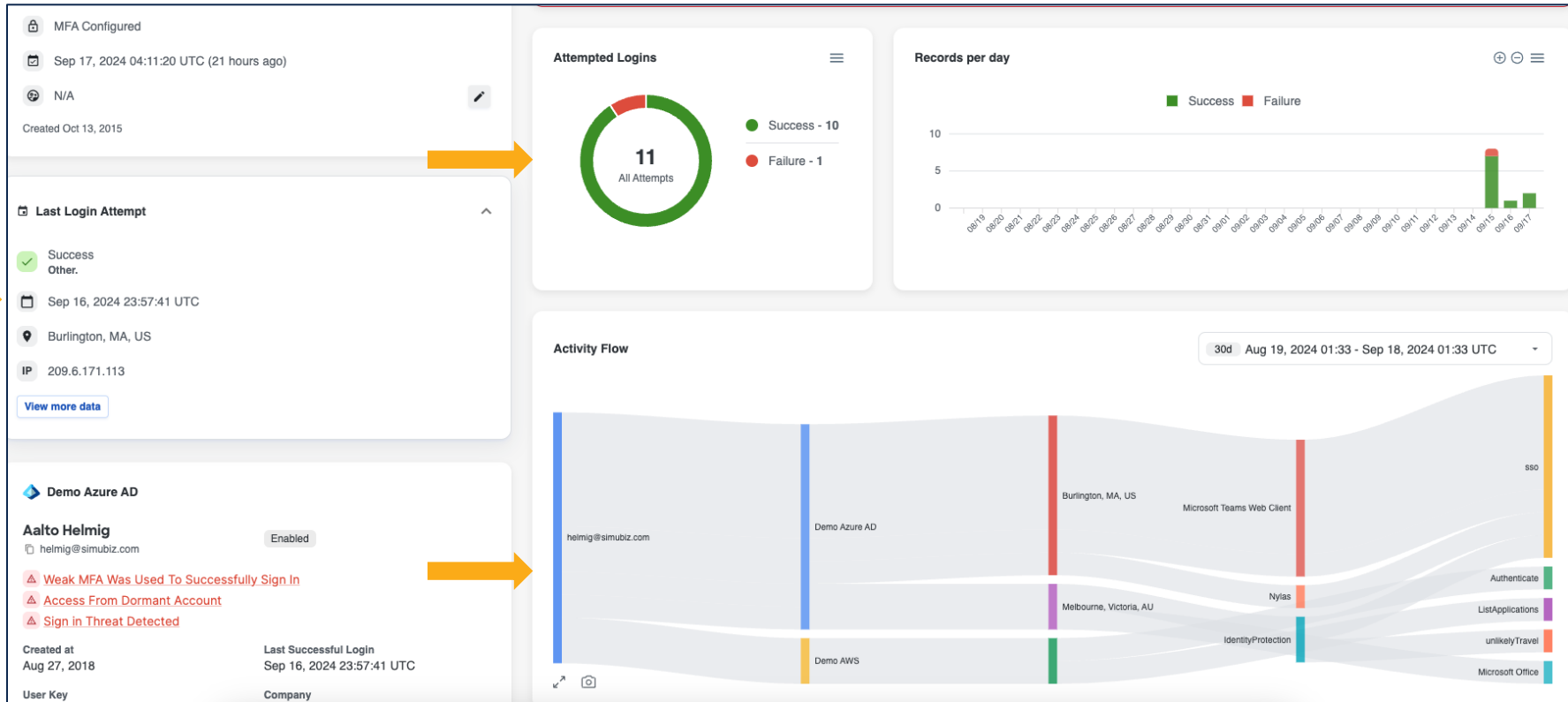
NOT Status:(3 conditions)

Search users, names, group, applications and IPs

237 users found

User ↓	Trust Score ↑	Checks ↑	# IPs ↑	# Logins ↑	Last Seen (UTC) ↑	Last IP Address ↑	Last Location
Aalto Helmig aalto.h@simubiz.com	Unknown		0	N/A	14 Hours Ago Sep 17, 2024 11:46:11	N/A	N/A
Aalto Helmig aalto.helmig@simubiz.com	Unknown	6	7	71	A Day Ago Sep 16, 2024 22:00:05	155.201.163.64	Tampa, FL, US
Aalto Helmig helmig@simubiz.com	Untrusted	6	3	10	21 Hours Ago Sep 17, 2024 04:11:20	N/A	N/A
Aalto Sekine aalto.sekine@simubiz.com	Questionable	5	7	78	A Day Ago Sep 16, 2024 18:15:04	136.158.43.155	Caloocan City, Metro Manila, PH
Adamchick Thome adamchick.thome@simubiz.com	Unknown	4	0	N/A	3 Years Ago Oct 8, 2021 11:48:56	N/A	N/A
Alice Jones alice@simubiz.com	Unknown	1	0	N/A	N/A	N/A	N/A
Altgilbers Yagi altgilbers.yagi@simubiz.com	Unknown	5	6	56	2 Days Ago Sep 16, 2024 12:59:36	59.1.219.28	Deltona, FL, US

User 360



User 360

Authentication Factors								Columns
Factor		Assurance Level ↑	Status ↑	# Changes ↑	Usage Count ↑	Device ↑	Phone Number ↑	Last Used (UTC) ↑
▼  Phone △ Weak Demo Azure AD 3179e48a-750b-4051-897c-87b9720928f7		△ Low	ACTIVE	0	1	+1 2222222222	+1 2222222222	Sep 16, 2024 23:57:4
▼  Password Demo Azure AD 28c10230-6103-485e-b985-444c60001490		△ Low	ACTIVE	0	0	N/A	N/A	N/A
▼  SMS △ Weak Demo Azure AD		△ Low	ACTIVE	0	0	+1 2222222222	+1 2222222222	N/A

User 360

The screenshot displays the Cisco User 360 interface for a user named Aalto Helmig (helmig@simubiz.com). The interface includes a navigation bar with tabs: Overview, Activity, Networks, Devices, Applications, Groups, Checks (6), and Actions. A yellow banner at the top states: "We identified other users with a similar username or the same employee ID as helmig@simubiz.com. Do you want to link them?" with Dismiss and Review buttons. An orange arrow points from the left to this banner.

