Identity Based Attacks

A Red Team

Nic Conroy
Security Architect

Blue Team Experience

Ned Zaldivar
Security Architect

Cisco Webex App

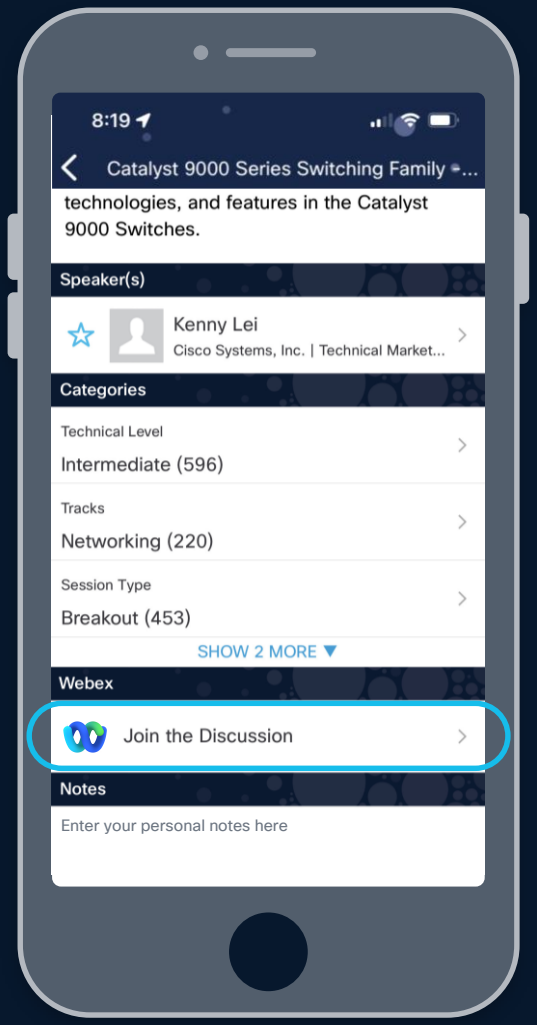
Questions?

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 June 13, 2025.



Cisco Live US Identity Security Learning Map

Sunday–8th

TECSEC-2013 2:00PM
Identity Zero to Hero: Understanding the Identity Security Space and Modern Auth

Monday–9th

BRKSEC-2100 8:00AM
ISE Your Meraki Network with Group Based Adaptive Policy

BRKSEC-1017 8:00AM
Achieving Industry Standards, Frameworks and Architectures Using Duo

BRKSEC-2096 8:00AM
Securing Industrial Networks: Where Do I Start?

○ **BRKSEC-2144** 9:00AM
Modern Authentication Explained to the Network Professional

BRKSEC-1383 9:30AM
Securing the Olympics: The Cybersecurity Architecture for Paris 2024

BRKSEC-2416 1:30PM
Cisco ISE Meets Azure Cloud. Deploy, Automate, Integrate with Entra ID and Intune

Tuesday–10th

○ **BRKSEC-2880** 2:00PM
Identity Under Siege: Strategies for Today's Threats

BRKSEC-2082 3:00PM
Breaking the Identity Provider Mold with Duo!

○ **BRKSEC-2162** 4:00PM
Identity Intelligence Demystified

BRKSEC-2347 4:00PM
ISE Deployment Improvements - Tips and Tricks

Wednesday–11th

BRKSEC-2164 1:30PM
Identity Based Attacks, a Red Team/Blue Team Experience

○ **BRKSEC-3707** 1:30PM
Advanced SGT - Multi Domain Context

○ **BRKSEC-2910** 2:30PM
Bridging the Gap: Integrating Identity Security Across Platforms

○ **VILSEC-1057** 2:30PM
Fifteen bars of connectivity in Healthcare, powered by Jamf, Apple, and Cisco Private 5G

○ **BRKSEC-2879** 3:30PM
Duo Identity Security: Protect your users and applications with SO MUCH more than MFA!

Thursday–12th

BRKSEC-2202 9:00AM
Demystifying the World of Passkeys

BRKSEC-2660 10:30AM
Setting the Stage for ISE Deployment Success: A Guide to Effective Planning

BRKSEC-2584 10:30AM
Innovative Authentication: Beyond Passwords

○ BU-led sessions

Who are your Speaker(s)

Nic Conroy

RED TEAM

- 6 Years at Cisco
- Enterprise Security Architect
- Love for Cyber Security, Jiu Jitsu, Travel, and being the most Rad Dad!

Ned Zaldivar

Blue Team

- 25+ years @ Cisco
- Global(s) Security Architect
- Cisco Live Speaker for 12+ years
- Photographer, Cars, Beekeeper and Scuba Diver

Session Disclaimer

What you will learn

- Threat Intelligence around Current Threat Landscape
- Several types of identity attacks will be displayed
- Several types of defensive measures will be shown
- Some tips towards best practices and the value of security mesh type architecture

What you will not learn

- Expertise on hacking tools
- Every defense possible
- Proprietary information on specific incidents
- How to make a million dollars Phishing your colleagues, enemies, frenemies, or financial institutions.
- Tools or Techniques beyond Identity (intital access) which Mitigate Blast Radius. For example segmentation, EDR or XDR solutions.

Agenda

01 Introduction

02 Vishing

03 Current Threat Landscape

04 Red Team / Blue Team

05 Session Hijacking

06 Valid Account

07 MFA Fatigue and Weak MFA

08 Summary

Vishing Demo

(11) Feed | LinkedIn

linkedin.com/feed/

Verify it's you

Search

Home | My Network 3 | Jobs | Messaging 2 | Notifications 6 | Me | For Business | Retry Premium

Nic Conroy

Security Solutions Architect

Durango, Colorado

Cisco

Profile viewers 285

Post impressions 1,060

Limited offer: Get up to 25% off Premium

Claim offer now

Saved items

Groups

Newsletters

Events

Start a post

Video | Photo | Write article

Sort by: Top

Dinesh Moudgil • 1st

Technical Leader, Technical Marketing Engineer - Cisco Security Busines...

1d • Edited •

Interested to get your hands dirty on Secure Firewall and learn how to simplify and secure your SD-WAN deployments ? ...more

Dinesh Verma and 57 others 3 reposts

Like | Comment | Repost | Send

Mahinur K. • 2nd

Co-Founder @ Grooic - Conversion Agency | Web3 Design Lead...

Promoted • Partnership with ClickUp

+ Follow

LinkedIn News

Top stories

Procter & Gamble to lay off 7,000
2m ago • 19,748 readers

US trade deficit shrinks by 56%
5m ago • 12,840 readers

Amazon preps humanoid deliveries
6m ago • 4,923 readers

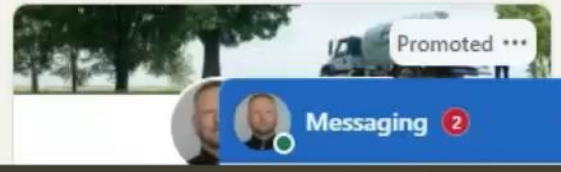
Hooters shutters 30 restaurants
9m ago • 1,823 readers

AI won't slow Alphabet hiring — yet
7m ago • 554 readers

Show more

Today's puzzle

Zip - a quick brain teaser
Solve in 60s or less!
151 connections played



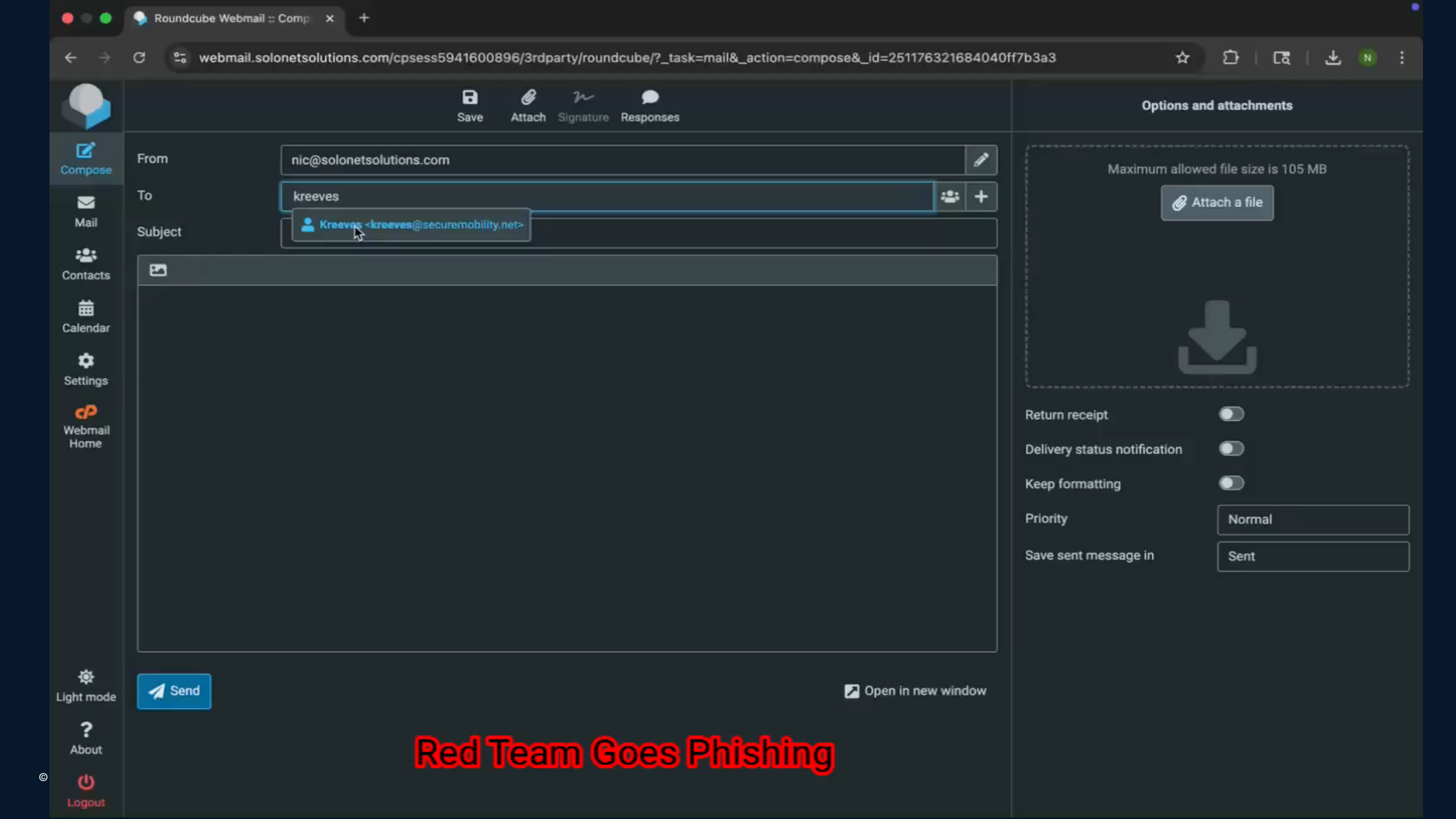
Messaging 2

Type here to search

61°F

10:27 AM
6/5/2025

Vishing Demo–Live Interaction


Roundcube Webmail :: Comp
webmail.solonetsolutions.com/cpsess5941600896/3rdparty/roundcube/?_task=mail&_action=compose&_id=251176321684040ff7b3a3
Save
Attach
Signature
Responses
Options and attachments
Compose
Mail
Contacts
Calendar
Settings
Webmail Home
From
nic@solonetsolutions.com
To
kreeves
Kreeves <kreeves@securemobility.net>
Subject
Maximum allowed file size is 105 MB
Attach a file
Return receipt
Delivery status notification
Keep formatting
Priority
Normal
Save sent message in
Sent
Send
Open in new window
Light mode
About
Logout
Red Team Goes Phishing

Anatomy of Attack

Vishing

Reconnaissance

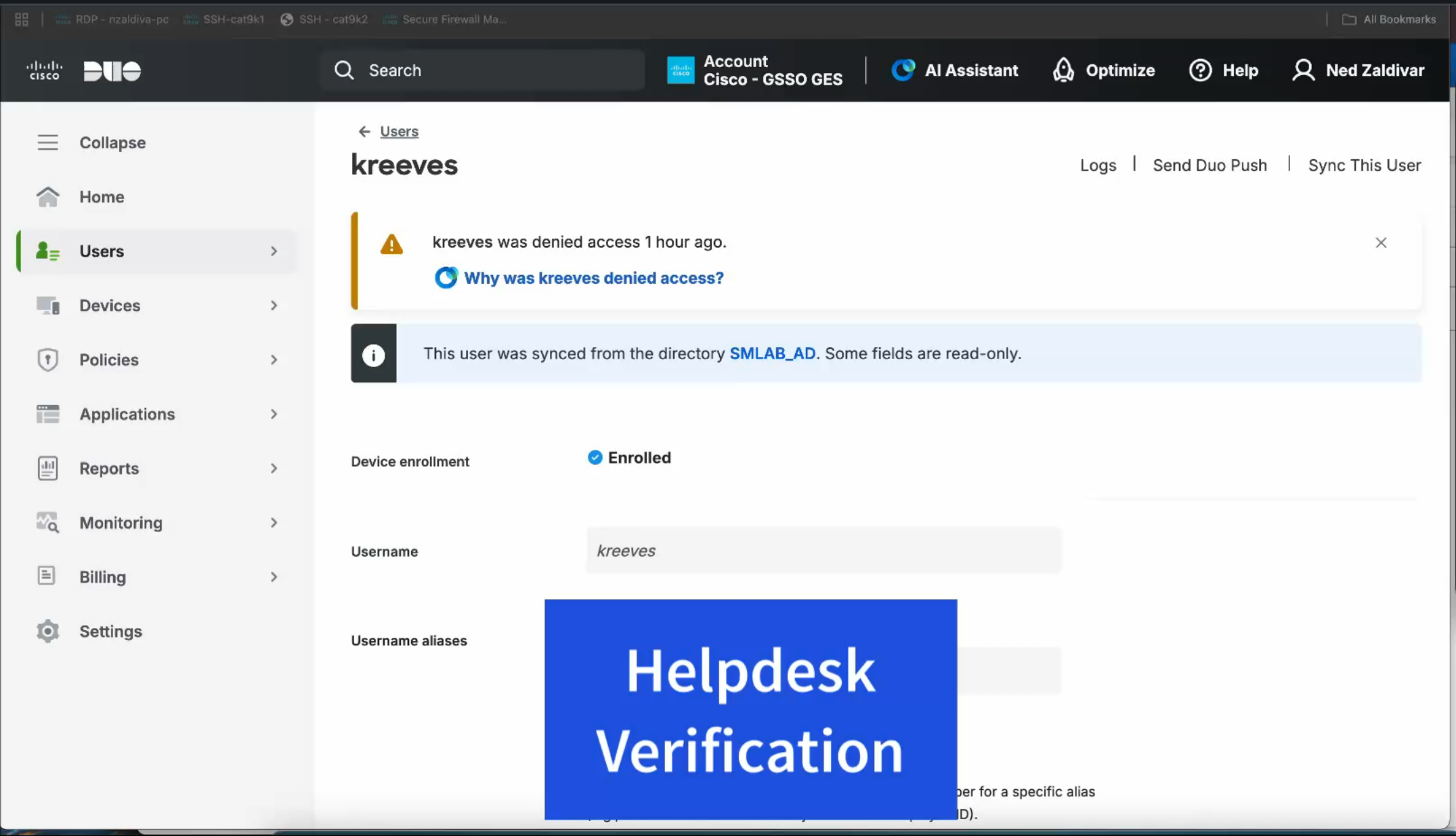
VISH

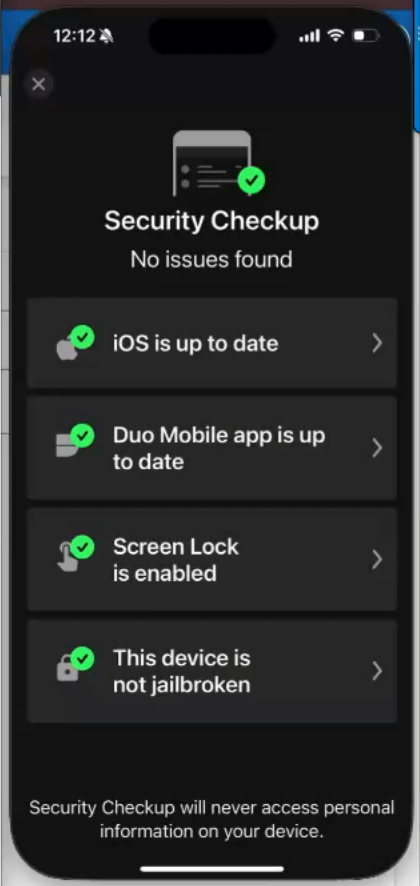
Phone Call, Social Engineering, Leveraging information gained in Reconnaissance to lower the guard and increase the trust of the internal employee.

PHISH using opensource or commercial tools

Chaos ensues to include, registration of MFA, Forwarding of Email, Privilege Escalations, etc.

BLUE TEAM


RDP - nzaldiva-pc
SSH-cat9k1
SSH - cat9k2
Secure Firewall Ma...
All Bookmarks
Search
Account
Cisco - GSSO GES
AI Assistant
Optimize
Help
Ned Zaldivar
Collapse
Home
Users
Devices
Policies
Applications
Reports
Monitoring
Billing
Settings
Users
kreeves
Logs | Send Duo Push | Sync This User
kreeves was denied access 1 hour ago.
Why was kreeves denied access?
This user was synced from the directory SMLAB_AD. Some fields are read-only.
Device enrollment
Enrolled
Username
kreeves
Username aliases
Helpdesk Verification
per for a specific alias
ID).


12:12
Security Checkup
No issues found
iOS is up to date
Duo Mobile app is up to date
Screen Lock is enabled
This device is not jailbroken
Security Checkup will never access personal information on your device.

