

Stop Identity-Based Attacks with Security-First Duo IAM

cisco Live !

Sheela Kishan
Solutions Engineer - Identity

Session ID: BRKSEC-2233

Your Speaker

- Based in Melbourne, Australia
- With Cisco for 14+ years
- Holds CCIE and CISSP certification
- Started with Large Scale networks design and deployment
- Focusing on Identity and Access Management last 5 years
- Enjoys photography, reading, and Lord of the Rings.



Cisco Webex App

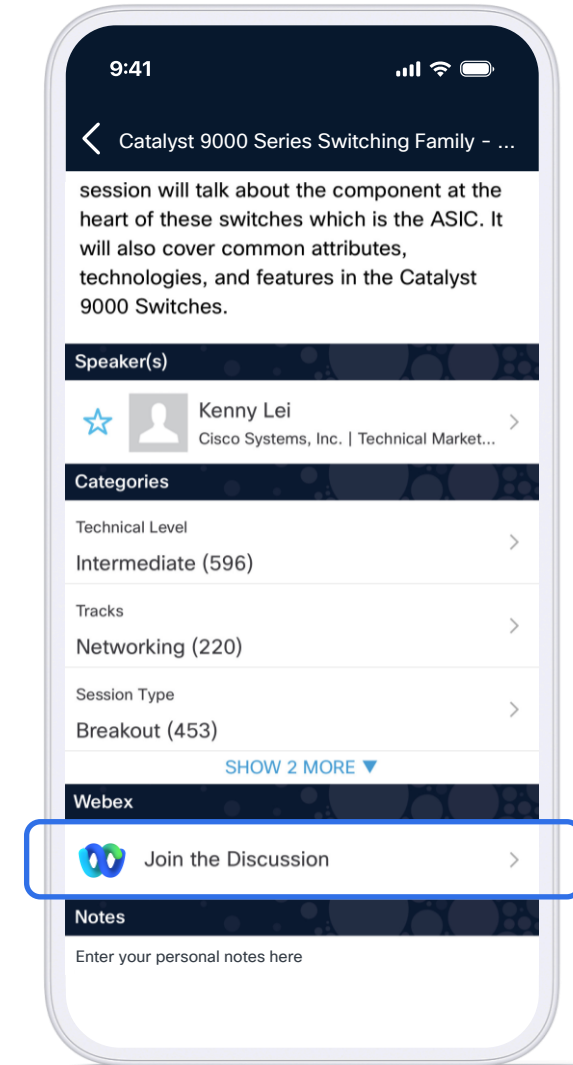
Questions?

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 14 November 2025.

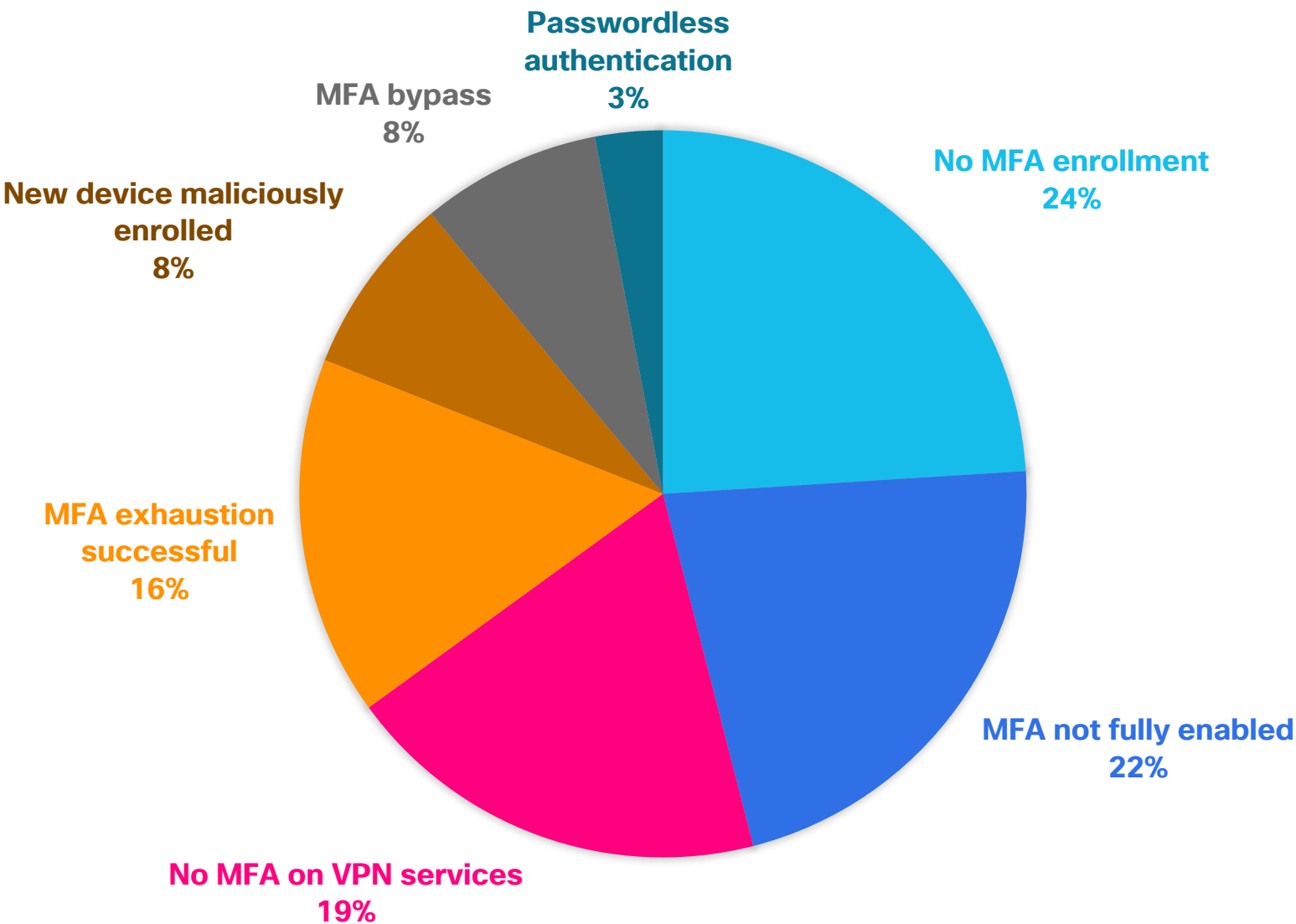


<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2233>

60%

More than half of Talos IR cases
had an **identity attack** component
in 2024.

Observed MFA trends during attacks



* From Cisco Talos Year In Review Report 2024

Agenda

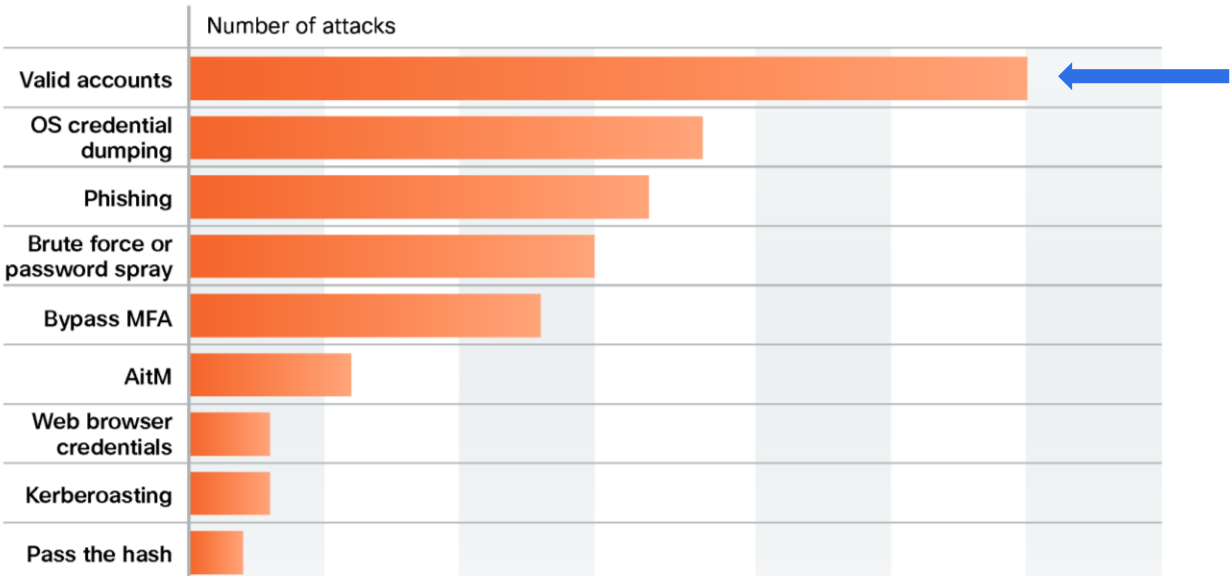
- 01 Identity Attack Trends**
- 02 Identity Security Challenges**
- 03 Phishing-resistant Authentication**
- 04 Session Theft Protection**
- 05 Protect your Infrastructure**
- 06 Identity Visibility**
- 07 Summary**

Identity Attack Trends

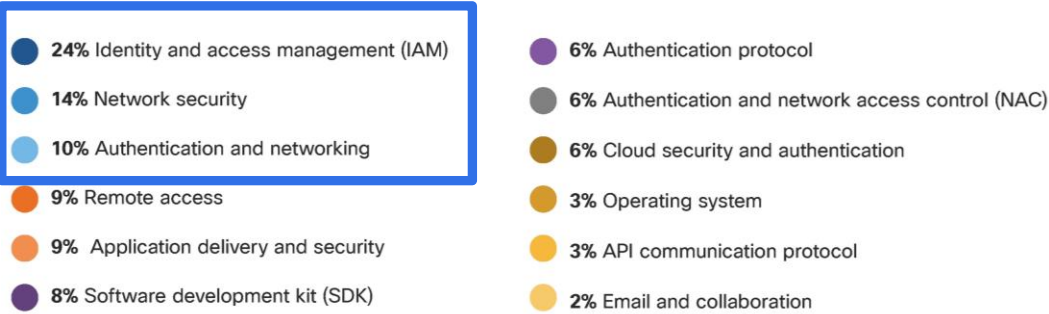
Attacks on Identity

- Valid accounts is the easiest way to gain access
- Nearly half of all identity attacks targeted Active Directory
- IAM applications most frequently targeted in MFA attacks
- Network Infrastructure is the new attack vector

Types of identity attacks observed in Talos IR



Types of applications targeted in MFA attacks

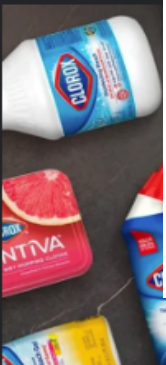


* Based on Cisco Talos Year In Review Report 2024

It's Happening Everywhere!

 THAT WAS EASY

After \$380M hack, Clorox sues its “service desk” vendor for simply giving out passwords



Cognizant Agent: How can I help you today?
Cybercriminal: Um my password on Okta was not working ...
Cognizant Agent: I’m going to have your password reset from my end right away. Ok. And we’ll see how it’s going to work. Ok. [Following a brief hold] Thank you ... I’m extremely sorry for the long hold. So ... password is going to be Clorox@123.

Cybercriminal: My Microsoft MFA isn’t working.
Cognizant Agent: Oh, ok...
Cybercriminal: Can you reset my MFA? It’s on my old phone ... [inaudible] old phone.
Cognizant Agent: [Following a brief hold]. So thanks for being on hold, Alex. So multifactor authentication reset has been done now. Ok. So can you check if you’re able to login ...
Cybercriminal: Alright. It let me sign in now. Thank you.

Qantas attack reveals one phone call is all it takes to crack cybersecurity’s weakest link: humans

Other sectors: finance and
Did the Qantas hackers use AI voice deepfakes?
Fingers pointed at Scattered Spider cybercrime group.

By Tom Williams on Jul 17 2025 01:25 PM

Marks & Spencer breach linked to Scattered Spider ransomware attack

By [Lawrence Abrams](#)

 April 28, 2025  04:28 PM

MGM Resorts breached by 'Scattered Spider' hackers: sources

By Zeba Siddiqui and Christopher Bing

September 14, 2023 9:15 AM GMT+10 · Updated September 14, 2023



It's Happening Everywhere!

 THAT WAS EASY

After \$380M
Clorox sues
“desk” vendor
giving out p

Cognizant Agent: How

Cybercriminal: Um my

Cognizant Agent: I’m g

away. Ok. And we’ll see

Thank you ... I’m extrer

be Clorox@123.

Cybercriminal: My M

Cognizant Agent: Ol

Cybercriminal: Can

phone.

Cognizant Agent: [F

multifactor authentic

you’re able to login ..

Cybercriminal: Alrig

 Australian Signals Directorate

91,404 followers

5h • 🌐

Today we have released a joint advisory with the U.S. and international partners on the tactics, techniques and procedures (TTPs) recently used by Scattered Spider threat actors against the commercial facilities sector and subsectors. ...more



JOINT CYBERSECURITY ADVISORY

Scattered Spider

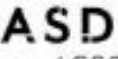


 Communications Security Establishment
Canadian Centre for Cyber Security

 Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

 National Cyber Security Centre
a part of GCHQ

 Australian Government
Australian Signals Directorate

 ASD
ACSC
Australian Signals Directorate

 AFP
Australian Federal Police

call is
's

ifakes?
ne group.

Scattered Spider ransomware

April 28, 2025 04:28 PM

Scattered





Case Study: Identity attack against a University



Adversary gains primary credentials through data leak/ dark web



Adversary sends phishing email to admin to activate MFA



More than 50 contractors as admins



Victim clicks activation link, adversary adds their own device as MFA



Adversary uses compromised account to gain access to internal email



Adversary targets other users in a mass phishing campaign

Identity Security Challenges

Evolution of Authentication & Attack Tactics

Password Tactics

- Password Spray
- Brute Force



MFA Bypass 1.0

- Telephony Attacks
- Social Engineering

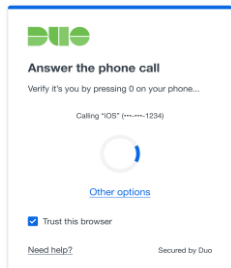
MFA Bypass 2.0

- Push Bombing
- Adversary-in-the-middle



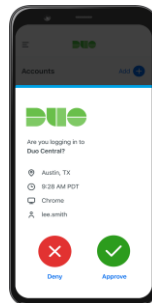
Next attack

- AI?
- Quantum Computing?