Below the banner, a modal titled "These accounts might belong to the same user" is open. It contains the following text: "Review the following users that we identified with the same employee ID or similar usernames to determine if the suggested users should be linked. Linking users does NOT merge the users' records or activity into one user. Select users you would like to link with helmig@simubiz.com. To add or remove existing linked users from this profile, go to the 'Linked Users' table." The modal lists three accounts with the same username: Aalto Helmig (aalto.h@simubiz.com), Aalto Helmig (aalto.helmig@simubiz.com), and Aalto Helmig (helmig@simubiz.com). Each account has a checkbox (all checked) and three radio buttons: Link, Reject, and Skip for now. An orange arrow points from the left to the modal.

The background shows a summary of the user's profile, including internal status, N/A fields, Simubiz affiliation, MFA configuration, and last updated time (Sep 17, 2024 04:11:20 UTC).

User trust score

Brian Hayes   brian.hayes@simubiz.com	Untrusted	8	10	26
Brzostowski Drebes   brzostowski.drebes@simubiz.com	Questionable	6	6	
Byran Laperuta   byran.laperuta@simubiz.com	Questionable	3	4	
CLS Admin   cls_admin@simubiz.com	Favorable	4	1	
Chanza Rosser   santos.rosser@simubiz.com	Untrusted	7	14	

Trust Score
Untrusted

Special account engaged in MFA flood attack
New country for tenant and special account.
New country for tenant, special account, resurrected account, and unmanaged device.

Additional details

Special Account
Resurrected Account
Failing Checks: [Access From Dormant Account](#)

MFA Flood
Failing Checks: [Telecom MFA Limit Reached](#)

New Country for Tenant
Failing Checks: [New Country for Tenant](#)

Unmanaged Device
Failing Checks: [Unmanaged Devices Access](#)

5 events matching score [View in Activity Tab](#) [View all activities with a score](#)

Identity checks

☐ Okta 44	
☐ Salesforce 13	
☐ Slack 2	
☐ Workday 3	
Compliance All	
☐ Full 7	
☐ Partial 56	
☐ Not Enabled 1	
Severity All	
☐ Critical 20	
☐ Low 16	
☐ Moderate 28	
Topic All	
☐ Compliance 30	
☐ Devices 1	
☐ Identity Posture Insight 31	
☐ Identity Threat Insight 33	
Frameworks All	
Scopes All	

All Checks			
Check		# Failing	# Excluded
<div><div>34%</div><div>No MFA Configured</div><div>Critical</div><div>End Users - Compliance, Identity Posture Insight</div></div>		157 → No change since last week → No change since last month	0
<div><div>77%</div><div>Unused Application for a User</div><div>Low</div><div>End Users - Compliance, Identity Posture Insight</div></div>		53 → No change since last week → No change since last month	0
<div><div>77%</div><div>User in IDP but not in HRIS</div><div>Critical</div><div>End Users - Compliance, Identity Posture Insight</div></div>		53 → No change since last week → No change since last month	0
<div><div>84%</div><div>New Country for Tenant</div><div>Moderate</div><div>End Users - Identity Threat Insight</div></div>		38 → No change since last week → No change since last month	0
<div><div>88%</div><div>Registered Location Mismatch</div><div>Low</div><div>End Users - Identity Threat Insight</div></div>		28 → No change since last week → No change since last month	0
<div><div>90%</div><div>Weak MFA Was Used To Successfully Sign In</div><div>Critical</div><div>End Users - Identity Posture Insight</div></div>		22 → No change since last week → No change since last month	0

Identity posture insight



Check	# Failing
<div><div>34%</div><div><div>No MFA Configured</div><div><div>Critical</div>End Users - Compliance, Identity Posture Insight</div></div></div> <div>157</div> <div><div>→ No change since last week</div><div>→ No change since last month</div></div>	
<div><div>77%</div><div><div>Unused Application for a User</div><div><div>LOW</div>End Users - Compliance, Identity Posture Insight</div></div></div> <div>53</div> <div><div>→ No change since last week</div><div>→ No change since last month</div></div>	
<div><div>77%</div><div><div>User in IDP but not in HRIS</div><div><div>Critical</div>End Users - Compliance, Identity Posture Insight</div></div></div> <div>53</div> <div><div>→ No change since last week</div><div>→ No change since last month</div></div>	
<div><div>90%</div><div><div>Weak MFA Was Used To Successfully Sign In</div><div><div>Critical</div>End Users - Identity Posture Insight</div></div></div> <div>22</div> <div><div>→ No change since last week</div><div>→ No change since last month</div></div>	
<div><div>90%</div><div><div>No Strong MFA Configured</div><div><div>Moderate</div>End Users - Compliance, Identity Posture Insight</div></div></div> <div>22</div> <div><div>→ No change since last week</div><div>→ No change since last month</div></div>	
<div><div>97%</div><div><div>User Password Expiration Failure</div><div><div>Moderate</div>End Users - Identity Posture Insight</div></div></div> <div>6</div> <div><div>→ No change since last week</div><div>→ No change since last month</div></div>	
<div><div>97%</div><div><div>User Stuck in Non-functional State</div><div><div>Moderate</div>End Users - Compliance, Identity Posture Insight</div></div></div> <div>5</div> <div><div>→ No change since last week</div><div>→ No change since last month</div></div>	

Identity posture insight



Details

Detects users defined in your IDP that your HR Information System (HRIS) cannot find.

Recommended Actions

We recommend removing these users. If the account is currently showing activity, we recommend contacting the manager.

