

The background features a vibrant, abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Authentication in a New Era – Enhanced with Identity Threat Detection & Response

Modern Defense for Modern Attacks

Brian Verenkoff – WW Director, Solutions Architecture – SSE & Zero Trust
BRKSEC-2076

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

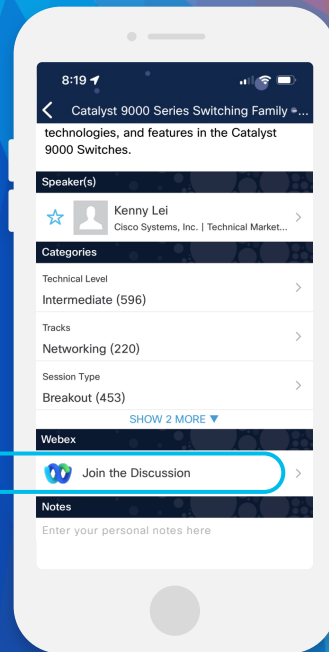
Questions?

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 December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2076>

Agenda

- New Login Breach Landscape
- Attacks Explained
- Modern Defenses
 - Improved Security
 - Improved Usability
 - Improved Visibility
- Zero Trust Demo
- Enhanced with Identity Threat Detection and Response (ITDR)
- ITDR Demo
- Closing & Q&A

Login Breaches and Attacks have Evolved

...



80% of organizations are
NOT prepared

[2023 Cisco's Cybersecurity Readiness Index](#)



2FA Compromise Led to
\$34M Crypto.com Hack



The Uber Hack Shows
Push Notification 2FA Has a
Downside: It's Too Annoying

VentureBeat

Russian hackers exploited
MFA and 'PrintNightmare'
vulnerability in NGO breach,
U.S. says



MFA Fatigue: How
Hackers Breached Uber,
Microsoft, and Cisco

IT WORLD CANADA

Oktapus phishing campaign exploit MFA
to compromise 130 companies



New Gmail Attack Bypasses
Passwords
and 2FA To Read All Email



Cybercriminals Launching
More MFA Bypass Attacks

Attacks made easy



Attack
Kits



Push
Bomb



Push
Spray



Enrollment of
Attackers' devices



OTP
Phishing

¹ Verizon Data Breach Investigations Report 2022

Targeting Cloud Applications

Scenario



Attacker obtains credentials for Cloud App

1



Attacker uses credentials to connect to Cloud App

2



Attacker uses MFA push phishing to bypass MFA

3



Attacker self-enrolls their device and set up MFA



Attacker gets access at will

Techniques Used

Valid Accounts
Gaining access using valid accounts

[MITRE ID T1078](#)

Device Registration
Register alternate devices to perform two-factor authentication (2FA)

[MITRE ID T1098.005](#)

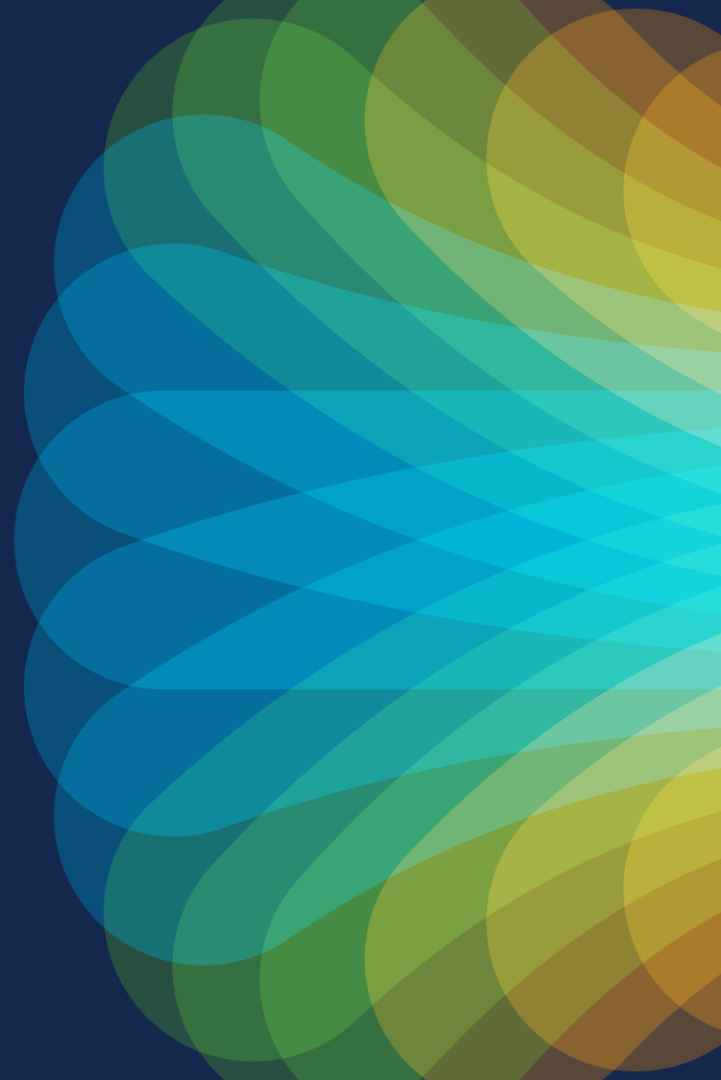
MFA Request Generation
Bypass MFA by fatiguing users with requests

[MITRE ID T1621](#)