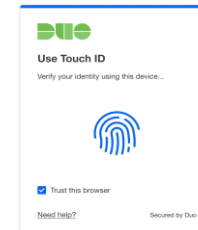
MFA 1.0

- SMS
- Phone Callback



MFA 2.0

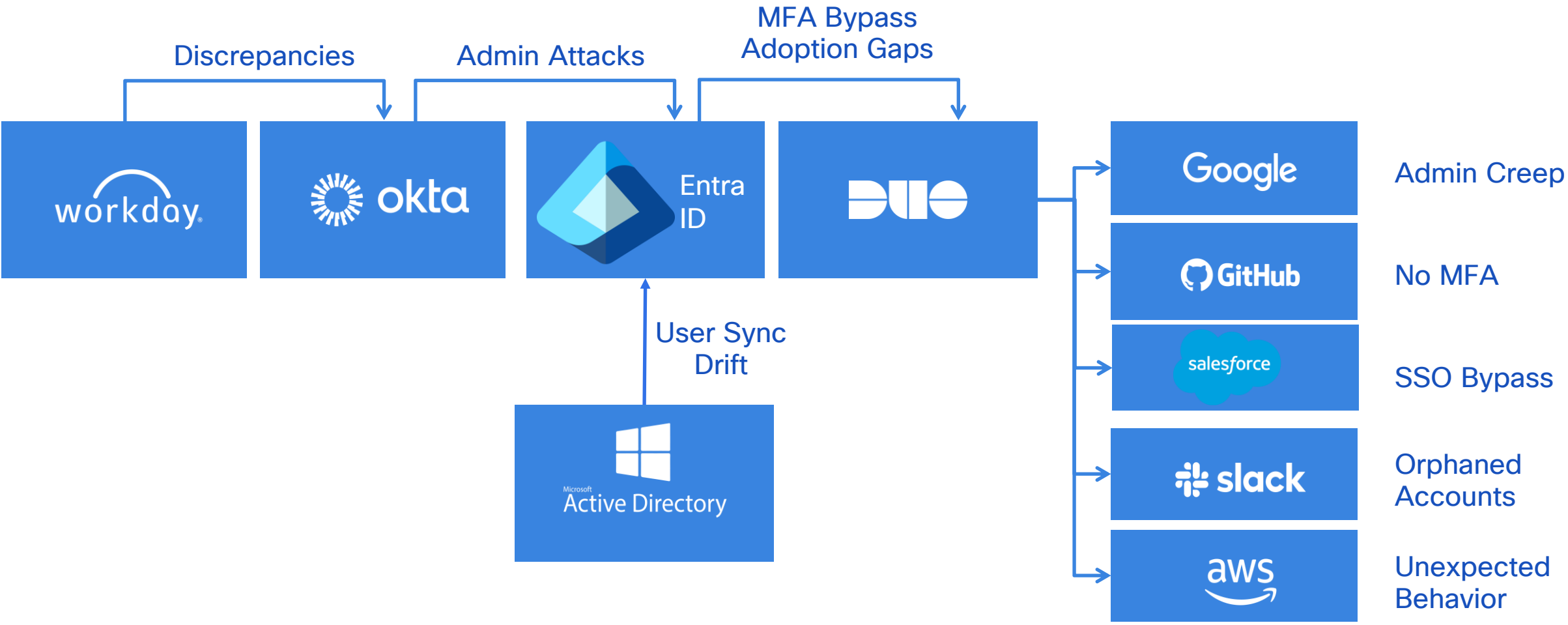
- Mobile
- Token

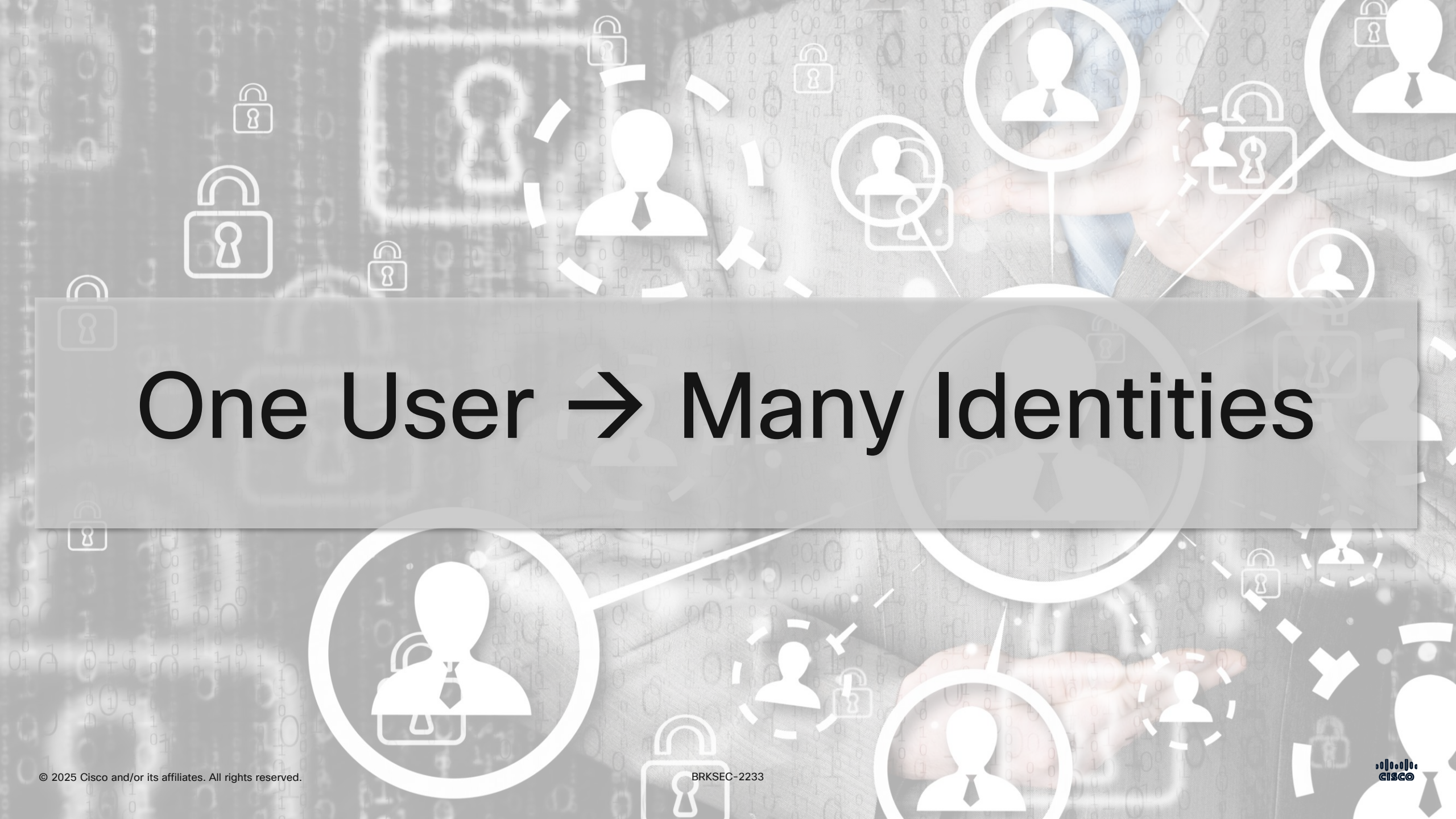


MFA 3.0

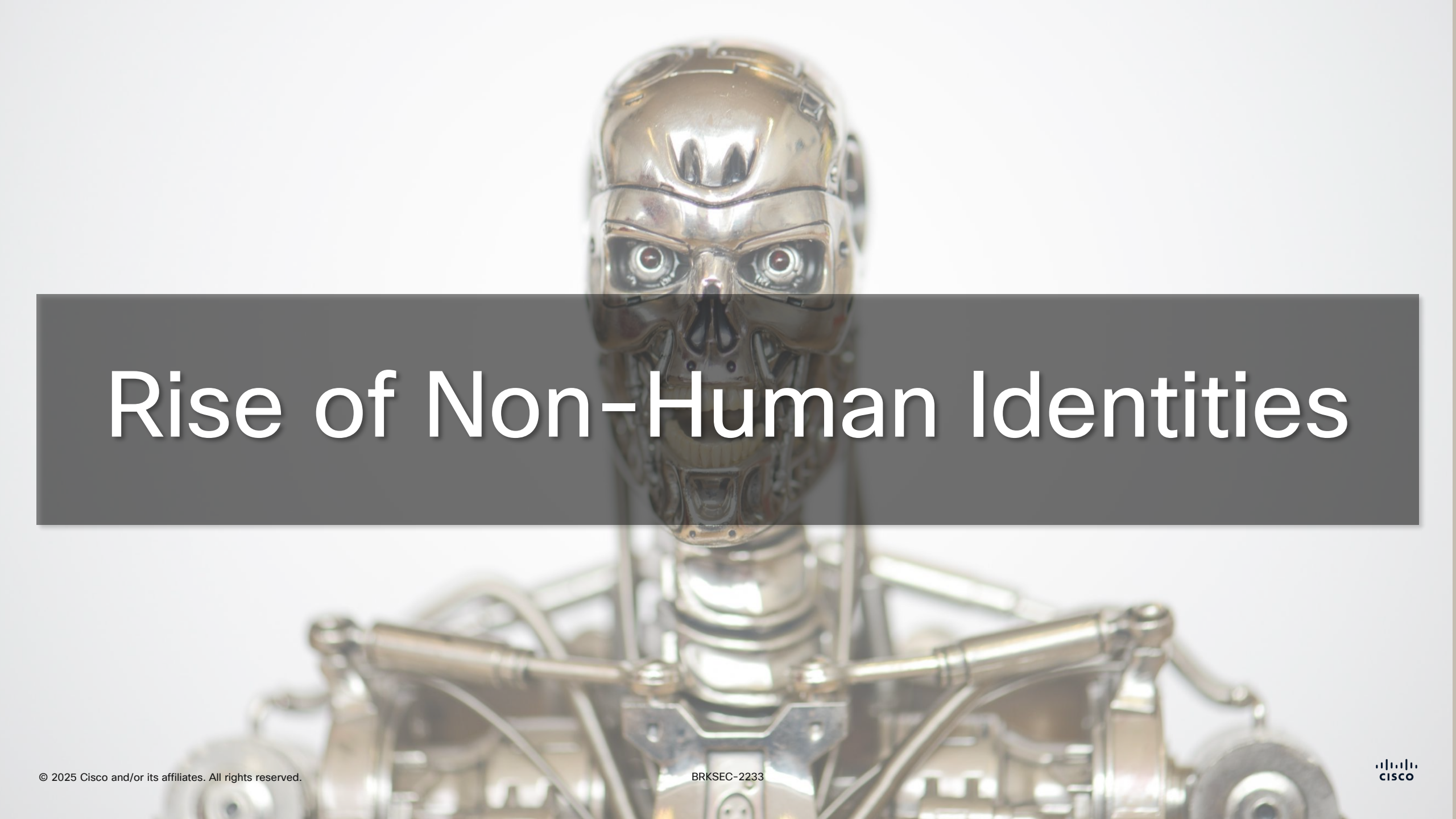
- WebAuthn
- Number Matching

Fragmented Visibility



The background of the slide is a grayscale image of a person's hands holding a transparent tablet. Overlaid on this are various white icons: several user silhouettes (some in circles, some with dashed outlines), and several padlocks (some open, some closed). A large, semi-transparent gray rectangle is centered horizontally, containing the main text.

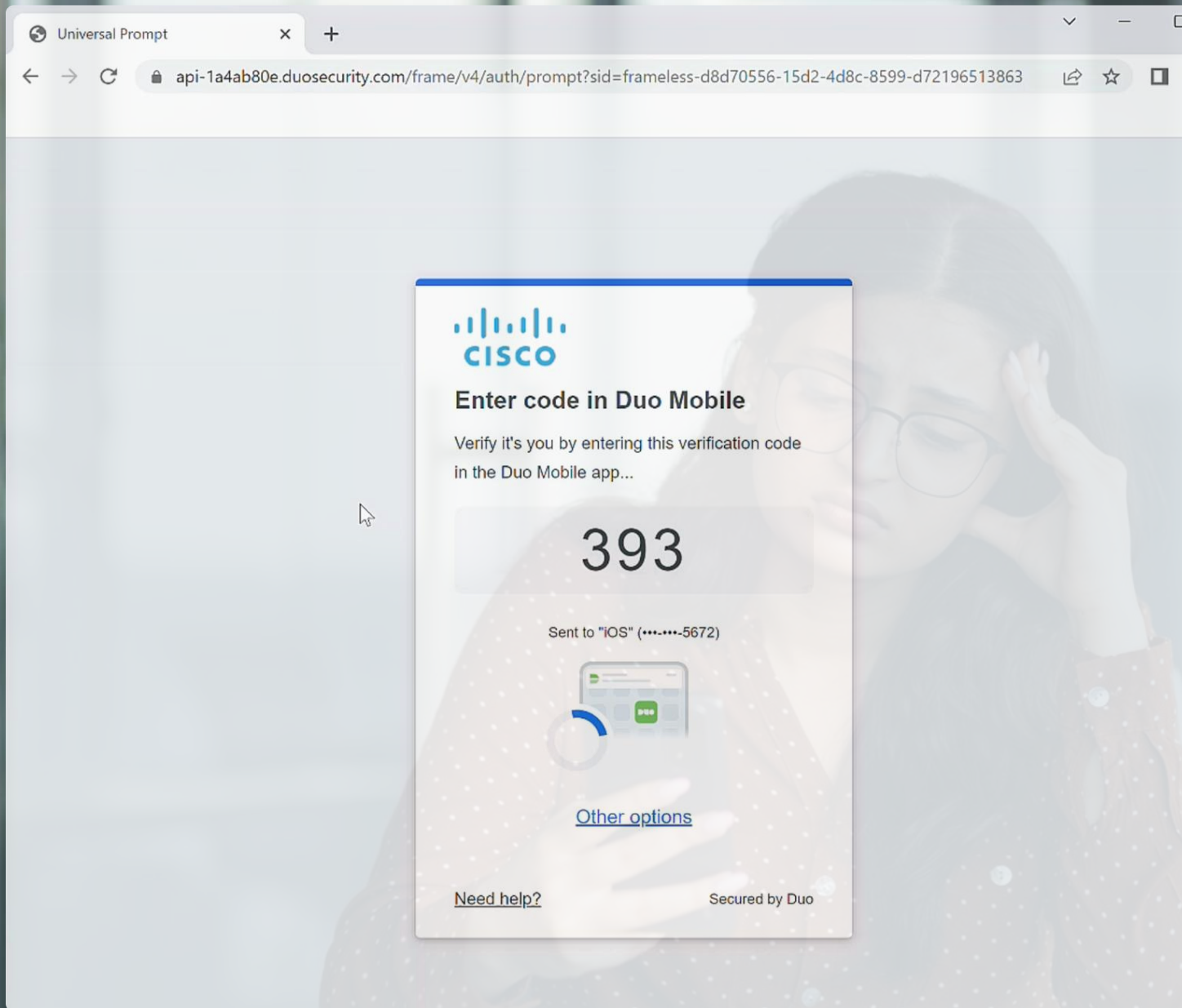
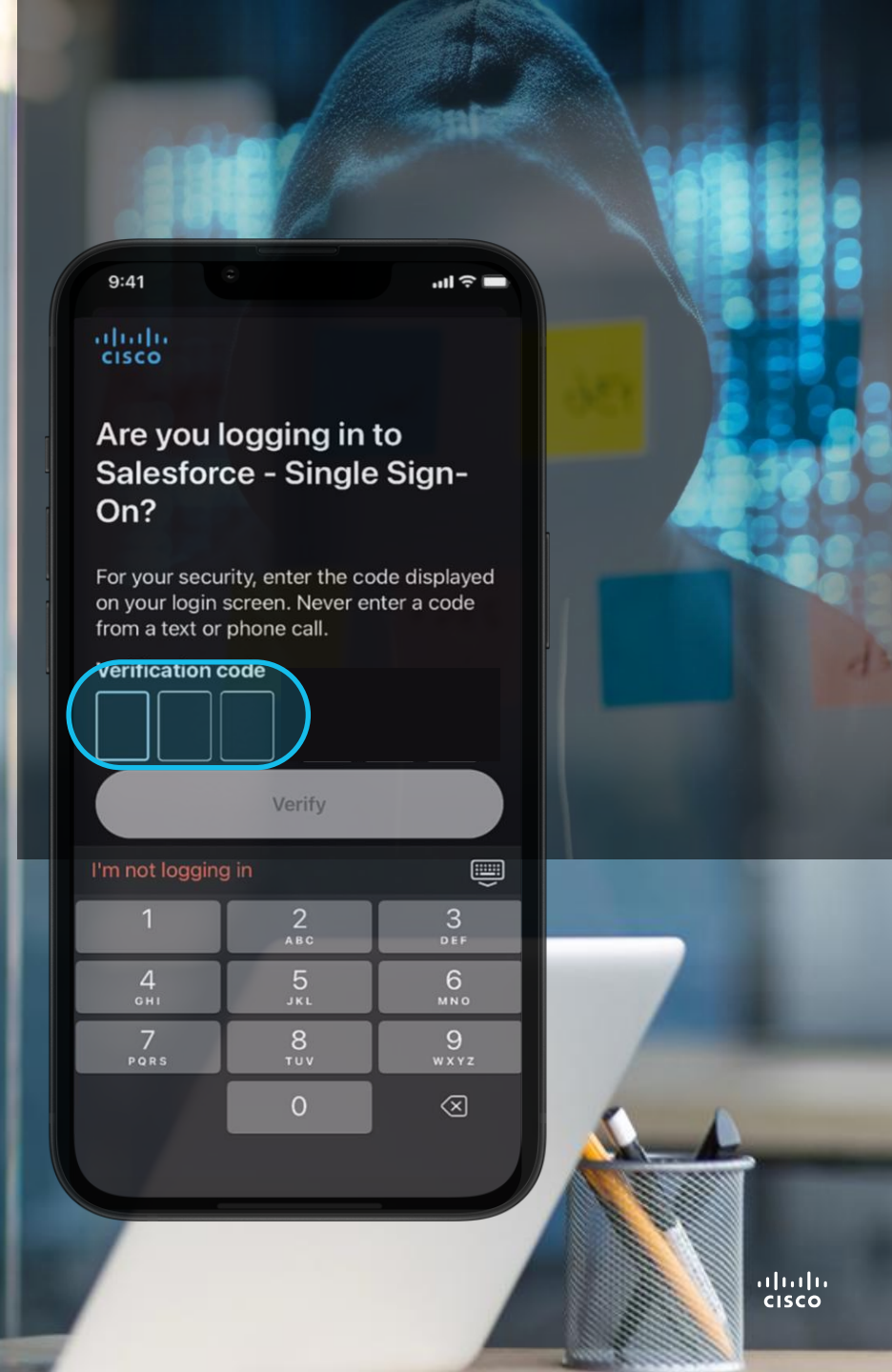
One User → Many Identities