Last Report Update

Sep 17, 2024 04:49:43 UTC

Topics

Compliance, Identity Posture

Frameworks

CIS 5.6

Compatibility

 HRIS  Workday

Tags

[+ Add tag](#)

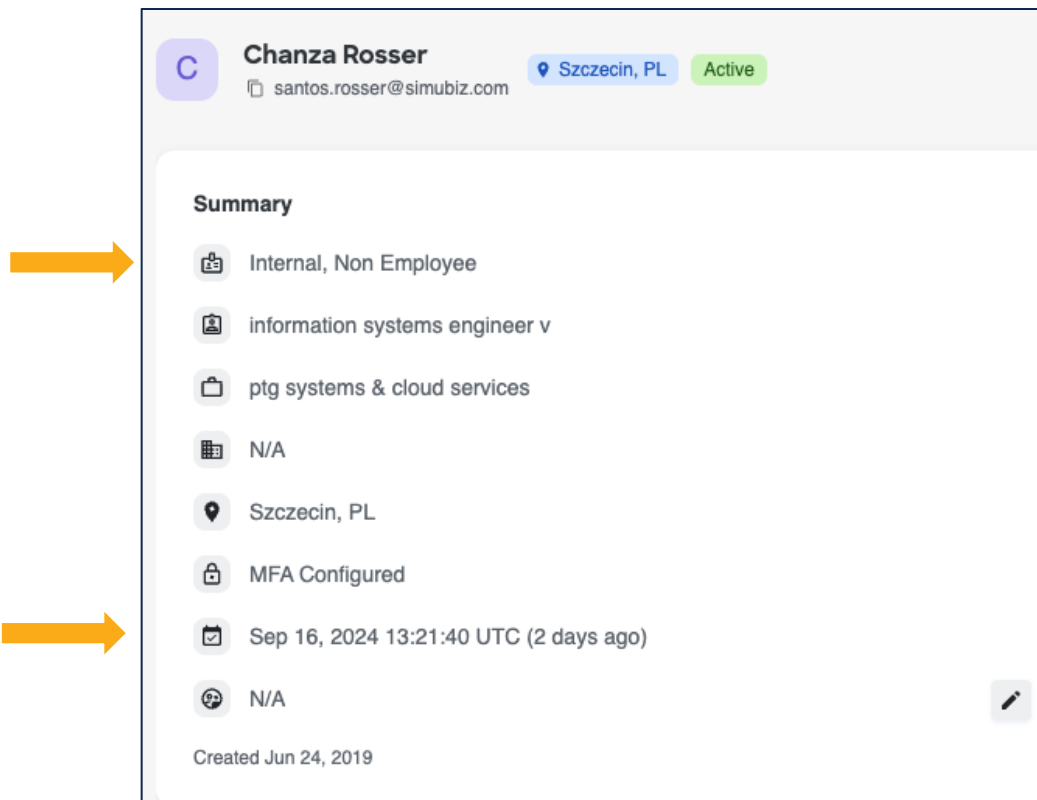


 Automated notifications for this check are not configured.
Please configure notifications if you wish to receive automated reports about users failing this check.

53 failing users

User	First Reported (UTC) ↑	Last Reported (UTC) ↑	Admin Notified
pagotto.morren@simubiz.com 	Sep 17, 2024 04:41:31	Sep 17, 2024 04:49:37	Not notified
santos.rosser@simubiz.com 	Sep 17, 2024 04:41:31	Sep 17, 2024 04:49:37	Not notified
schildknecht.sadorra@simubiz.com 	Sep 17, 2024 04:41:31	Sep 17, 2024 04:49:37	Not notified

Identity posture insight



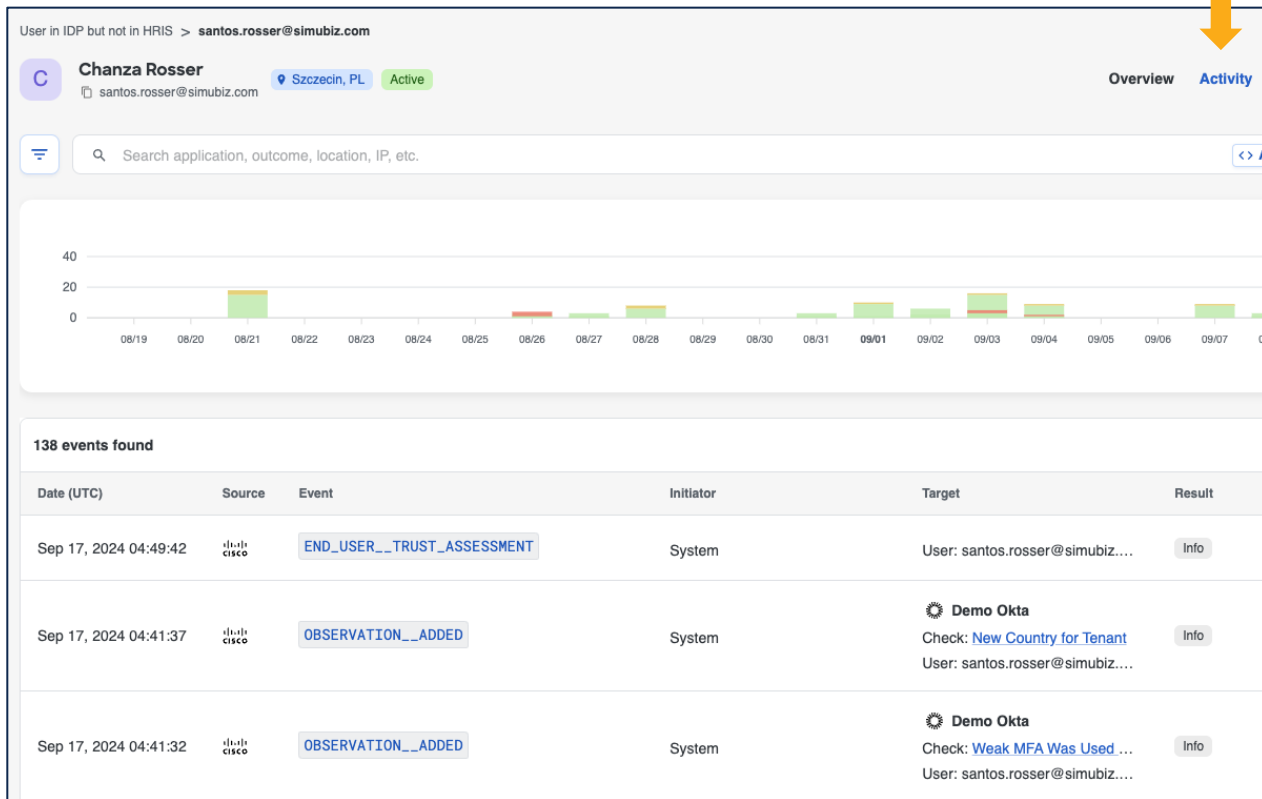
Chanza Rosser
santos.rosser@simubiz.com
Szczecin, PL Active