Attacks & Defenses: Duo

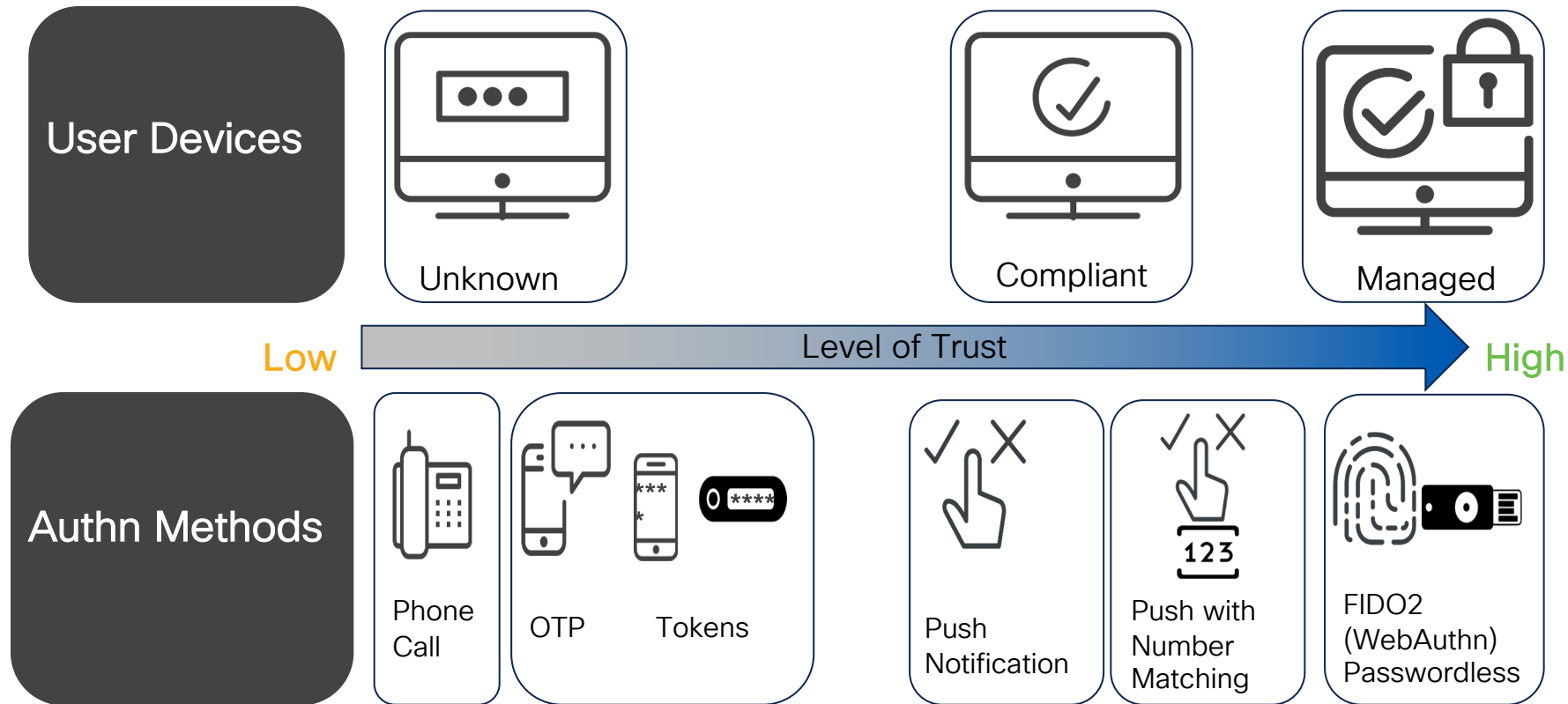


Better Security
Better User Experience
Better Visibility



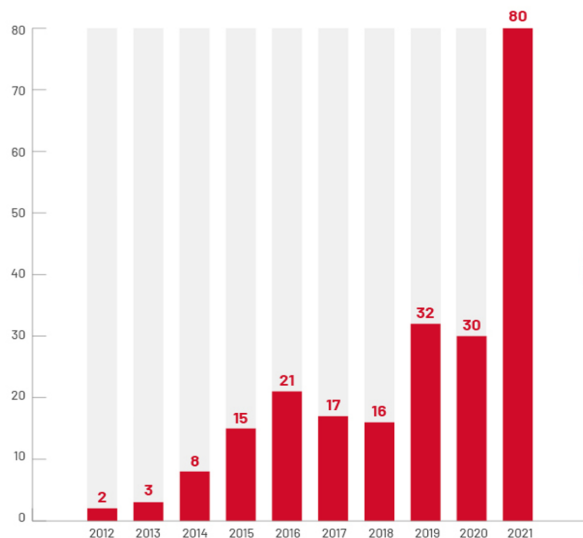
Better Security

Strengthen Authentication

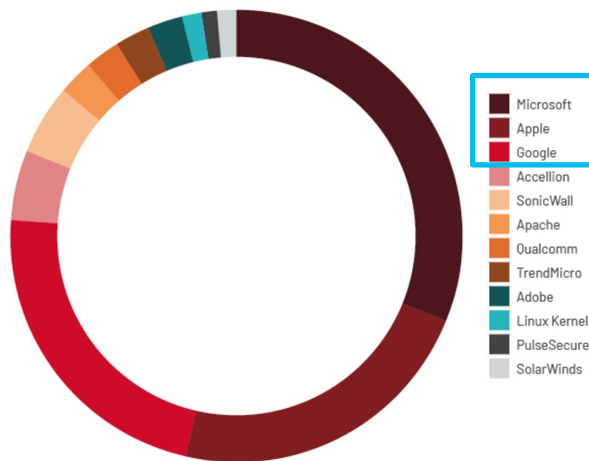


0-Day Landscape Worsening

Zero-Days Exploited
2012-2021



Vendors Targeted by Zero-Day Exploits



SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe | 2022 CISO F

SECURITY OPERATIONS SUMMIT
TUESDAY, DECEMBER 6, 2022
WATCH ON DEMAND

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Security

Home > Endpoint Security

Google Patches Ninth Chrome Zero-Day of 2022

By Ionut Arghire on December 05, 2022

[Share](#) [Tweet](#) [Recommend](#) [RSS](#)

Google on Friday announced an emergency Chrome 108 update to patch a zero-day vulnerability in the browser, the ninth to be fixed this year.

Displays the importance of a mechanism to ensure users maintain up-to-date software

Zero Trust Application Access Design

		Users Role-Based	Location	Auth Factors	Session Duration	Device Trust	OS	Browser	EDR/AV
Crown Jewel Applications	   	Privileged	Restricted	Verified Push with Biometrics OR WebAuthN	No Remembered Session	Managed Device (no BYOD)	Up-to-date Only	Chrome: Up-to-date Only	Active with Threat Intelligence
Sensitive Applications	 	Knowledge Workers	Any	Push with <u>Risk-Based</u> OR WebAuthN	<u>Risk-Based</u> Remembered Sessions	Acceptable BYOD	Grace Period if out of date	Grace Period if out of date	Active
Commodity Applications	 	All	Any	Push WebAuthN SMS OTP	Remembered Sessions	Any	Non-EOL	Grace Period if out of date	Any

Better User Experience

Broad Range of Authentication Options

- Configure authentication options for each application or group of users
- Enable multiple option for users for ease of use and flexibility



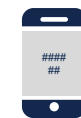
Wearables



Push



Phone
Call



Soft Token



Biometrics



U2F

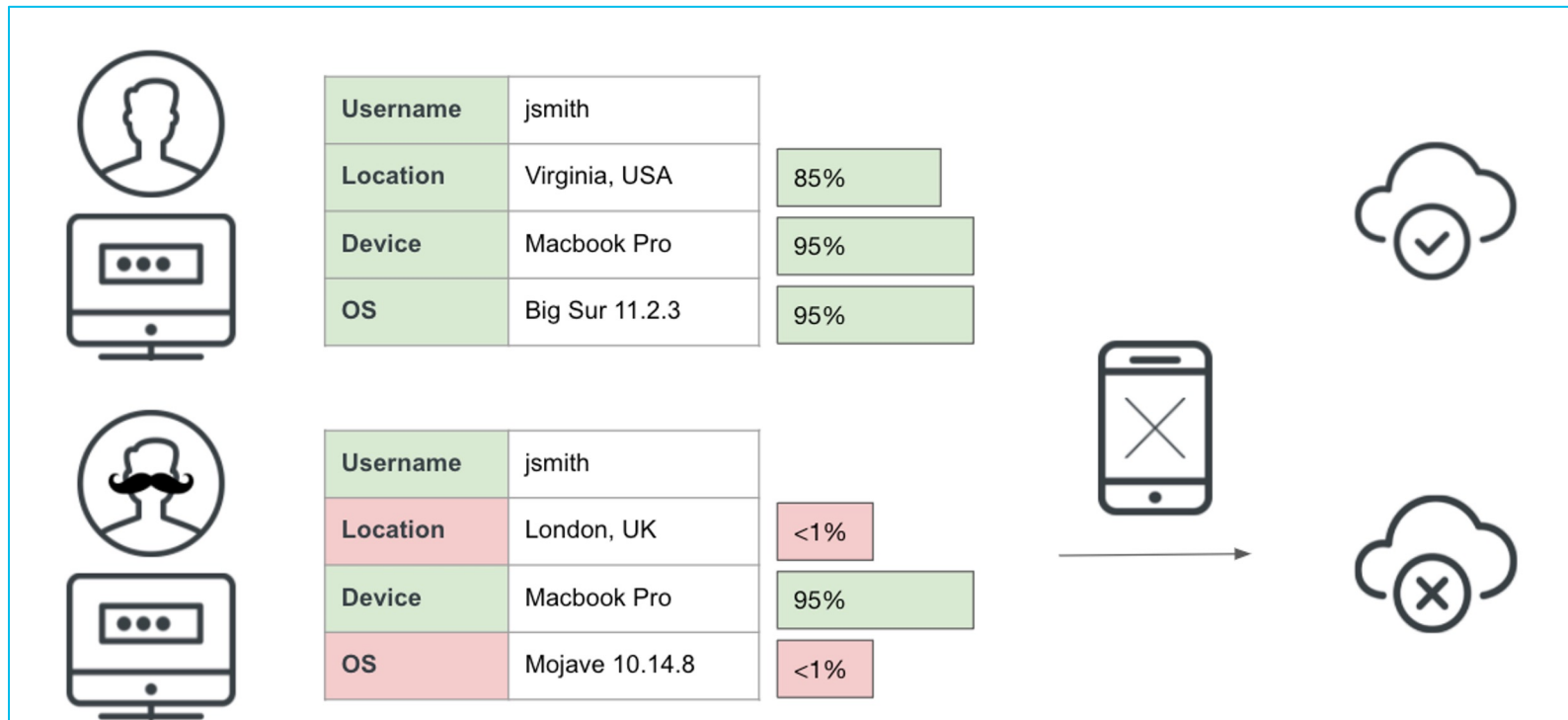


Hardware
Tokens



SMS

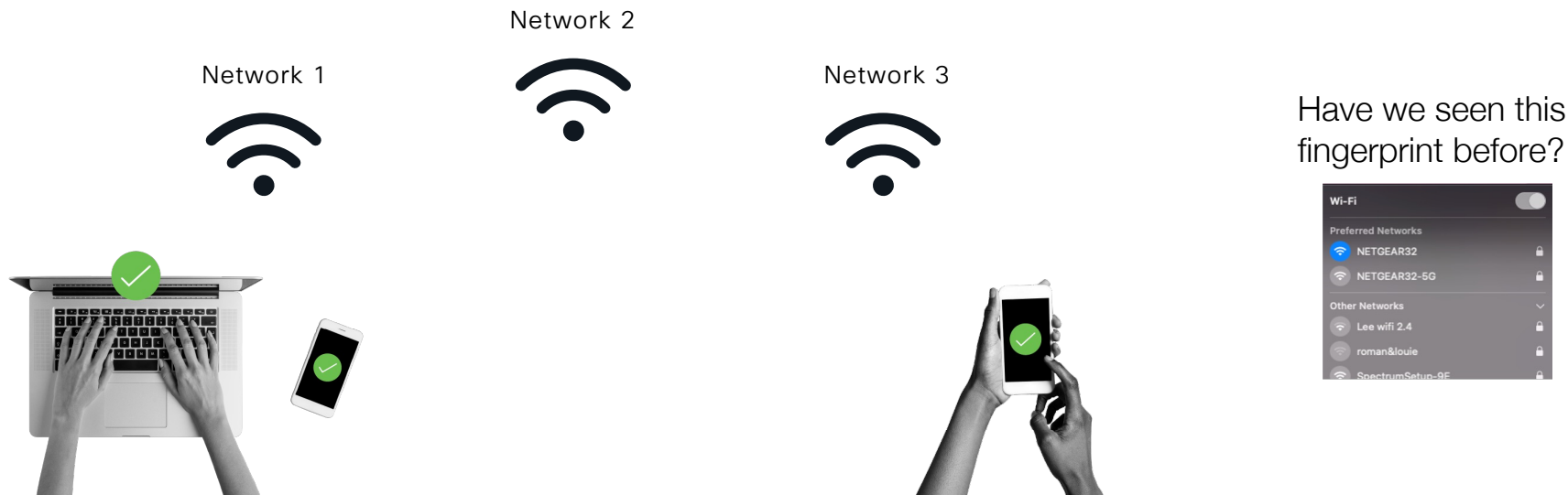
Anomaly Detection – Less Friction when "Normal"



Risk Based Authentication

Timestamp (CDT) ▼	Result	User	Application	Trust Assessment 1	Access Device	Authentication Method
3:06:28 PM OCT 4, 2022	<div>✗ Denied Country code mismatch detected with risk-based factor selection</div>	brian	Cisco Meraki	Normal	<div>Mac OS X 12.6 (21G115) As reported by Device Health Hostname BNV-Cisco Firefox 105.0 Flash Not installed Java Not installed Device Health Application Installed Firewall On Encryption On Password Set Security Agents Running: Cisco Secure Endpoint</div> <div>Zurich, ZH, Switzerland 31.7.60.211</div> <div>Not a Trusted Endpoint doesn't have a Duo certificate or the Duo certificate has expired</div>	<div>Duo Push Brian's iPhone 14 Pro (512-423-0269) DPX46KOOLWIC2KUBV41Z Austin, TX, United States 24.28.71.146</div>

Risk-Based Authentication: Wi-Fi Fingerprint



Anonymized Wi-Fi network data provides a strong risk signal.

Low Risk: Familiar network fingerprint

High Risk: Novel network fingerprint

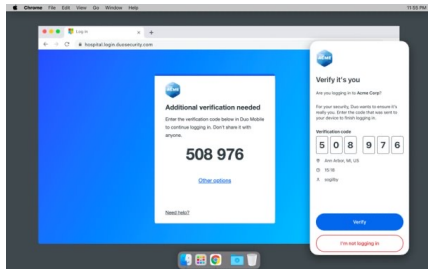
Risk Based Approach

End User Attempts Access

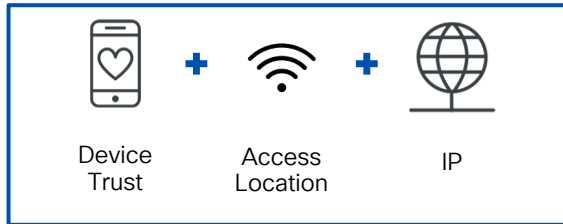


Risk-Based remembered devices
Require MFA, disable token

Risk-Based Step up authentication
Verified Push / Webauthn biometric



Verify Trust



And Adapt

Low Trust:
More Friction
for End user

Additional
verification
from end user
required

Normal Trust:
Less Friction
for End user

Regular policy
enforced

End User Gains Access



Better Visibility

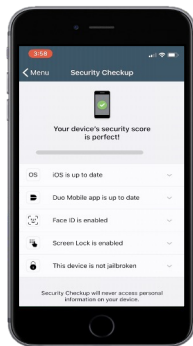


What Information to Gather?



Mobile Devices

- Corp managed asset status
- Biometrics (Touch/Face) status
- Screen lock status
- OS condition (tampered) status
- Encryption status
- Platform type
- Device OS type
- Device OS version
- Device owner
- Duo Mobile version



Laptops / Desktops

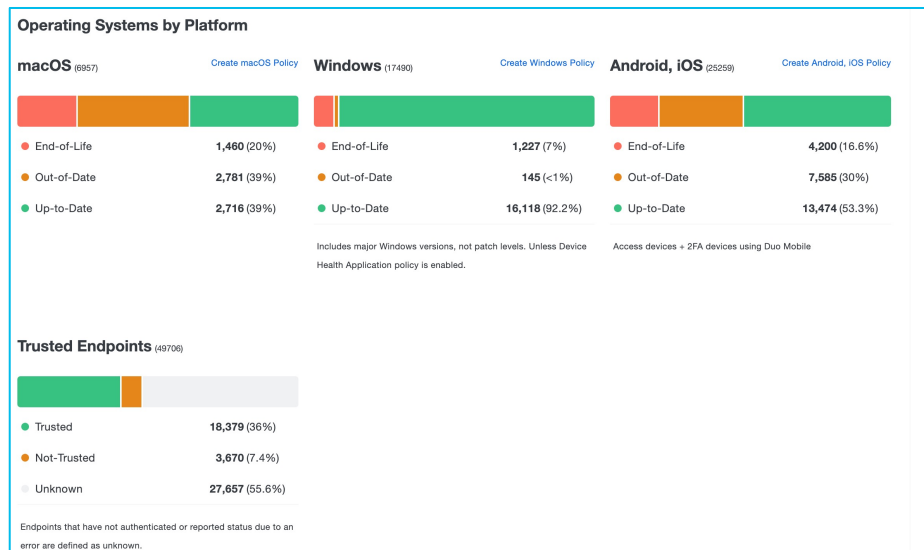
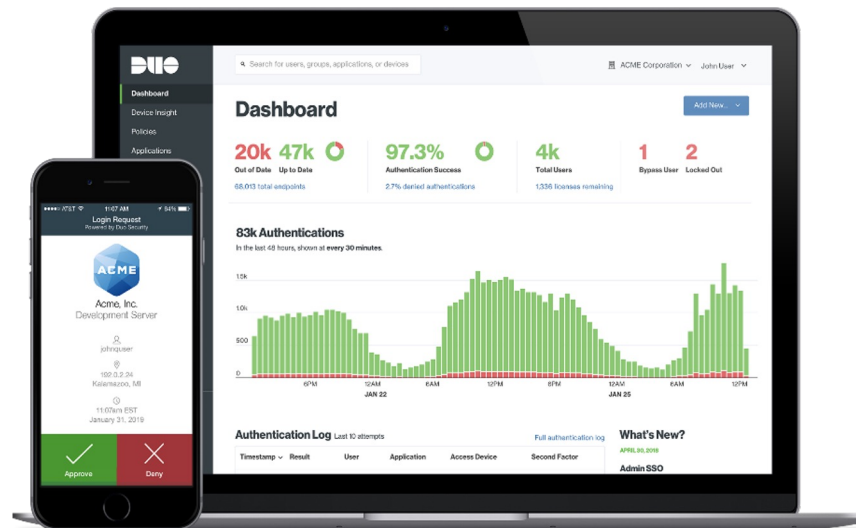
- Disk encryption
- Firewall enabled
- Device password
- OS patch level (Win 10)
- Third party agents
- Corp managed asset status*
- OS type & versions
- Browser type & versions
- Flash & Java plugins versions
- OS, browser and plugins status



[Learn more about Unified Device Visibility](#)

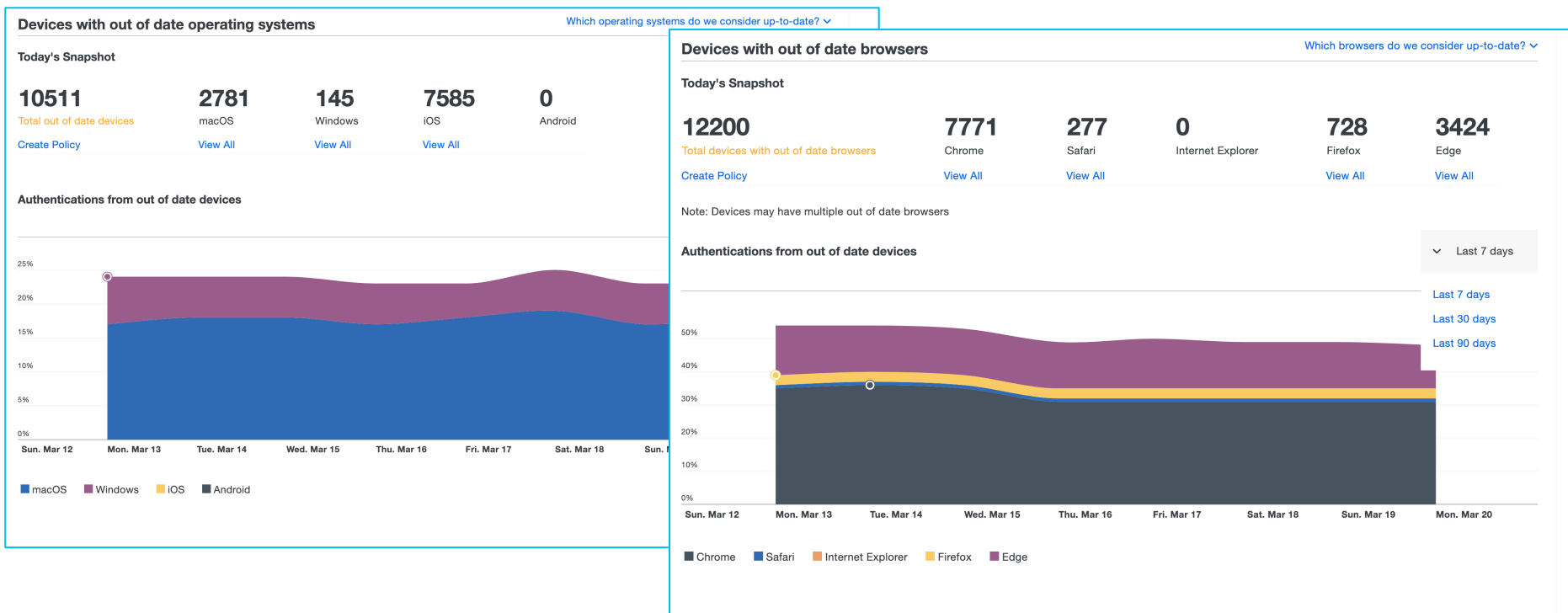
Complete Visibility

Gain complete visibility into all your devices



Complete Visibility

Gain complete visibility into all your devices



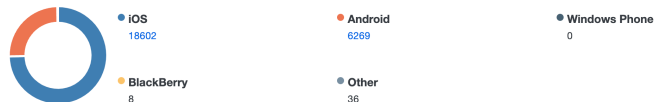
Complete Visibility

Gain complete visibility into all your devices

Mobile Devices

Device Breakdown

out of 24915 total devices



iOS

Data may be unknown for devices running versions of Duo Mobile prior to iOS 8.

Version	Devices	
Unknown	2	View devices
iOS 16.3	5565	View devices
iOS 16.2	253	View devices
iOS 16.1	824	View devices
iOS 16.0	1094	View devices
iOS 15.7	6028	View devices
iOS 15.6	503	View devices
iOS 15.5	240	View devices
iOS 15.4	534	View devices
iOS 15.3	570	View devices
iOS 15.2	500	View devices

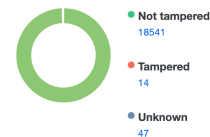
Android

Data may be unknown for devices running versions of Duo Mobile prior to 3.5.

Version	Devices	
Unknown	1	View devices
13.0	620	View devices
13	3	View devices
12.1	1	View devices
12.0	582	View devices
11.0	708	View devices
10.0	617	View devices
9.0	200	View devices
8.1	8	View devices
8.0	3527	View devices
7.1	2	View devices

Tampered

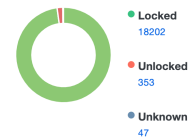
These devices may be less secure due to being jailbroken. [What is a tampered device?](#)



✓ Your global policy blocks tampered iOS and Android devices. To make changes, [edit global policy](#).

Screen Lock

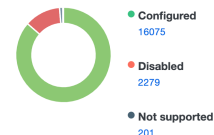
Enforcing a screen lock can help prevent against unwanted access.



✓ Your global policy blocks iOS and Android devices without a screen lock. To make changes, [edit global policy](#).

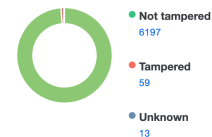
Mobile device biometrics

Fingerprint (Touch ID) and Face ID are biometric alternatives to passcodes and passwords on supported iOS devices.



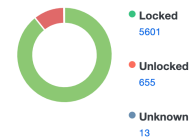
Tampered

These devices may be less secure due to being rooted or failing Google's SafetyNet device attestation. [What is a tampered device?](#)



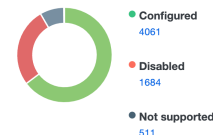
Screen Lock

Enforcing a screen lock can help prevent against unwanted access.



Mobile device biometrics

Fingerprint is a biometric alternative to passcodes and passwords on supported Android devices.



Demo !

Demo Setup

App Policies

Search

Account Cisco (BV)

Help

brian@verenoff.com

Dashboard

Device Insight

Policies

Applications

Protect an Application

Single Sign-On

Users

Groups

Endpoints

2FA Devices

Administrators

Trusted Endpoints

Dashboard > Applications

Applications

Protect an Application

Manage your update to the new Universal Prompt experience, all in one place.

See My Progress

Get More Information

66

All Applications

2

End of Support

Export

aws

Name	Type	Application Policy	Group Policies
Amazon Web Services (AWS)	Amazon Web Services - Single Sign-On	Zero Trust High - Critical Apps	
Salesforce	Salesforce - Single Sign-On	Minimum Device Health	

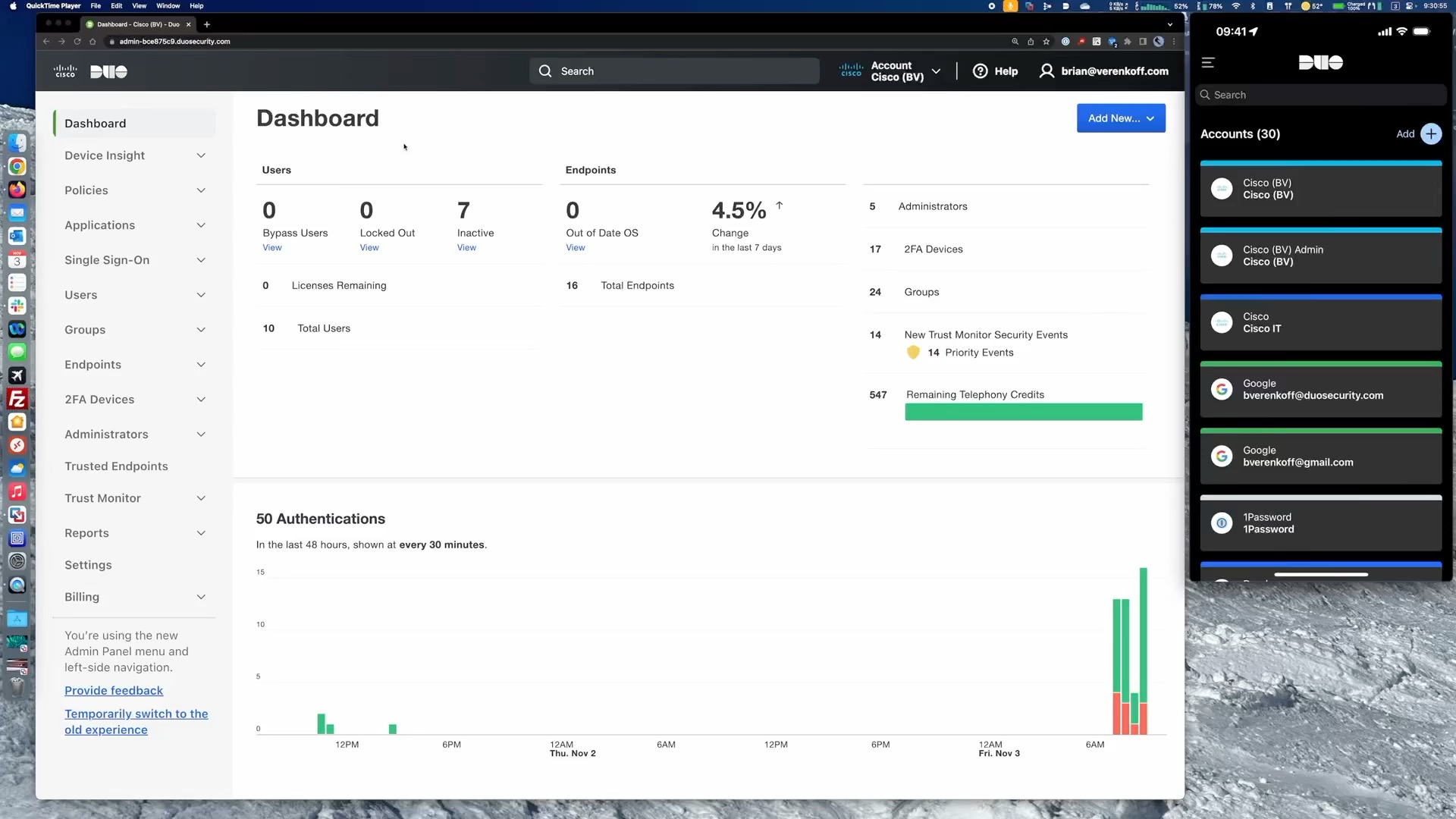
CISCO *Live!*

#CiscoLiveAPJC

BRKSEC-2076

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

27



Search

Account Cisco (BV)

Help

brian@verenkoff.com

Dashboard

- Device Insight
- Policies
- Applications
- Single Sign-On
- Users
- Groups
- Endpoints
- 2FA Devices
- Administrators
- Trusted Endpoints
- Trust Monitor
- Reports
- Settings
- Billing

You're using the new Admin Panel menu and left-side navigation.

[Provide feedback](#)
[Temporarily switch to the old experience](#)

Dashboard

Add New...

Users

0 Bypass Users
[View](#)

0 Locked Out
[View](#)

7 Inactive
[View](#)

0 Licenses Remaining

10 Total Users

Endpoints

0 Out of Date OS
[View](#)

4.5% ↑
Change in the last 7 days

16 Total Endpoints

5 Administrators

17 2FA Devices

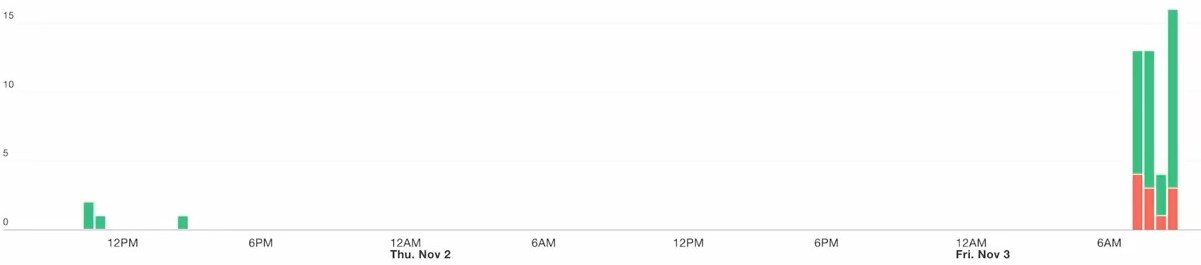
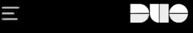
24 Groups

14 New Trust Monitor Security Events
14 Priority Events

547 Remaining Telephony Credits

50 Authentications

In the last 48 hours, shown at every 30 minutes.



Search

Accounts (30)

Add

Cisco (BV)
Cisco (BV)

Cisco (BV) Admin
Cisco (BV)

Cisco
Cisco IT

Google
bverenkoff@duosecurity.com

Google
bverenkoff@gmail.com

1Password
1Password

Enhanced with ITDR

Identity Threat Detection & Response

Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response

Published 20 October 2022 - ID G00765882 - 21 min read

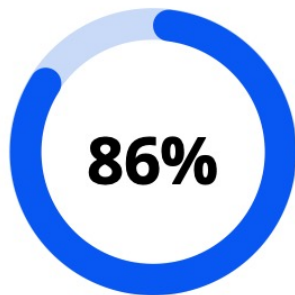
Conventional identity and access management and security preventive controls are insufficient to protect identity systems from attack. To enhance cyberattack preparedness, security and risk management leaders must add ITDR capabilities to their security infrastructure.

What is ITDR?

...a security discipline that encompasses threat intelligence, best practices, a knowledge base, tools, and processes to protect identity systems. It works by implementing detection mechanisms, investigating suspicious posture changes and activities, and responding to attacks to restore the integrity of the identity infrastructure...

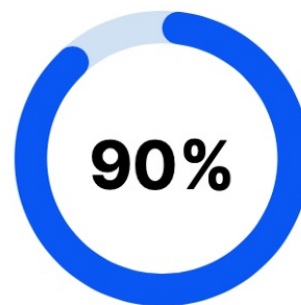
Gartner

Identity Security is Top of Mind



Of businesses have "managing and securing identities" in their top 5 priorities.

IDSA, 2023



Of organizations will use some embedded identity threat detection and response function by 2026.

Gartner, 2022

Identity Security Split into 2 Distinct Focuses

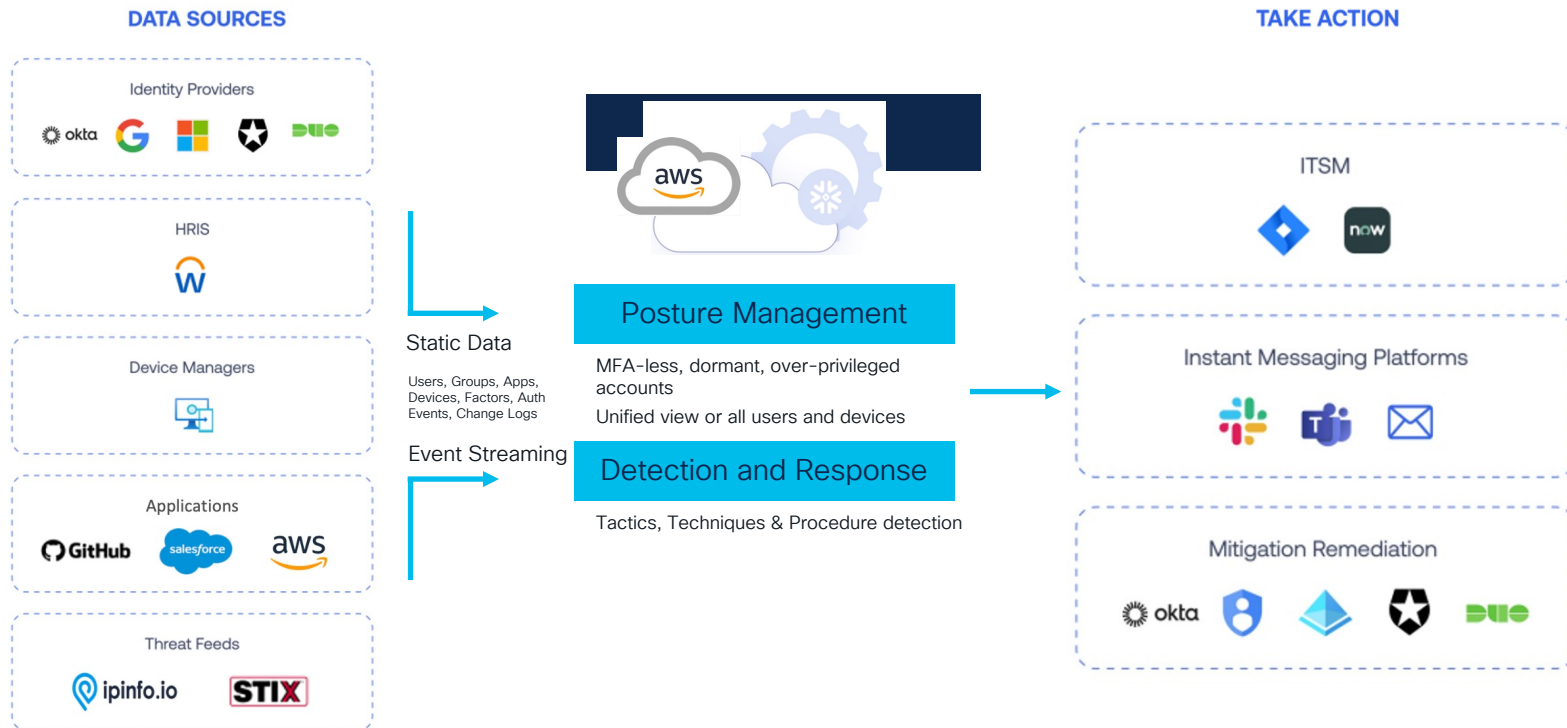
PROACTIVE

- Focuses on misconfigurations, policy infractions.
- Weak MFA configured
- No MFA configured
- Dormant accounts
- Unused accounts
- Sudden frequent use

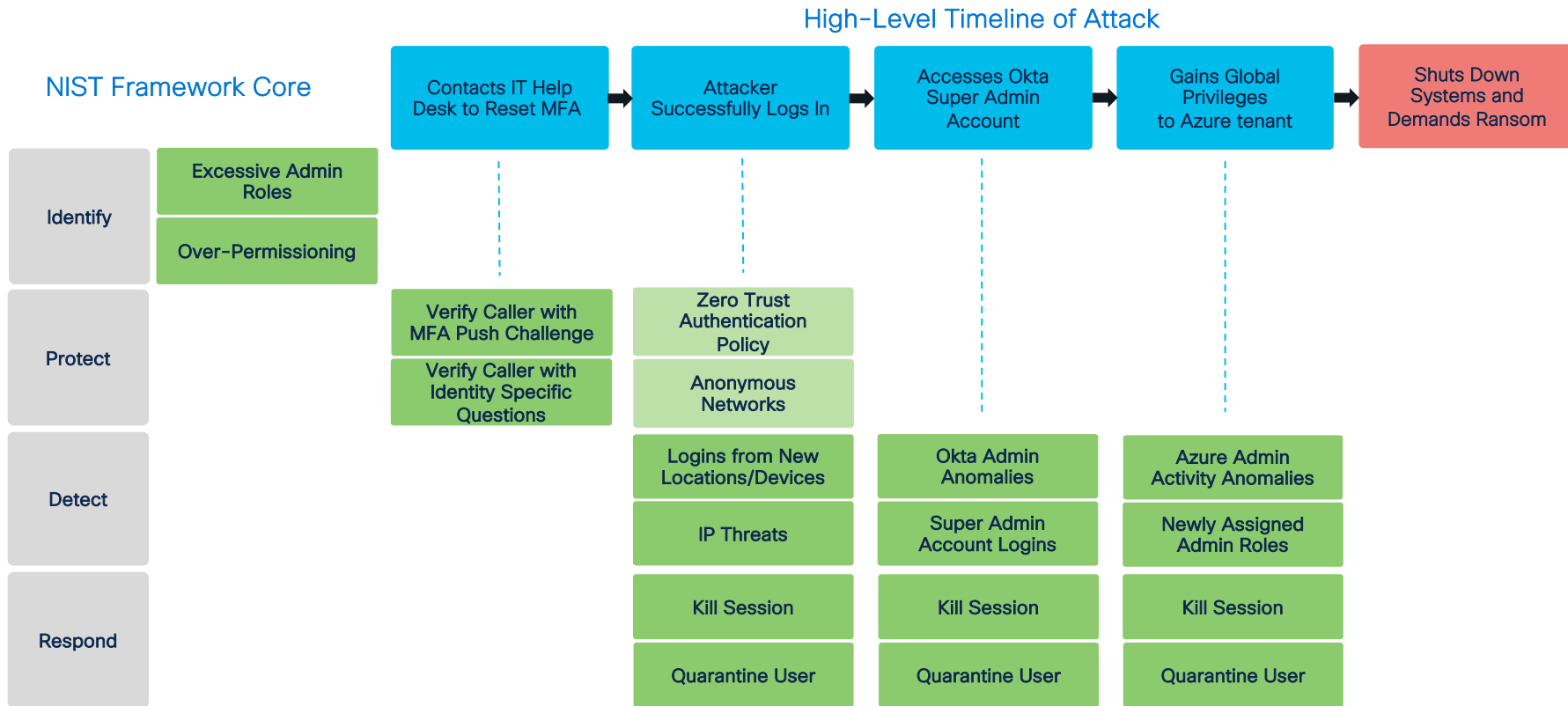
REACTIVE

- Leverages detection logic (Tactics, Techniques and Procedures (TTPs)) and analytics across all identity and authentication sources in the organization
- Integrates Identity-related threats into the incidents for a complete picture
- Automation to eradicate, recover from, and remediate identity threats

Cisco ITDR



Cisco ITDR Against a Recent Attack



Cisco ITDR Outcomes

Reduce Risk of A Breach

How will Cisco's ITDR solution change your security program?

- ✓ 80% Faster Investigations
 - Quicker, One-Click Response
 - Reduced Identity Attack Surface
-

- ✓ Improve Compliance
 - Fewer Audit Findings
 - Improve Strong MFA Usage
 - Continuous Monitoring
-

- ✓ Cost Savings
 - Revoke Idle Licenses
 - 2X Quicker Helpdesk Support

Demo !!!

genie



Integration Status

10 Providers Synced

[Last data collection](#)

Providers

-  **Demo AWS**
Success
Average Traffic: 26 records
-  **Demo Azure AD**
Success
Average Traffic: 25 records
-  **Demo GSuite**
Success
Average Traffic: 65 records
-  **Demo Okta**
Success
Average Traffic: 133 records
-  **Demo Workday**
Success
Average Traffic: 43 records

-  **Demo Auth0**
Success
Average Traffic: 45 records
-  **Demo Duo**
Success
Average Traffic: 59 records
-  **Demo GitHub**
Success
Average Traffic: 19 records
-  **Demo Salesforce**
Success
Average Traffic: 44 records
-  **Slack - oort-teamdata-testing**
Success
Average Traffic: 10 records

Ticketing

-  **Oort Jira**
-  **ServiceNow Instance**

Notification Targets

-  **Okta Workflow**
-  **oort-demo**

Identities

230

Total

230

In Protected Population

1

Never Logged In

2

Inactive Guest Users

1

Inactive Account Probing

3

User Type Missing

MFA Status

160

No MFA Configured

20

No strong MFA configured

22

Weak MFA Was Used To
Successfully Sign In

1

MFA Flood

1

Telecom MFA Limit Reached

3

Admins with Weak MFA

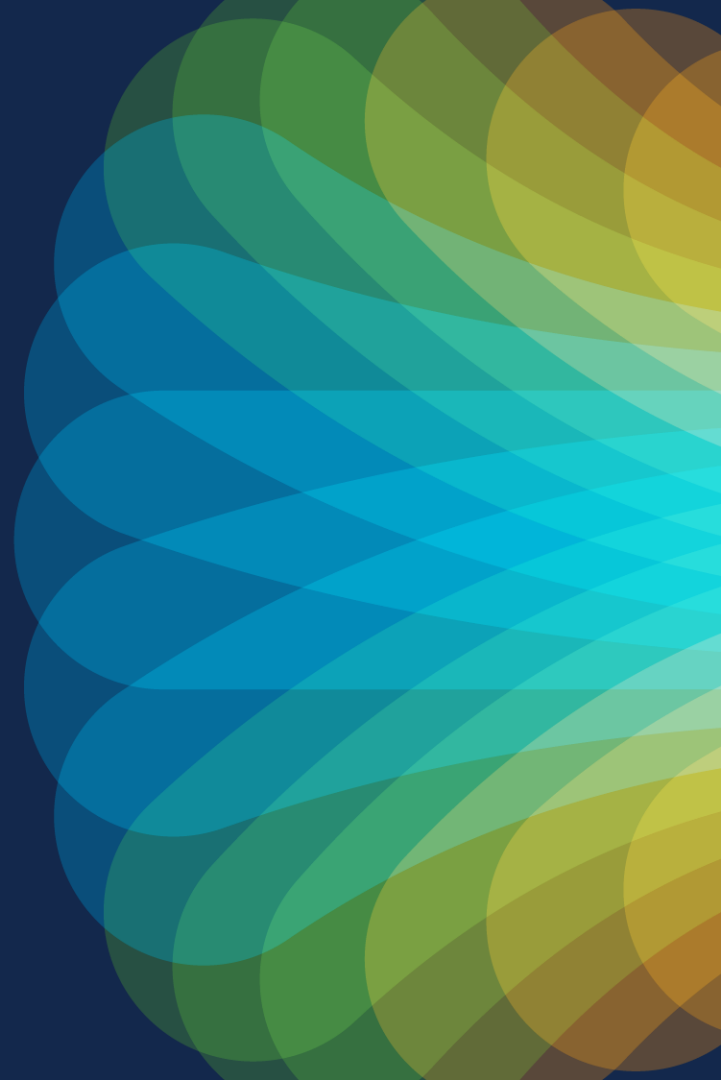
Administrators per Source



Administrators Logins

Cisco ITDR to be Included in Duo Advantage and Duo Premier

Start your Journey !





Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background is a vibrant, abstract graphic featuring a spectrum of colors (red, orange, yellow, green, blue) arranged in a radial pattern that resembles a stylized sunburst or a rainbow. The colors transition smoothly from red on the left to blue on the right, with yellow and green in the center. The overall effect is bright and energetic.

cisco *Live!*

Let's go

#CiscoLiveAPJC