Reference

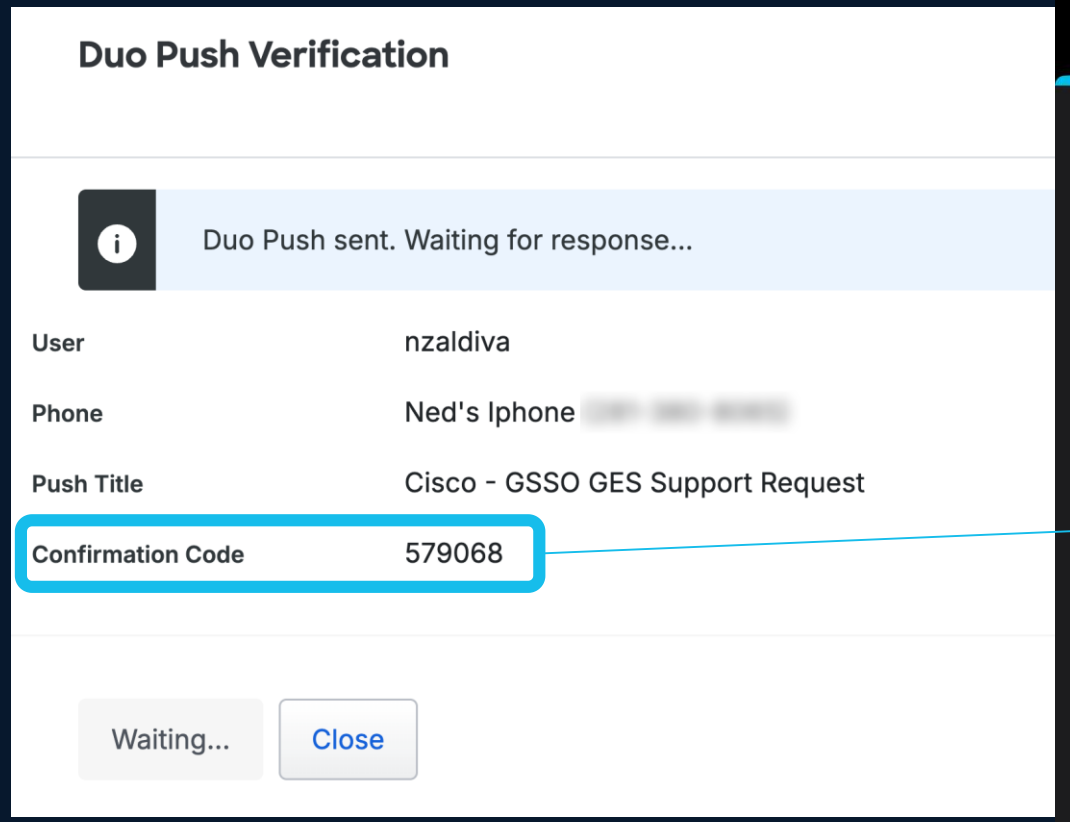
TOOLS USED: FEATURES: RESOURCES

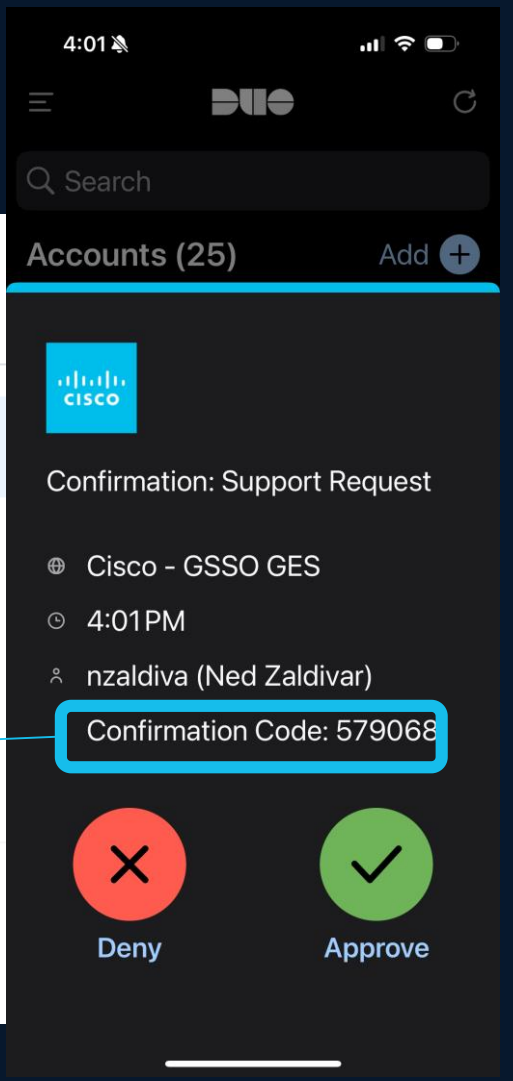
Helpdesk Verification by sending Duo Push, Code confirmation

Duo > Users > <Specific User>

> Send Duo Push

Available in GUI and Admin API



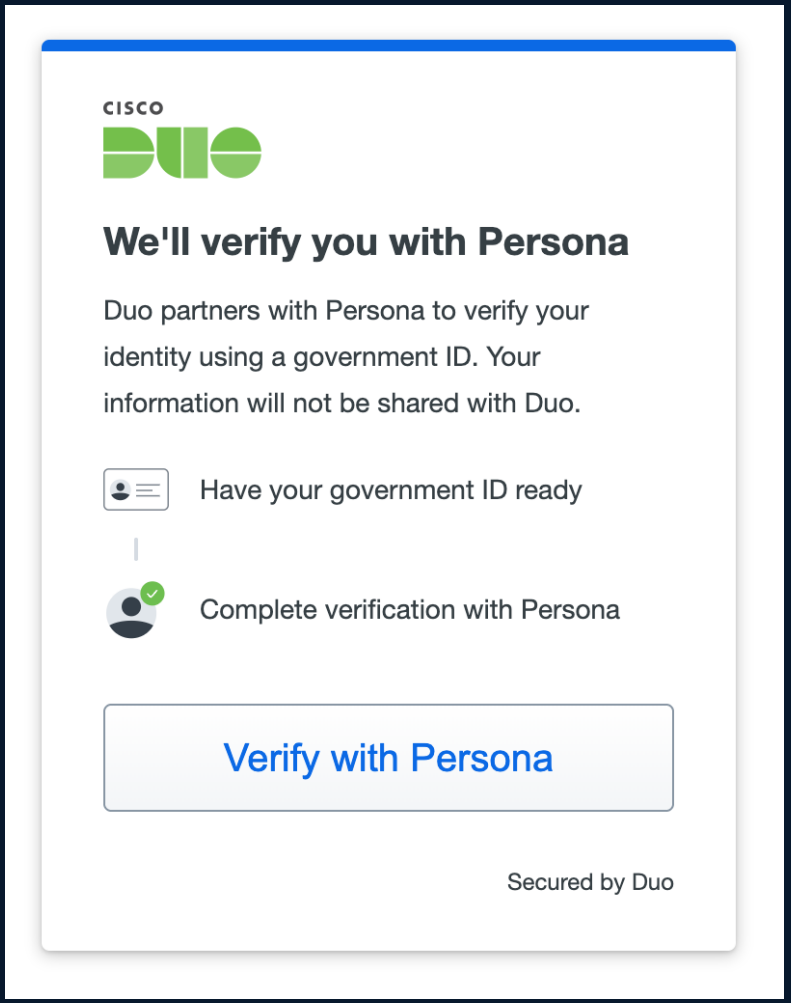


https://duo.com/docs/administration-users#verifying-users-with-duo-push

Duo Identity Verification Integration

Establish deep trust

- Introducing IDV workflows during critical moments in the workforce user's lifecycle
- First phase is a partnership with Persona. This partner was chosen for:
  - Flexibility and broad options
  - Global support
  - Strategic alignment with Cisco & Duo
- Key workflows:
  - Help Desk Verification (Private Preview now)
  - Remote Onboarding (Private Preview coming in July)
  - Self-Service



To establish trust, users must match information that has been stored in Duo – then provide government ID and a selfie.

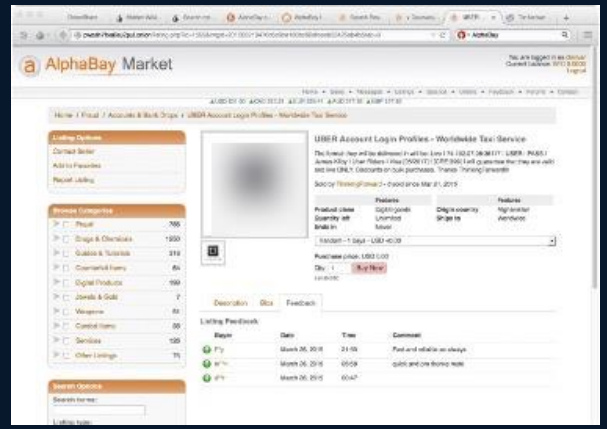
Helpdesk Identity Verification

Why does Vishing work?

We trust inherently

Your Identity and Personal Details and Your Connections are out there (Reconnaissance)

Your passwords are for sale (Credentials)



Human Voice has emotion and the ability to persuade (Gain Access or More Reconnaissance)

Other Ways to Trust but Verify User

- Call Back – if they have spoofed the number, then they can't get a call back (or won't be available via main number)
- Verbal Passwords (pre-shared)
- Email Verification – if they are spoofing the number and don’t control your mailbox.
- SMS Verification – if they have spoofed the number, then it would be hard for them to get an SMS
- If it is an IT support Vish. Ask to speak to manager. Verify identity.

Current Threat Landscape

Talos Threat Intelligence : Talos' Published Year in Review 2024 Analyzes data from...

193 Countries

46 Million Devices

886 Billion Security Events Daily

https://blog.talosintelligence.com/2024yearinreview/

Threat Intelligence

Talos

60%

Identity-based attacks were dominant, accounting for 60% of all Cisco Talos Incident Response cases.

48%

Ransomware actors successfully disabled security solutions in 48% of their attacks last year

Generative AI

Generative AI tools have enabled more sophisticated social engineering attacks

"GPT-4 was able to successfully attack 87% of vulnerabilities tested when given a description of the exploit from CVE, the public database of common security issues." -UIUC

https://blog.talosintelligence.com/2024yearinreview/

Threat Intelligence

Our Peers Concur

Crowdstrike

Breaches with stolen credentials take 292 days to detect. Adversaries move laterally undetected with valid credentials.

Unit 42

77% of intrusions are suspected to be caused by three initial access vectors: phishing, exploitation of known software vulnerabilities, and brute force Credentials attacks- focused primarily on remote desktop protocol.

Top Identity Attacks and Techniques Defined

Phishing

Email with malicious link

Credential Stuffing

Automated injection of stolen creds

Social Engineering

Trick end user into doing something

Pass-the-hash

Stolen hashed creds to gain access

AiTM

Attacker intercepts data (creds..., used for MFA Bypass)

Identity Theft

Leverage stolen credentials

Red Team / Blue Team

Red Team / Blue Team Defined

Reference

Red Team - Offensive

A Red Team is a group of people who simulate an attack on an organization's systems to identify vulnerabilities. The goal is to improve the organization's security.

Blue Team - Defense

A Blue Team is a group of cybersecurity professionals who protect an organization's computer systems and networks. They analyze security, identify vulnerabilities, and respond to security incidents.

What is a Purple Team?

Red Team

Creating Attacks Leveraging Tactics, Techniques and Procedures

Social Engineering

Social engineering is the psychological manipulation of individuals to trick them into divulging confidential information or performing actions that compromise security, often exploiting trust or human behavior.

Open-Source Tools

57% of Talos Incident Response Cases used open source tools:

Impacket, Mimikatz, and GoPhish are common examples of Open Source tools.

Commercial Tools

26% of Talos Incident Response Cases used Commercial Tools:

Cobalt, Rapid7, even HAK5 gear commercially available are examples of these tools.

LOLBINS

17% of Talos Incident Response Engagements leveraged LOLBINS (Living off Land Binaries)

- PowerShell (powershell.exe)
- Mshta (mshta.exe)
- CertUtil (certutil.exe)

Blue Team

Defending Using these tools

Email Security

Email Threat Defense

- API/Gateway
- Advanced phishing technique identification and blocking
- Protects M365 Email

Identity Security

Duo

- MFA – Validated User
- Phishing Resistance
- Trusted Endpoints
- Primary, Secondary Authentication
- IAM, IDP

Identity Threat Detection

Cisco Identity Intelligence

- Identity Threat Detection and Response
- Builds Identity Graph
- Multi-sourced, vendor-agnostic solution that works across your existing identity stack and brings together authentication and access insights.

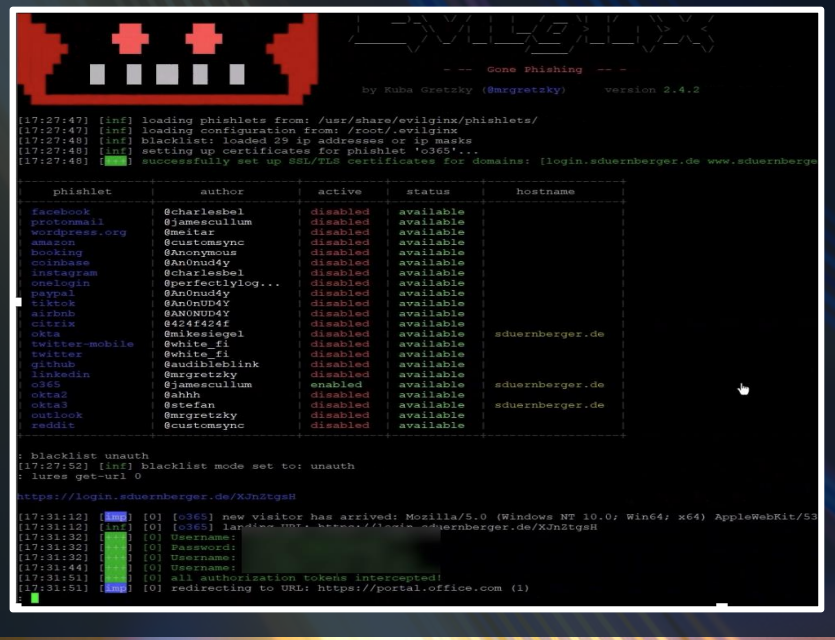
Network Security

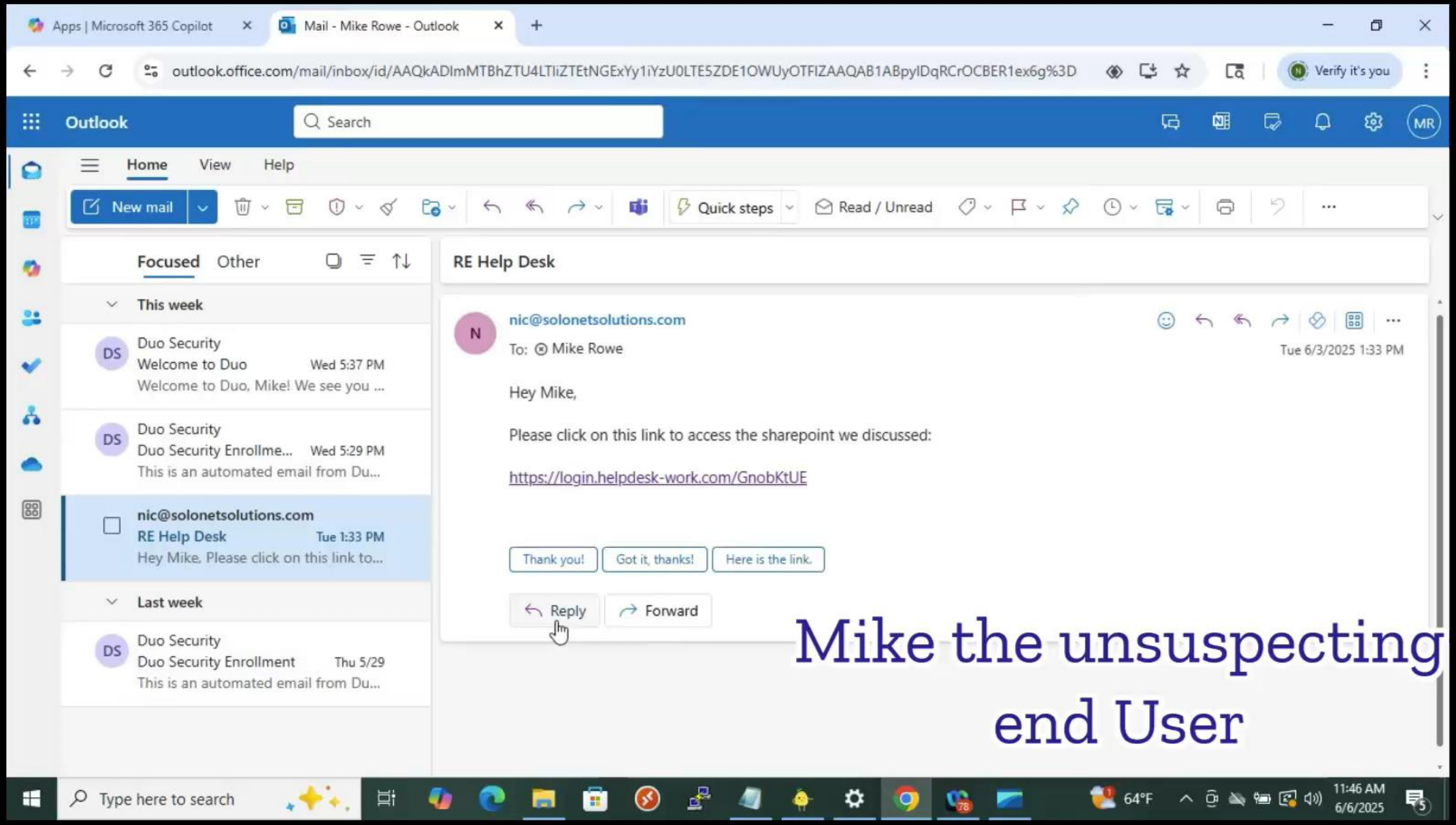
Umbrella

Secure Access

- DNS Security
- Secure Web Gateway
- FWaaS
- Zero Trust/VPNaaS
- Experience Insights