Summary

- Internal, Non Employee
- information systems engineer v
- ptg systems & cloud services
- N/A
- Szczecin, PL
- MFA Configured
- Sep 16, 2024 13:21:40 UTC (2 days ago)
- N/A

Created Jun 24, 2019

Identity posture insight



Identity posture insight

Check	# Failing
 User in IDP but not in HRIS • Critical End Users - Compliance, Identity Posture Insight	53 → No change since last week → No change since last month
 Weak MFA Was Used To Successfully Sign In • Critical End Users - Identity Posture Insight	22 → No change since last week → No change since last month
 No Strong MFA Configured • Moderate End Users - Compliance, Identity Posture Insight	22 → No change since last week → No change since last month
 User Password Expiration Failure • Moderate End Users - Identity Posture Insight	6 → No change since last week → No change since last month
 User Stuck in Non-functional State • Moderate End Users - Compliance, Identity Posture Insight	5 → No change since last week → No change since last month
 Upcoming App Key Expiration • Low End Users - Identity Posture Insight	5 → No change since last week → No change since last month
 Inactive Users • Moderate End Users - Compliance, Identity Posture Insight	4 → No change since last week → No change since last month

Identity posture insight

Weak MFA Was Used To Successfully Sign In (Last reported: Less than 1 day ago) [View activity from all IPs](#) [Factor Used](#) ✕

Factor Used

sms

Event Date: Aug 18, 2024 06:11:39 UTC

Action ↑	TargetResource ↑
Verify user identity	N/A
User single sign on to app	workday
User single sign on to app	five9 plus adapter for salesforce

sms

Event Date: Sep 4, 2024 06:05:06 UTC

Action ↑	TargetResource ↑
Verify user identity	N/A
User single sign on to app	cisco asa vpn (saml)

sms

Event Date: Sep 7, 2024 18:14:23 UTC

Action ↑	TargetResource ↑
User single sign on to app	microsoft office 365
Verify user identity	N/A

Identity threat insight



Check	# Failing
<div>99%</div> <div>Inactive Account Probing</div> <div><div>Critical</div>End Users - Identity Threat Insight</div>	2 → No change since last week → No change since last month
<div>99%</div> <div>A Bypass Code Was Used To Successfully Sign In</div> <div><div>Critical</div>End Users - Identity Threat Insight</div>	2 → No change since last week → No change since last month
<div>99%</div> <div>Login to Admin Console in Okta</div> <div><div>Low</div>End Users - Compliance, Identity Threat Insight</div>	2 → No change since last week → No change since last month
<div>99%</div> <div>Admin Role Assigned to User</div> <div><div>Moderate</div>End Users - Compliance, Identity Threat Insight</div>	2 → No change since last week → No change since last month
<div>99%</div> <div>Risky Parallel Sessions</div> <div><div>Critical</div>End Users - Compliance, Identity Threat Insight</div>	2 → No change since last week → No change since last month
<div>99%</div> <div>Sign in Threat Detected</div> <div><div>Moderate</div>End Users - Identity Threat Insight</div>	2 → No change since last week → No change since last month
<div>99%</div> <div>Active Account under Heavy Attack</div> <div><div>Low</div>End Users - Identity Threat Insight</div>	1 → No change since last week → No change since last month



Identity threat insight

[Checks](#) > **Compromised Session**

Compromised Session  Moderate

Details

An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials.

To identify such sessions, Identity Intelligence alerts on successful login from 2 or more IP-Device pairs for a single session ID.

Recommended Actions

First, make sure that 'Enforce device binding for creating sessions' parameter is Enabled.

Second, contact the end-user to verify the origin of the actions.

Identity threat insight

Compromised Session (Last reported: Less than 1 day ago)
📄 fellmeth.emery@simubiz.com

First, make sure that 'Enforce device binding for creating sessions' parameter is Enabled.

Second, contact the end-user to verify the origin of the actions.

Providers Failing Check Demo Okta

Sessions  102disvYQmOSb6SLnuT7W8Rng

User Title senior software development engineer

User Level Of Trust NEUTRAL

Activity targets

App cisco asa vpn (saml)

User Fellmeth Emery

Identity threat insight

2 events found												Last data collection
Date (UTC)	Source	Event	Initiator	Target	Result	Geo IP	Trust Score	Tags	OS	Browser	Device Type	
Sep 16, 2024 20:04:41		<div>user.authentication.sso</div> <div>Type: WEB</div>	fellmeth.emery@simubiz.com Session: 102disvYQmOSb6SLnu...	<div> cisco asa vpn (saml)</div> <div>User: fellmeth.emery@simubiz....</div>	Success	<div>77.9.12.3</div> <div>Munich, Bavaria, DE</div>	Neutral	<div> 1 failing check</div> <div> New ISP</div>	<div></div> <div></div>	Mobile		
Sep 16, 2024 20:03:34		<div>user.authentication.sso</div> <div>Type: WEB</div>	fellmeth.emery@simubiz.com Session: 102disvYQmOSb6SLnu...	<div> cisco asa vpn (saml)</div> <div>User: fellmeth.emery@simubiz....</div>	Success	<div>77.9.98.7</div> <div>Munich, Bavaria, DE</div>	Neutral	<div> 1 failing check</div> <div> New ISP</div>	<div></div> <div></div>	N/A		

Notification and remediation

Notification Targets

**Email**

Email address to be used for Identity Intelligence notifications. Adding a different address as CC is supported.

[+ Add Email Target](#)

**Microsoft Teams**

Install our bot in your Microsoft Teams to get all the latest updates in any public channel you choose.

[+ Add MS Teams Target](#)

**Slack**

Install our app in your Slack Workspace to get all the latest updates directly or in any channel you choose.

[+ Add Slack Target](#)

**Webhook**

Connect Identity Intelligence failed check notifications with your automated processes via webhooks.

[+ Add Webhook Target](#)

**Webex**

Install our app in your Webex Workspace to get failed check notifications.

[+ Add Webex Target](#)

Ticketing

Identity Intelligence integrates with ticketing services to open new tickets and discover existing tickets related to discovered users.