Rise of Non-Human Identities

Phishing-resistant Authentication





Push Phishing Attack

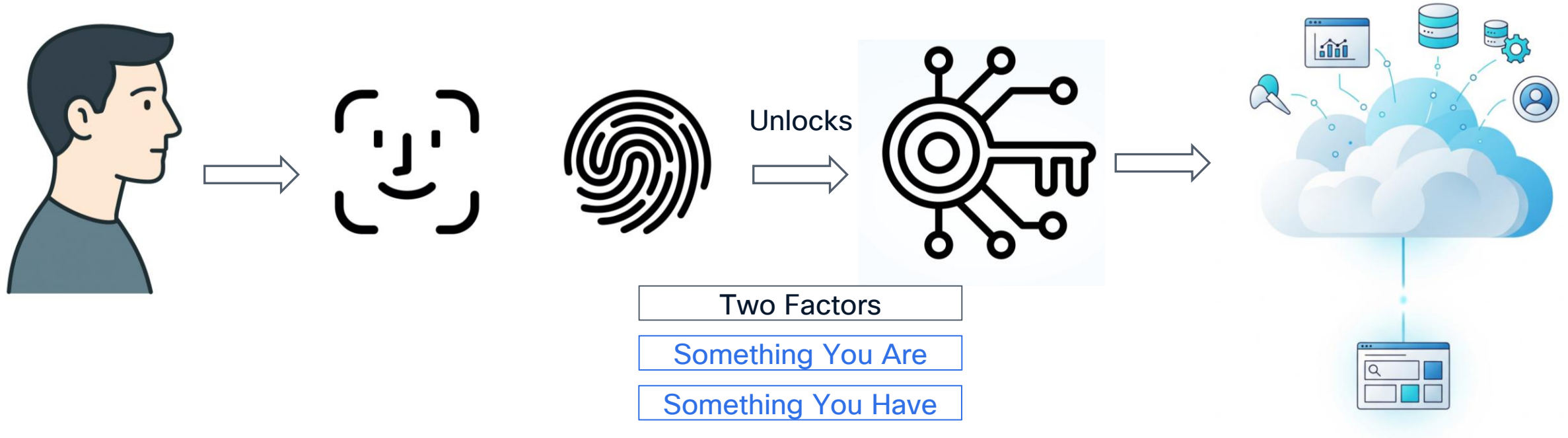


Adversary: *I'm calling from the IT department. We see suspicious activity in your work computer. Confirm your identity or lose access!*

User: *How can I verify my identity?*

Adversary: *I will send you a Push notification. Enter the code to verify.*

Passwordless Authentication



Passwordless Deployment



19%

Have fully implemented FIDO2

61%

want to move to passwordless
access, but **expect challenges**



Bluetooth Low Energy (BLE)

Proximity Verification



Are you logging into
Windows-X85735?

📍 Austin, TX

🕒 9:28 AM CDT

💻 Hostname goes here

👤 lee.smith

✅ You're nearby

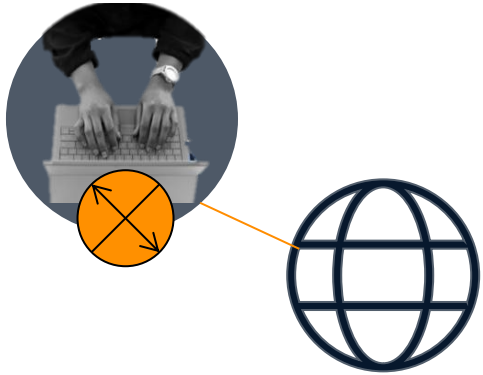


Deny

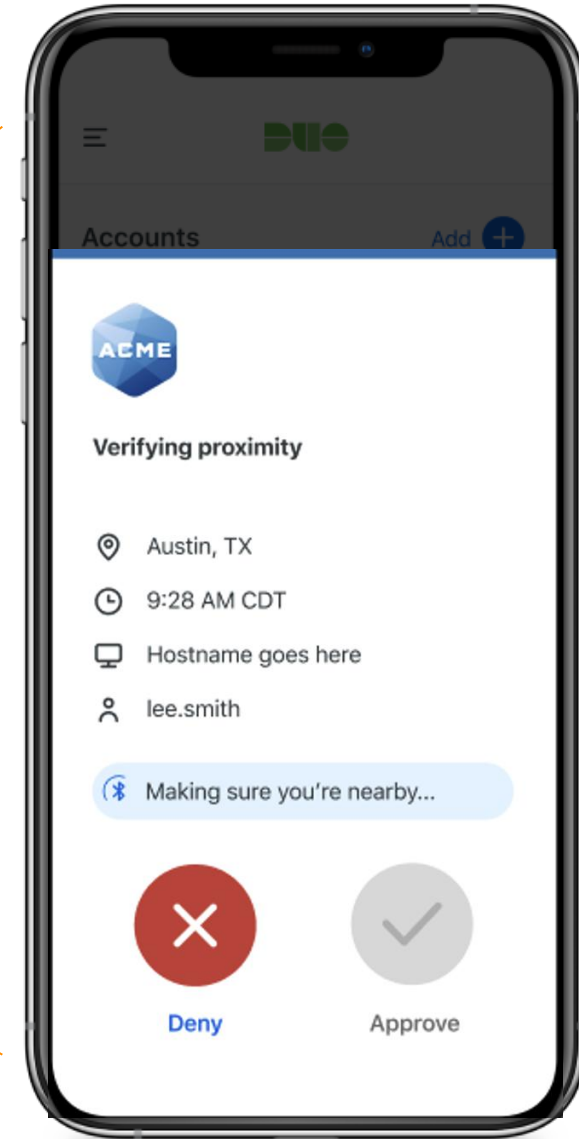


Approve

Proximity Verification



Nullifies remote MFA bypass techniques like push phishing and adversary-in-the-middle.



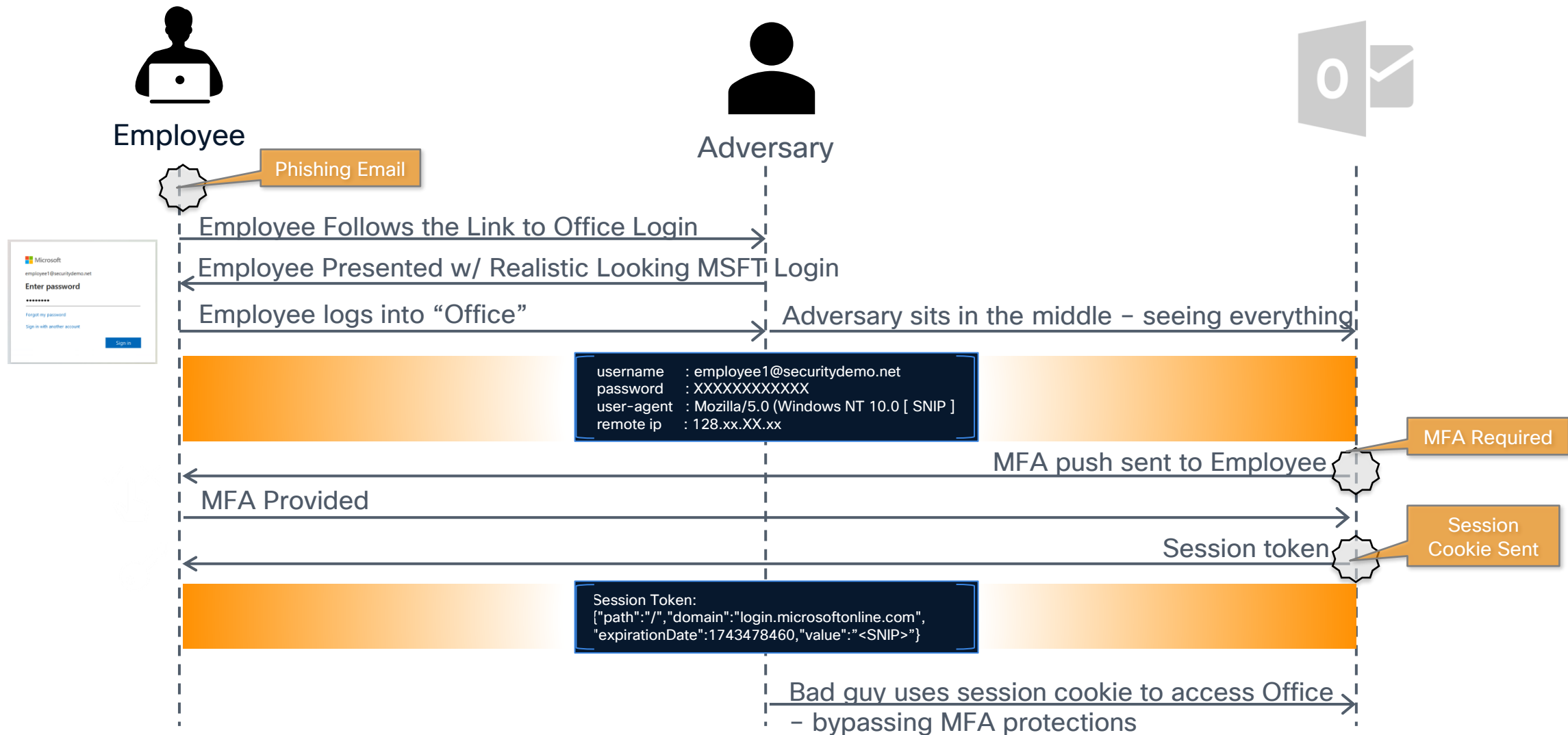
Phishing Resistant User Experience

Session Theft Protection

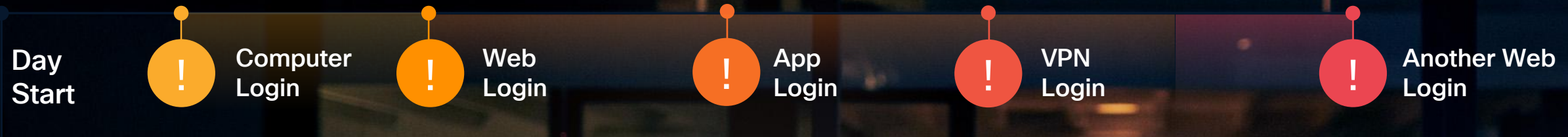
Eight different cookies are arranged in a circle around the word "COOKIES!". The cookies include: a dark chocolate chip cookie, a plain vanilla cookie, a white chocolate chip cookie, a brownie cookie, a chocolate chip cookie, a peanut butter cookie, a M&M's cookie, and a chocolate chip cookie with white chocolate chips. The word "COOKIES!" is written in a large, bold, black, sans-serif font in the center of the image.

COOKIES!

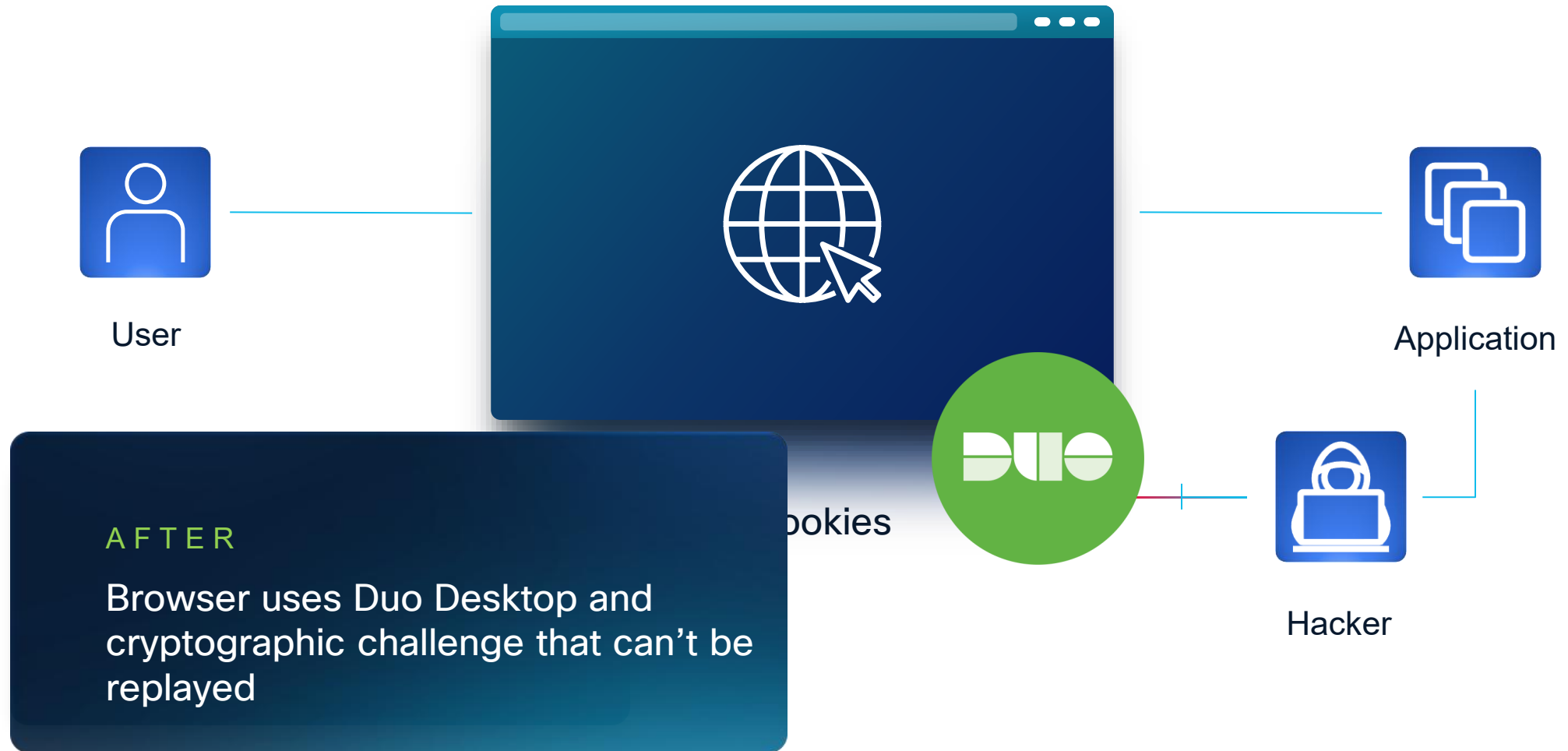
How to steal a Cookie*



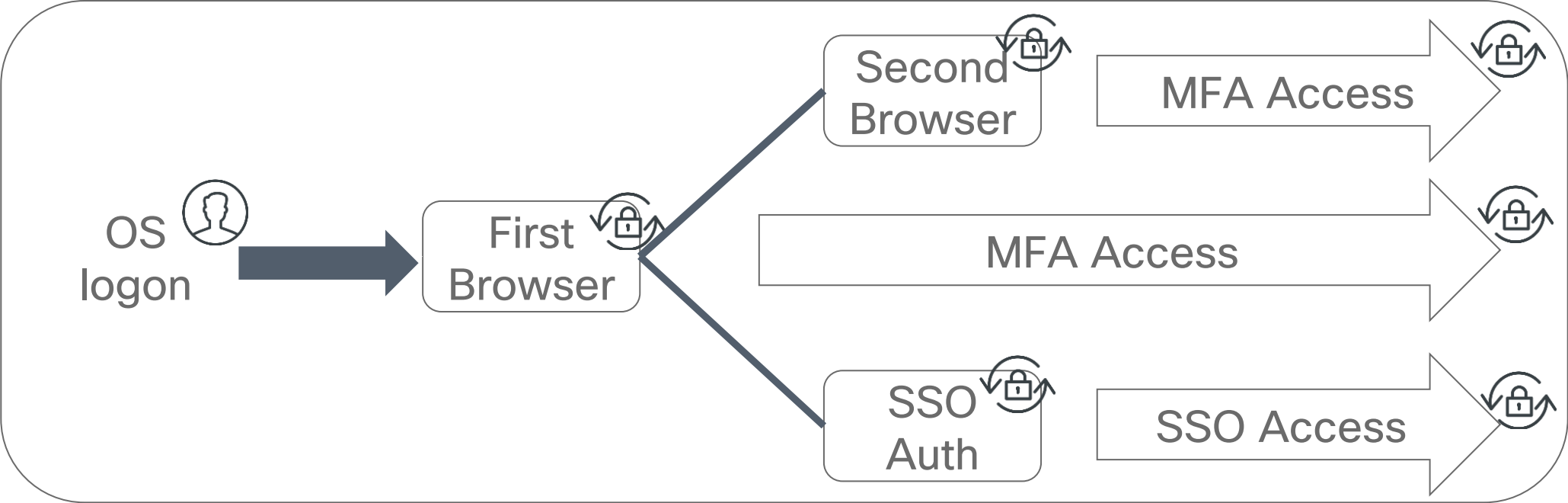
Users are frustrated



Session Theft Protection



Duo Passport

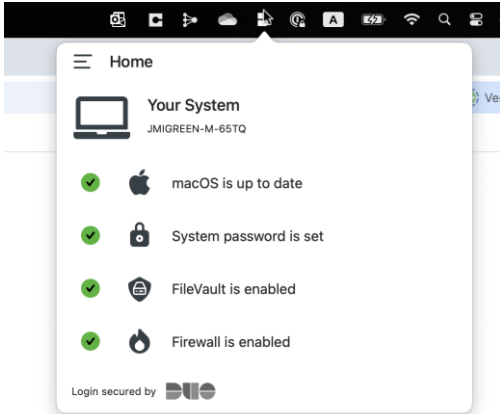
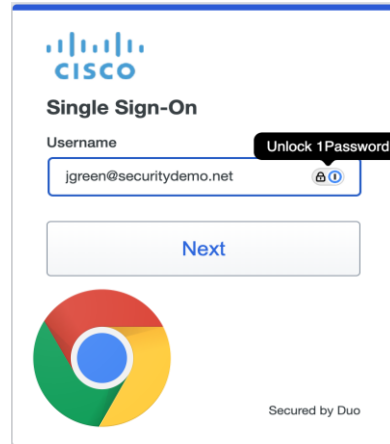
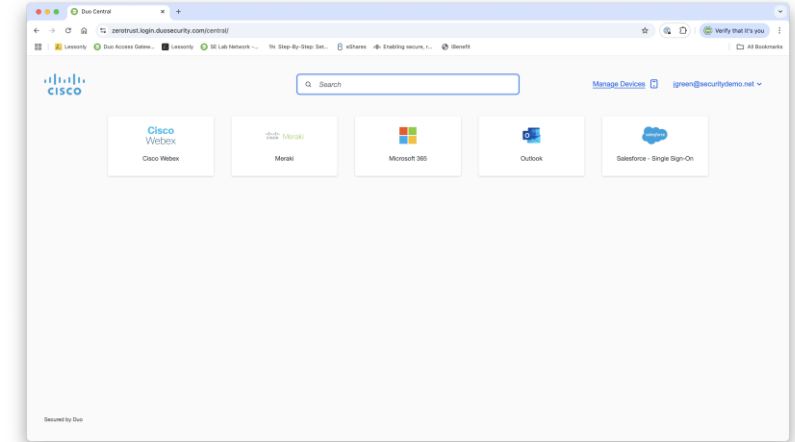


Granular Policy Coverage

Low Friction Authentication: Posture and Risk

	Interactive authentication - end user friction
	Authentication brokered through device, Duo, and Duo Desktop

Session Theft Protection with Duo Passport



Duo Desktop sends signed user and device profile to Duo Cloud

User accesses a Duo-protected application via any browser

Duo Desktop sends an updated profile to the cloud

User is logged in to the application

Duo Cloud records this profile.

Duo requests a fresh user & device profile from the device

Does the new profile match the original profile?

Duo issues a new session for the application

Duo Passport Configuration

☰ Collapse

🏠 Home

👤 Users >

💻 Devices >

🛡️ Policies

📄 Applications >

📊 Reports >

📈 Monitoring >

👤 Accounts >

📄 Billing >

⚙️ Settings

Policies

×

Policies

Policy Calculator

Self-Service Portal

Passport ✓

User Enrollment and Account Management

Session token theft protection.

←

Authentications, without sacrificing security

to extend the reach of your

our users can authenticate less

🖥️ OS Login

🌐 Browsers

📱 Apps

Without Passport	🔒	🔒	🔒
Passport	🔒	🔒➡️	
Passport with Windows Logon	🔒➡️		

Duo Passport Configuration

Required

Install Duo Desktop

Passport requires Duo Desktop to be installed on each device. Users with

Your current Duo Desktop Usage: ✖ Not Used

Percent of total users with Duo Desktop

7 of your users are not using Duo Desktop.

[Duo Desktop Installation Instructions](#)

 **Preferences**

Duo Desktop
Version 7.11.0.0
Updated on 3 Sep 2025
[Release notes](#)
[Privacy statement](#)
[Data FAQ](#)

☒ Automatically download and install updates
The app will automatically download and install updates in the background.

☒ Launch Duo Desktop automatically when I log in

☐ Enable detailed diagnostic reports

☒ Remember sessions in Duo Desktop

Duo Passport Configuration

All applications are Passport-ready

Enable remembered devices policy

Enable remembered devices policy for the applications you want to use with Passport. [Learn more](#)

Global policy Enabled

Devices

- ✓ Trusted Endpoints
- ✓ Duo Desktop & device health
- ✓ Remembered devices
- ✓ Operating systems
- ✓ Browsers
- ✓ Plugins

Remembered devices

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

☒ Remember devices for browser-based applications



Remember devices with risk-based protection for

8

hours

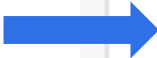


Duo Passport Configuration

Required

Select Passport users

Choose which users will have access to Duo Passport. You can enable Passport for all users at once, or restrict it to specific user groups for an incremental roll - out.

- ☒ Off for all users
-  ☐ On for certain groups

Turn on Passport for these groups only

No groups selected

- ☐ On for all users **Recommended**

Save

End User Experience True SSO with Duo Passport

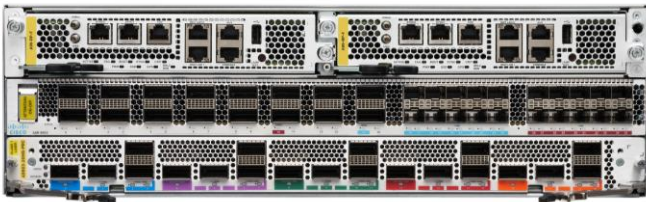
Protect your Infrastructure

Infrastructure under Attack!

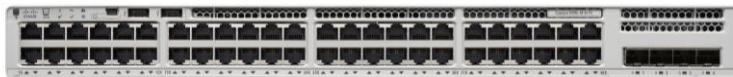
Cyber threat actors compromising networks of major global telecommunications providers



Salt Typhoon lateral movement and data collection

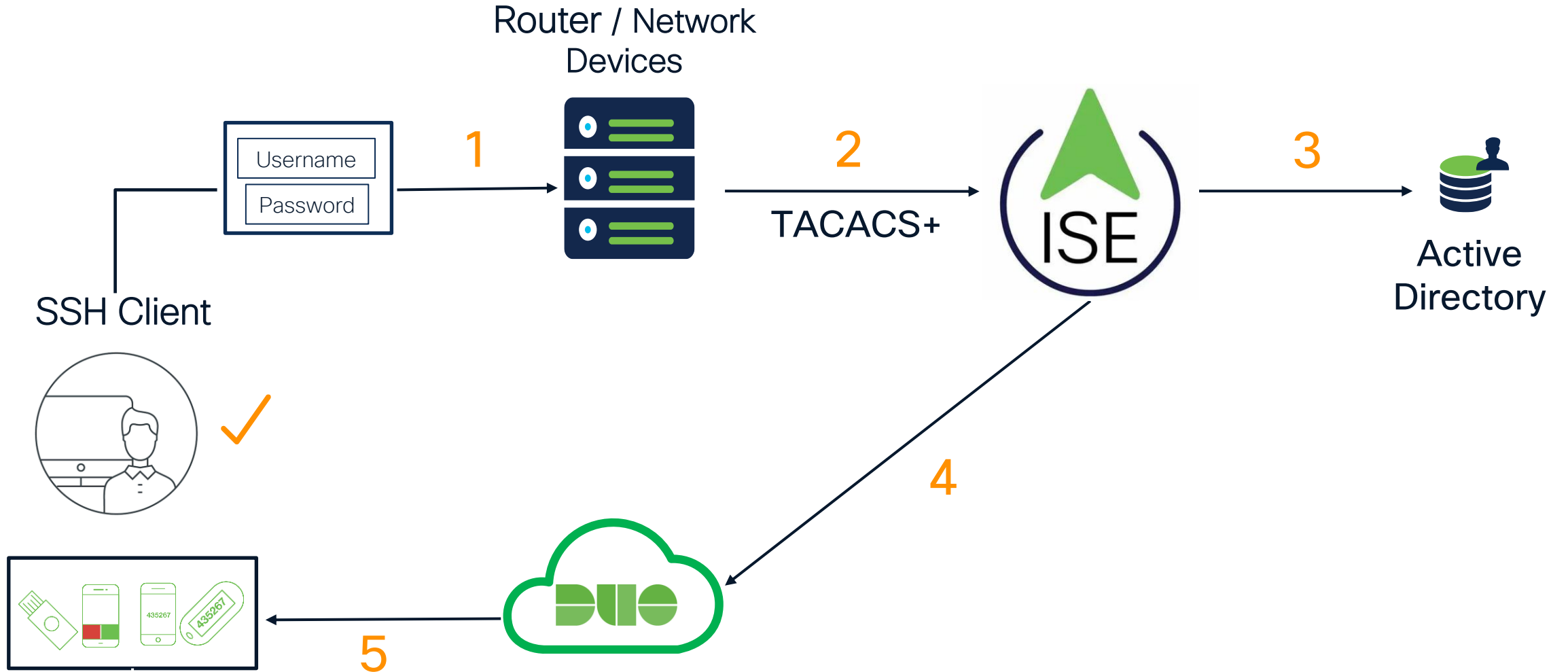


In order to move deeper inside networks, the attackers over leverage existing authentication protocols such as Terminal Access Controller Access Control System Plus (TACACS+) and Remote Authentication Dial-In User Service (RADIUS). The Managed Information Base (MIB), various router interfaces, Resource Reservation Protocol (RSVP) sessions, Border Gateway Protocol (BGP) routes and software already installed on the devices are also targeted for abuse.



The attackers also search configuration files and provider-held data such as subscriber information, customer records, network diagrams, device configurations, vendor lists, passwords and more.

Protect Device Login (Duo + ISE)



Collapse

Home

Users >

Devices >

Policies >

Applications >

Reports >

Monitoring >

Billing >

Settings

Home

Add new... ▾



Duo setup progress

Duo trial ends in 13 days



Get started with Duo



2/3 complete

In progress

Resume

Set up your administrators



0/1 complete

Not started

Start

Establish device trust



0/2 complete

Not started

Start

[View all journeys](#)

2 of 2 enrolled

100% enrollment

[View full deployment](#)

Users

[Add user](#)

2 total

Locked out

Bypassed BRKSEC-2233

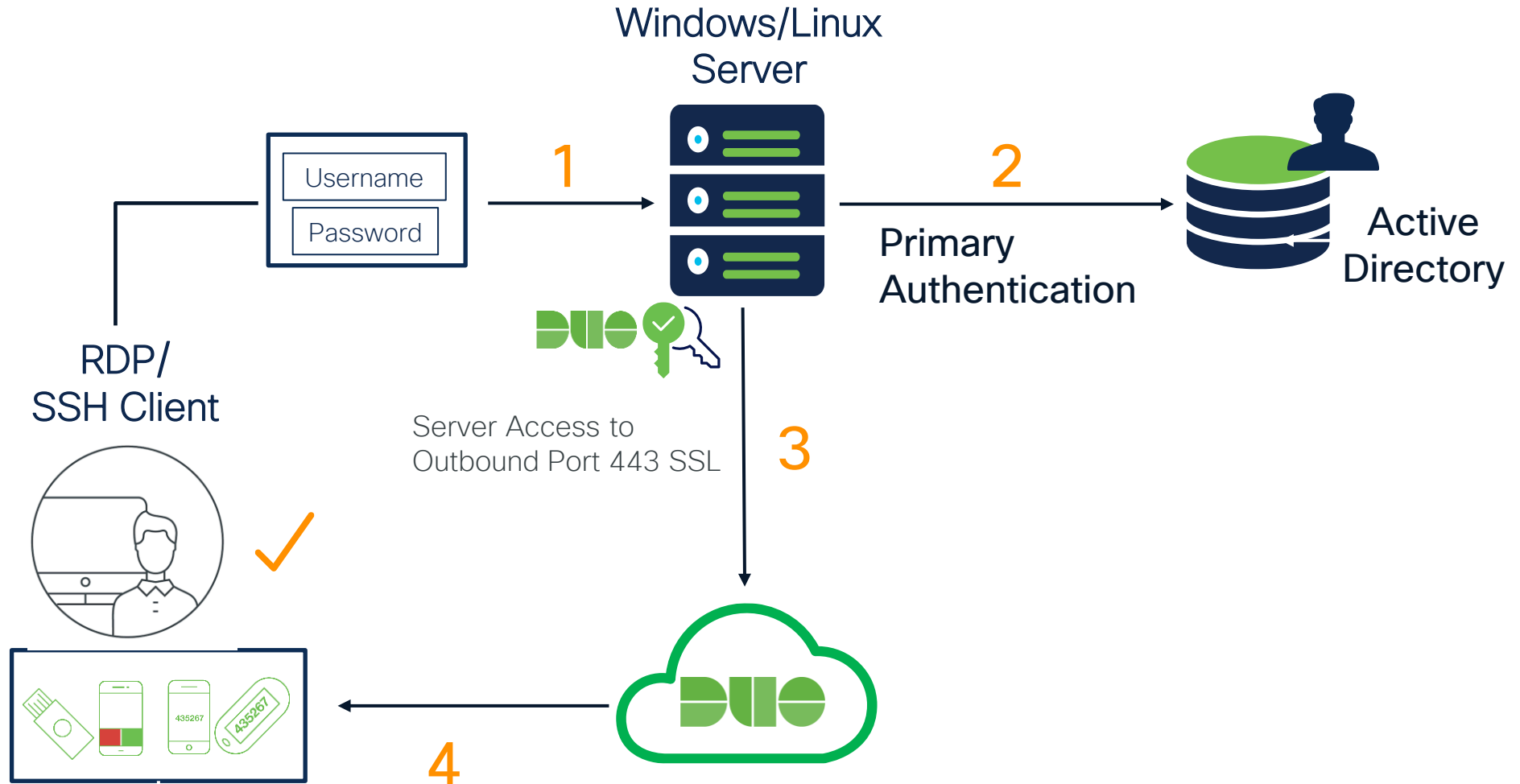
Devices

[View insights](#)

2 total

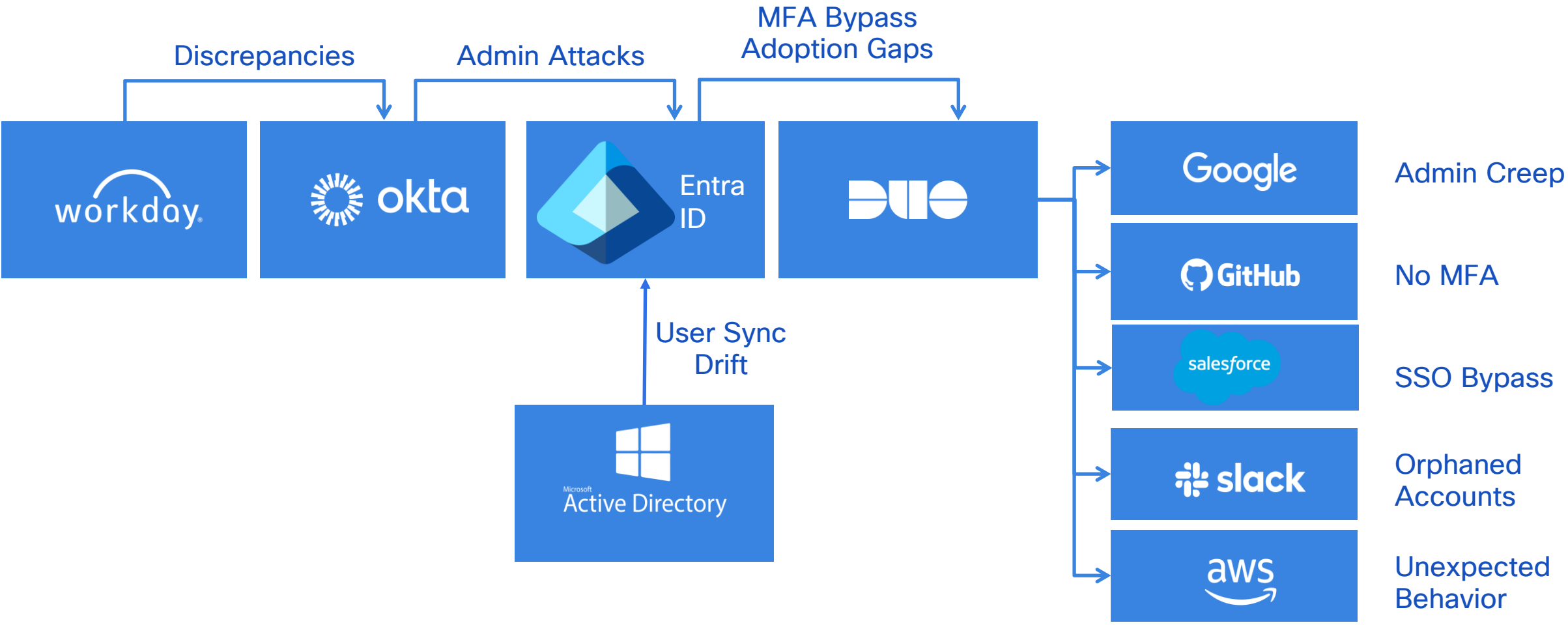
Out-of-date OS

Protect Server Login (RDP/SSH)

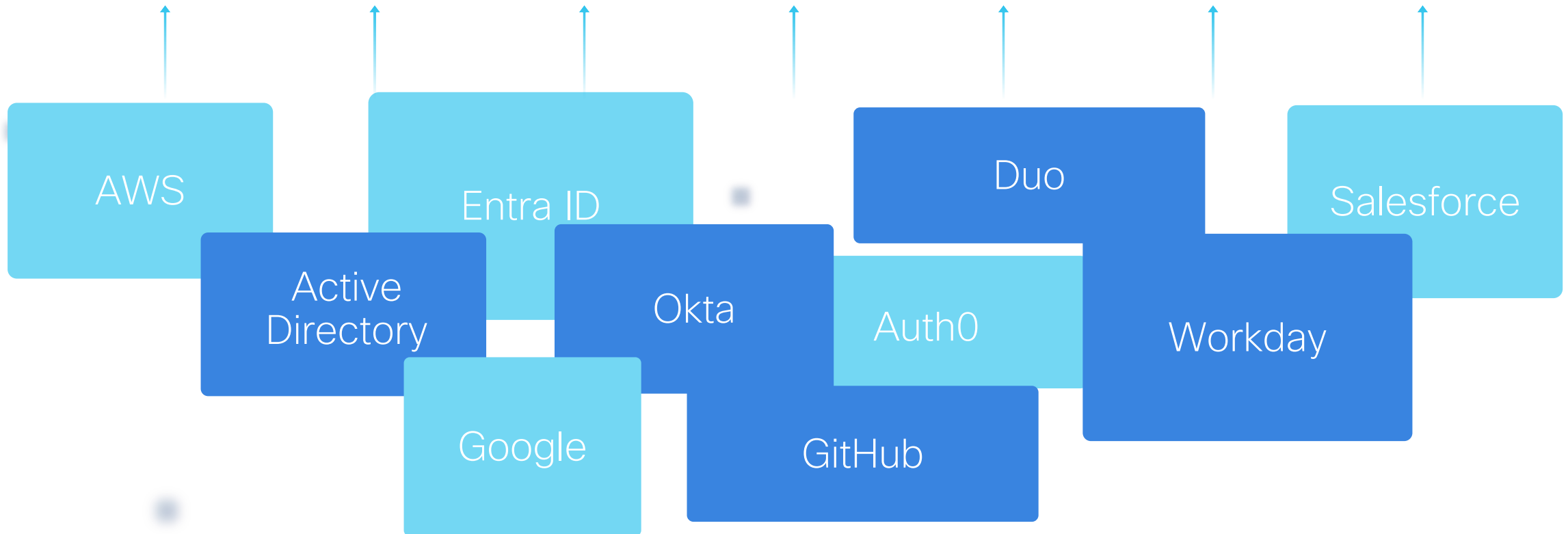


Identity Visibility

Fragmented Visibility



Identity Intelligence



Cisco Identity Intelligence



Unified User Visibility

Identity Intelligence

Search

skishan@cisco.c...
genie-api

Sources

All

Filter values...

☐

Demo Auth0

2

☐

Demo AWS

5

☐

Demo Azure AD

13

☐

Demo Azure Lab

47

☐

Demo Duo

9

☐

Demo GitHub

8

☐

Demo GSuite

8

☐

Demo Jamf

2

☐

Demo Okta

211

☐

Demo Salesforce

11

☐

Demo SCIM

1

☐

Demo Snowflake

2

☐

Demo Workday

6

☐

Slack - dummy-slack

2

☐

Users HRIS

2

301 users found

Columns

User ↓	Trust Level ↑	# Logins ↑	Last Seen (UTC) ↑	Last IP Address ↑	Last Location	MFA ↑
<div>Aalto Helmig </div> <div> aalto.helmig@simubiz.com</div>	Trusted	71	<div>A Day Ago</div> <div>Sep 15, 2025 22:00:05</div>	172.58.201.188	Tampa, FL, US	
<div>Aalto Helmig </div> <div> helmig@simubiz.com</div>	Neutral	10	<div>12 Hours Ago</div> <div>Sep 16, 2025 16:07:11</div>	209.6.171.113		
<div>Aalto Sekine </div> <div> aalto.sekine@simubiz.com</div>	Neutral	78	<div>A Day Ago</div> <div>Sep 15, 2025 18:15:29</div>	136.158.43.155	N/A	
<div>Adamchick Thome </div> <div> adamchick.thome@simubiz.com</div>	Unknown	N/A	<div>4 Years Ago</div> <div>Oct 8, 2021 11:48:56</div>	N/A	N/A	

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-2233

Unified User Visibility

Identity Intelligence

SourcesAll

Filter values...

☐

Demo Auth0

2

☐

Demo AWS

5

☐

Demo Azure AD

13

☐

Demo Azure Lab

47

☐

Demo Duo

9

☐

Demo GitHub

8

☐

Demo GSuite

8

☐

Demo Jamf

2

☐

Demo Okta

211

☐

Demo Salesforce

11

☐

Demo SCIM

1

☐

Demo Snowflake

2

☐

Demo Workday

6

☐

Slack - dummy-slack

2

☐

Users HRIS

2

301 users found

User

Aalto Helmig

Aalto Helmig

Aalto Sekine

Adamchick Thome

☐		Demo Auth0	2
☐		Demo AWS	5
☐		Demo Azure AD	13
☐		Demo Azure Lab	47
☐		Demo Duo	9
☐		Demo GitHub	8
☐		Demo GSuite	8
☐		Demo Jamf	2
☐		Demo Okta	211
☐		Demo Salesforce	11
☐		Demo SCIM	1
☐		Demo Snowflake	2
☐		Demo Workday	6

search

skishan@cisco.c...
genie-api

applications and IPs

Columns

TC) ↑

Last IP Address ↑

Last Location

MFA ↑

22:00:05

172.58.201.188

Tampa, FL, US

✓

go 16:07:11

209.6.171.113

✓

18:15:29

136.158.43.155

N/A

✓

1:48:56

N/A

N/A

✗

User 360

301 users found			Columns
User ↓	Trust Level ↑	# Logins ↑	Last Seen (UTC) ↑
<div>Clincy Bursi</div> <div>clincy.bursi@simubiz.com</div>	Neutral	3	<div>2 Days Ago</div> <div>Sep 15, 2025 12:54:42</div>
<div>Cramblit Mitra</div> <div>cramblit.mitra@simubiz.com</div>	Untrusted	37	<div>2 Days Ago</div> <div>Sep 15, 2025 06:05:25</div>
<div>Daled Arba</div> <div>arba.daled@simubiz.com</div>	Unknown	N/A	<div>18 Hours Ago</div> <div>Sep 16, 2025 10:16:27</div>

User 360

C

Cramblit

Mitra

cramblit.mitra@s

Kiev, UA

Active

Significant Change

Overview

Activity

Networks

Devices

More

Actions

Summary

Internal, Non Employee

lead engineer ii

order management

N/A

Kiev, UA

MFA Configured

Sep 15, 2025 06:05:25 UTC (2 days ago)

N/A

Trust Level

Last Updated: Sep 16, 2025 16:26:27 UTC

Untrusted

The level changed to Untrusted because of the following factors:

New priority account signed in from new country for tenant and IP with bad reputation

New priority account signed in from new country for tenant

New priority account signed in using weak MFA

Additional details

Failing Checks:

New Country for Tenant

IP Threat Detected

Weak MFA Was Used To Successfully Sign In

User 360

C

Cramblit
Mitra

cramblit.mitra@s

Kiev, UA

Active

Significant Change

Overview

Activity

Networks

Devices

More

Actions

Summary

Internal, Non Employee

lead engineer ii

order management

N/A

Kiev, UA

MFA Configured

Sep 15, 2025 06:05:25 UTC (2 days ago)

N/A

Trust Level ⓘ

Last Updated: Sep 16, 2025 16:26:27 UTC

Untrusted

The level changed to Untrusted because of the following factors:

New priority account signed in from new country for tenant and IP with bad reputation

New priority account signed in from new country for tenant

New priority account signed in using weak MFA

Additional details

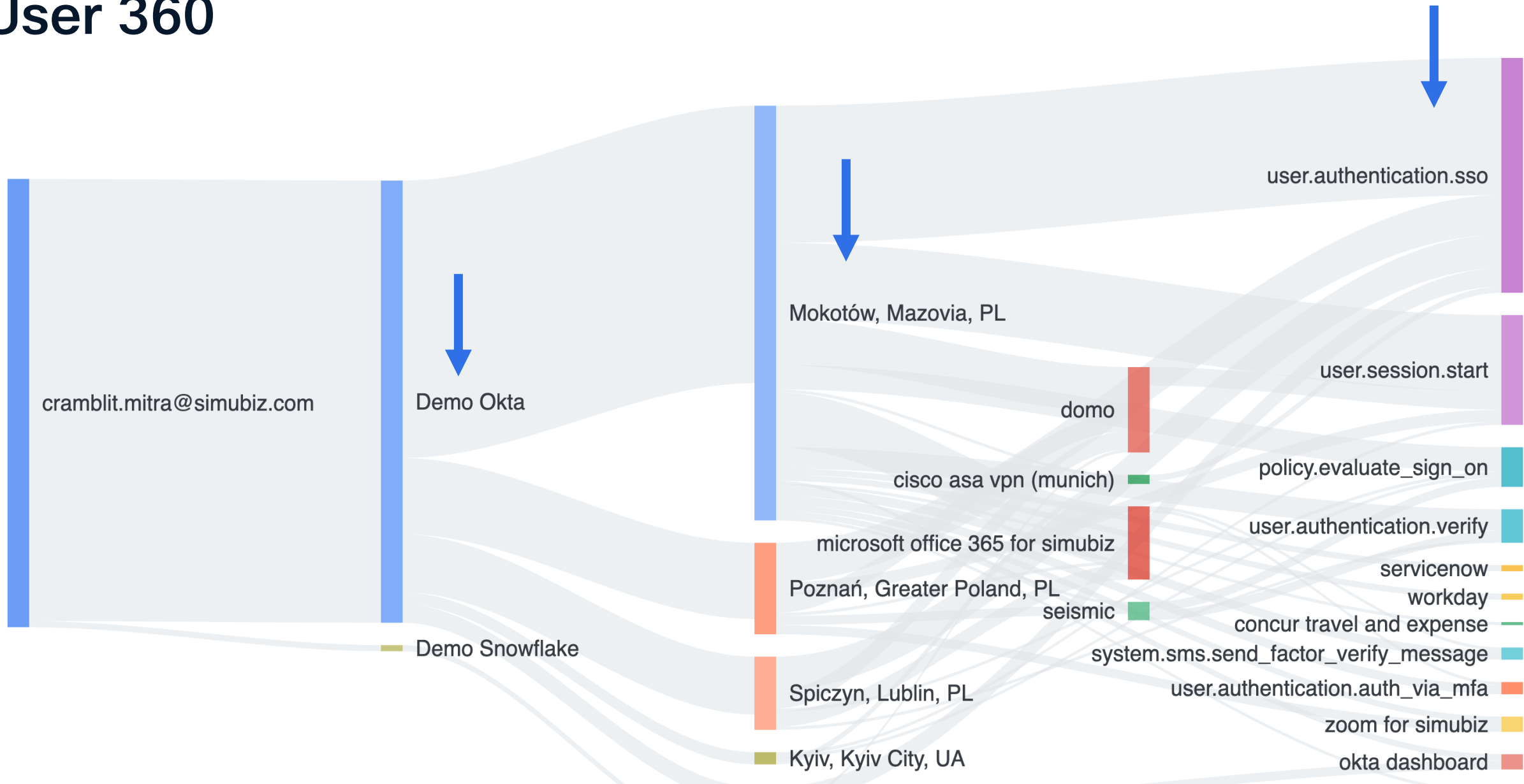
Failing Checks:

[New Country for Tenant](#)

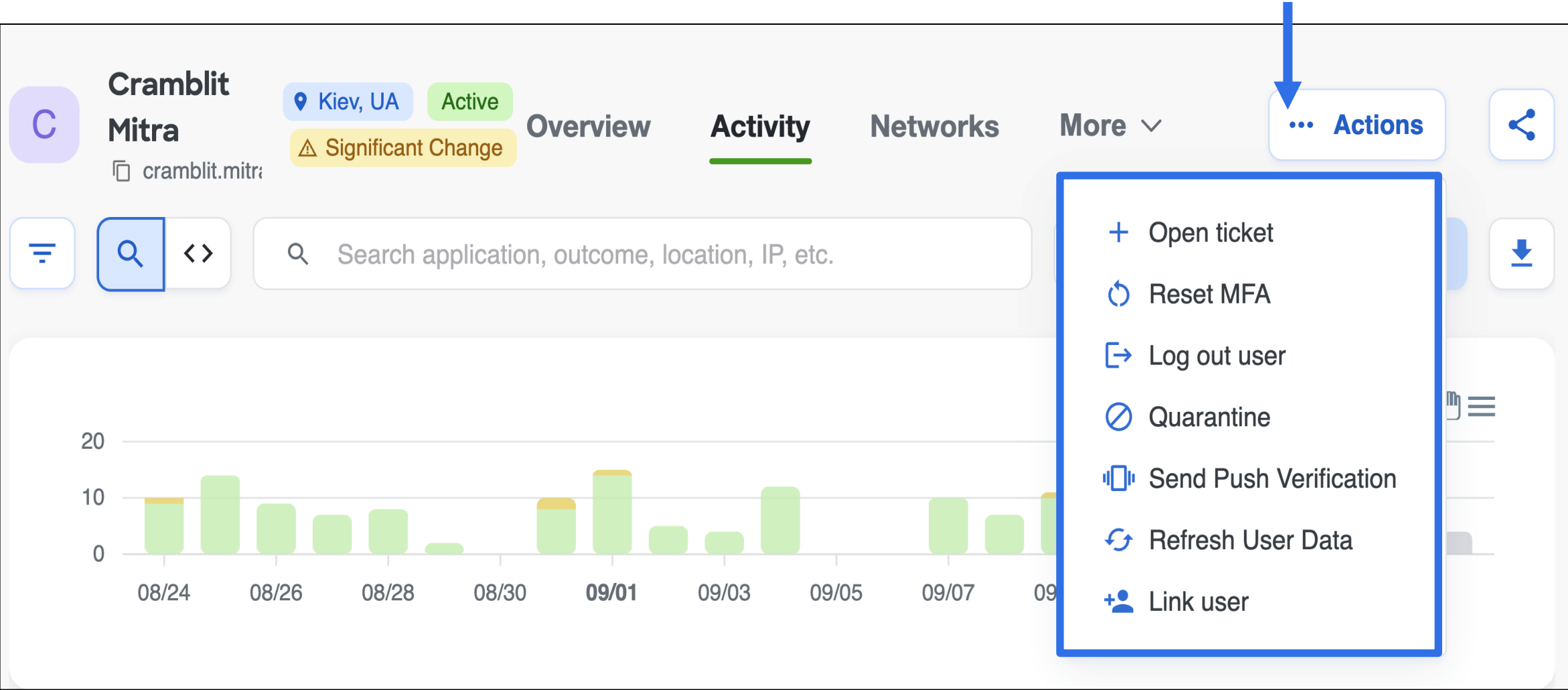
[IP Threat Detected](#)

[Weak MFA Was Used To Successfully Sign In](#)

User 360



User 360



Identity Security Posture Management (ISPM)

Topic:Identity Posture Insight X Search by title or description X

Request check

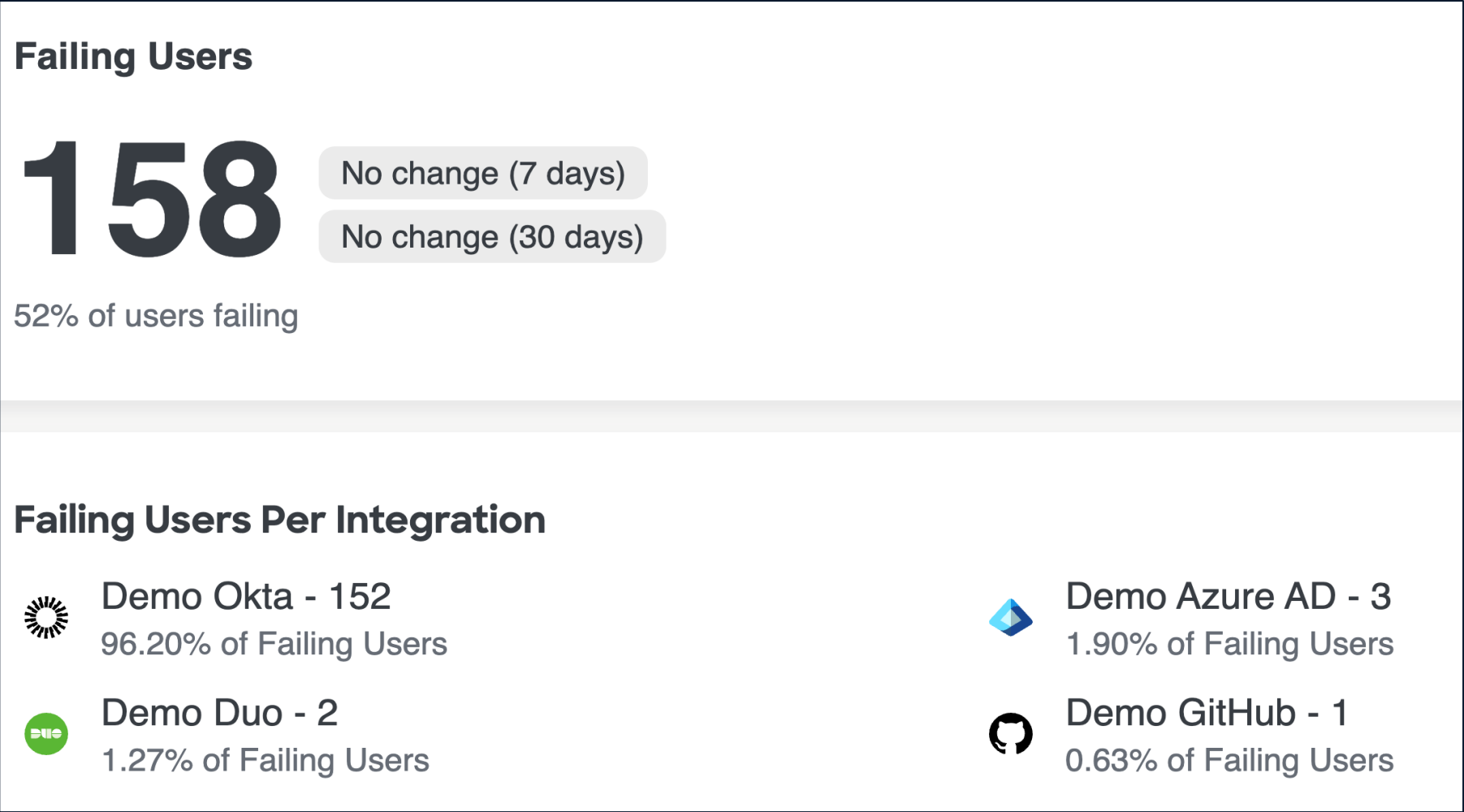
Run checks now

All Checks

Last run: Sep 16, 2025 1

Check	# Failing <div>i</div>	# Excluded	Report Channels
<div><div>47%</div><div>No MFA Configured <div></div></div><div><div>Critical</div>End Users - Compliance, Identity Posture Insight</div></div>	158 <div>→ No change since last week</div> <div>→ No change since last month</div>	0	<div>+ Add</div>
<div><div>81%</div><div>User in IDP but not in HRIS <div></div></div><div><div>Critical</div>End Users - Compliance, Identity Posture Insight</div></div>	57 <div>→ No change since last week</div> <div>→ No change since last month</div>	0	<div>+ Add</div>
<div><div>92%</div><div>Weak MFA Was Used To Successfully Sig... <div></div></div><div><div>Critical</div>End Users - Identity Posture Insight</div></div>	22 <div>→ No change since last week</div> <div>→ No change since last month</div>	0	<div>+ Add</div>
<div><div>93%</div><div>No Strong MFA Configured <div></div></div><div><div>Moderate</div>End Users - Compliance, Identity Posture Insight</div></div>	21 <div>→ No change since last week</div> <div>→ No change since last month</div>	0	<div>+ Add</div>

Identity Security Posture Management (ISPM)



Identity Security Posture Management (ISPM)

158 failing users		<div><div> View users</div><div> Download List</div></div>		
User	First Reported (UTC) ↑	Last Reported (UTC) ↑	User/ID	
staller.fohey@gmail.com 	Sep 16, 2025 16:18:35	Sep 16, 2025 16:26:22	Not n	 
simone.briggs@simubiz.com 	Sep 16, 2025 16:16:23	Sep 16, 2025 16:26:22	Not n	 
jonty.holman@simubiz.com 	Sep 16, 2025 16:15:25	Sep 16, 2025 16:26:22	Not n	 

Identity Security Posture Management (ISPM)

158 failing users

View users

Download List

User	First Reported (UTC) ↑	Last Reported (UTC) ↑	User/ID
staller.fohey@gmail.com	Sep 16, 2025 16:18:35	Sep	
simone.briggs@simubiz.com	Sep 16, 2025 16:16:23	Sep	
jonty.holman@simubiz.com	Sep 16, 2025 16:15:25	Sep 16, 2025 16:26:22	Not n

Send notification

View logs

Exclude from check

Identity Security Posture Management (ISPM)

Topic:Identity Posture Insight X Search by title or description X

Request check

Run checks now

All Checks

Last run: Sep 16, 2025 1

Check

47%

No MFA Configured

Critical

End Users - Compliance, Identity Posture

81%

User in IDP but not in HRIS

Critical

End Users - Compliance, Identity Posture

92%

Weak MFA Was Used To Successfully Si

Critical

End Users - Identity Posture Insight

93%

No Strong MFA Configured

Moderate

End Users - Compliance, Identity Posture Insight

21

No change since last week

No change since last month

0

+ Add

User in IDP but not in HRIS

Critical

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.

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-2233

CISCO

Identity Security Posture Management (ISPM)

altgilbers.yagi@simubiz.com

adamchick.thome@simubiz.com

aalto.sekine@simubiz.com

A

Adamchick Thome

adamchick.thome@:

Dublin 24, Dublin...
Inactive

Overview

Summary

Internal, Non Employee

import/export specialist

order management

N/A

Dublin 24, Dublin, IE

MFA Missing

Oct 8, 2021 11:48:56 UTC (4 years ago)

Identity Security Posture Management (ISPM)

All Checks			
Check		# Failing	
	 Critical End Users - Compliance, Identity Posture Insight		
	User Has Directly Assigned Application   Low End Users - Compliance, Identity Posture Insight	3	 No change since last week  No change since last month
	Never Logged In    Critical End Users - Compliance, Identity Posture Insight	3	 No change since last week  No change since last month
	Non-Human Identity Password Expiration Failure   Moderate End Users - Identity Posture Insight, Non-Human Identities	3	 No change since last week  No change since last month
	Personal VPN Usage   Low End Users - Compliance, Identity Posture Insight	3	 No change since last week  No change since last month

Identity Security Posture Management (ISPM)

All Checks

Check

99%

Critical

User Has Directly Assigned Application

Low

End Users - Compliance, Identity Posture Insight

99%

Critical

Never Logged In

End Users - Compliance, Identity Posture Insight

99%

Moderate

Non-Human Identity Password Expiration Failure

End Users - Identity Posture Insight, Non-Human Identities

99%

Low

Personal VPN Usage

End Users - Compliance, Identity Posture Insight

P

Pantomima Visholdo

panto.visho@simubiz.com

Inactive

Summary

External, Non Employee

N/A

N/A

Simubiz

N/A

MFA Missing

N/A

N/A

Created Aug 27, 2018

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-2233

Identity Threat Detection and Response (ITDR)

All Checks			
Check		# Failing ⓘ	# Excluded
 Critical End Users - Identity Threat Insight			
 Moderate Access From Dormant Non-Human Identity ⓘ End Users - Compliance, Identity Threat Insight, Non-Human Ide...		5 → No change since last week → No change since last month	0
 Moderate Impossible Travel ⓘ  End Users - Identity Threat Insight		5 → No change since last week → No change since last month	0
 Critical A Bypass Code Was Used To Successfully Sign In ⓘ End Users - Identity Threat Insight		5 → No change since last week → No change since last month	0
 Moderate Access From Dormant Account ⓘ End Users - Compliance, Identity Threat Insight		4 → No change since last week → No change since last month	0

Identity Threat Detection and Response (ITDR)

All Checks				
Check		# Failing ⓘ		# Excluded
 Critical End Users - Identity Threat Insight				
 Access From Dormant Non-Human Identity ⓘ • Moderate End Users - Compliance, Identity Threat Insight, Non-Human Ide...		5 → No change since last week → No change since last month		0
 Impossible Travel ⓘ • Moderate End Users - Identity Threat Insight		5 → No change since last week → No change since last month		0
 A Bypass Code Was Used To Successfully Sign In ⓘ • Critical End Users - Identity Threat Insight		5 → No change since last week → No change since last month		0
 Access From Dormant Account ⓘ 		4 → No change since last week → No change since last month		0

Identity Threat Detection and Response (ITDR)

All Checks			
Check		# Failing ⓘ	# Excluded
<div><div>99%</div><div>Accounts With Unusually High Activity </div><div><div>Critical</div>End Users - Identity Threat Insight</div></div>		1 → No change since last week → No change since last month	0
<div><div>99%</div><div>New IDP Created </div><div><div>Critical</div>End Users - Identity Threat Insight</div></div>		1 → No change since last week → No change since last month	0
<div><div>99%</div><div>MFA Flood </div><div><div>Critical</div>End Users - Identity Threat Insight</div></div>		1 → No change since last week → No change since last month	0
<div><div>99%</div><div>Admin Impersonation in Okta </div><div><div>Critical</div>End Users - Compliance, Identity Threat Insight</div></div>		1 → No change since last week → No change since last month	0
<div><div>99%</div><div>Risky Parallel Sessions </div><div><div>Critical</div>End Users - Compliance, Identity Threat Insight</div></div>		1 → No change since last week → No change since last month	0

Identity Threat Detection and Response (ITDR)

All Checks			
Check		# Failing ⓘ	# Excluded
<div><div>99%</div><div>Accounts With Unusually High Activity ⓘ</div><div><div>Critical</div>End Users - Identity Threat Insight</div></div>	1	<div>→ No change since last week</div> <div>→ No change since last month</div>	0
<div><div>99%</div><div>New IDP Created ⓘ</div><div><div>Critical</div>End Users - Identity Threat Insight</div></div>	1	<div>→ No change since last week</div> <div>→ No change since last month</div>	0
<div><div>99%</div><div>MFA Flood ⓘ</div><div><div>Critical</div>End Users - Identity Threat Insight</div></div>	1	<div>→ No change since last week</div> <div>→ No change since last month</div>	0
<div><div>99%</div><div>Admin Impersonation in Okta ⓘ</div><div><div>Critical</div>End Users - Compliance, Identity Threat Insight</div></div>	1	<div>→ No change since last week</div> <div>→ No change since last month</div>	0
<div><div>99%</div><div>Risky Parallel Sessions ⓘ</div><div><div>Critical</div>End Users - Compliance, Identity Threat Insight</div></div>	1	<div>→ No change since last week</div> <div>→ No change since last month</div>	0

Identity Threat Detection and Response (ITDR)

• Critical

New Country for Tenant

• Moderate

Registered Location Mismatch

• Low

Risky Parallel Sessions

• Critical

User in IDP but not in HRIS

• Critical

IP Details

171.76.86.89

203.192.253.117

Providers failing check

Demo Okta

externalSession...

102cmxH11JUSdW1J8sZ_9PPBB

102z0f8ZaV8QR66X2M3_drYBB

User Title

senior site reliability engineer

User Trust Level

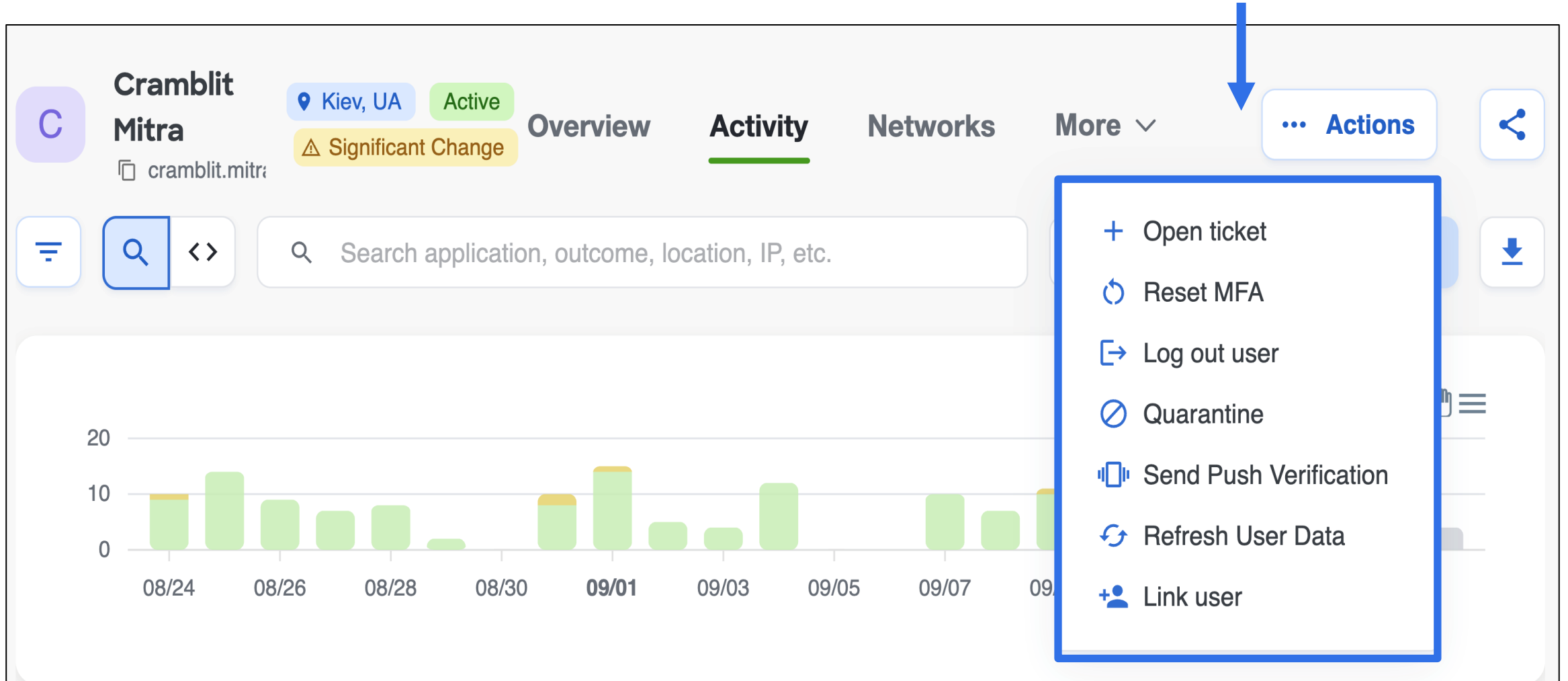
NEUTRAL

Devices

0: "Windows 10|IE11"

1: "Windows 8|IE11"

Identity Threat Detection and Response (ITDR)



Identity Threat Detection and Response (ITDR)

Notification Targets

After you connect a notification target, you can configure notification settings on checks to receive alerts about failing users.



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](#)



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](#)

Identity Threat Detection and Response (ITDR)

Ticketing

Identity Intelligence integrates with ticketing services to open new tickets and display 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](#)

SIEM



Azure Sentinel

Azure Sentinel is a scalable, cloud-native solution that provides SIEM and SOAR capabilities.

[+ Add Azure Sentinel](#)

splunk> **Splunk**

Integrate Splunk with Cisco Identity Intelligence to transmit check failures information to your Splunk instance, strengthening your security operations.

[+ Add Splunk](#)

Non-Human Identities

	Access From Dormant Non-Human Identity  Moderate End Users - Compliance, Identity Threat Insight, Non-Human Identities	5	→ No change since last week → No change since last month
	Non-Human Identity Password Expiration Failure  Moderate End Users - Identity Posture Insight, Non-Human Identities	3	→ No change since last week → No change since last month
	Admin Role Assigned to Non-Human Identity  Moderate End Users - Compliance, Identity Threat Insight, Non-Human Identities	1	→ No change since last week → No change since last month
	Service Principal Risk Detected  Moderate Application - Identity Threat Insight, Non-Human Identities	1	→ No change since last week → No change since last month
	Non-Human Identity with Interactive Browser Access  Moderate End Users - Compliance, Identity Threat Insight, Non-Human Identities	0	→ No change since last week → No change since last month



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!!!

User 360

C

Cramblit
Mitra

cramblit.mitra@s

Kiev, UA

Active

Significant Change

Overview

Activity

Networks

Devices

More

Actions

Summary

Internal, Non Employee

lead engineer ii

order management

N/A

Kiev, UA

MFA Configured

Sep 15, 2025 06:05:25 UTC (2 days ago)

N/A

Trust Level ⓘ

Last Updated: Sep 16, 2025 16:26:27 UTC

Untrusted

The level changed to Untrusted because of the following factors:

New priority account signed in from new country for tenant and IP with bad reputation

New priority account signed in from new country for tenant

New priority account signed in using weak MFA

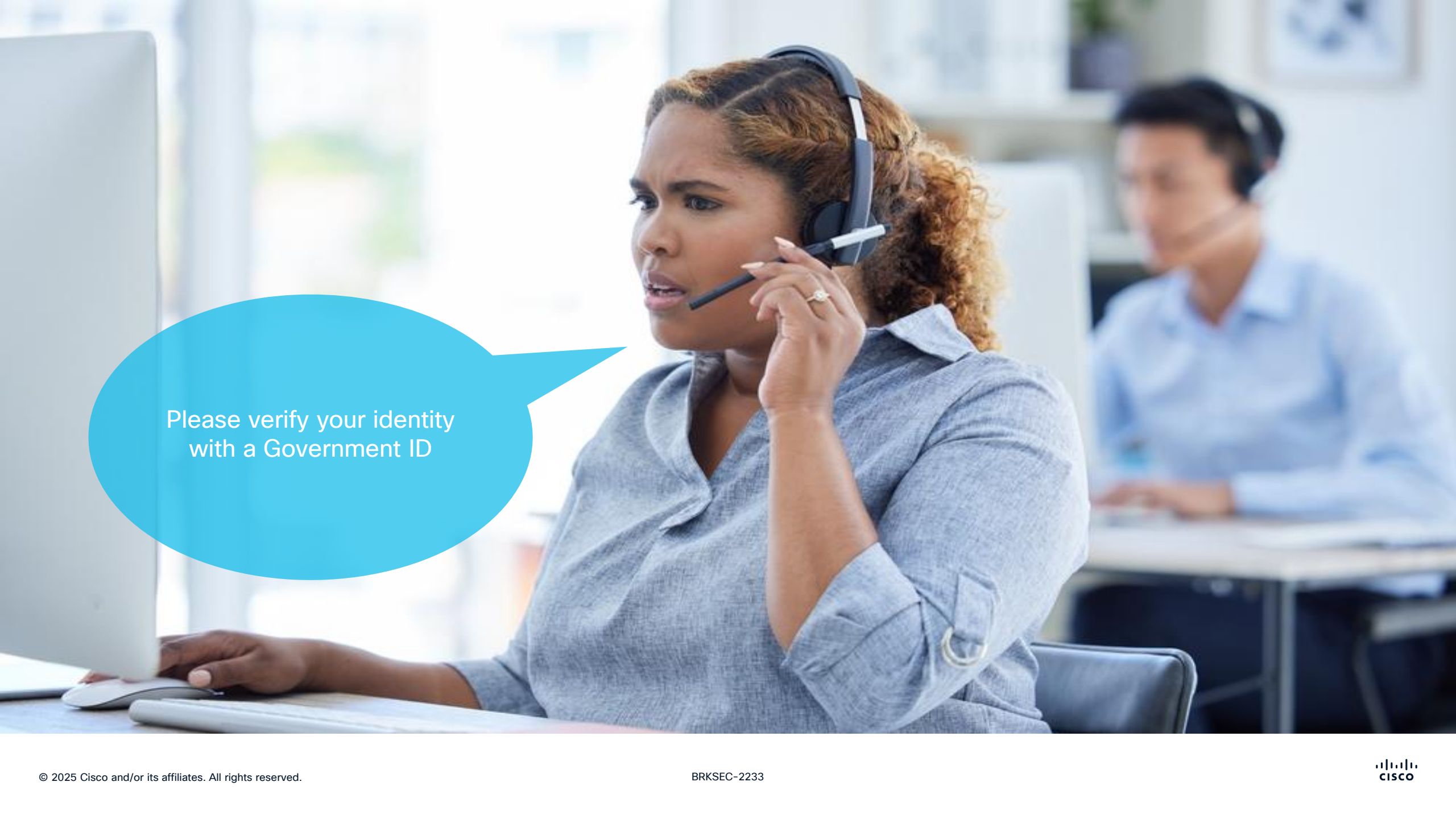
Additional details

Failing Checks:

[New Country for Tenant](#)

[IP Threat Detected](#)

[Weak MFA Was Used To Successfully Sign In](#)



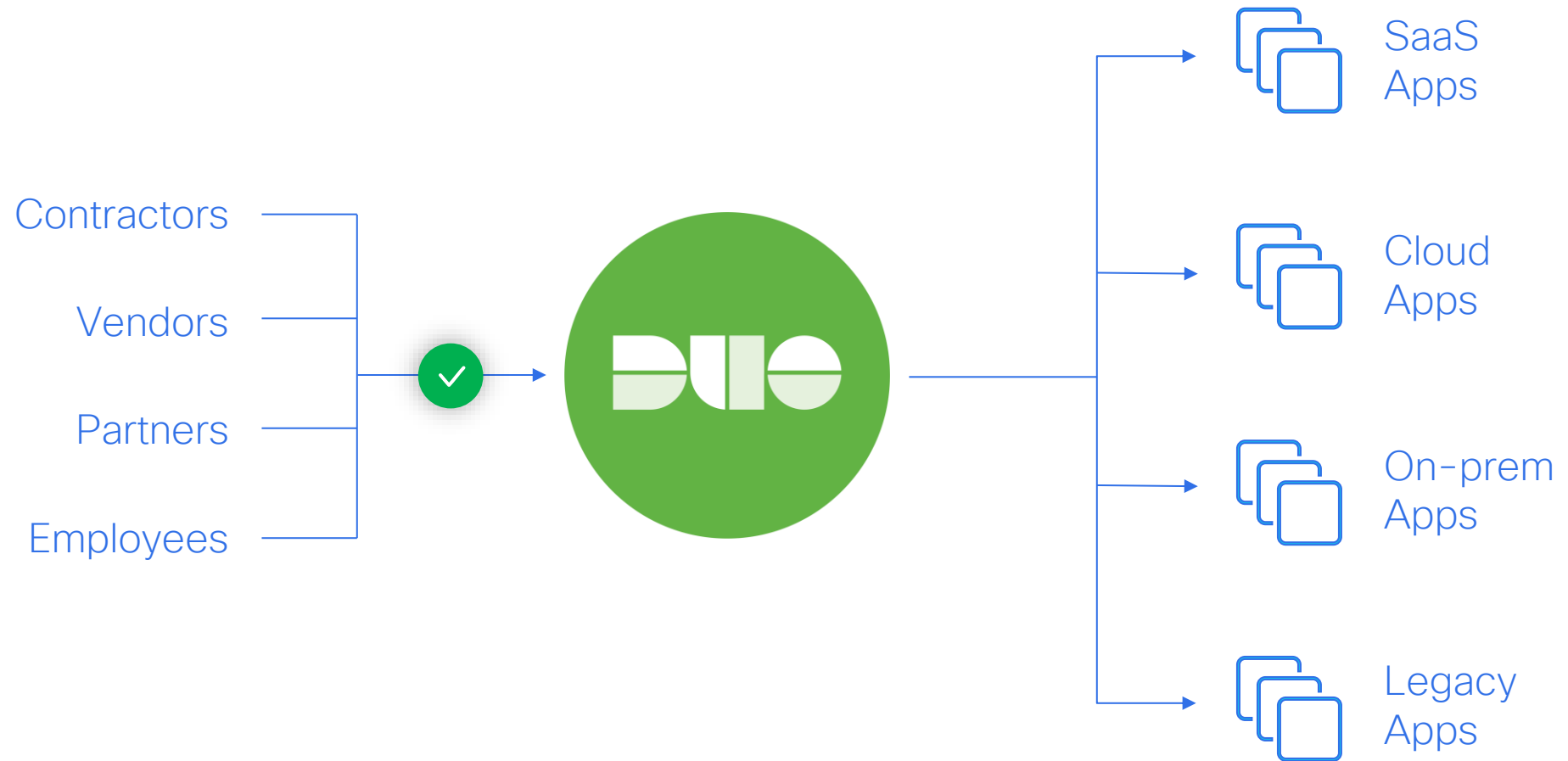
Please verify your identity
with a Government ID

Helpdesk Identity Verification – Full Verification With ID

Standalone IAM
when required

Alternate directory for
third-party users

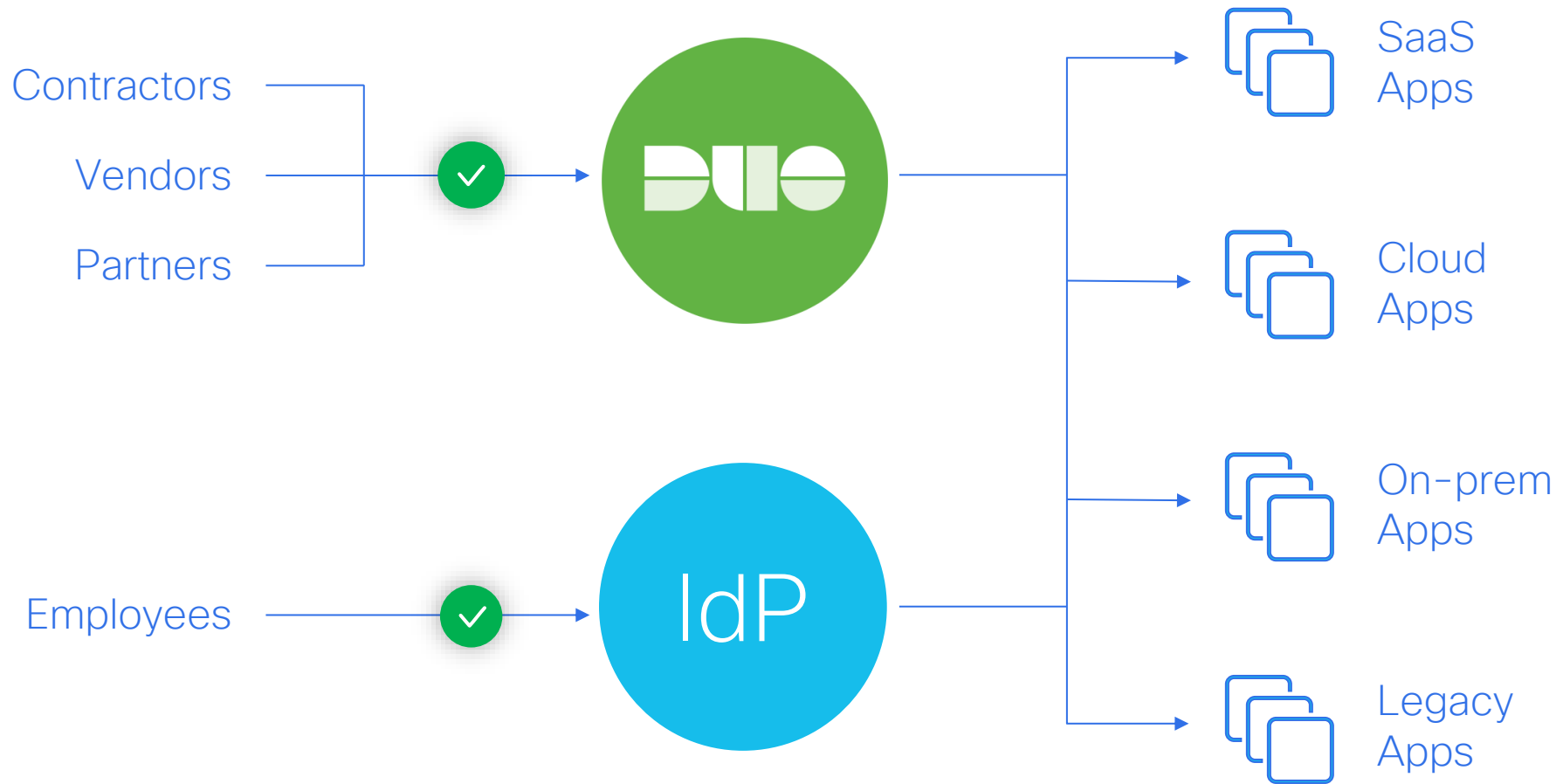
Identity broker
for existing IAM



Standalone IAM
when required

Alternate directory for
third-party users

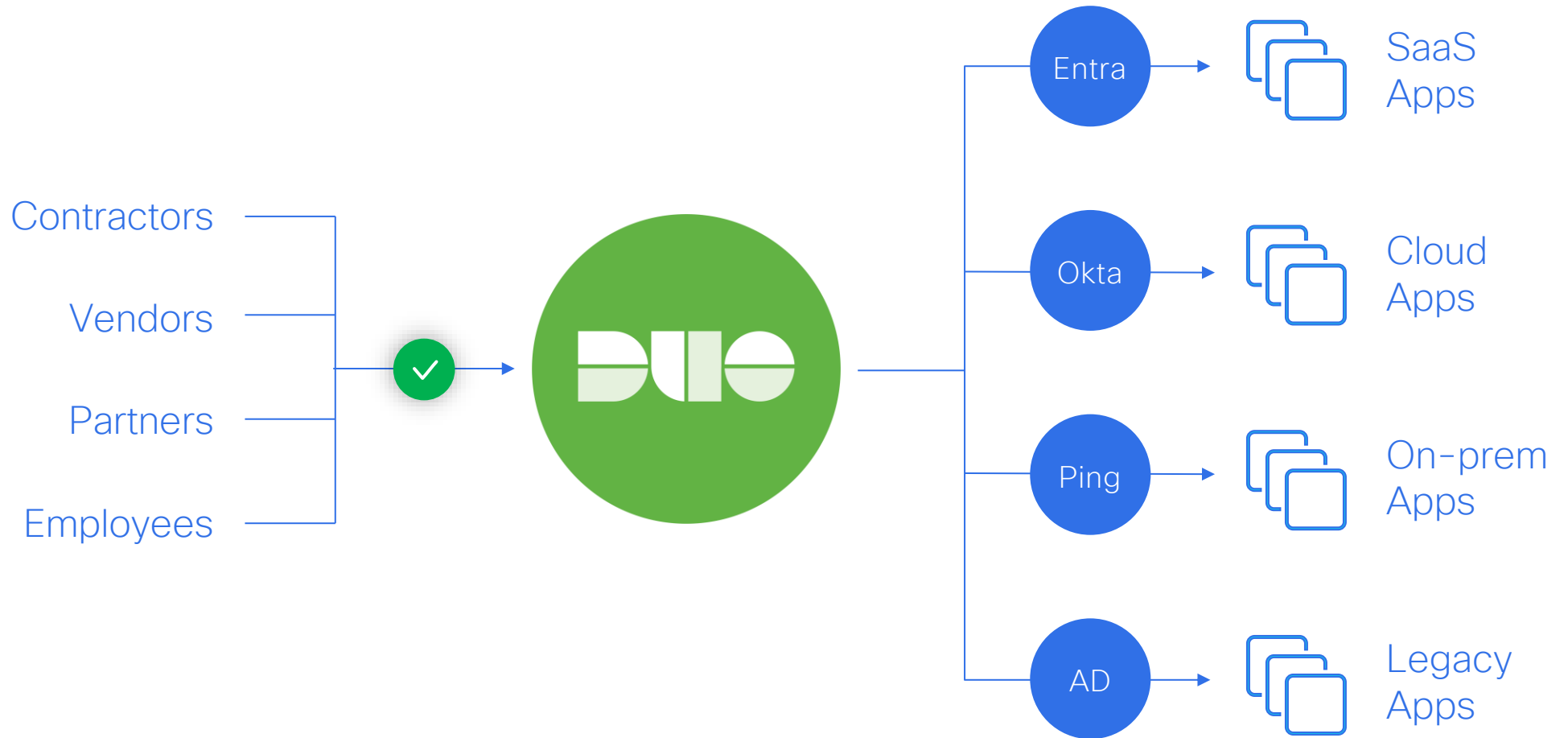
Identity broker
for existing IAM



Standalone IAM
when required

Alternate directory for
third-party users

Identity broker for
existing IAM



Summary

Summary

- **Incomplete MFA** coverage is a critical risk vector.
- Gaps in Phish-resistant MFA due to **complex deployment** and **inconsistent coverage** are leading vectors of identity-based attack.
- **Helpdesk identity verification** is crucial in preventing identity compromise.
- **Unseen** identities and **privileged** accounts are high-risk blind spots.
- Dispersed identity data hampers **unified** security enforcement and makes **visibility** across identity providers challenging.

Recommendations

- Assess FIDO2 tokens for high-risk user groups, in combination with **deployable cost-effective** phishing-resistant authentication methods like **proximity-based verification**
- Incorporate **Helpdesk verification** in security procedures
- Regular **identity security posture** checks can help identify gaps and weakness before they can be compromised.
- Invest in solutions that **unify and operationalize identity** data across platforms.

Free Identity Assessment

An easy-to-implement, short term assessment that delivers unique visibility into customer's identity ecosystem

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

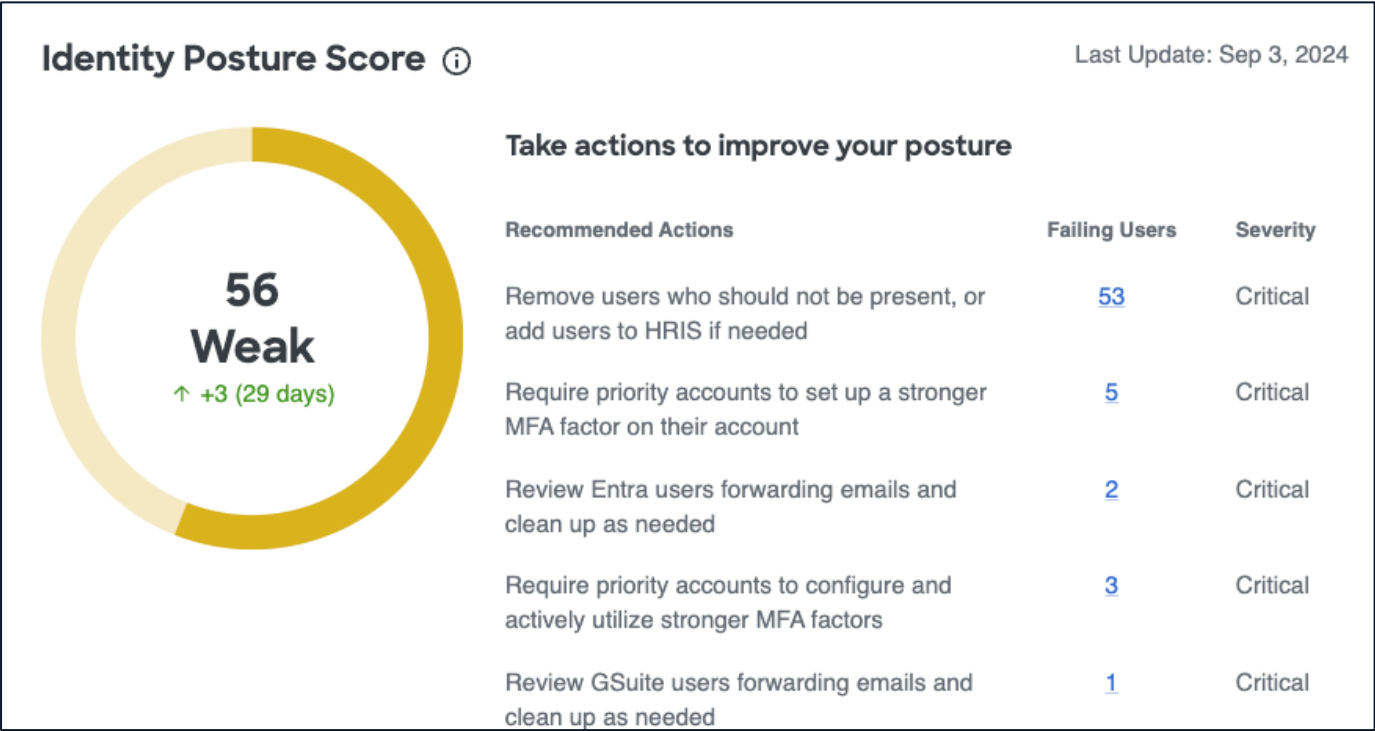
Insight into identity-related attacks

Compliance & security framework monitoring

View alignment across CIS, CMMC, MITRE, NIST, PCI, & SOX standards

License usage

Idle license insight



Complete your session evaluations



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



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: <https://www.linkedin.com/in/sheelaknetwork/>

skishan@cisco.com

Thank you

CISCO Live !