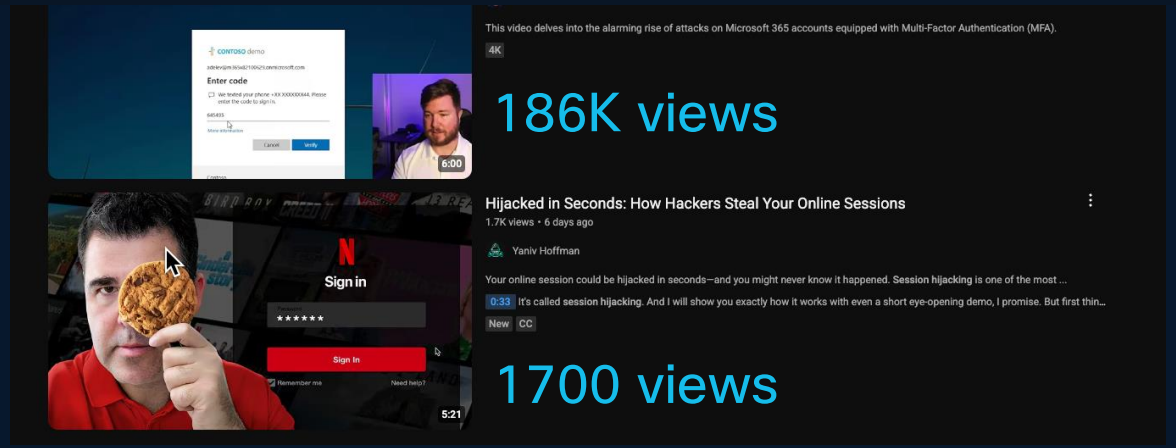
Session Hijacking





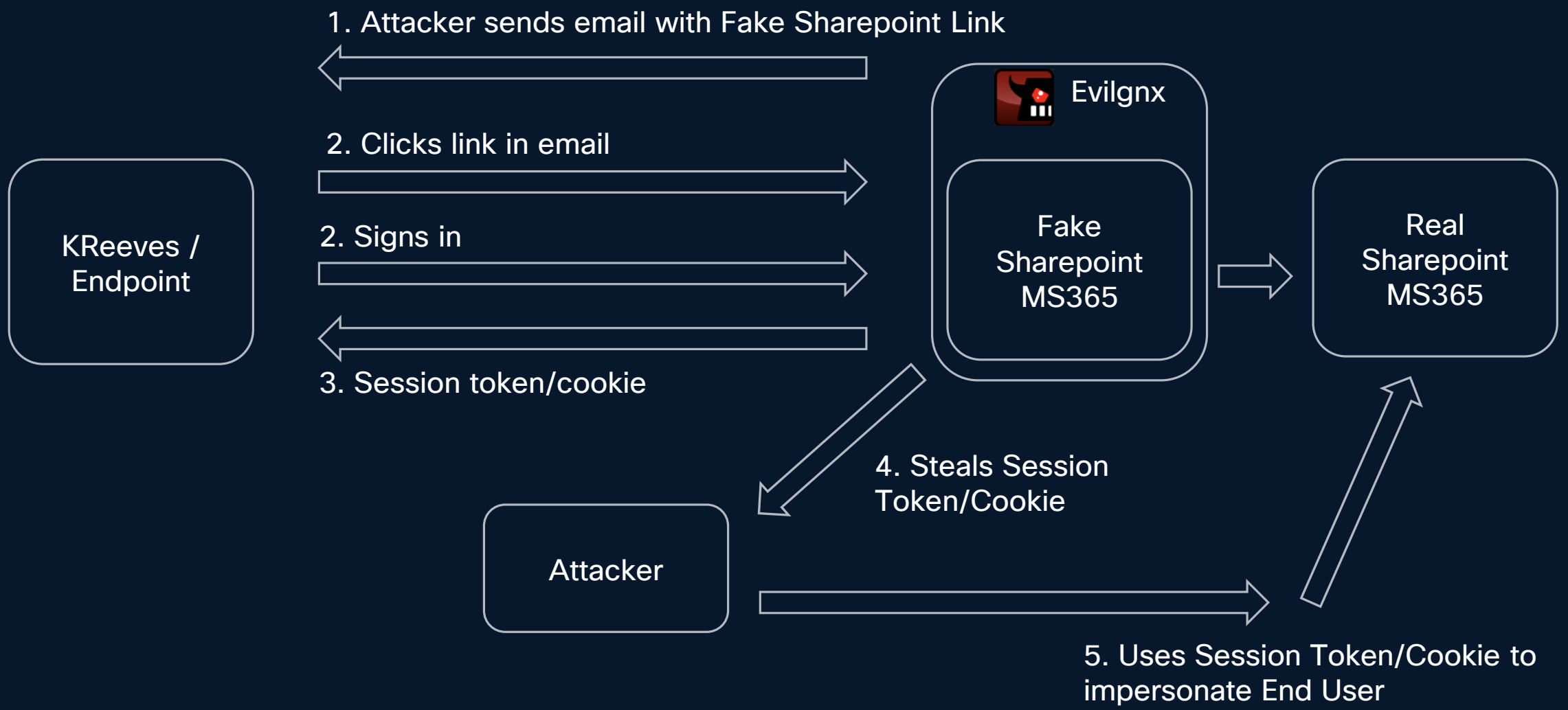
Mike the unsuspecting end User

Anyone can learn to do Session Hijacking



Anatomy of Attack

MFA Bypass Session Hijacking



Blue Team

Umbrella/Secure Access DNS Security

Email Threat Defense Phishing Protection

Duo Passport

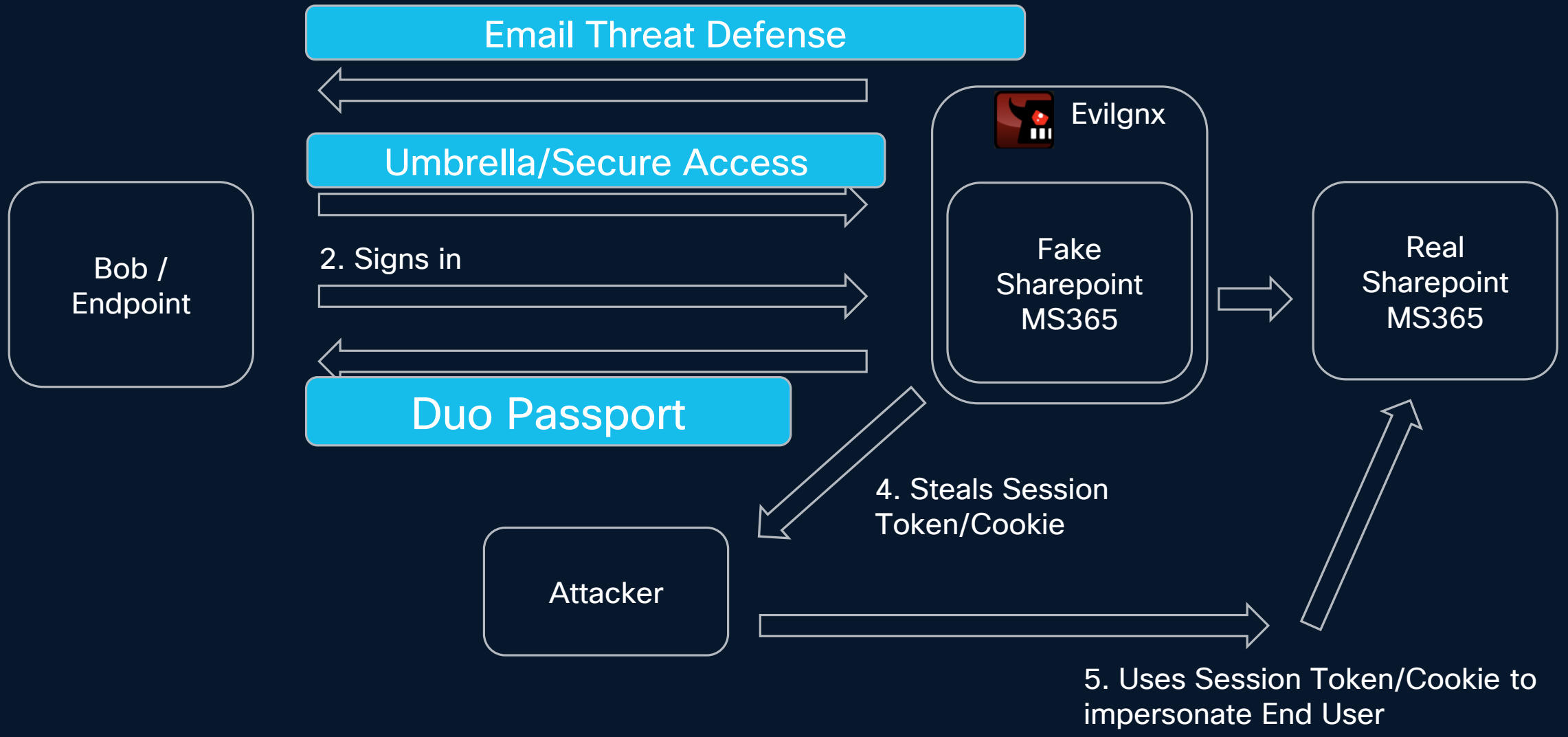
Session Token Threat Protection

Cookie-less Session

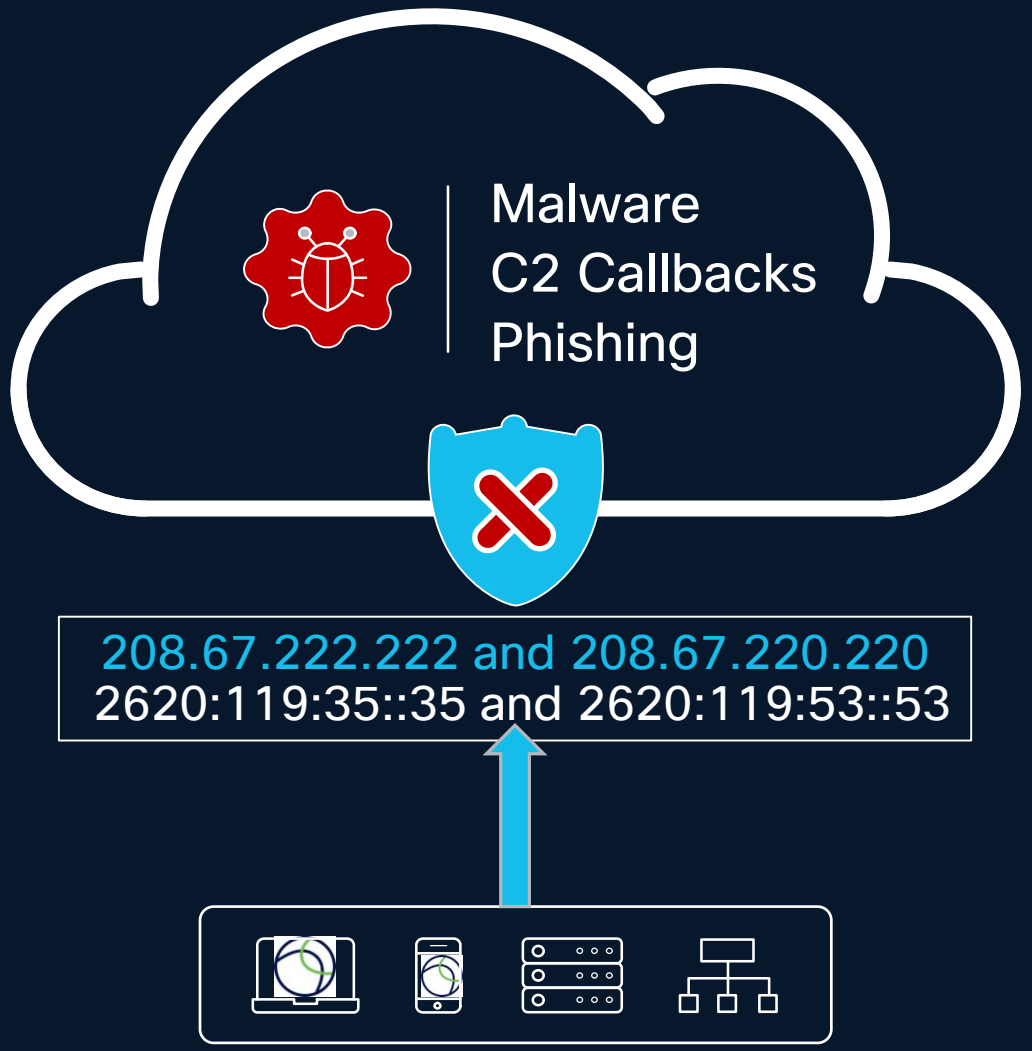
Login once, Access Everything

Tools Used to Protect

MFA Bypass Session Hijacking

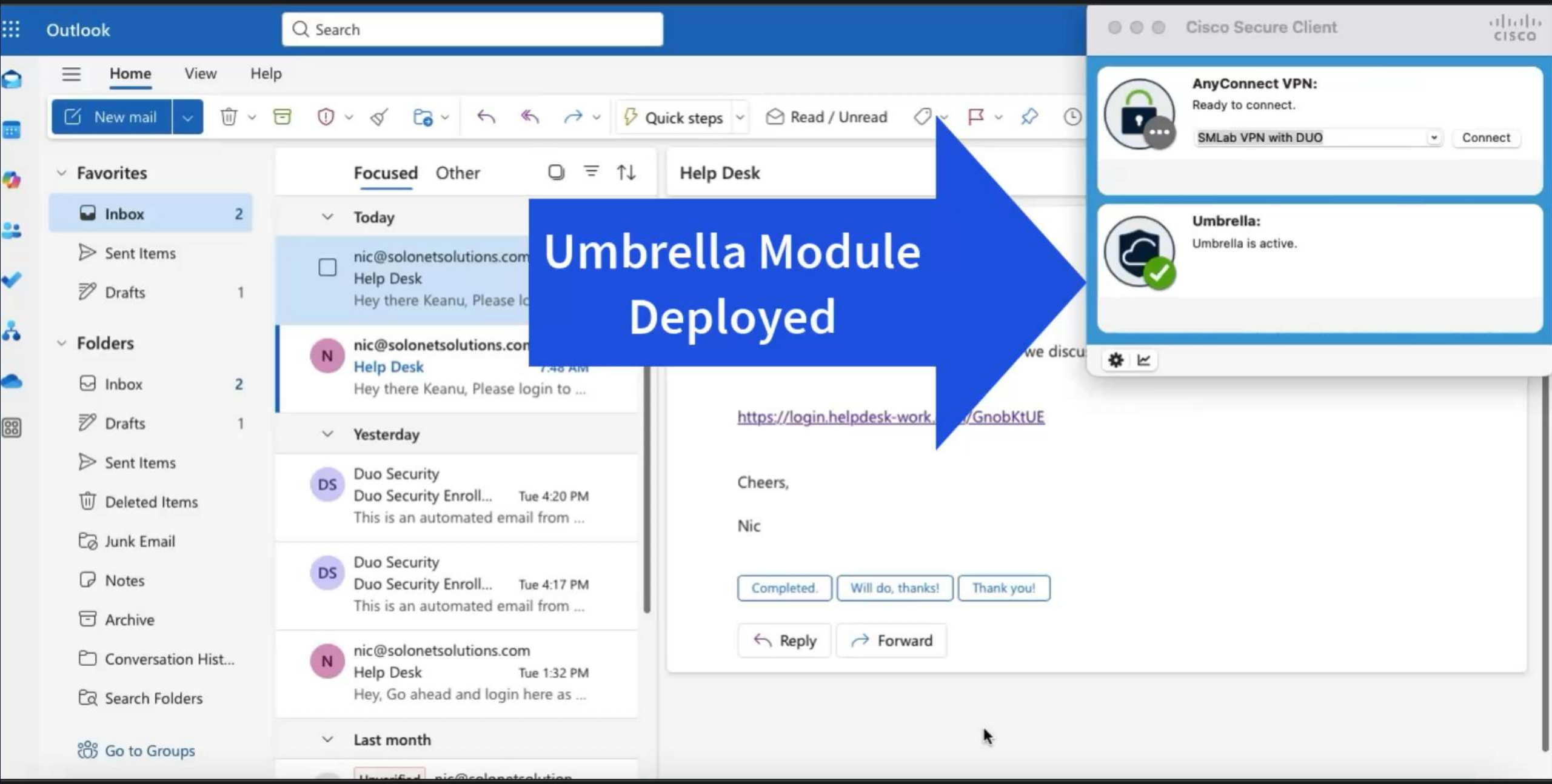


What is Umbrella/Secure Access?



- Umbrella / Secure Access DNS Protection
- SaaS
- DNS Recursive Resolved
- DNS protection via DNS Forwarding or using Cisco Secure Client: Umbrella Module

- *Secure Access includes other functions not used in this session (SWG, ZTNA, VPNaaS, FWaas, Experience Insights)


Outlook
Search
Home
View
Help
New mail
Quick steps
Read / Unread
Favorites
Inbox 2
Sent Items
Drafts 1
Folders
Inbox 2
Drafts 1
Sent Items
Deleted Items
Junk Email
Notes
Archive
Conversation Hist...
Search Folders
Go to Groups
Focused
Other
Today
nic@solonetsolutions.com
Help Desk
Hey there Keanu, Please lo
nic@solonetsolutions.com
Help Desk
Hey there Keanu, Please login to ...
Yesterday
Duo Security
Duo Security Enroll...
Tue 4:20 PM
This is an automated email from ...
Duo Security
Duo Security Enroll...
Tue 4:17 PM
This is an automated email from ...
nic@solonetsolutions.com
Help Desk
Tue 1:32 PM
Hey, Go ahead and login here as ...
Last month
Help Desk
https://login.helpdesk-work.
/GnobKtUE
Cheers,
Nic
Completed.
Will do, thanks!
Thank you!
Reply
Forward
Umbrella Module Deployed
Cisco Secure Client
AnyConnect VPN:
Ready to connect.
SMLab VPN with DUO
Connect
Umbrella:
Umbrella is active.