**Jira**

JIRA is a platform that provides issue tracking and project management functions for software projects.

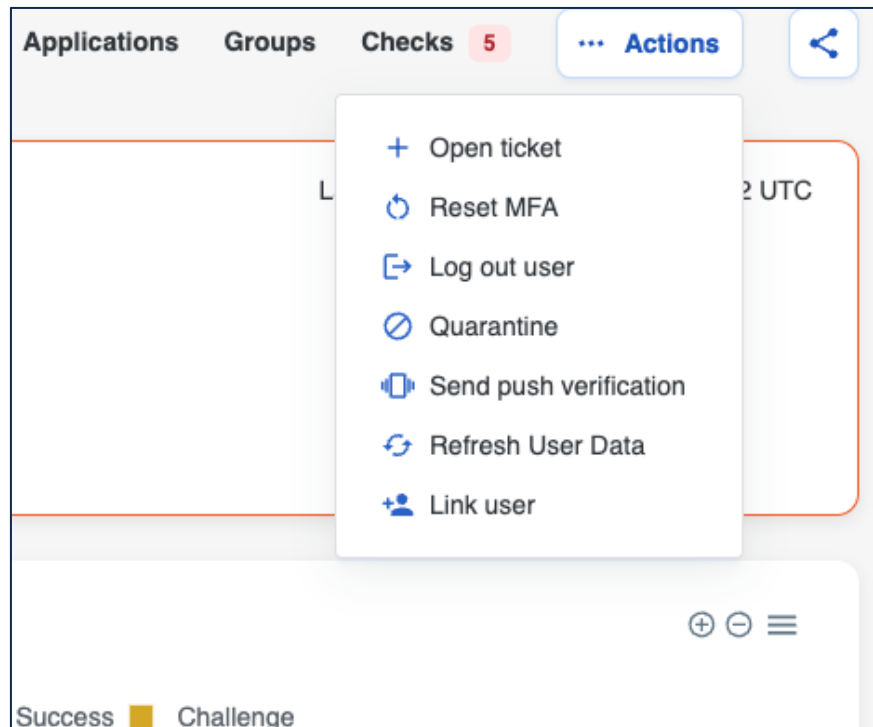
[+ Add Jira Cloud](#)

**ServiceNow**

ServiceNow is a leading IT Service Management and Ticketing tool.

[+ Add ServiceNow](#)

Notification and remediation





Hi! I lost my phone.
I'm unable to
authenticate. Can you
add my new phone. I
need to meet a
customer in 10
minutes. It's urgent!!!

*Image(s) used under license from Shutterstock.com

Help Desk Verification

Trust Score

Untrusted

New country for tenant and special account.

Risk from Entra ID reported special account

^ Additional details

New Country for Tenant

Failing Checks: [New Country for Tenant](#)

Special Account

Risk From Azure

Failing Checks: [Sign in Threat Detected](#)

Help Desk Verification

Name ↑	Source ↑	Status ↑	Assignments	Owners	Usage Count ↑	Last Access (UTC) ↑	Result ↑
 cisco asa vpn (munich) deatrick.deroberts@simubiz.com	 Demo Okta		 vpn-full-access-ipsec	Not supported	96	Sep 13, 2024 14:17:34	Success
 five9 plus adapter for sale... Sensitive deatrick.deroberts@simubiz.com	 Demo Okta		 sg-okta-simubiz-fulltime	Not supported	31	Sep 16, 2024 12:36:52	Success
 microsoft office 365 for simubiz deatrick.deroberts@simubiz.com	 Demo Okta		 sg-okta-simubiz-fulltime	Not supported	6	Sep 16, 2024 06:24:30	Success
 atlassian cloud deatrick.deroberts@simubiz.com	 Demo Okta		 sg-jira-endusers	Not supported	3	Sep 10, 2024 09:53:16	Success
 cisco asa vpn (pinewood uk) deatrick.deroberts@simubiz.com	 Demo Okta		 vpn-full-access-ipsec	Not supported	3	Sep 5, 2024 17:54:53	Success
 servicenow Sensitive deatrick.deroberts@simubiz.com	 Demo Okta		 sg-okta-simubiz-fulltime	Not supported	3	Sep 4, 2024 05:13:31	Success
 workday Sensitive zumbrum@simubiz.com	 Demo Okta		 sg-okta-simubiz-fulltime	Not supported	1	 Sep 16, 2024 06:38:23	Success

Help Desk Verification

▼	 Duo Mobile Demo Duo DPUW9OMLI9IU8XFVU4RF	Medium	ACTIVE	0	0	Apple iPhone 14 Pro Max	+9722222222
▼	 Push Demo Duo DPUW9OMLI9IU8XFVU4RF	Medium	ACTIVE	0	0	Apple iPhone 14 Pro Max	+9722222222
▼	 Call ⚠ Weak Demo Duo DPUW9OMLI9IU8XFVU4RF	⚠ Low	ACTIVE	0	0	Apple iPhone 14 Pro Max	+9722222222
▼	 SMS ⚠ Weak Demo Duo DPUW9OMLI9IU8XFVU4RF	⚠ Low	ACTIVE	0	0	Apple iPhone 14 Pro Max	+9722222222
▼	 Push Demo Okta opf11otl4mIH4efn357	Medium	ACTIVE	1	15	Pixel 3	N/A
▼	 Microsoft Authenticator App Demo Azure AD e74c2660-857e-4d54-9666-e1c5316d3d57	Medium	PENDING	0	0	iPhone 12 Pro Max	N/A

A woman with curly hair, wearing a headset and a grey button-down shirt, is sitting at a desk in a call center. She is looking at a computer monitor. In the background, another person is also working at a desk. Two blue speech bubbles are overlaid on the image, containing text related to Multi-Factor Authentication (MFA).

I see another
device enrolled for
MFA. Do you have
access to the
device?

When was the last
time you
successfully logged
into Workday?

*Image(s) used under license from Shutterstock.com

Duo Passport

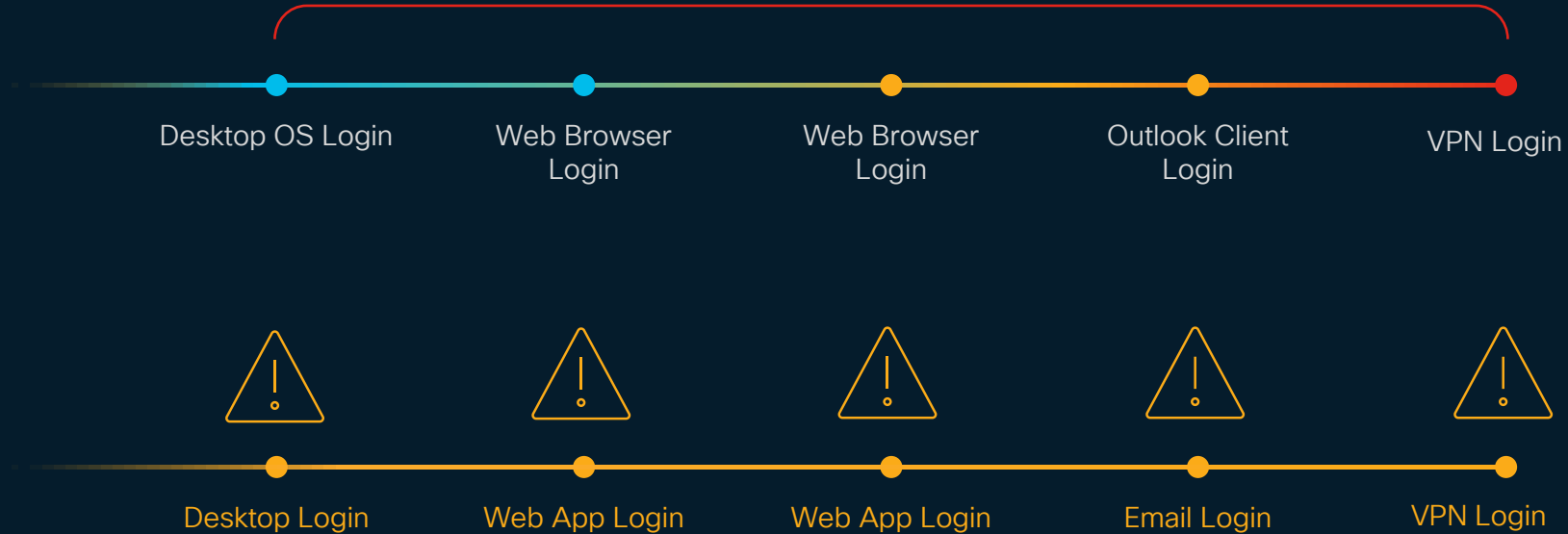




*Image(s) used under license from Shutterstock.com

Anatomy of frustration

Authentication Experience



Duo Passport

User
authentication
experience



User
authentication
experience with
Duo Passport