Reference

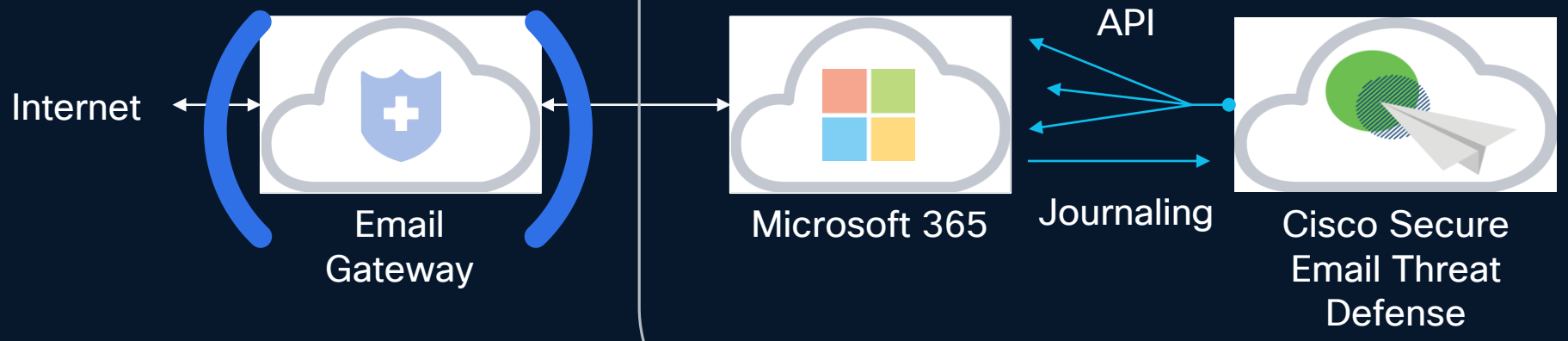
What is Email Threat Defense?

Secure Email Gateway

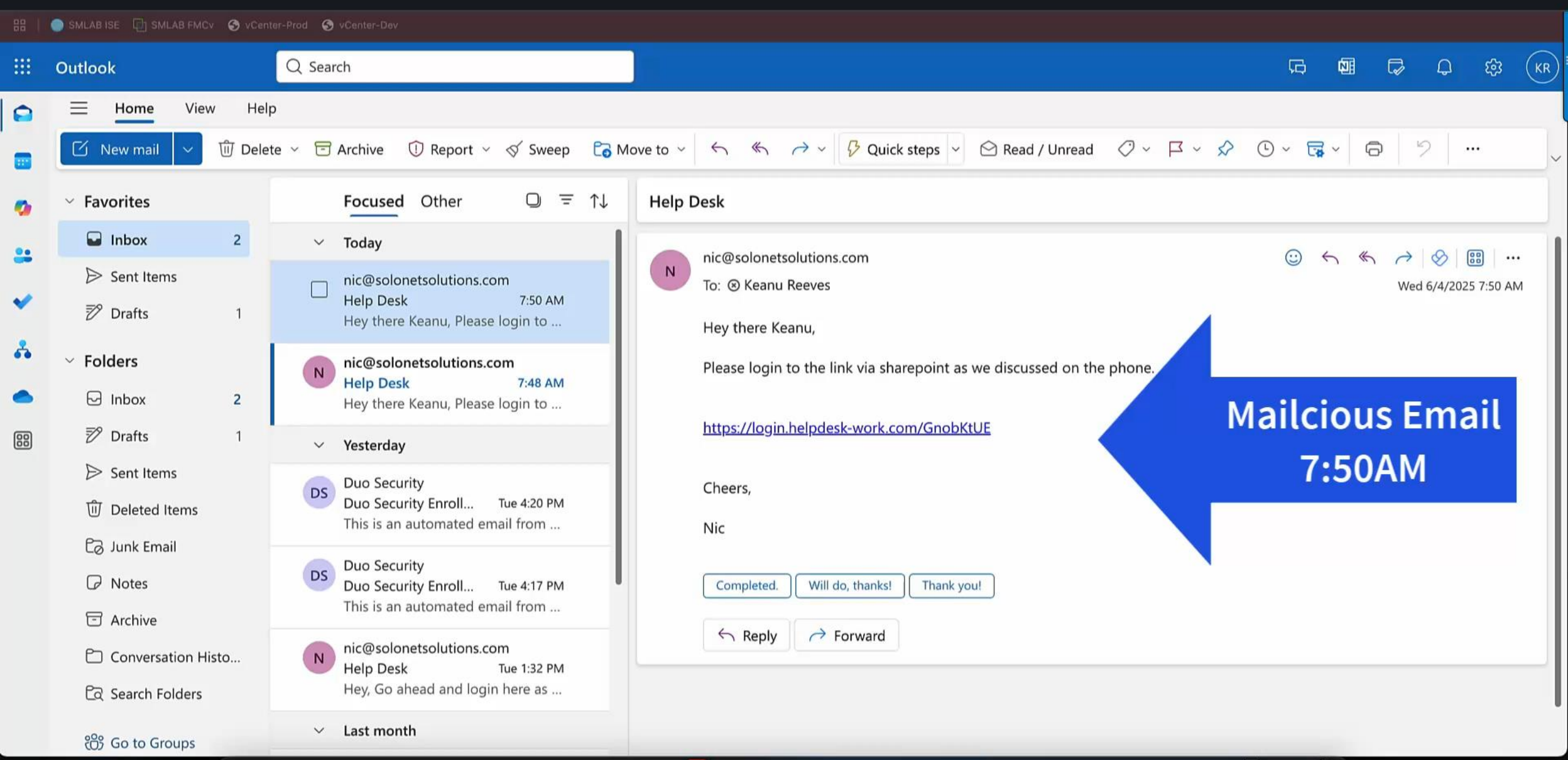
Modifies and filters **inbound** and **outbound** messages that cross the perimeter

Cisco Secure Email Threat Defense

Has complete visibility of **inbound**, **outbound and internal** messages

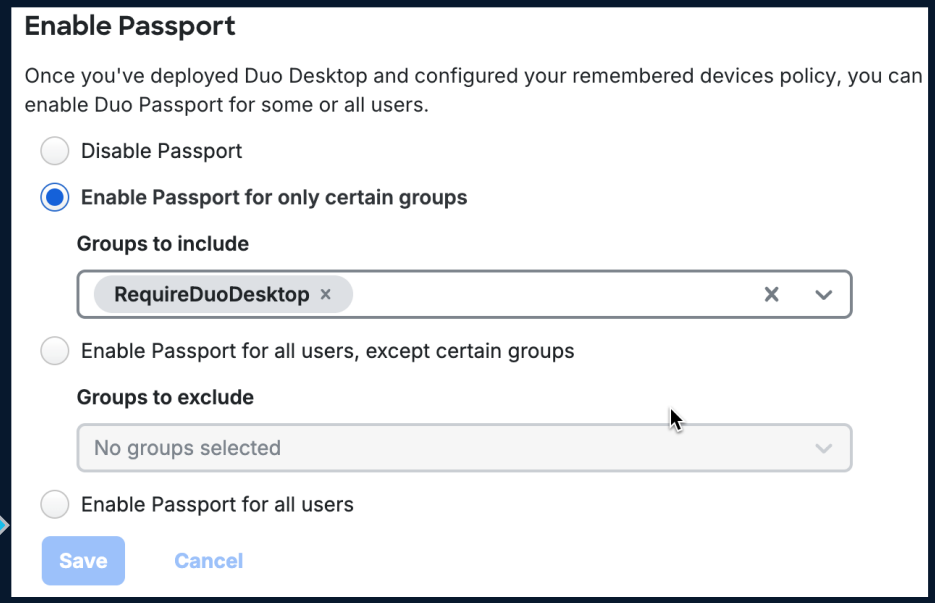


- SaaS
- Integrated Cloud Email Security
- Agile Development
- Built with Cloud Native Services
- Advanced Analytics on Emails


SMLAB ISE
SMLAB FMCv
vCenter-Prod
vCenter-Dev
Outlook
Search
KR
Home
View
Help
New mail
Delete
Archive
Report
Sweep
Move to
Quick steps
Read / Unread
Favorites
Inbox 2
Sent Items
Drafts 1
Folders
Inbox 2
Drafts 1
Sent Items
Deleted Items
Junk Email
Notes
Archive
Conversation Histo...
Search Folders
Go to Groups
Focused
Other
Today
nic@solonetsolutions.com
Help Desk 7:50 AM
Hey there Keanu, Please login to ...
nic@solonetsolutions.com
Help Desk 7:48 AM
Hey there Keanu, Please login to ...
Yesterday
Duo Security
Duo Security Enroll... Tue 4:20 PM
This is an automated email from ...
Duo Security
Duo Security Enroll... Tue 4:17 PM
This is an automated email from ...
nic@solonetsolutions.com
Help Desk Tue 1:32 PM
Hey, Go ahead and login here as ...
Last month
Help Desk
nic@solonetsolutions.com
To: Keanu Reeves
Wed 6/4/2025 7:50 AM
Hey there Keanu,
Please login to the link via sharepoint as we discussed on the phone.
https://login.helpdesk-work.com/GnobKtUE
Cheers,
Nic
Completed.
Will do, thanks!
Thank you!
Reply
Forward
Mailcious Email
7:50AM

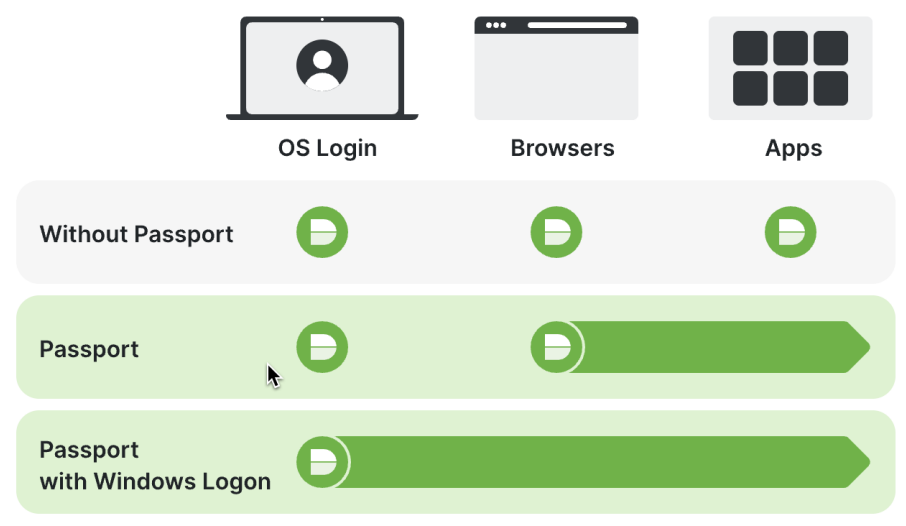
Duo Passport for Session Token Theft Protection

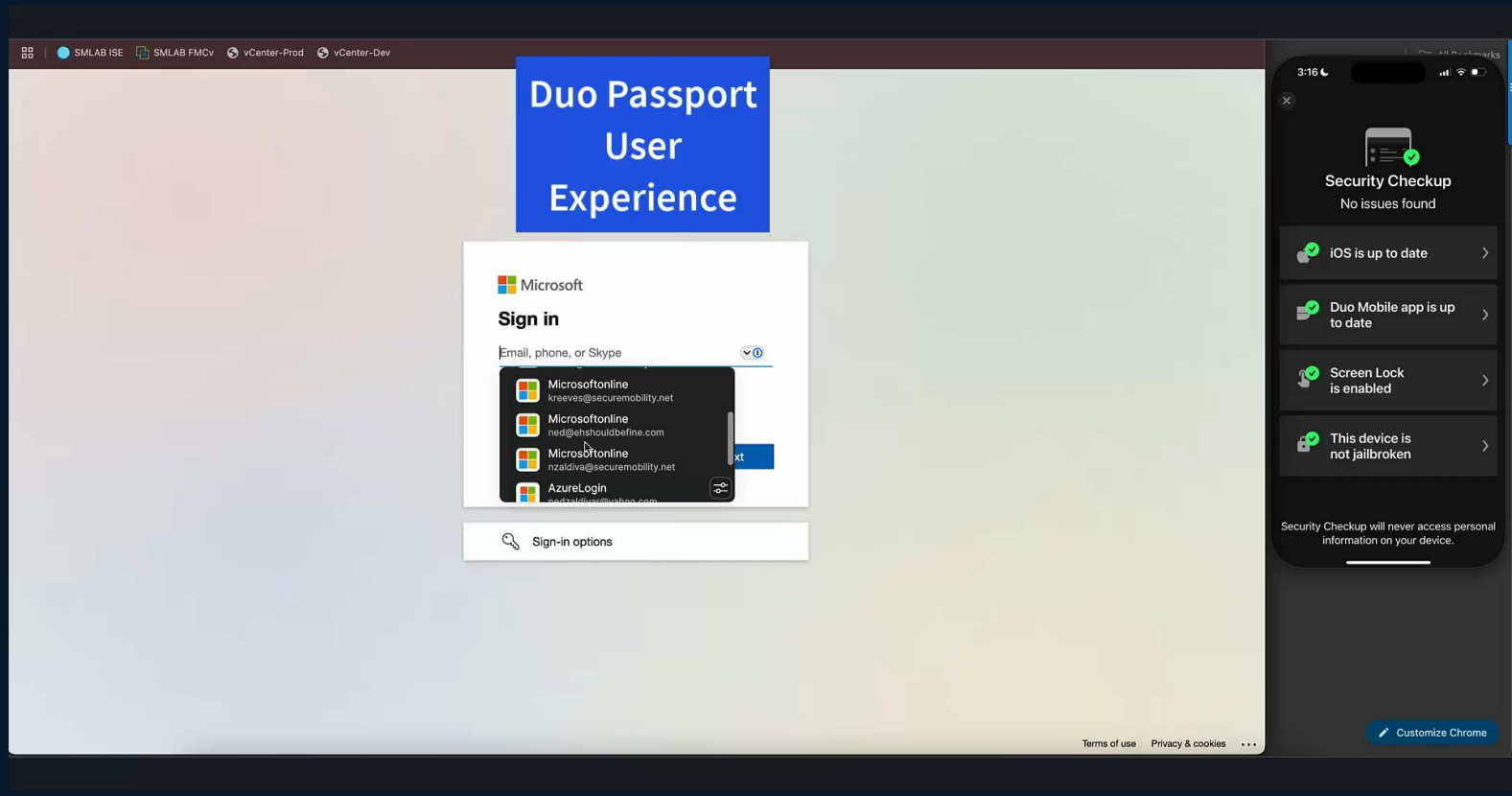
- Duo Passport Session Token Theft Protection (STTP) reduces the risk of session hijacking by minimizing the use of cookies.
- Instead of setting a cookie when a Passport session is detected for authentication, STTP submits the Passport session directly, eliminating the need for a cookie entirely
- Duo > Policies > Passport



Timestamp (CDT)	Duo Passport Sessions	User	Application	Risk-Based Policy Assessment	Access Device	Authentication Method
3:16:03 PM JUN 2, 2025	✓ Granted Authentication trusted by Risk-based remembered devices via Passport	nzaldiva	Microsoft Azure Active Directory	**Session verified** Session verified	Mac OS X 15.5 (24F74) As reported by Duo Desktop	Remembered Device Location Unknown
3:14:33 PM JUN 2, 2025	✓ Granted Authentication trusted by Risk-based remembered devices via Passport	nzaldiva	Cisco Firepower Threat Defense VPN - Single Sign-On	**Session verified** Session verified	Mac OS X 15.5 (24F74) As reported by Duo Desktop	Remembered Device Location Unknown

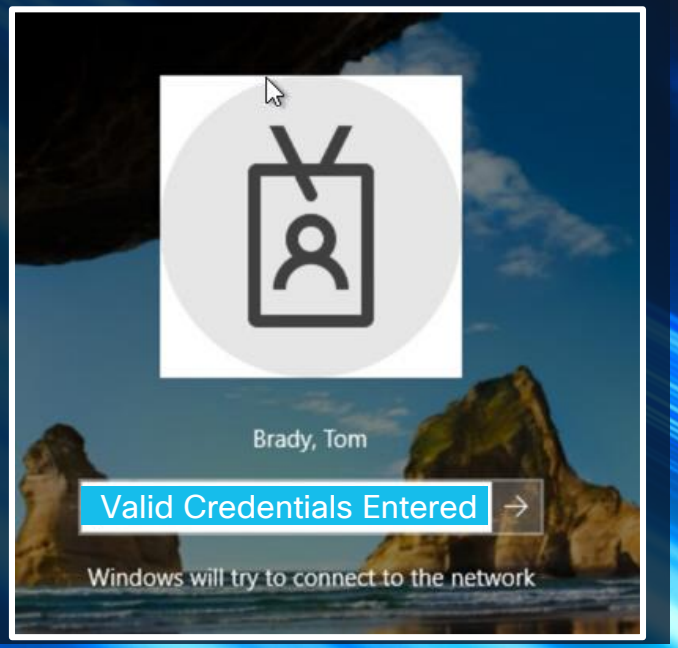
Duo Passport for Session Token Theft Protection





Duo Passport brings Duo Desktop together with the remembered devices policy, so your users can authenticate less often. It works with MFA, passwordless, SSO, and Duo Authentication for Windows Logon.

Valid Account



Abacus Darknet Market: official | Home | Abacus Market

abacus2cmdqhvoei3oiwarxf5aukg32ru4y6g7vuphisgjd7xdq4xmyd.onion

abacus market

Logged in as usmcnic97... Logout
BTC: 0.00000000 / XMR: 0.00000000

▲USD 104,153.11 ▲CAD 142,449.91 ▲EUR 91,201.62 ▲AUD 160,435.69 ▲GBP 76,946.74

HOME | ORDERS (0) | MESSAGES (0) | WALLETS | PROFILE | SUPPORT (0) | FORUMS | START SELLING | VERIFY URL | HARM REDUCTION

Home

usmcnic97... (0) *100%*
Trust Level: 1

Notifications (1)

Bitcoin 0.00000000
Monero 0.00000000

My Orders | My Favorites
My Settings | Log Out

MY ABACUS +

WHAT'S NEW FOR ME?

1 unread notifications
Click here to see all

Transferring data from abacus2cmdqhvoei3oiwarxf5aukg32ru4y6g7vuphisgjd7xdq4xmyd.onion...

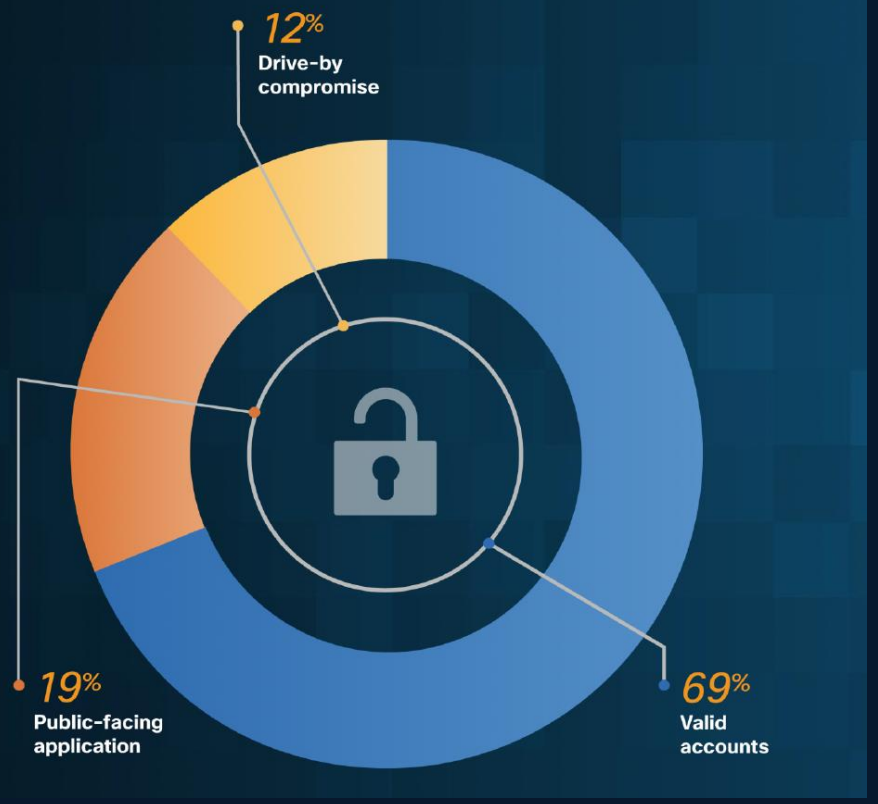
Type here to search

8:16 AM
6/6/2025

Initial Access and Valid Accounts

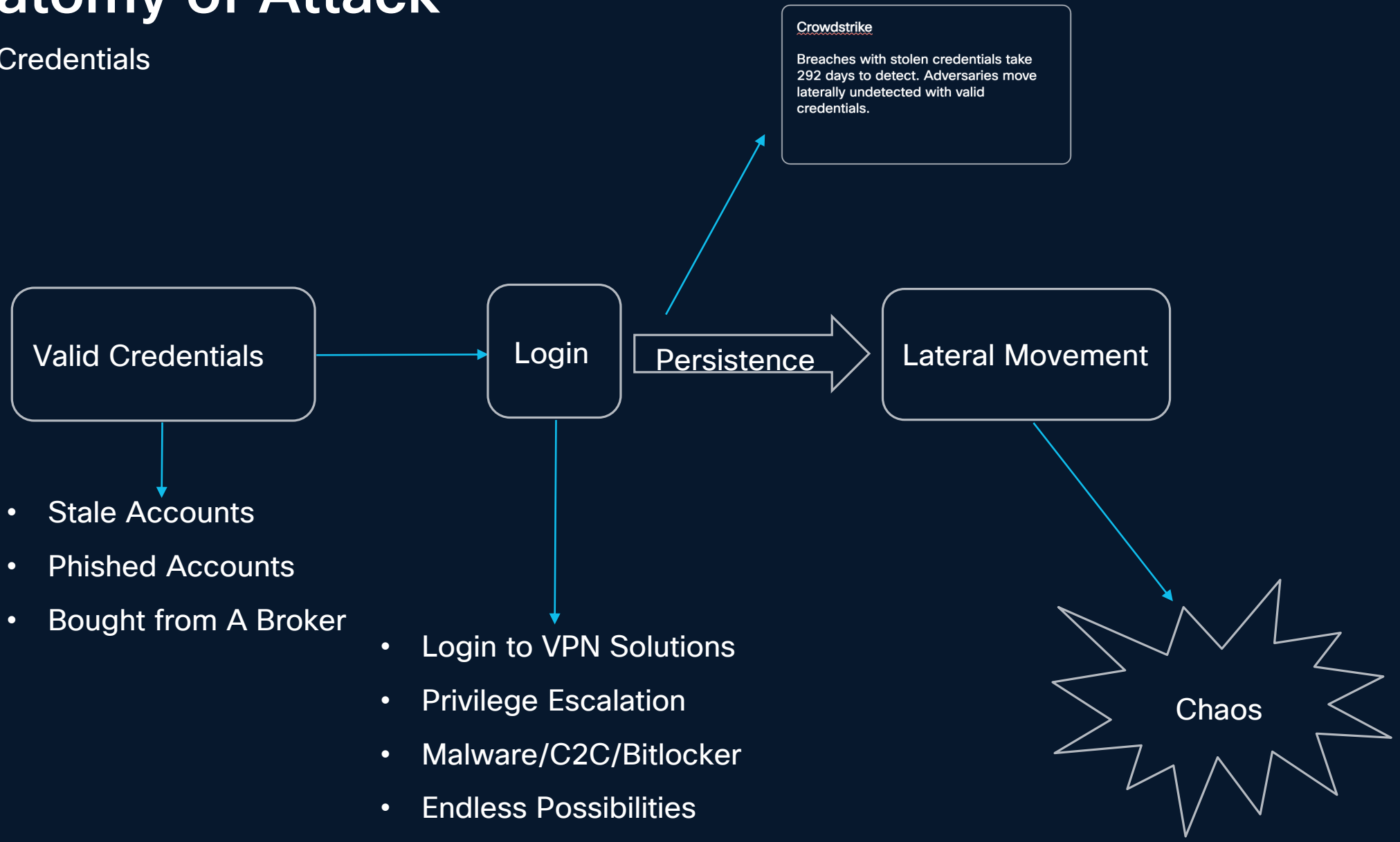
Initial access and valid accounts

Ransomware actors overwhelmingly leveraged valid accounts for initial access in 2024, with this tactic appearing in almost 70% of related cases



Anatomy of Attack

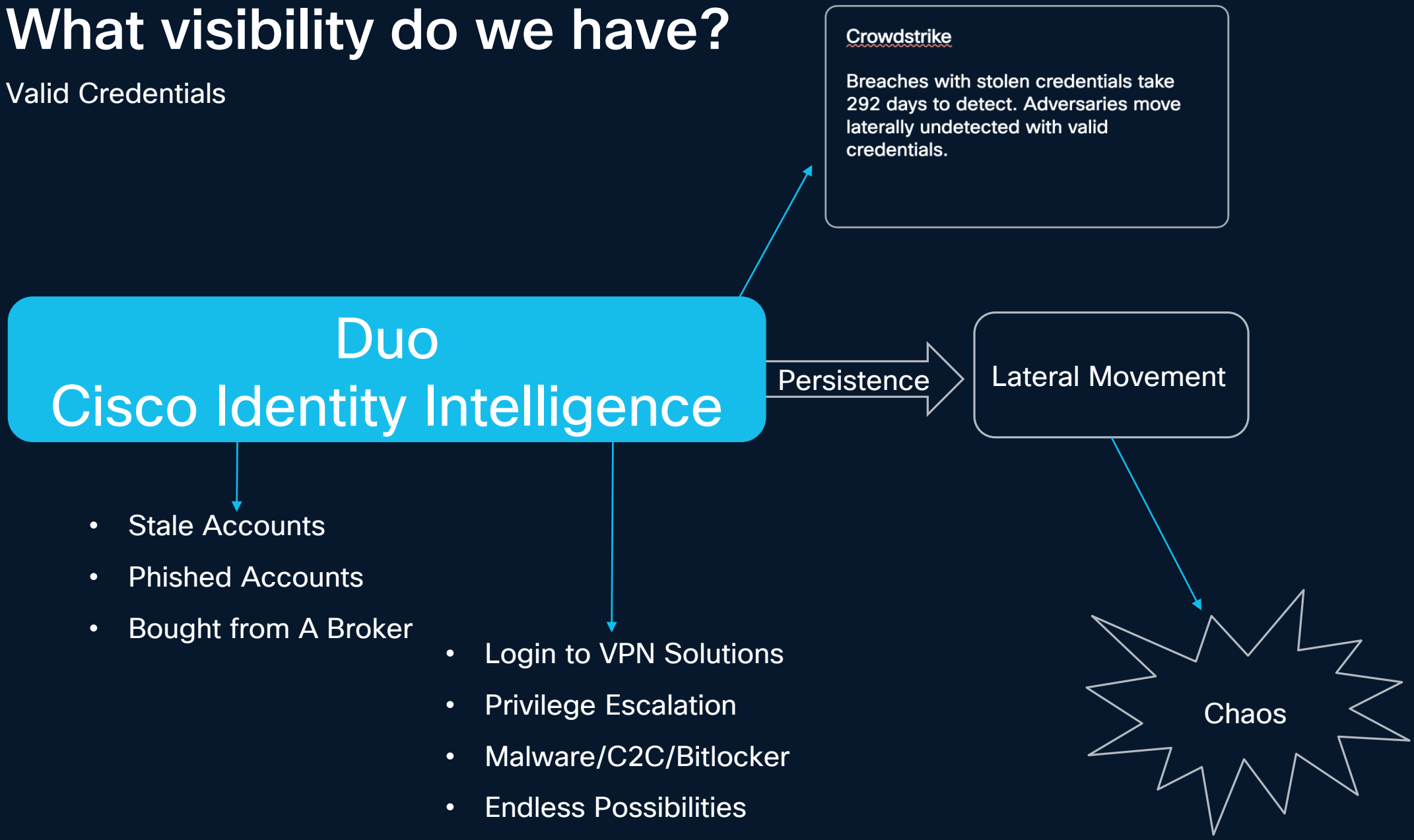
Valid Credentials



Blue Team

What visibility do we have?

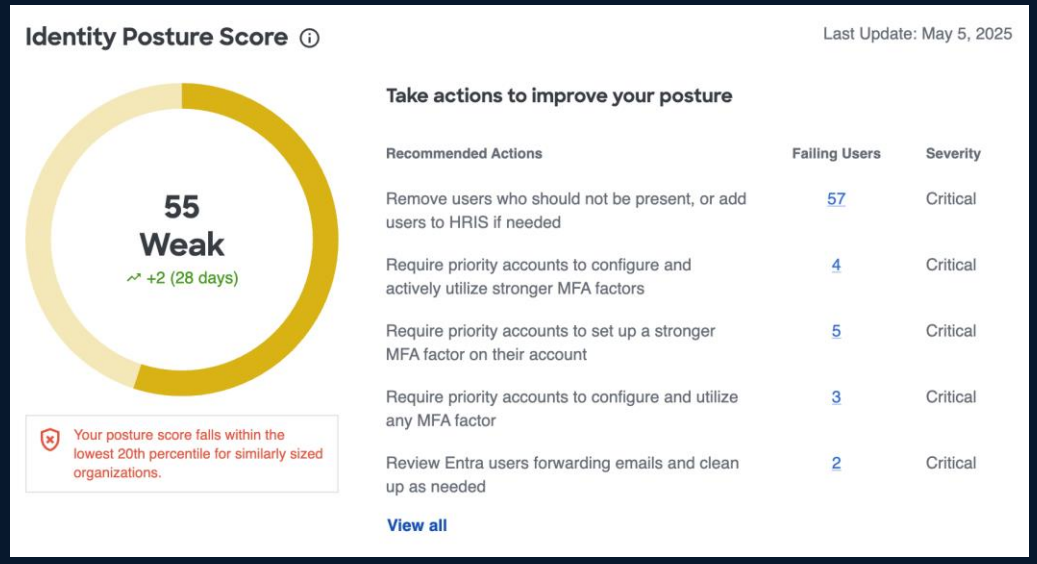
Valid Credentials

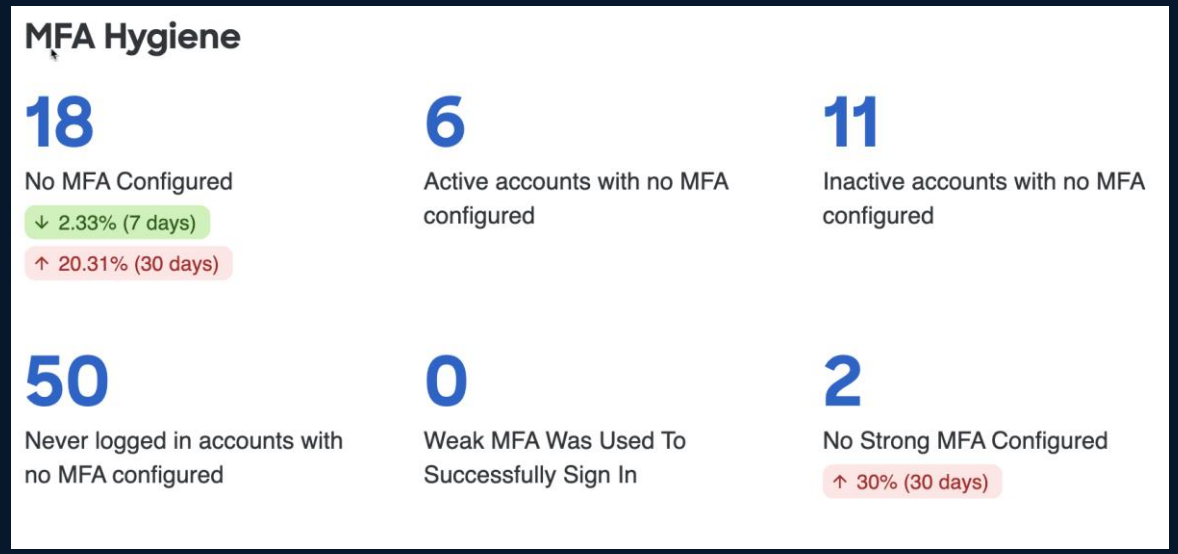


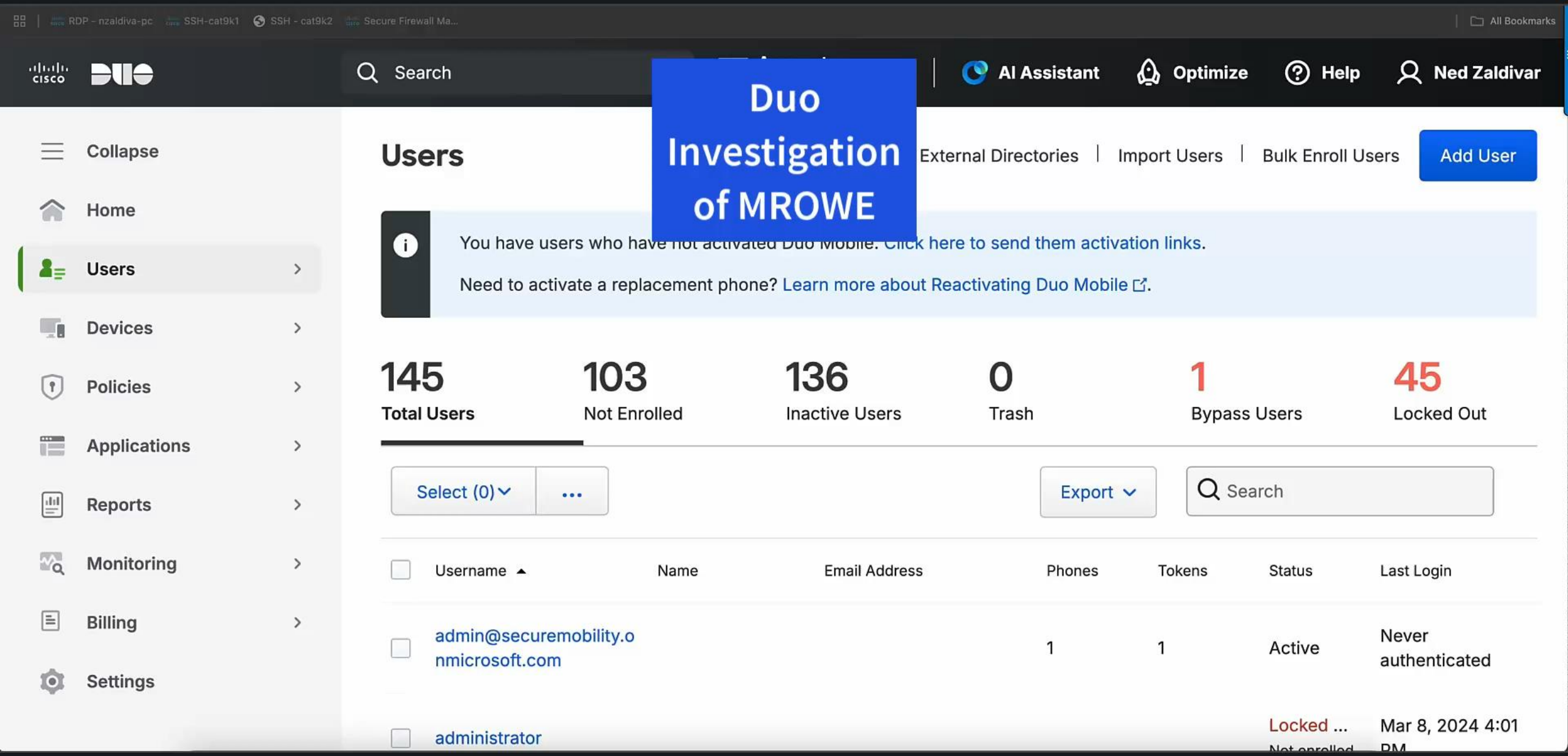
Reference

What is Cisco Identity Intelligence

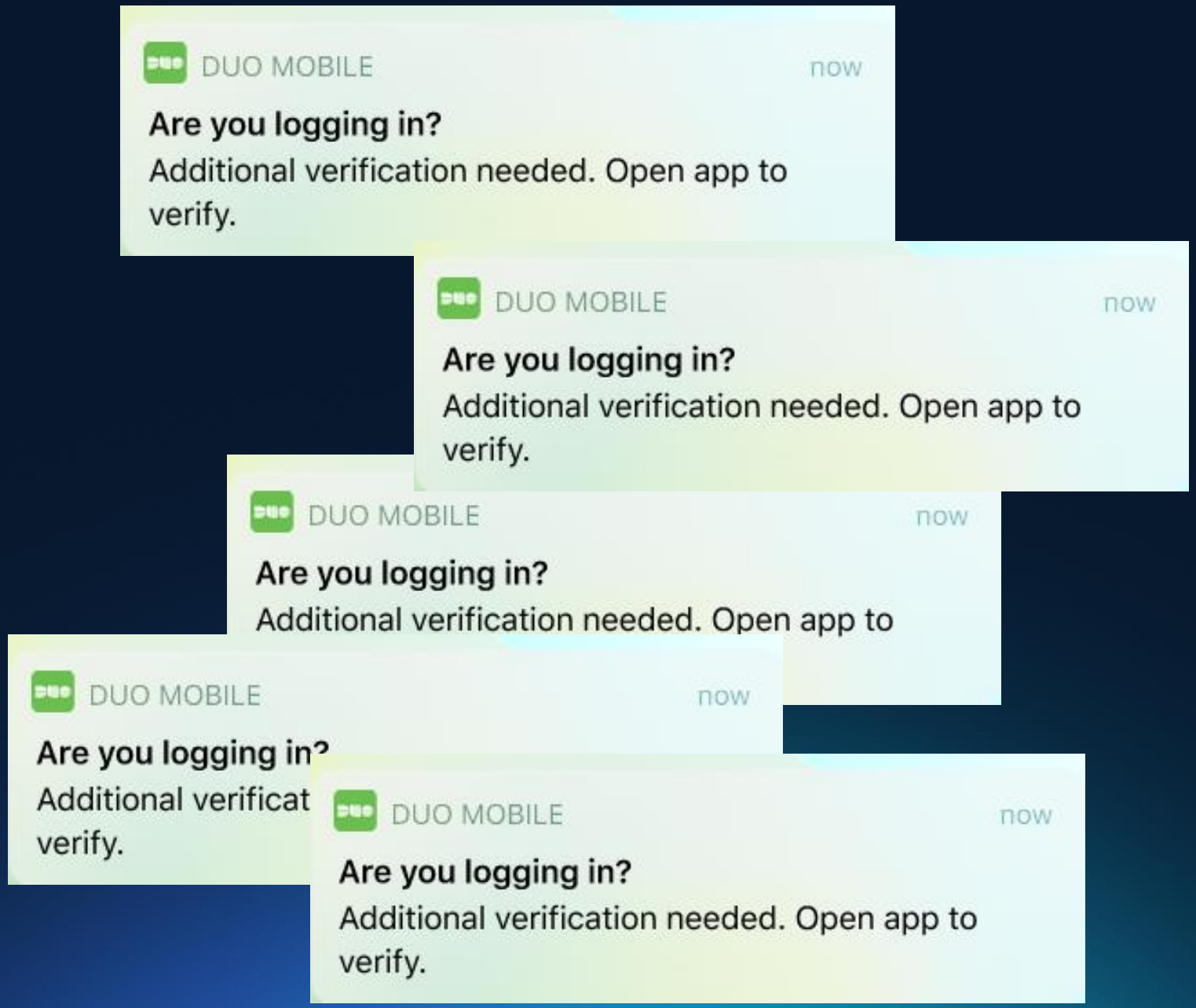
- Identity Threat Detection Response
- Aggregates multiple Identity Sources
- Identity Posture
- MFA Hygiene
- MFA Threats
- User, Device and Application Inventory
- SaaS

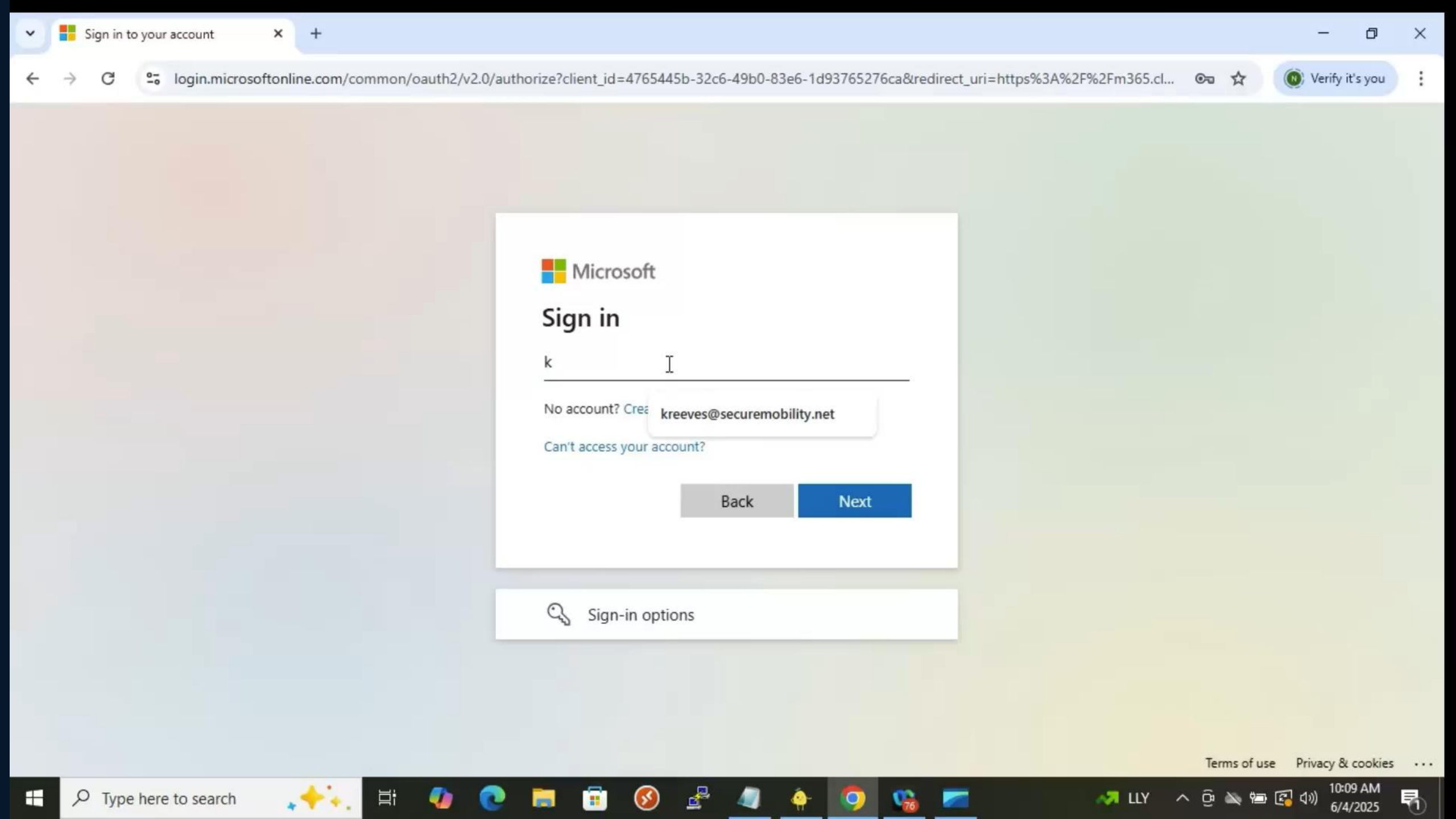





RDP - nzaldiva-pc
SSH-cat9k1
SSH - cat9k2
Secure Firewall Ma...
All Bookmarks
Search
AI Assistant
Optimize
Help
Ned Zaldivar
Duo Investigation of MROWE
Collapse
Home
Users
Devices
Policies
Applications
Reports
Monitoring
Billing
Settings
Users
External Directories
Import Users
Bulk Enroll Users
Add User
You have users who have not activated Duo Mobile. Click here to send them activation links.
Need to activate a replacement phone? Learn more about Reactivating Duo Mobile.
145 Total Users
103 Not Enrolled
136 Inactive Users
0 Trash
1 Bypass Users
45 Locked Out
Select (0)
Export
Search
Username
Name
Email Address
Phones
Tokens
Status
Last Login
admin@securemobility.onmicrosoft.com
1
1
Active
Never authenticated
administrator
Locked ...
Mar 8, 2024 4:01 PM

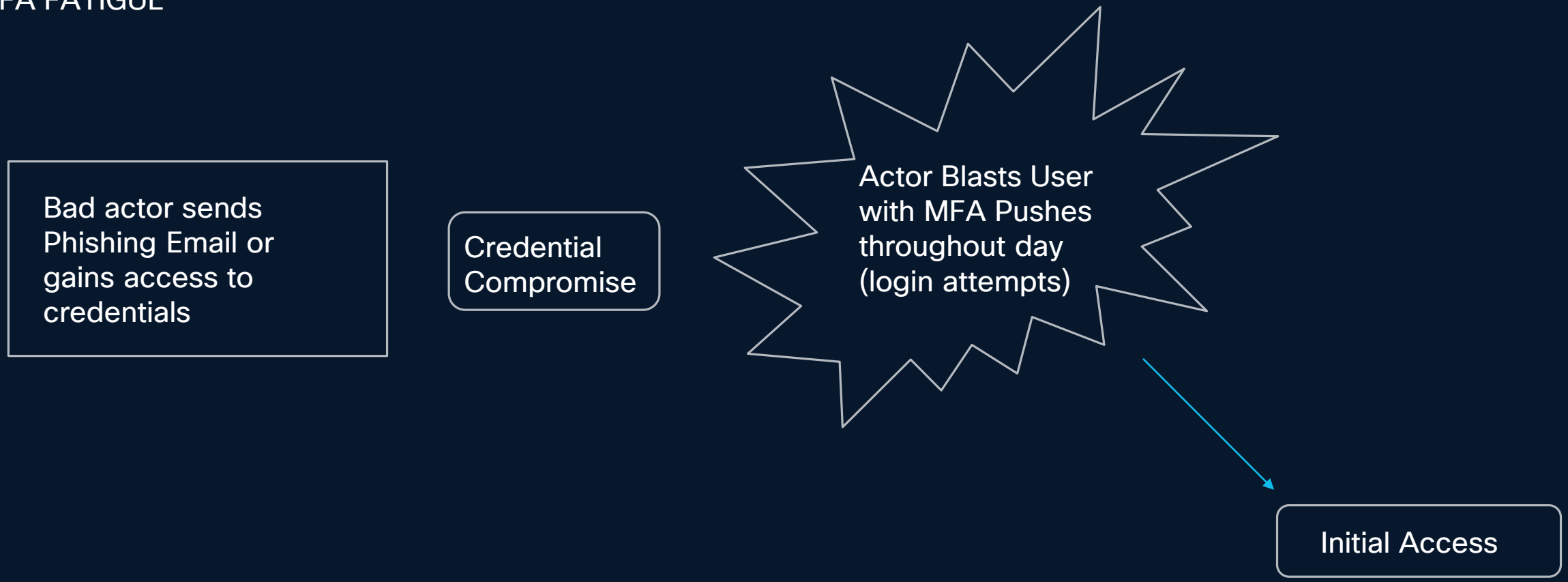
MFA Fatigue and other Weak MFA Authentications: SMS and Phone



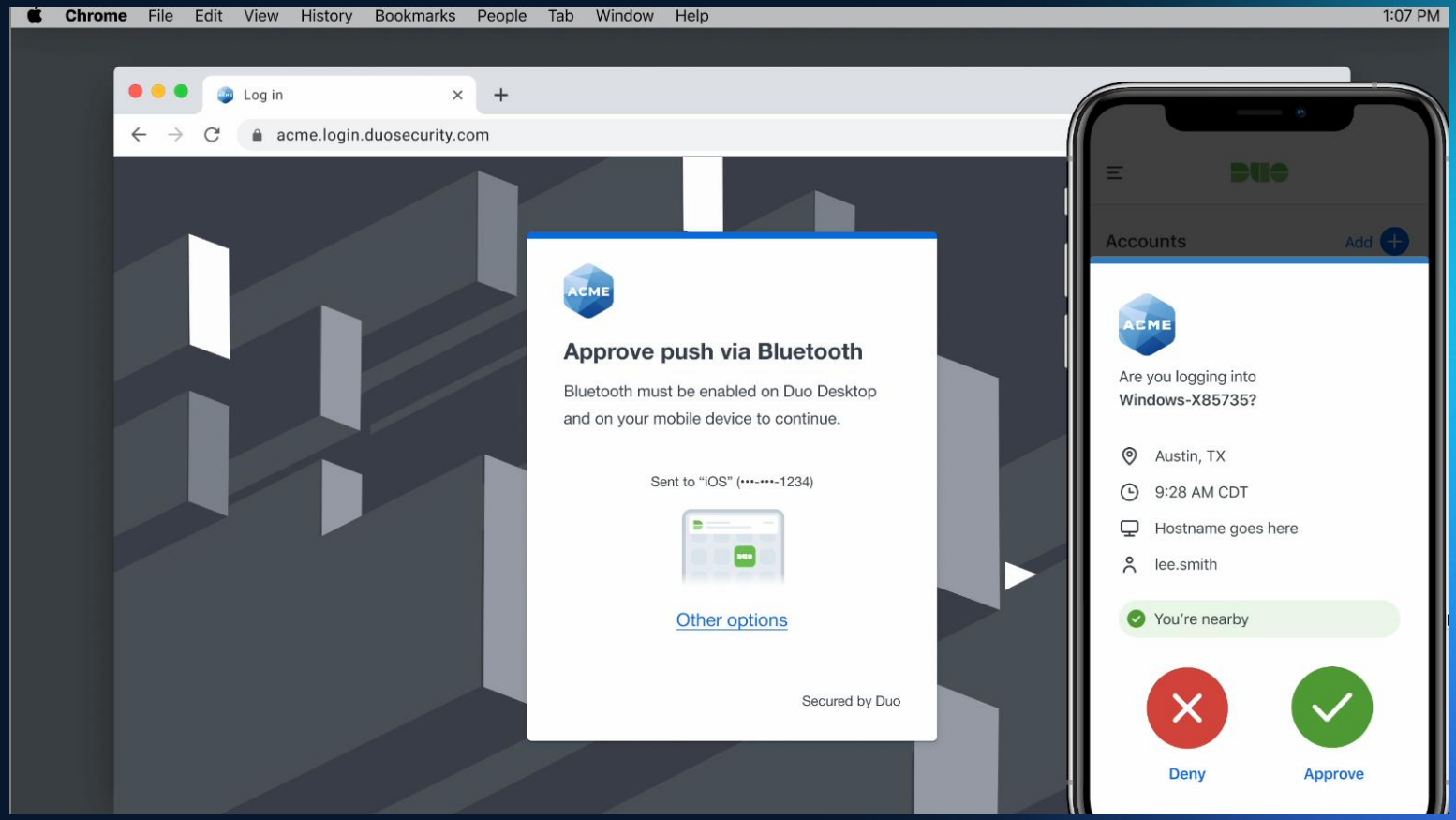

Sign in to your account
login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fm365.cl...
Verify it's you
Microsoft
Sign in
k
No account? Crea
kreeves@securemobility.net
Can't access your account?
Back
Next
Sign-in options
Terms of use
Privacy & cookies
Type here to search
LLY
10:09 AM
6/4/2025

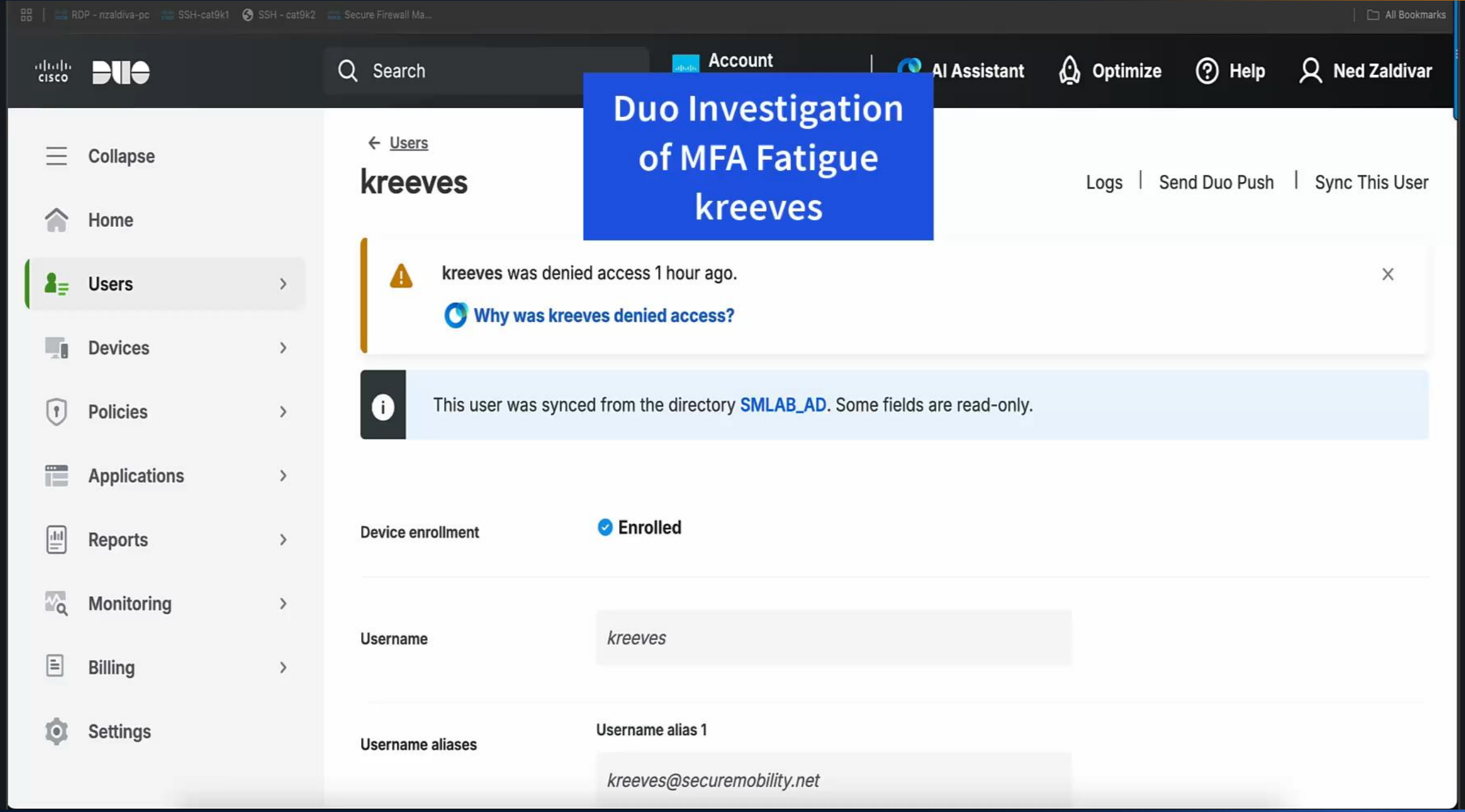
Anatomy of Attack

MFA FATIGUE



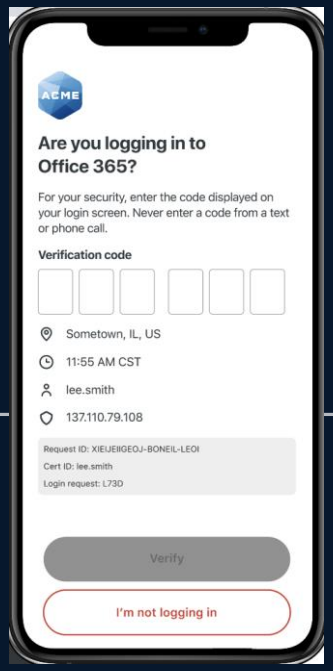
Blue Team for MFA Fatigue



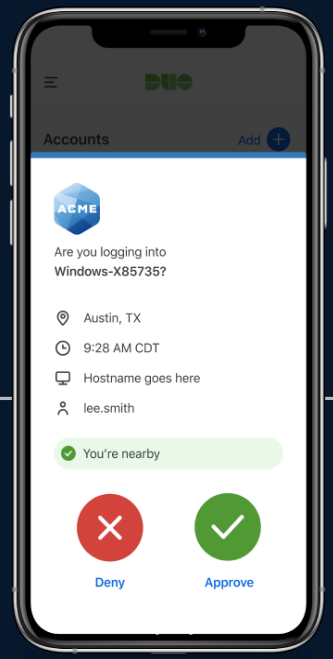

RDP - nzaldiva-pc
SSH-cat9k1
SSH - cat9k2
Secure Firewall Ma...
All Bookmarks
Search
Account
AI Assistant
Optimize
Help
Ned Zaldivar
Duo Investigation of MFA Fatigue kreeves
Collapse
Home
Users
Devices
Policies
Applications
Reports
Monitoring
Billing
Settings
Users
kreeves
Logs
Send Duo Push
Sync This User
kreeves was denied access 1 hour ago.
Why was kreeves denied access?
This user was synced from the directory SMLAB_AD. Some fields are read-only.
Device enrollment
Enrolled
Username
kreeves
Username aliases
Username alias 1
kreeves@securemobility.net

Tools/Features Used:

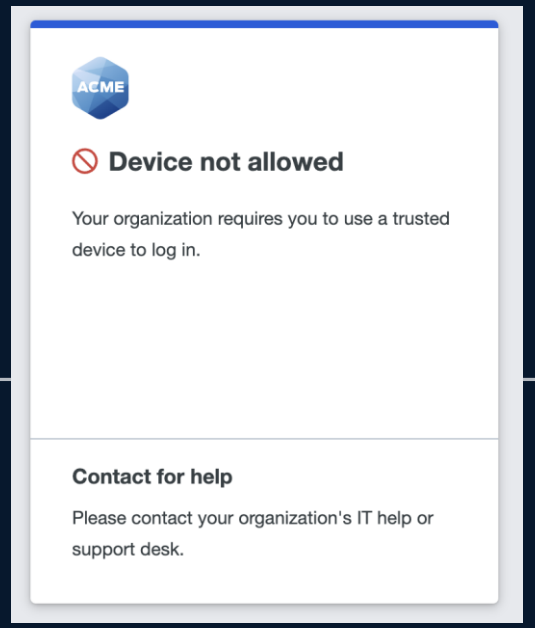
MFA Fatigue



Verified Push



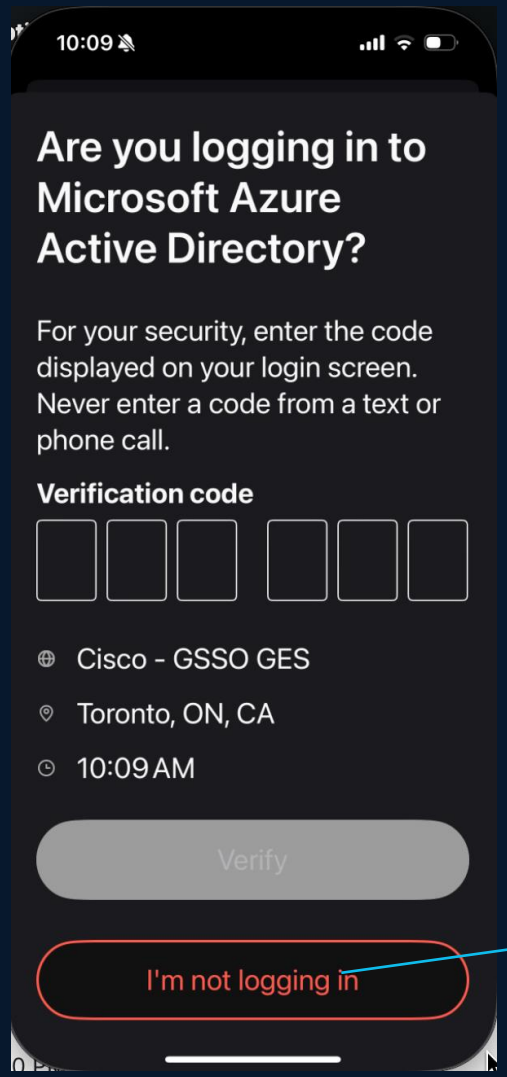
Duo Mobile Proximity Verification

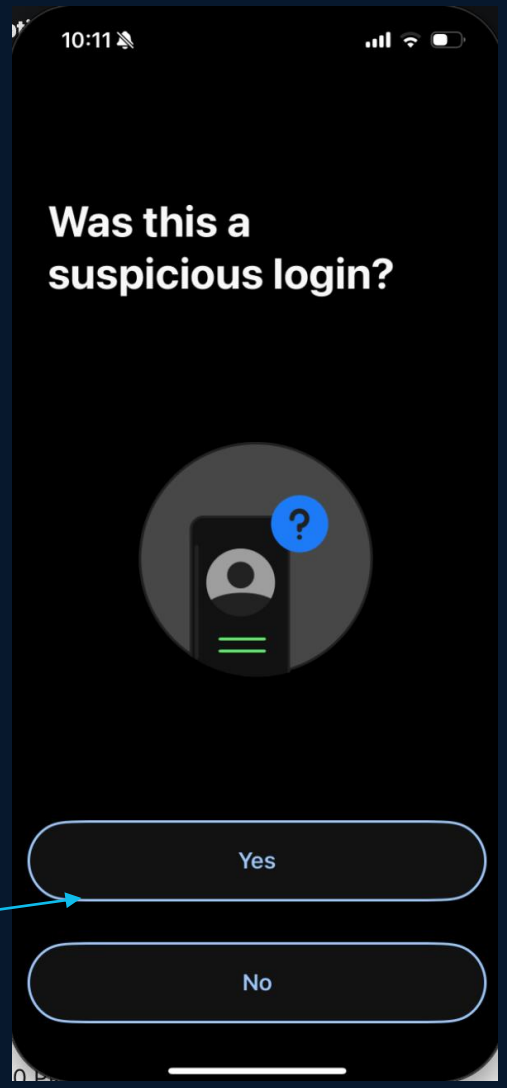


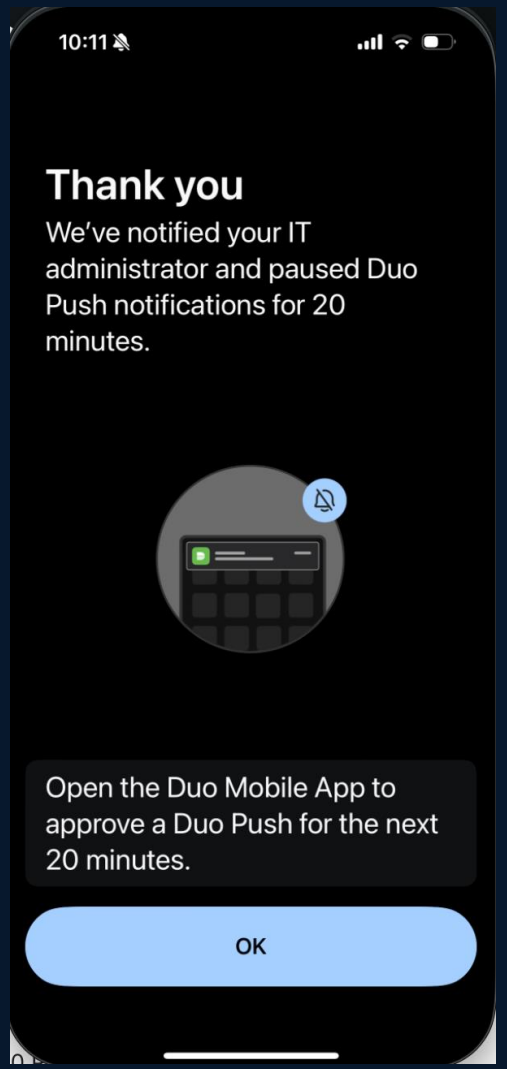
Trusted Device

MFA Fatigue – Verified Push (Code enabled)

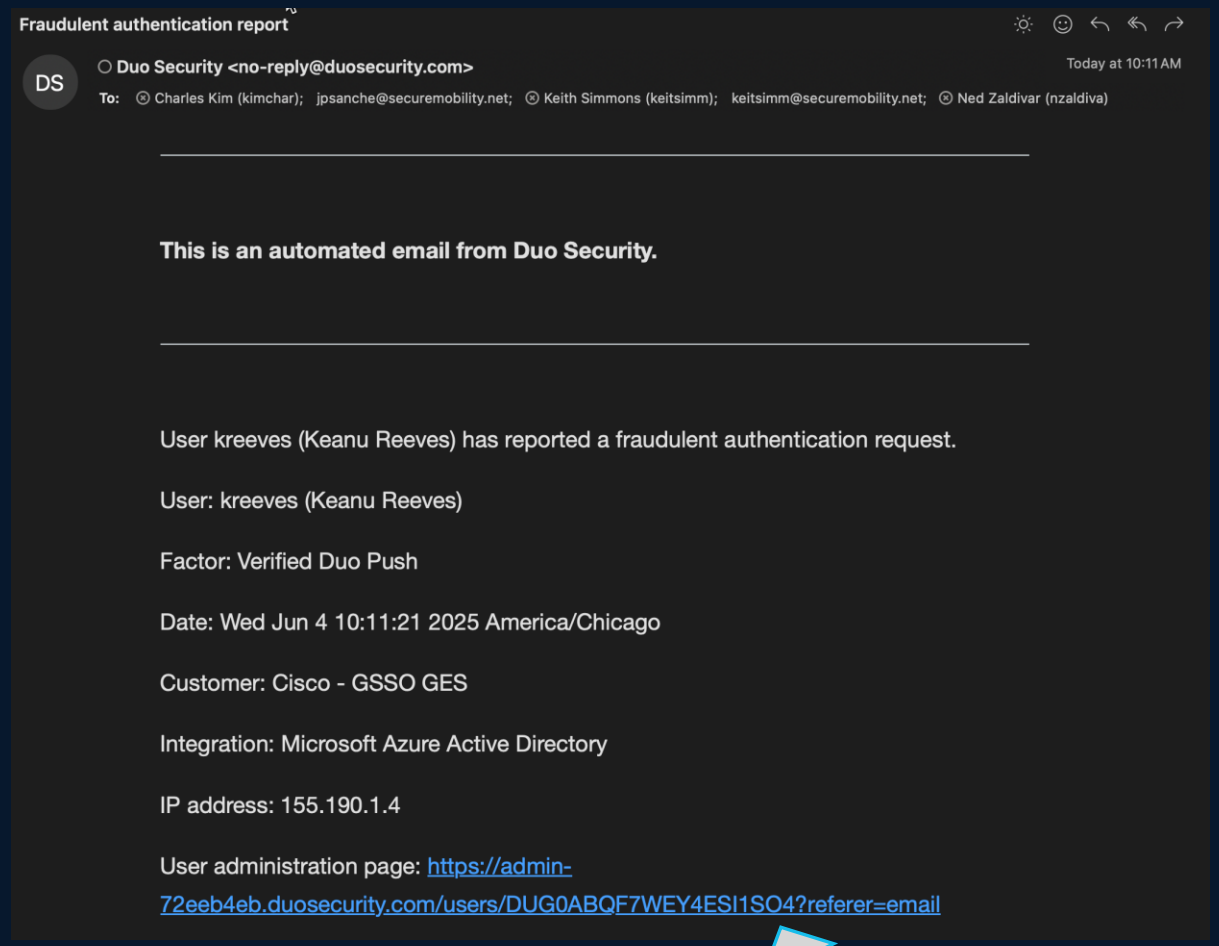
Suspicious login available across all options







Fraudulent Report + User Lockout Examples



Fraudulent authentication report

DS

Duo Security <no-reply@duosecurity.com>

Today at 10:11 AM

To: Charles Kim (kimchar); jpsanche@securemobility.net; Keith Simmons (keitsimm); keitsimm@securemobility.net; Ned Zaldivar (nzaldiva)

This is an automated email from Duo Security.

User kreeves (Keanu Reeves) has reported a fraudulent authentication request.

User: kreeves (Keanu Reeves)

Factor: Verified Duo Push

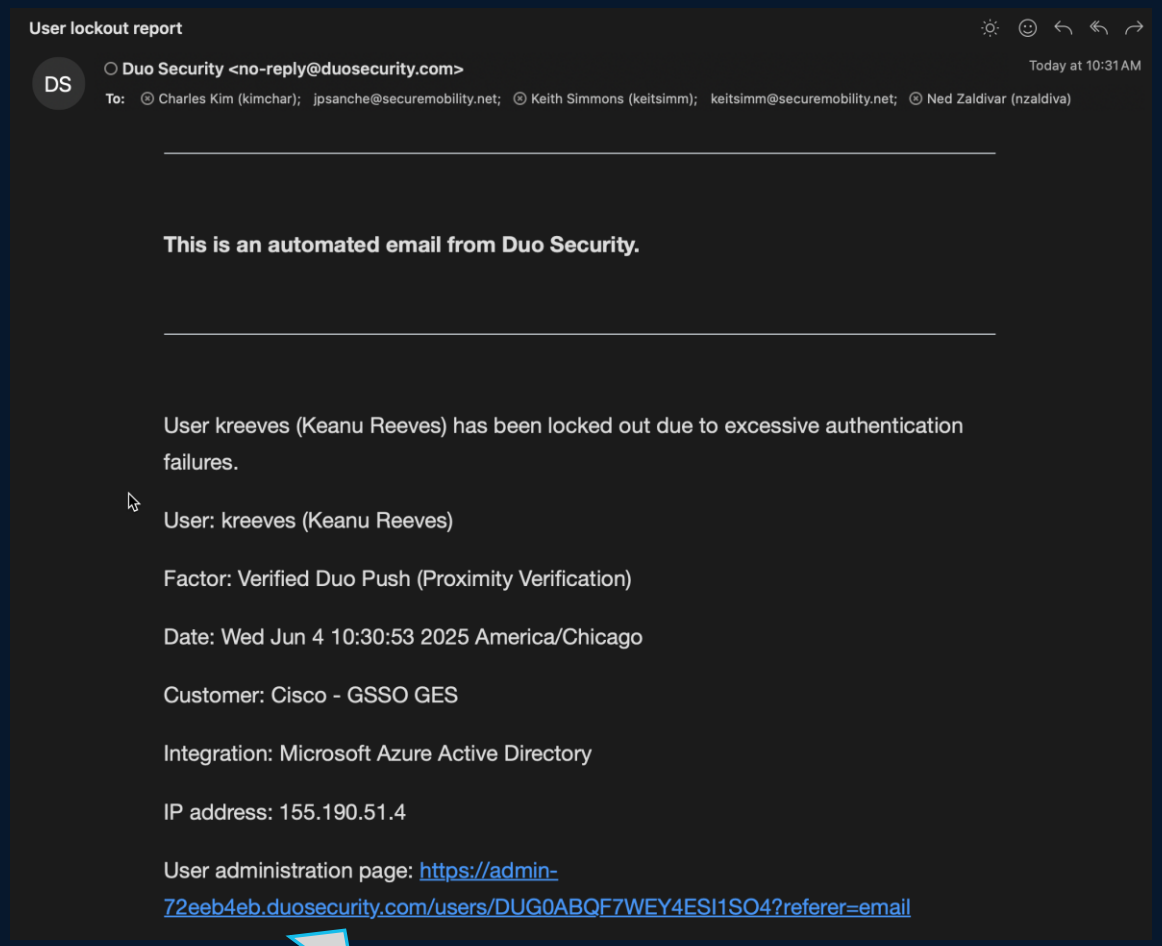
Date: Wed Jun 4 10:11:21 2025 America/Chicago

Customer: Cisco - GSSO GES

Integration: Microsoft Azure Active Directory

IP address: 155.190.1.4

User administration page: https://admin-72eeb4eb.duosecurity.com/users/DUG0ABQF7WEY4ESI1SO4?referer=email



User lockout report

DS

Duo Security <no-reply@duosecurity.com>

Today at 10:31 AM

To: Charles Kim (kimchar); jpsanche@securemobility.net; Keith Simmons (keitsimm); keitsimm@securemobility.net; Ned Zaldivar (nzaldiva)

This is an automated email from Duo Security.

User kreeves (Keanu Reeves) has been locked out due to excessive authentication failures.

User: kreeves (Keanu Reeves)

Factor: Verified Duo Push (Proximity Verification)

Date: Wed Jun 4 10:30:53 2025 America/Chicago

Customer: Cisco - GSSO GES

Integration: Microsoft Azure Active Directory

IP address: 155.190.51.4

User administration page: https://admin-72eeb4eb.duosecurity.com/users/DUG0ABQF7WEY4ESI1SO4?referer=email

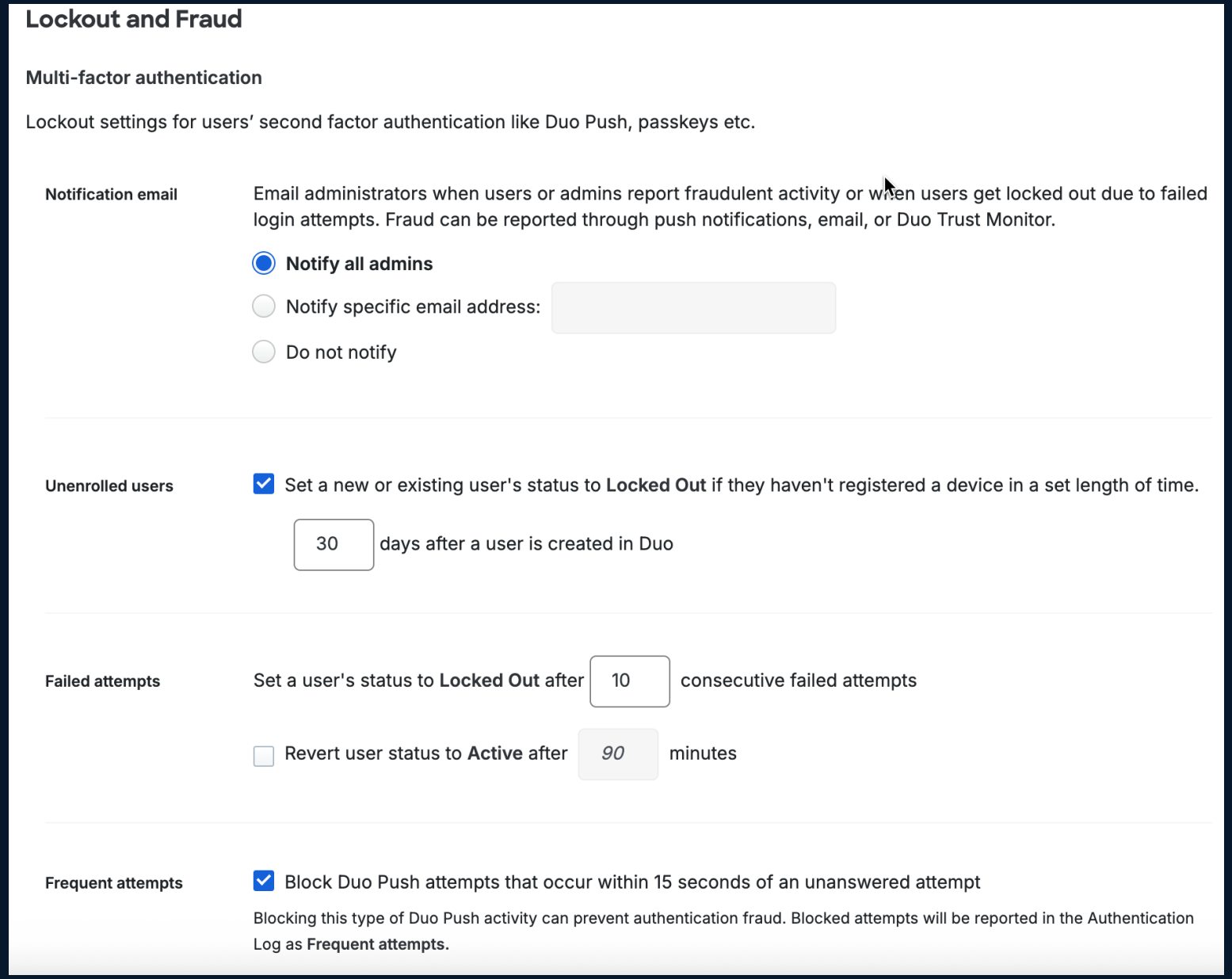
Link to admin portal to start investigation

Duo Policy Options

Notification of Fraud

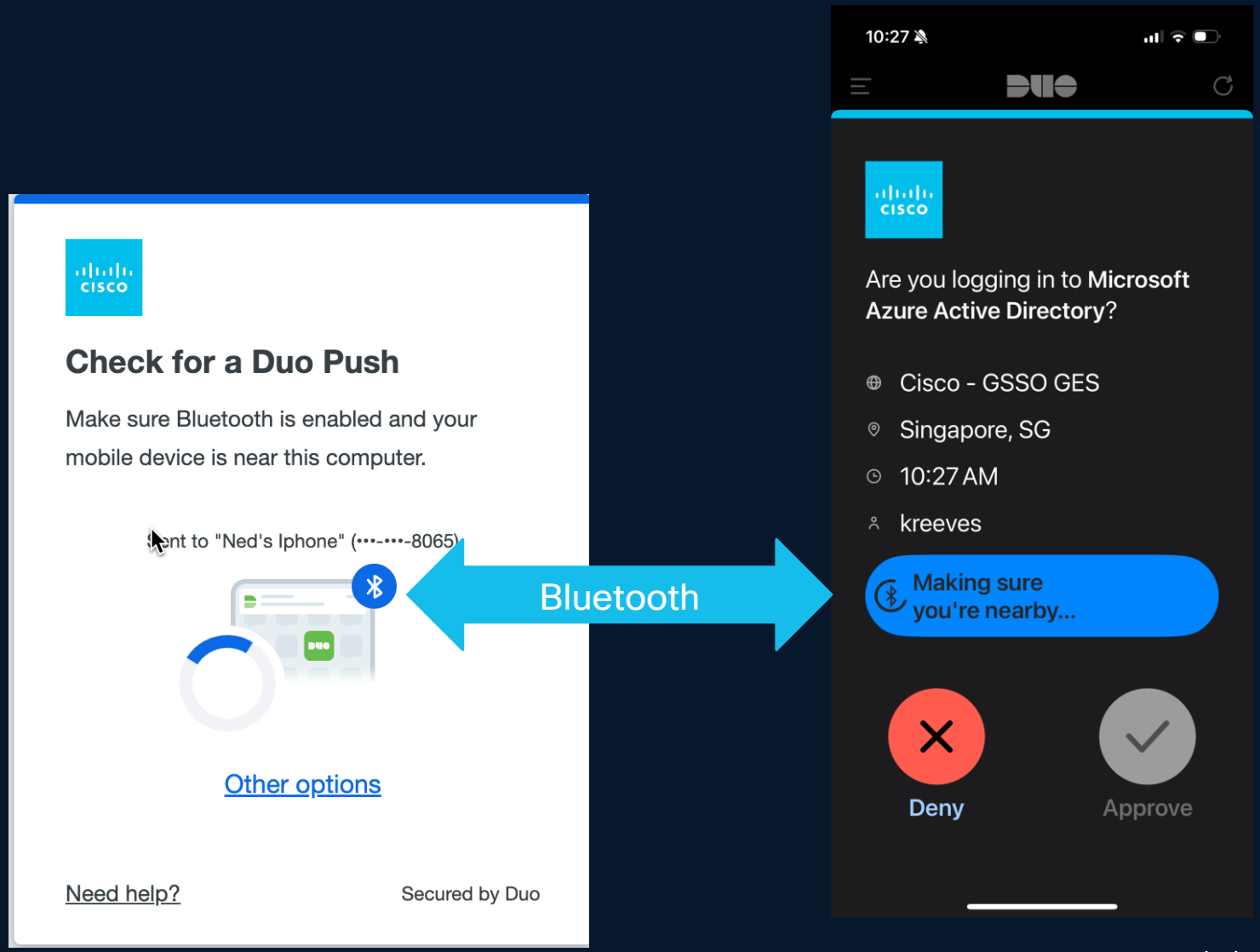
Other Lockout and Fraud settings

- Unenrolled users
- Failed Attempts
- Frequent Attempts



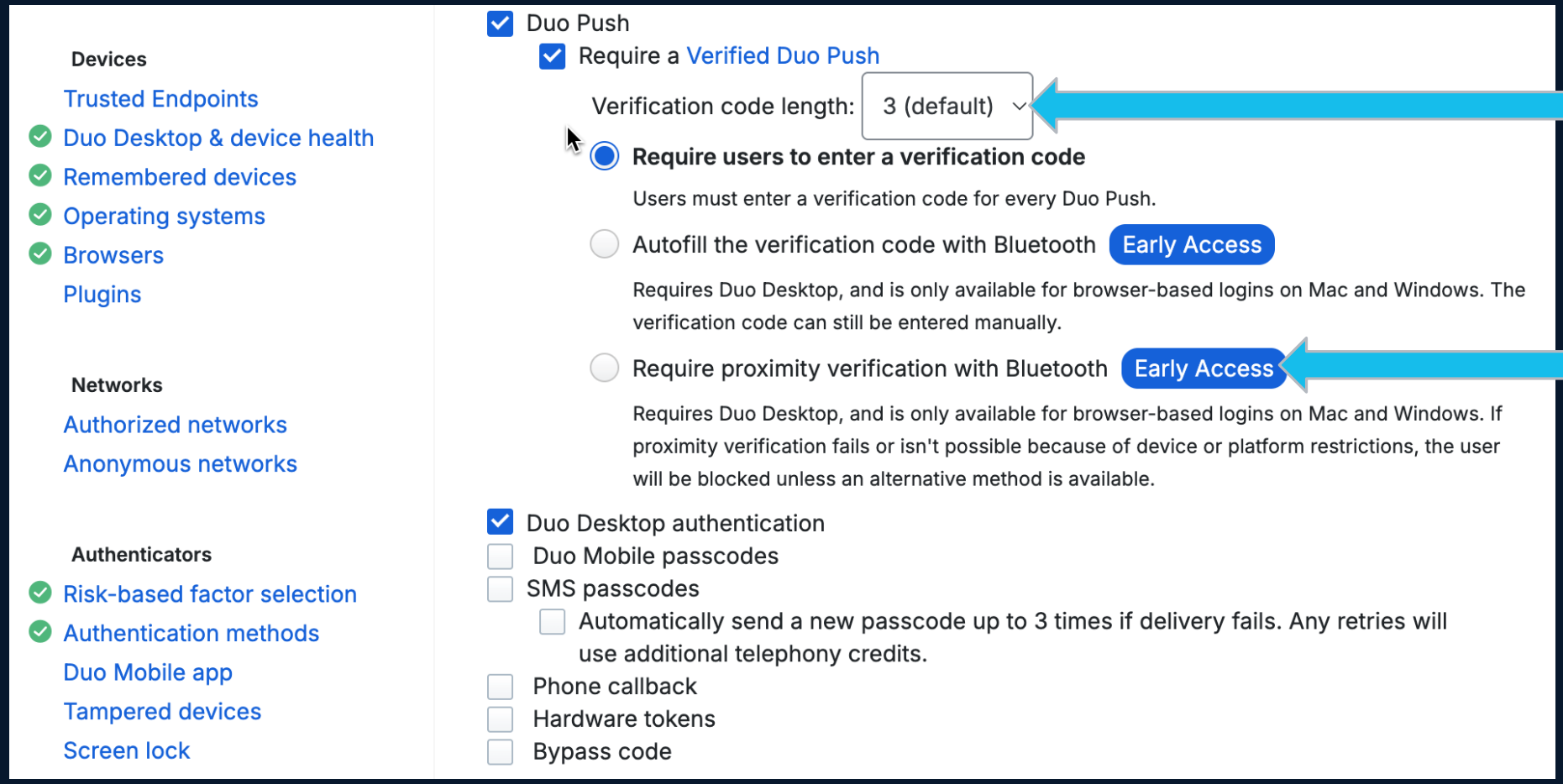
MFA Fatigue – Verified Push with Proximity (patent pending)

- End user cannot approve
- Attacker Authentication not in Bluetooth Range of Authenticator
- Eliminates the human error



Universal Prompt from Authentication

Duo Policy Options for MFA Fatigue

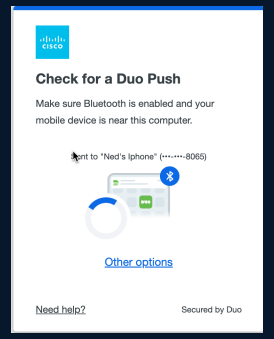


Verified Push with Code

Verified Push with Proximity

How Trusted Device Verification Works With Duo Desktop (Win/macOS/Linux)

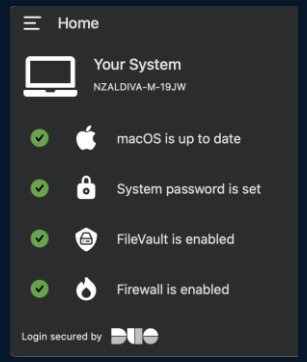
Authentication from Windows,MacOS, Linux Device



Duo

Policy Settings include Trusted Endpoints

Duo Desktop



3rd Party Device Mgmt

Duo matches the device information reported by Duo Desktop with managed device information obtained from Intune, Jamf... via API. Other methods, Chrome DTC, Edge DTC, Duo Mobile

https://duo.com/docs/trusted-endpoints

Microsoft | Microsoft 365 Outlook P ns and pricing More Buy now Sign in

Untrusted Device

Outlook for everyday email and calendars

Stay on top of multiple accounts with email, calendars, and contacts in one place. Available on desktop, mobile, and web.

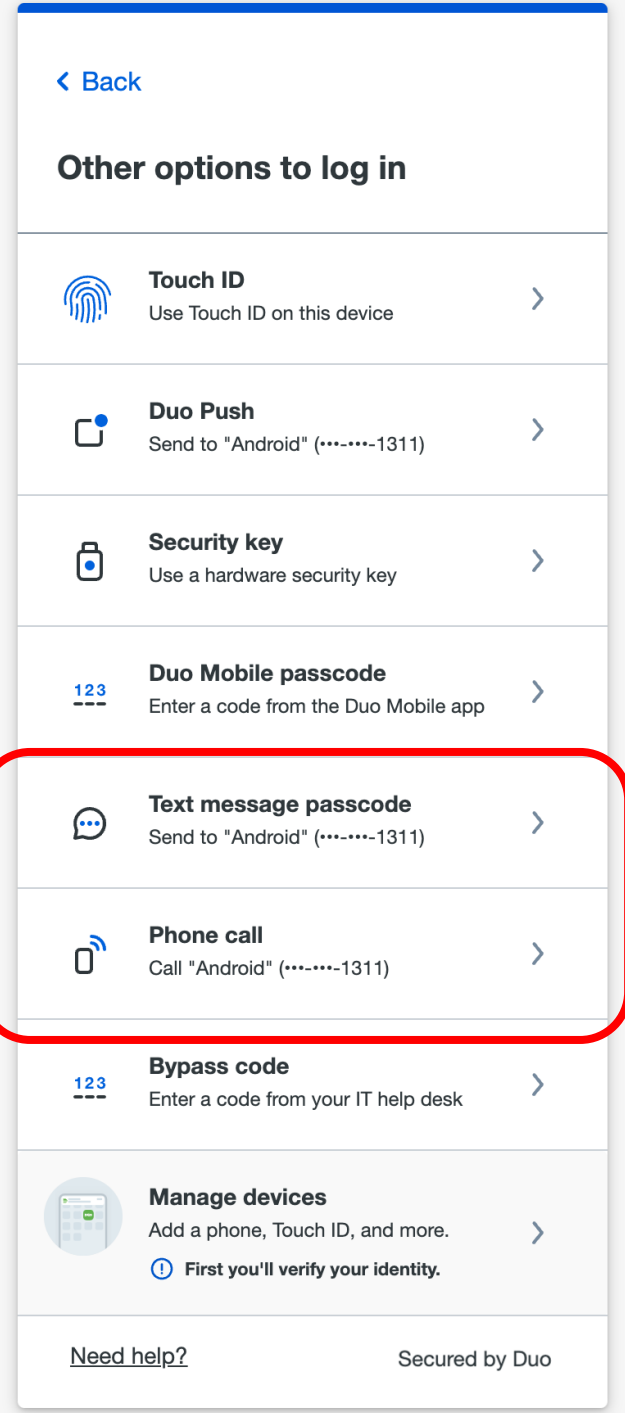
Sign in | Create free account

See plans and pricing

Phone / SMS MFA is Insecure

- Interception (sms) SS7/Network Vulnerabilities, Phone Malware
- Not Encrypted (sms) – RCS and iMessage are encrypted as well as other 3rd party messaging apps.
- Sim Swapping (both) – Getting your phone linked to an existing account
- Social Engineering (both)

How to protect?
- Who is using it?
  - Duo Reporting
  - Cisco Identity Intelligence-> across all identities
- Policy Changes
  - Disable both SMS and Phone
  - Turn off inline enrollment -> https://help.duo.com/s/article/7769?language=en_US



Summary

- Identity Attacks are going to happen
- These attacks are well known, but take diligence to mitigate

- Visibility is key!
- For Threat & Compliance

- MFA is not a checkbox activity
- MFA is a must not just for critical apps, but all applications
- MFA Phishing Resistance is a must

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education

Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

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

Contact me at: nconroy@cisco.com nzaldiva@cisco.com

Cisco Live US Identity Security Learning Map

Sunday–8th

TECSEC-2013 2:00PM
Identity Zero to Hero: Understanding the Identity Security Space and Modern Auth

Monday–9th

BRKSEC-2100 8:00AM
ISE Your Meraki Network with Group Based Adaptive Policy

BRKSEC-1017 8:00AM
Achieving Industry Standards, Frameworks and Architectures Using Duo

BRKSEC-2096 8:00AM
Securing Industrial Networks: Where Do I Start?

BRKSEC-2144 9:00AM
Modern Authentication Explained to the Network Professional

BRKSEC-1383 9:30AM
Securing the Olympics: The Cybersecurity Architecture for Paris 2024

BRKSEC-2416 1:30PM
Cisco ISE Meets Azure Cloud. Deploy, Automate, Integrate with Entra ID and Intune

Tuesday–10th

BRKSEC-2880 2:00PM
Identity Under Siege: Strategies for Today's Threats

BRKSEC-2082 3:00PM
Breaking the Identity Provider Mold with Duo!

BRKSEC-2162 4:00PM
Identity Intelligence Demystified

BRKSEC-2347 4:00PM
ISE Deployment Improvements - Tips and Tricks

Wednesday–11th

BRKSEC-2164 01:30PM
Identity Based Attacks, a Red Team/Blue Team Experience

BRKSEC-3707 01:30PM
Advanced SGT - Multi Domain Context

BRKSEC-2910 2:30PM
Bridging the Gap: Integrating Identity Security Across Platforms

VILSEC-1057 2:30PM
Fifteen bars of connectivity in Healthcare, powered by Jamf, Apple, and Cisco Private 5G

BRKSEC-2879 3:30PM
Duo Identity Security: Protect your users and applications with SO MUCH more than MFA!

Thursday–12th

BRKSEC-2202 9:00AM
Demystifying the World of Passkeys

BRKSEC-2660 10:30AM
Setting the Stage for ISE Deployment Success: A Guide to Effective Planning

BRKSEC-2584 10:30AM
Innovative Authentication: Beyond Passwords

BU-led sessions

Thank you


CISCO