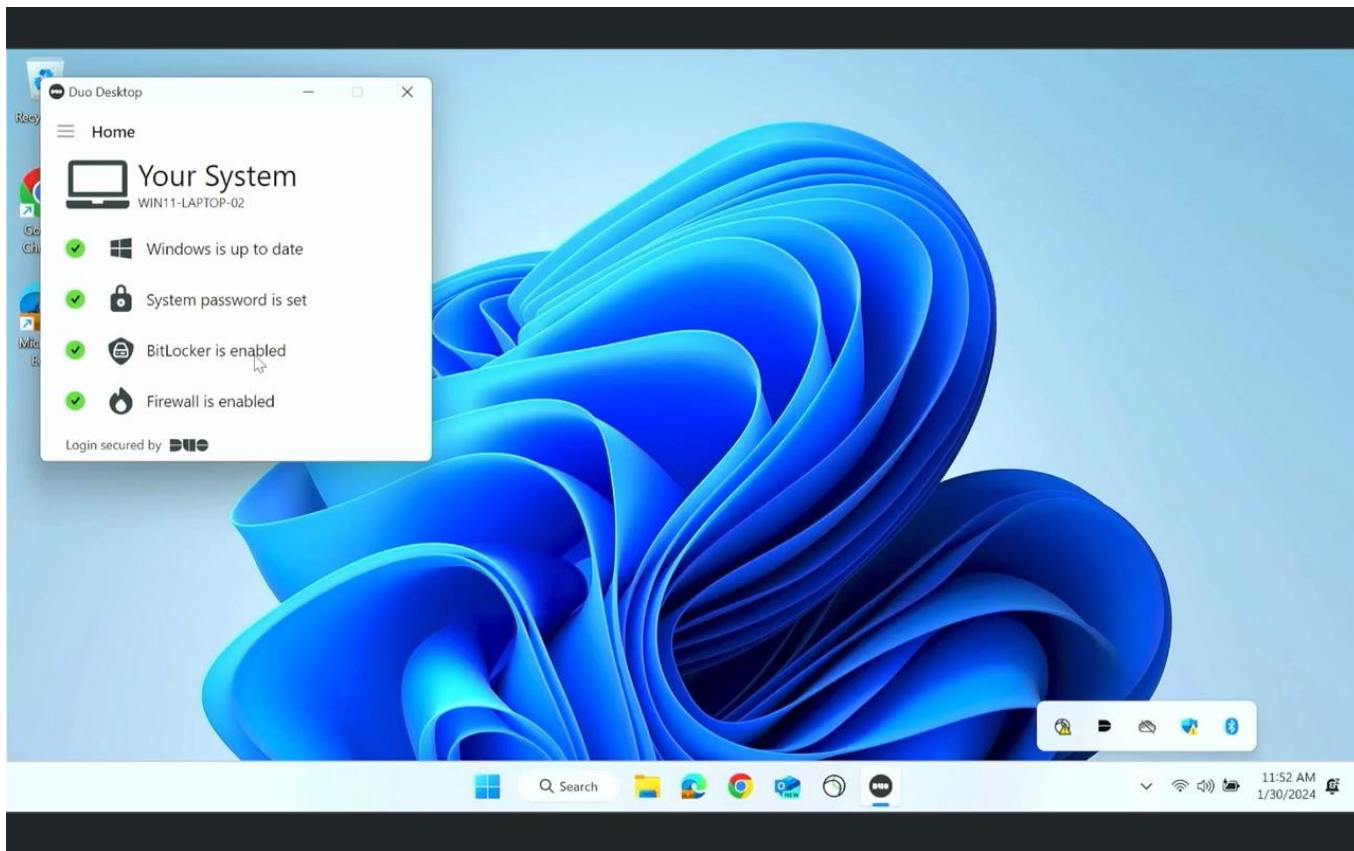


Duo Passport

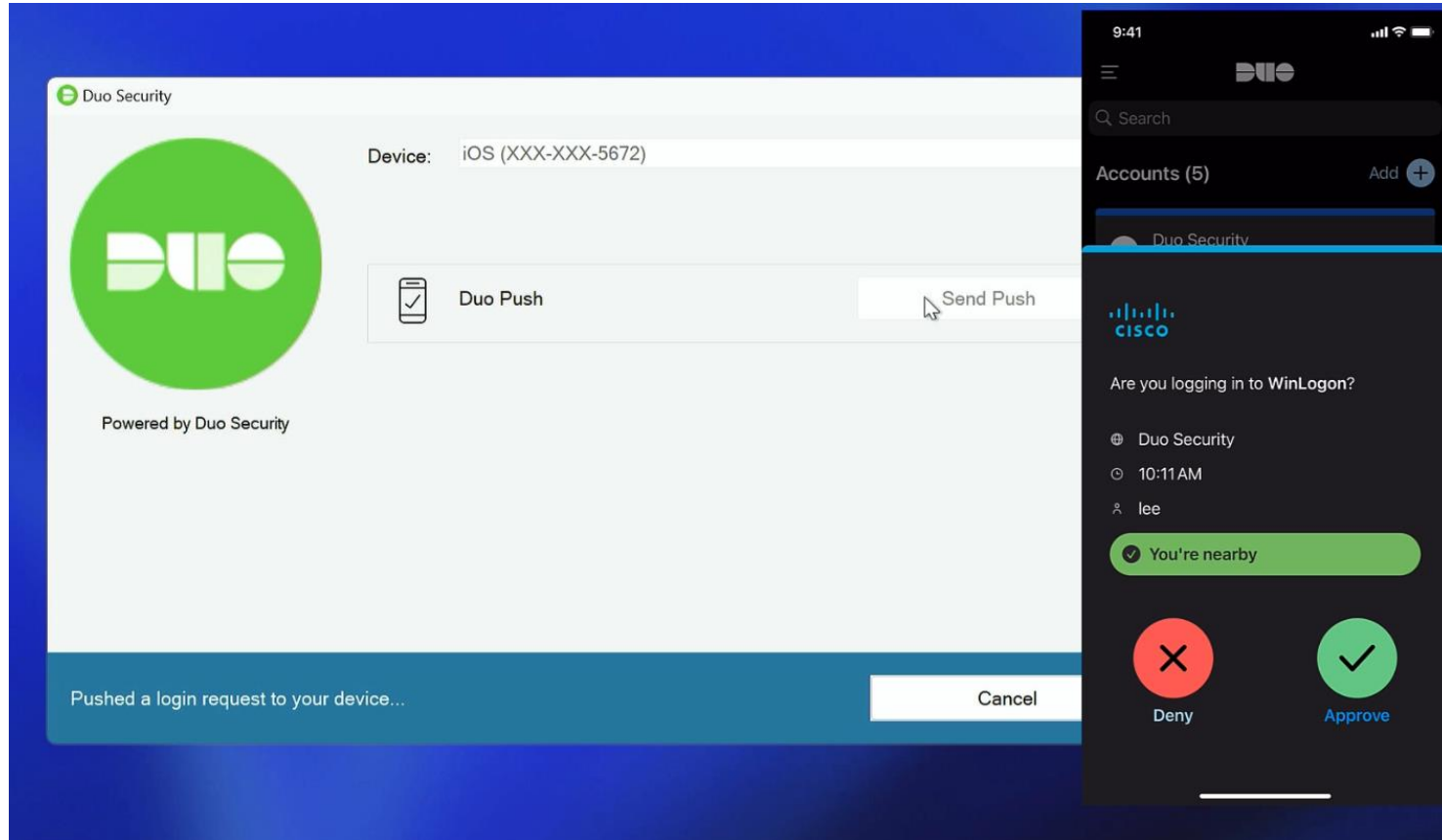
Secure Passwordless Desktop Login

Log in once

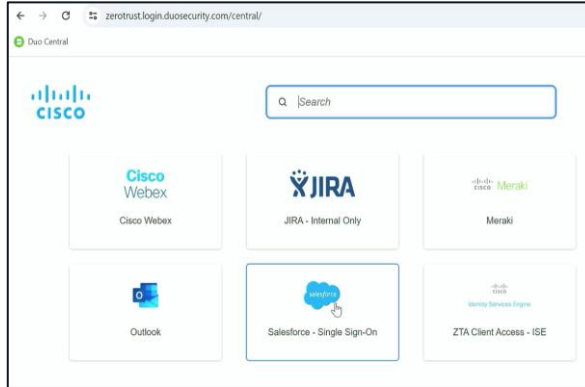
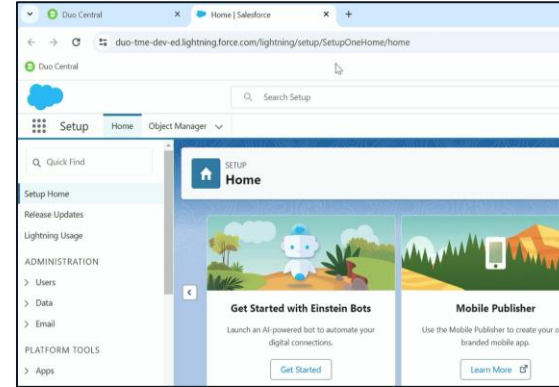
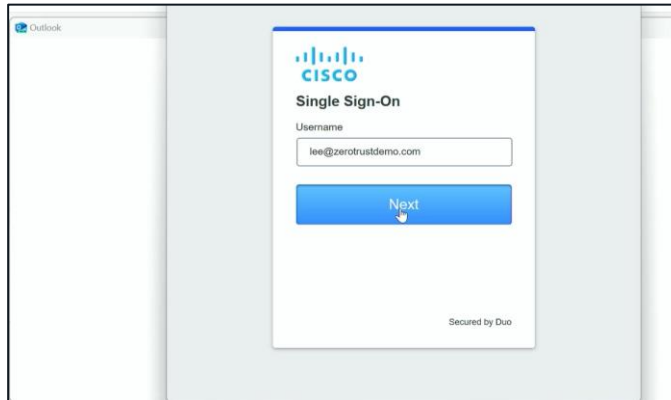
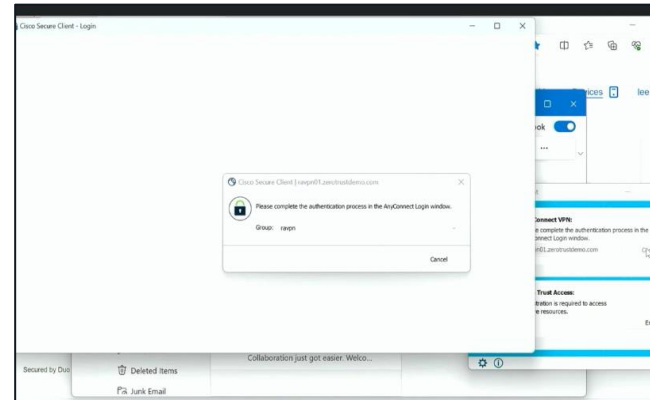
Duo Passport – User Experience



Duo Passport – User Experience



Duo Passport – User Experience



Duo Passport – User Experience



Duo Passport – Admin Experience

Enable Passport

Once you've deployed Duo Desktop and configured your remembered devices policy, you can enable Duo Passport for some or all users.

- ☐ Disable Passport
- ☐ Enable Passport for only certain groups

Groups to include

No groups selected

- ☐ Enable Passport for all users, except certain groups

Groups to exclude

No groups selected

- ☒ Enable Passport for all users

Save

Cancel

Remembered devices allow users to skip subsequent 2FA and passwordless login requests.

☒ Remember devices for browser-based applications

☒ Allow users to remember their devices for 8 hours

☐ After a user has confirmed for any application, their device will be remembered for all applications.

☒ Remember devices for Windows Logon

Allow users to remember their device for 1 hours. Note: 2FA will be enforced after users sign-out, reboot, or change networks

1:47:59 PM
18 SEP 2024

✓ **Granted**
Remembered device via Passport

skishan-
admin@bdreams.co

Secure Access-
SSO

No detections

› Windows 11, version 22H2
(22621.3155)
As reported by Duo Desktop

Remembered Device
Location Unknown

1:47:57 PM
18 SEP 2024

✓ **Granted**
Remembered device via Passport

skishan-
admin@bdreams.co

Secure Access-
SSO

No detections

› Windows 11, version 22H2
(22621.3155)
As reported by Duo Desktop

Remembered Device
Location Unknown

Key Takeaways

Re-think Identity Security



Identify

- Process and policy
- Governance and lifecycle management
- Identity inventory



Protect

- Effective MFA on every application
- Device posture and trust
- Build dynamic, risk-based access policy



Detect

- Cross platform identity visibility
- Establish behaviour
- Analyse suspicious activity



Respond

- Step-up or block risky logins
- Powerful remediation actions
- Automate quarantine actions

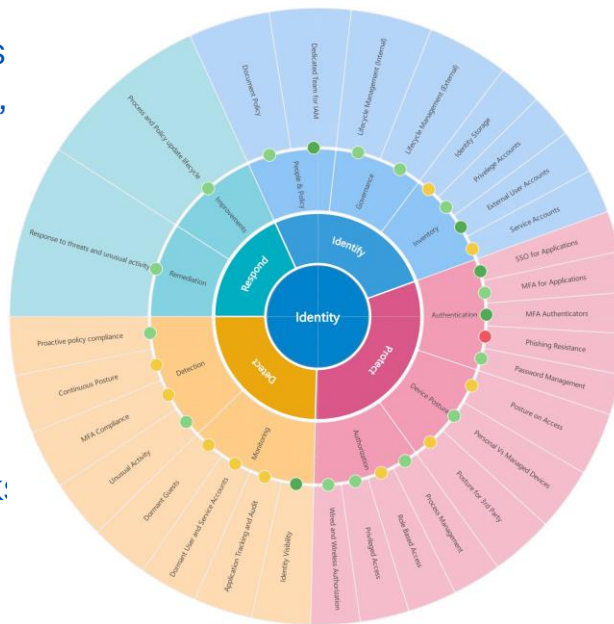
Free Identity Security Assessment

IAM posture evaluation
IAM hygiene review that identifies
no/weak MFA, dormant accounts,
over-privileged users and more

Identity population insight
Unified view of all identities with
detailed
activity and device mappings

Identity threats
Insight into identity-related attacks

License usage
Idle license insight



Identity Security Workshop /
Identity Security Assessment -
Register Interest



<https://forms.office.com/r/xJBCxyLdRX>

Identity Posture Score

Last Update: Sep 3, 2024



Take actions to improve your posture

Recommended Action	Failing Users	Severity
Remove users who should not be present, or add users to HRIS if needed	53	Critical
Require priority accounts to set up a stronger MFA factor on their account	5	Critical
Review Entra users forwarding emails and clean up as needed	2	Critical
Require priority accounts to configure and actively utilize stronger MFA factors	3	Critical
Review GSuite users forwarding emails and clean up as needed	1	Critical

Key Takeaways

- Identity threats are constantly evolving
- Identity Security needs to go beyond password and MFA controls
 - Identify
 - Protect
 - Detect
 - Respond
- User Experience is equally important
- Cisco Identity Intelligence with Duo Passport provides [seamless secure authentication experience](#)

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel
Better Employee
and Customer
Experiences

Level 1
Room 106



Smart, Secure,
Seamless:
Transforming
Experiences with
Next-Generation
Networking

Level 2
Room 204



Harness a Bold
New Era:
Transform Data
Centre and
Service Provider
Connectivity

Level 2
Room 203



Securing User to
Application and
Everything in
Between

Level 2
Melbourne Room 2



Unlocking
Digital Resilience
through Unified
Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Register your interest in Identity Security Workshop and Assessment
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC