NIST CYBER

Cybersecurity Considerations for Telework

Cybersecurity Coalition

VENABLE LLP

NIST
CYBER

Cybersecurity Considerations for Telework

Monday | March 23, 2020

3:00PM – 4:15PM

Security for Enterprises

ITL BULLETIN

ITL BULLETIN MARCH 2020

Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions

Karen Scarfone[1], Jeffrey Greene, and Murugiah Souppaya
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

Many people *telework* (also known as *telecommuting*), which is the ability for an organization's employees, contractors, business partners, vendors, and other users to perform work from locations other than the organization's facilities. Teleworkers use various client devices, such as desktop and laptop computers, smartphones, and tablets, to read and send email, access websites, review and edit documents, and perform many other tasks. These client devices may be controlled by the organization, by third parties (the organization's contractors, business partners, or vendors), or by the users themselves (e.g., BYOD). Most teleworkers use *remote access*, which is the ability for an organization's users to access its non-public computing resources from external locations other than the organization's facilities.

The National Institute of Standards and Technology (NIST) has guidelines on telework and remote access to help organizations mitigate security risks associated with the enterprise technologies used for teleworking, such as remote access servers, telework client devices, and remote access communications. NIST Special Publication (SP) 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* was issued in 2016, and its recommendations are still relevant today. This Information Technology Laboratory (ITL) Bulletin summarizes key concepts and recommendations from SP 800-46 Revision 2. They include deploying some or all of the following security measures:

- Developing and enforcing a telework security policy, such as having tiered levels of remote access
- Requiring multi-factor authentication for enterprise access

[1] Karen Scarfone is a NIST Associate from Scarfone Cybersecurity.

Enterprise Planning

Plan telework-related security policies and controls based on a zero-trust model.

- Encrypt client devices’ storage, encrypt all sensitive data stored on client devices, or don’t store sensitive data on client devices
- Use strong authentication, preferably multi-factor, for enterprise access
- Use encryption technologies to protect the confidentiality and integrity of communications
- Authenticate each endpoint to the other to verify their identities

Develop a telework security policy that defines telework, remote access, and BYOD requirements.

- Define in the policy which forms of remote access are permitted and how the remote access servers will be administered
- Make risk-based decisions about what levels of remote access should be permitted from which types of telework client devices

Enterprise Implementation

Ensure that remote access servers are secured effectively and configured to enforce telework security policies.

- Keep remote access servers fully patched
- Only allow remote access servers to be managed from trusted hosts by authorized administrators
- Carefully choose the placement of each remote access server

Secure organization-controlled telework client devices against common threats, and maintain their security regularly.

- Ensure all types of telework client devices are secured, including smartphones and tablets
- Include all of the local security controls used for non-telework client devices, such as applying updates promptly, disabling unneeded services, and using anti-malware software (for desktops and laptops)
- Use additional security controls, such as encrypting sensitive data stored on the devices

Additional Resources

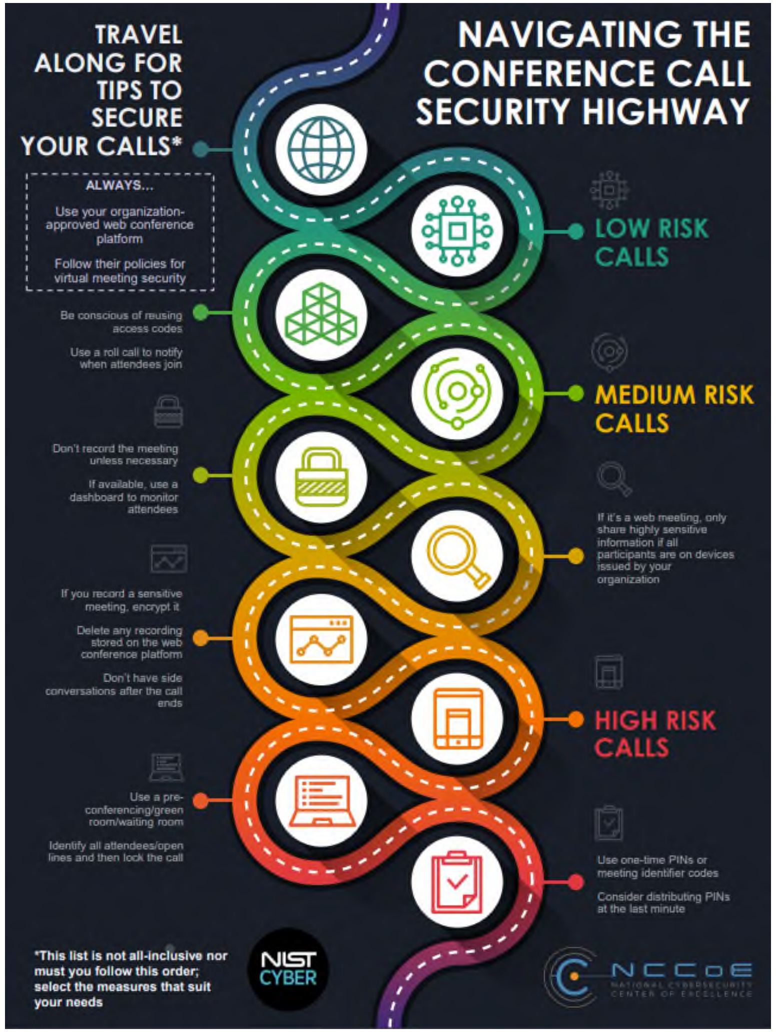
- NIST SP 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
- NIST SP 800-77 Revision 1 (Draft), Guide to IPsec VPNs
- NIST SP 800-52 Revision 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- NIST SP 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-40 Revision 3, Guide to Enterprise Patch Management Technologies
- NIST SP 1800-4, Mobile Device Security: Cloud and Hybrid Builds
- NIST SP 1800-21 (Draft), Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)

Questions? Email karen@scarfonecybersecurity.com

Security & Privacy

Virtual Meeting Security

- First Rule: use common sense
- *Second Rule: use common sense*
- Follow your organization's rules
- The toothpaste won't go back in the tube
- Not all calls are created equal
- Low
    - Beware of lurkers
- Medium
    - Simple things go a long way
- High
    - Your mission if you choose to accept it



NAVIGATING THE CONFERENCE CALL SECURITY HIGHWAY

TRAVEL ALONG FOR TIPS TO SECURE YOUR CALLS*

ALWAYS...

Use your organization-approved web conference platform

Follow their policies for virtual meeting security

LOW RISK CALLS

Be conscious of reusing access codes

Use a roll call to notify when attendees join

MEDIUM RISK CALLS

Don't record the meeting unless necessary

If available, use a dashboard to monitor attendees

If it's a web meeting, only share highly sensitive information if all participants are on devices issued by your organization

If you record a sensitive meeting, encrypt it

Delete any recording stored on the web conference platform

Don't have side conversations after the call ends

HIGH RISK CALLS

Use a pre-conferencing/green room/waiting room

Identify all attendees/open lines and then lock the call

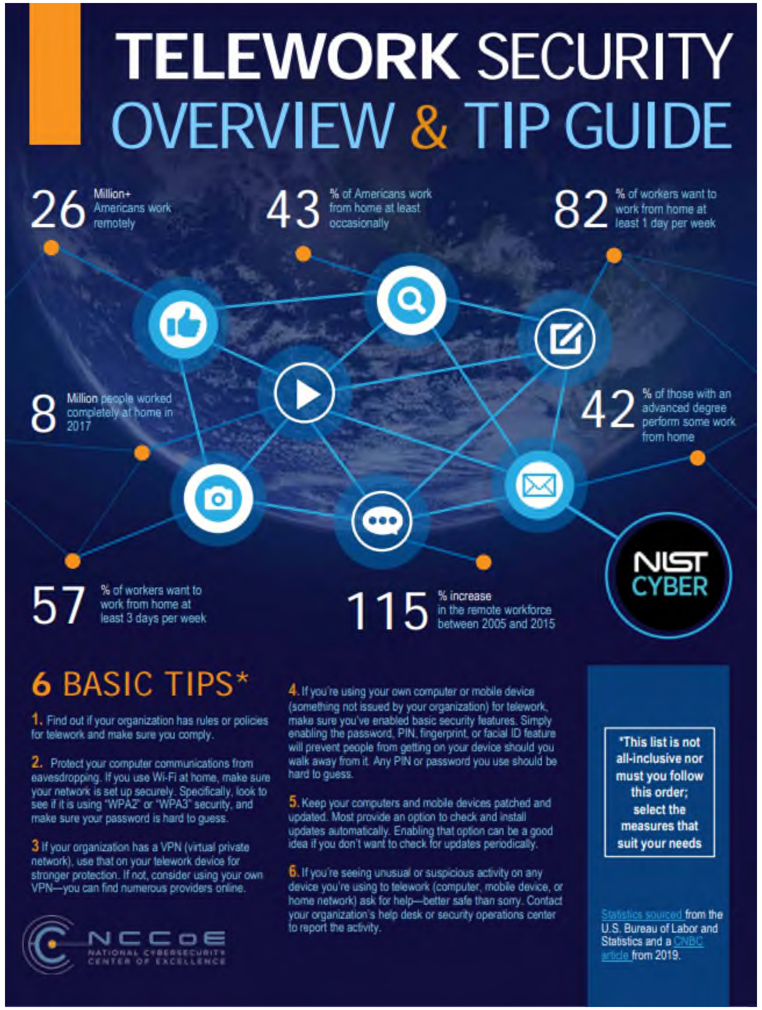
Use one-time PINs or meeting identifier codes

Consider distributing PINs at the last minute

*This list is not all-inclusive nor must you follow this order; select the measures that suit your needs

Telework Security Basics

- First Rule: use common sense
- *Second Rule: use common sense*
- Follow your organization's rules
- Build a wall
- Dig a tunnel
- Post a guard
- Plug the holes
- Be suspicious



TELEWORK SECURITY OVERVIEW & TIP GUIDE

26 Million+ Americans work remotely

43 % of Americans work from home at least occasionally

82 % of workers want to work from home at least 1 day per week

8 Million people worked completely at home in 2017

42 % of those with an advanced degree perform some work from home

57 % of workers want to work from home at least 3 days per week

115 % increase in the remote workforce between 2005 and 2015

NIST CYBER

6 BASIC TIPS*

1. Find out if your organization has rules or policies for telework and make sure you comply.

2. Protect your computer communications from eavesdropping. If you use Wi-Fi at home, make sure your network is set up securely. Specifically, look to see if it is using "WPA2" or "WPA3" security, and make sure your password is hard to guess.

3 If your organization has a VPN (virtual private network), use that on your telework device for stronger protection. If not, consider using your own VPN—you can find numerous providers online.

4. If you're using your own computer or mobile device (something not issued by your organization) for telework, make sure you've enabled basic security features. Simply enabling the password, PIN, fingerprint, or facial ID feature will prevent people from getting on your device should you walk away from it. Any PIN or password you use should be hard to guess.

5. Keep your computers and mobile devices patched and updated. Most provide an option to check and install updates automatically. Enabling that option can be a good idea if you don't want to check for updates periodically.

6. If you're seeing unusual or suspicious activity on any device you're using to telework (computer, mobile device, or home network) ask for help—better safe than sorry. Contact your organization's help desk or security operations center to report the activity.

*This list is not all-inclusive nor must you follow this order; select the measures that suit your needs

Statistics sourced from the U.S. Bureau of Labor and Statistics and a CNBC article from 2019.

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Questions? Email jeffrey.greene@nist.gov

Additional Resources

Blogs

- https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings

- https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics

Jeff Greene
Director, NCCoE
Jeffrey.Greene@nist.gov

Karen Scarfone
Sr. Computer Scientist, NIST
karen@scarfonecybersecurity.com

Matt Scholl
Cybersecurity Division Chief, ITL
Matthew.Scholl@nist.gov

CİTRIX

Secure Remote Access using Citrix Workspace

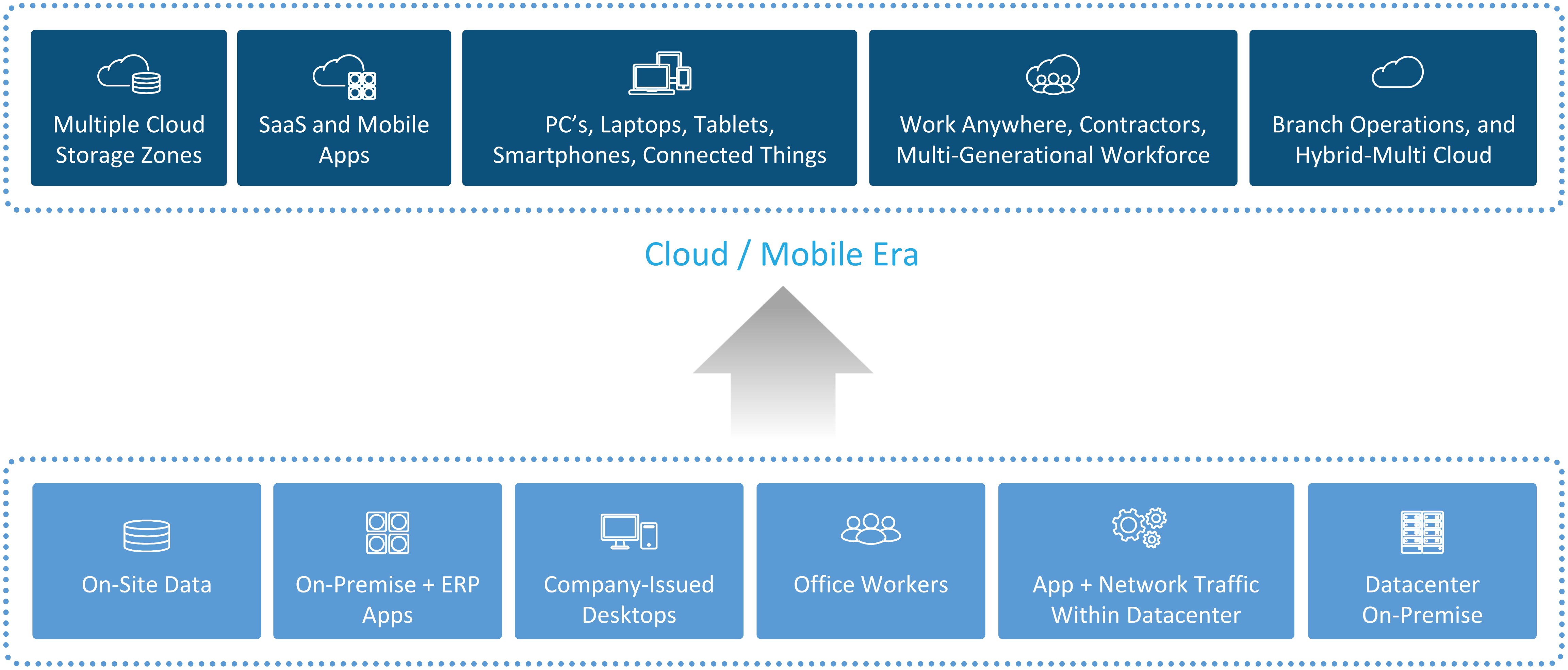
Sridhar Mullapudi

SVP, Products, Workspace Product Group
@sridharcitrix

MAR 23, 2020

The way we work has changed

MOST COMPANIES ARE MID-TRANSFORMATION



Multiple Cloud Storage Zones

SaaS and Mobile Apps

PC’s, Laptops, Tablets, Smartphones, Connected Things

Work Anywhere, Contractors, Multi-Generational Workforce

Branch Operations, and Hybrid-Multi Cloud

Cloud / Mobile Era

On-Site Data

On-Premise + ERP Apps

Company-Issued Desktops

Office Workers

App + Network Traffic Within Datacenter

Datacenter On-Premise

Remote Work can complicate life for workers; Increased security risk to manage

Traditional VPNs are not the answer

3+ Devices/Day

BYO and unmanaged devices are considered risk

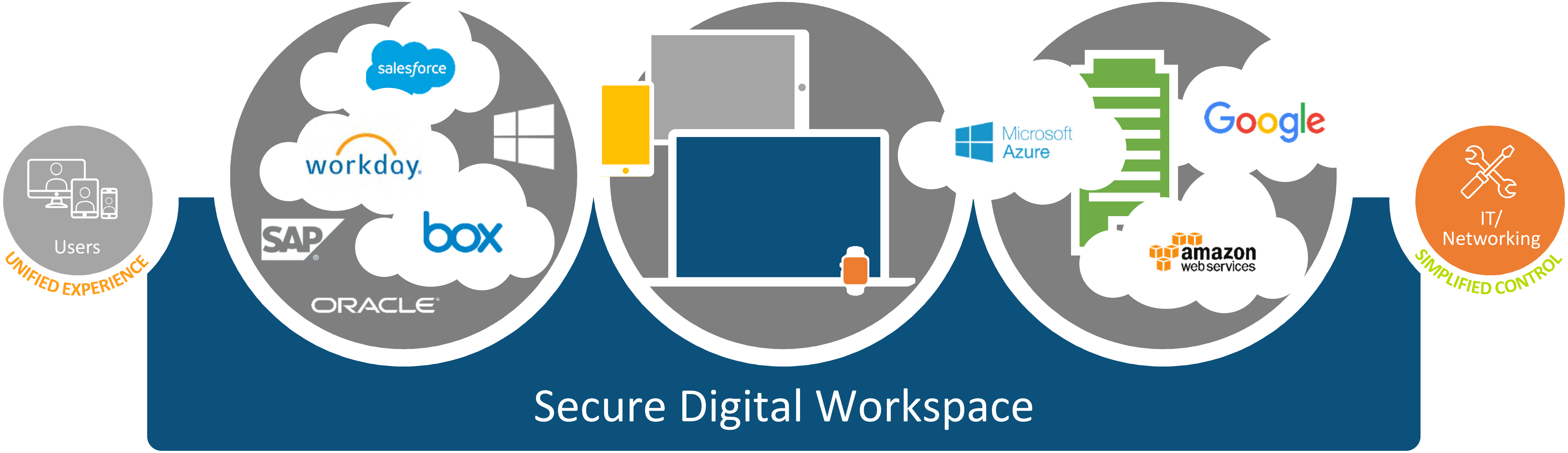
Multiple access solutions

3+ Locations/Day

6+ Passwords
25 Accounts

Citrix Workspace: unified experience, simplified security

Secure, simplified access and control of apps and data across any device, platform, or cloud



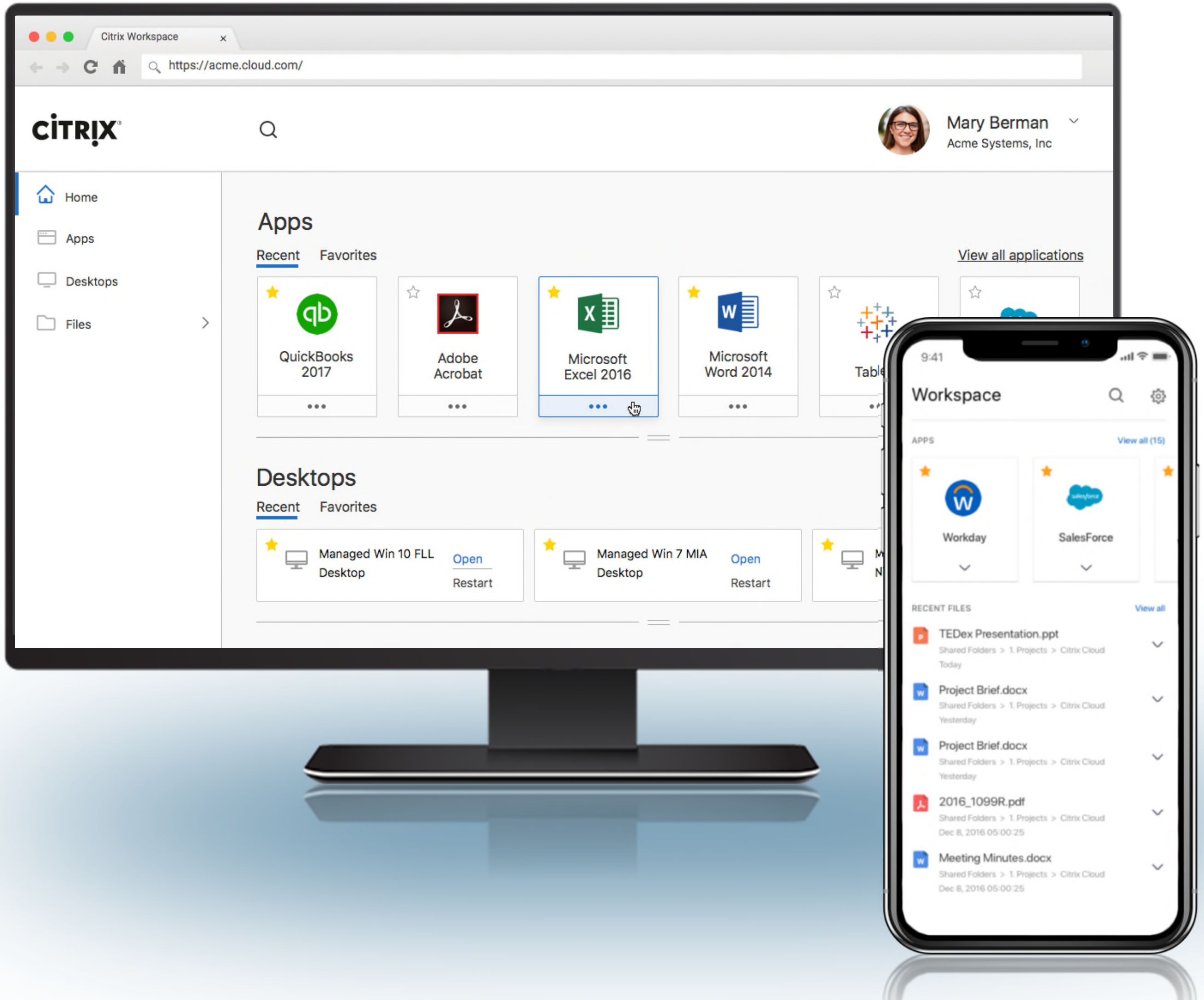
Users

UNIFIED EXPERIENCE

IT/ Networking

SIMPLIFIED CONTROL

Secure Digital Workspace



CITRIX WORKSPACE

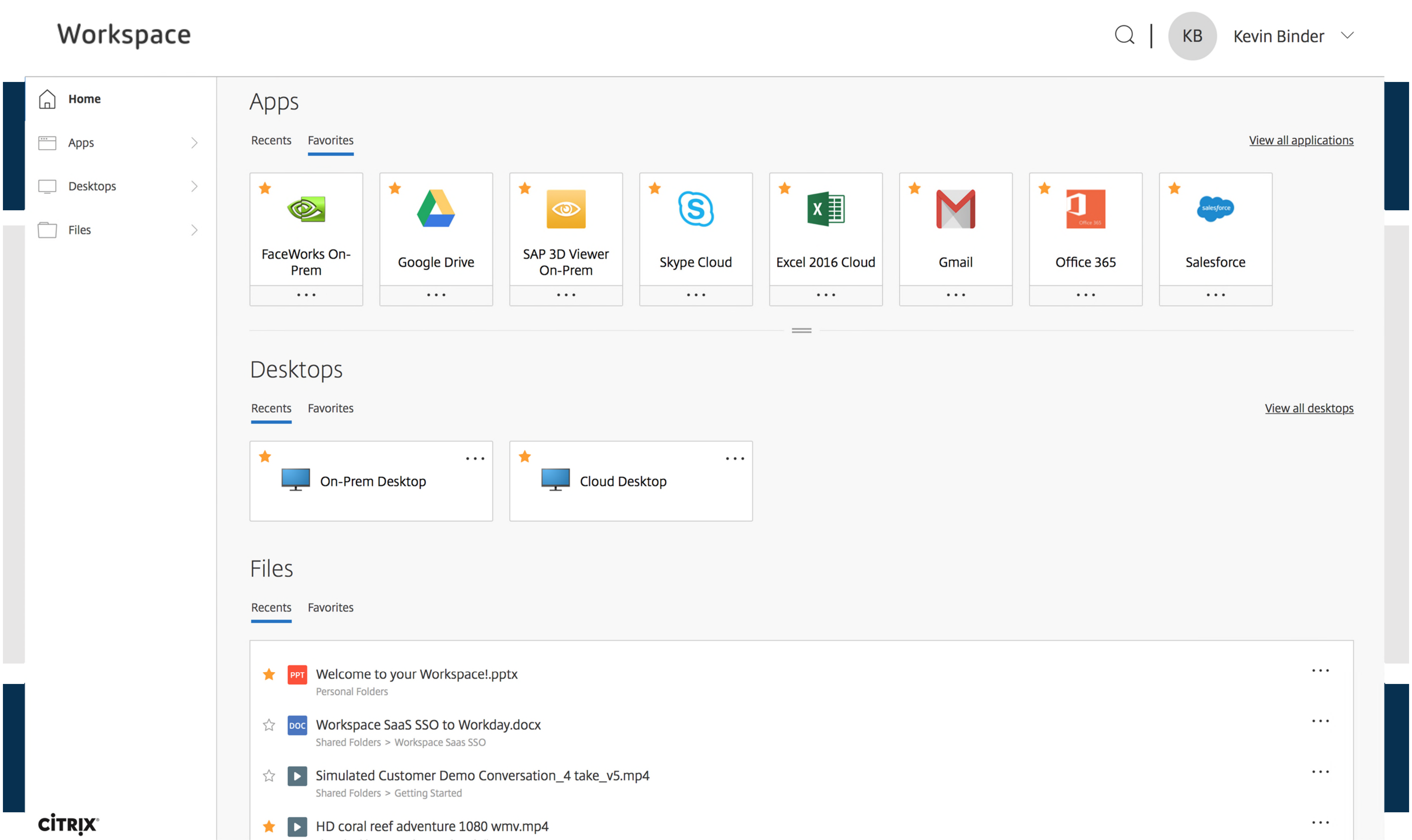
One consumer-like experience across every device

Single sign-on to all your apps & data

VPN less approach reduces security risk

Easy to scale and on-board new users

Contextual security & performance



Workspace

KB Kevin Binder

Home

Apps

Desktops

Files

Apps

Recents Favorites

View all applications

★ FaceWorks On-Prem ...

★ Google Drive ...

★ SAP 3D Viewer On-Prem ...

★ Skype Cloud ...

★ Excel 2016 Cloud ...

★ Gmail ...

★ Office 365 ...

★ Salesforce ...

Desktops

Recents Favorites

View all desktops

★ On-Prem Desktop ...

★ Cloud Desktop ...

Files

Recents Favorites

★ PPT Welcome to your Workspace!.pptx ...
Personal Folders

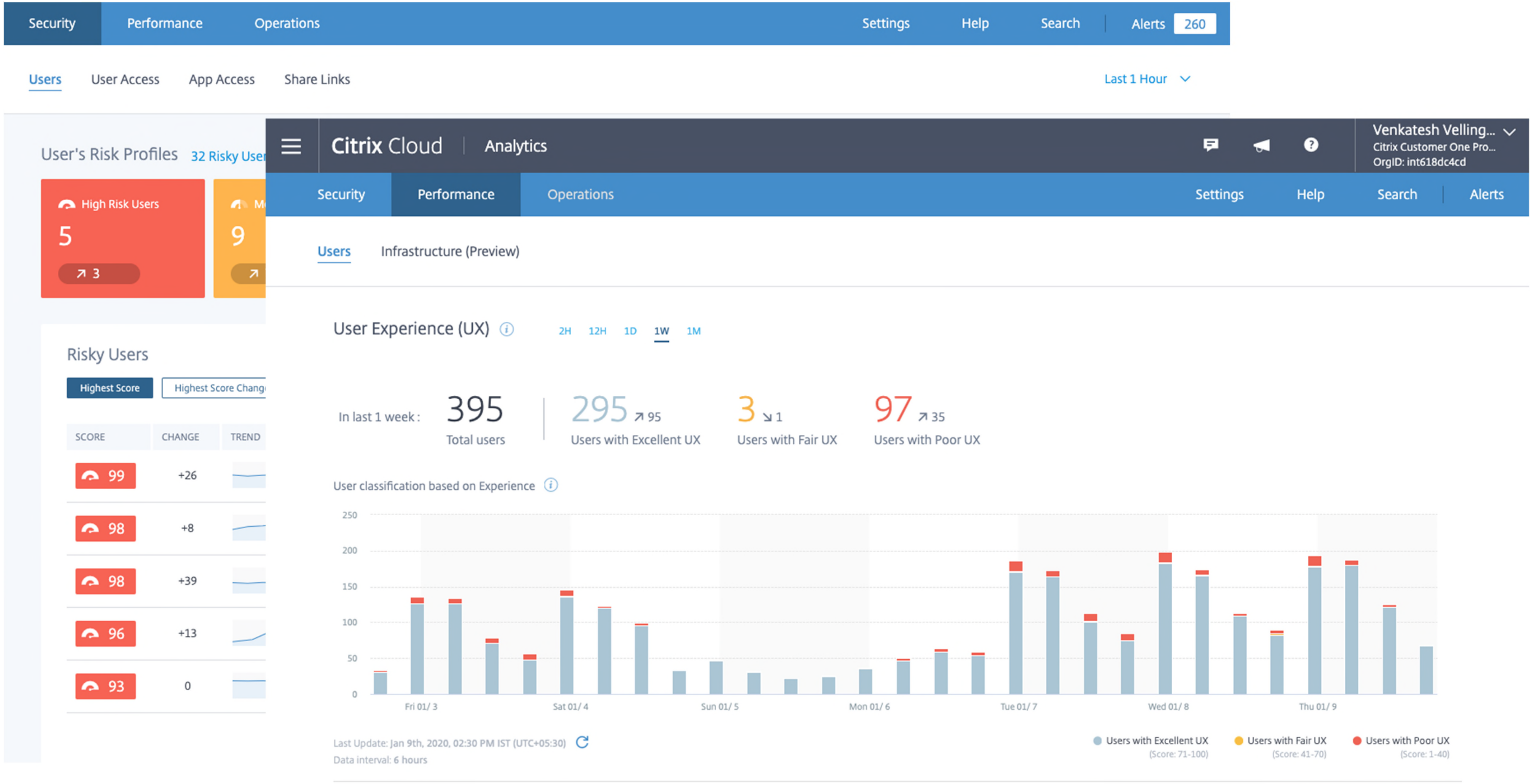
☆ DOC Workspace SaaS SSO to Workday.docx ...
Shared Folders > Workspace Saas SSO

☆ Simulated Customer Demo Conversation_4 take_v5.mp4 ...
Shared Folders > Getting Started

★ HD coral reef adventure 1080 wmv.mp4 ...

CITRIX

With built in Security & Performance Analytics



User's Risk Profiles 32 Risky User

High Risk Users 5 ↗ 3

M 9 ↗

Risky Users

SCORE	CHANGE	TREND
99	+26	
98	+8	
98	+39	
96	+13	
93	0	

User Experience (UX)

In last 1 week : 395 Total users | 295 ↗ 95 Users with Excellent UX | 3 ↘ 1 Users with Fair UX | 97 ↗ 35 Users with Poor UX

User classification based on Experience

Last Update: Jan 9th, 2020, 02:30 PM IST (UTC+05:30)
Data interval: 6 hours

● Users with Excellent UX (Score: 71-100)
● Users with Fair UX (Score: 41-70)
● Users with Poor UX (Score: 1-40)

Our Zero Trust Approach to Security Provides…

Contextual & Secure Access

BYO and Any Device Security

Reduced Exposure to Internal & External Threats

Secure Content Collaboration

Governance Risk and Compliance

Continuous monitoring and Continuous Assurance

Standards Based Compliance & Certifications

PCI Security Standards Council®

HIPAA
Health Insurance Portability and Accountability Act

GDPR

Common Criteria

FIPS VALIDATED 140-2

FR FedRAMP

AICPA Service Organization Control Reports℠
AICPA
SOC 2
Formerly SAS 70 Reports

CITRIX®

Everything Ch-Ch-Ch-Changes…..

Telework… it's a thing

Sean Frazier Advisory CISO - Federal
sean@duo.com | @seanfsez

GNN
GNN
1 DAY

Hi-Tech Communications

YOU ARE HERE

:(

Your users ran into a problem using this process, so now they’re just going to ignore it.

You can probably figure out how this will go: HINT_NOT_VERY_WELL

Telework Enablers

salesforce

zoom

Cisco
webex

Office 365

Webex Teams

slack

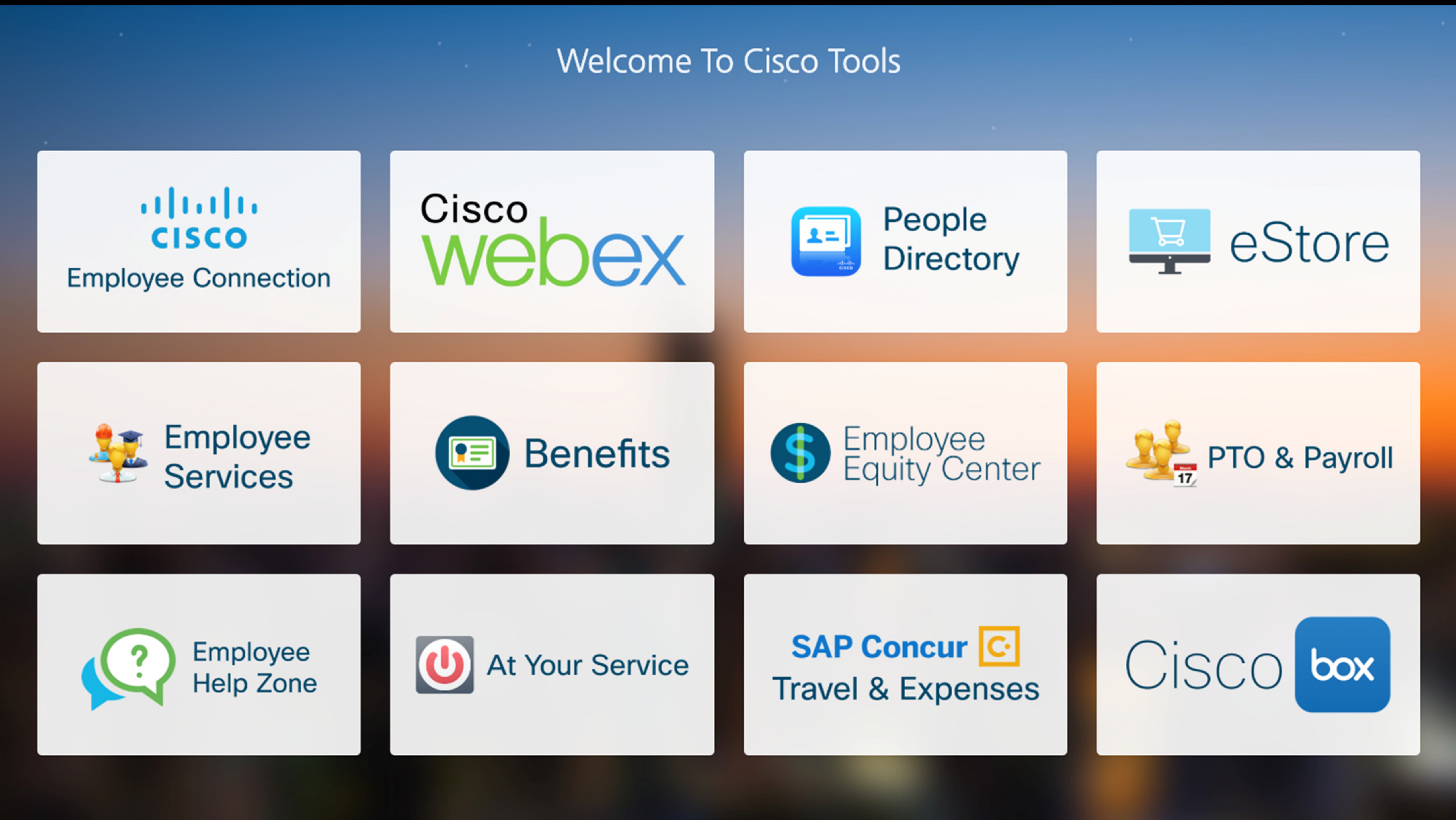
CONCUR.

Lucky Charms®

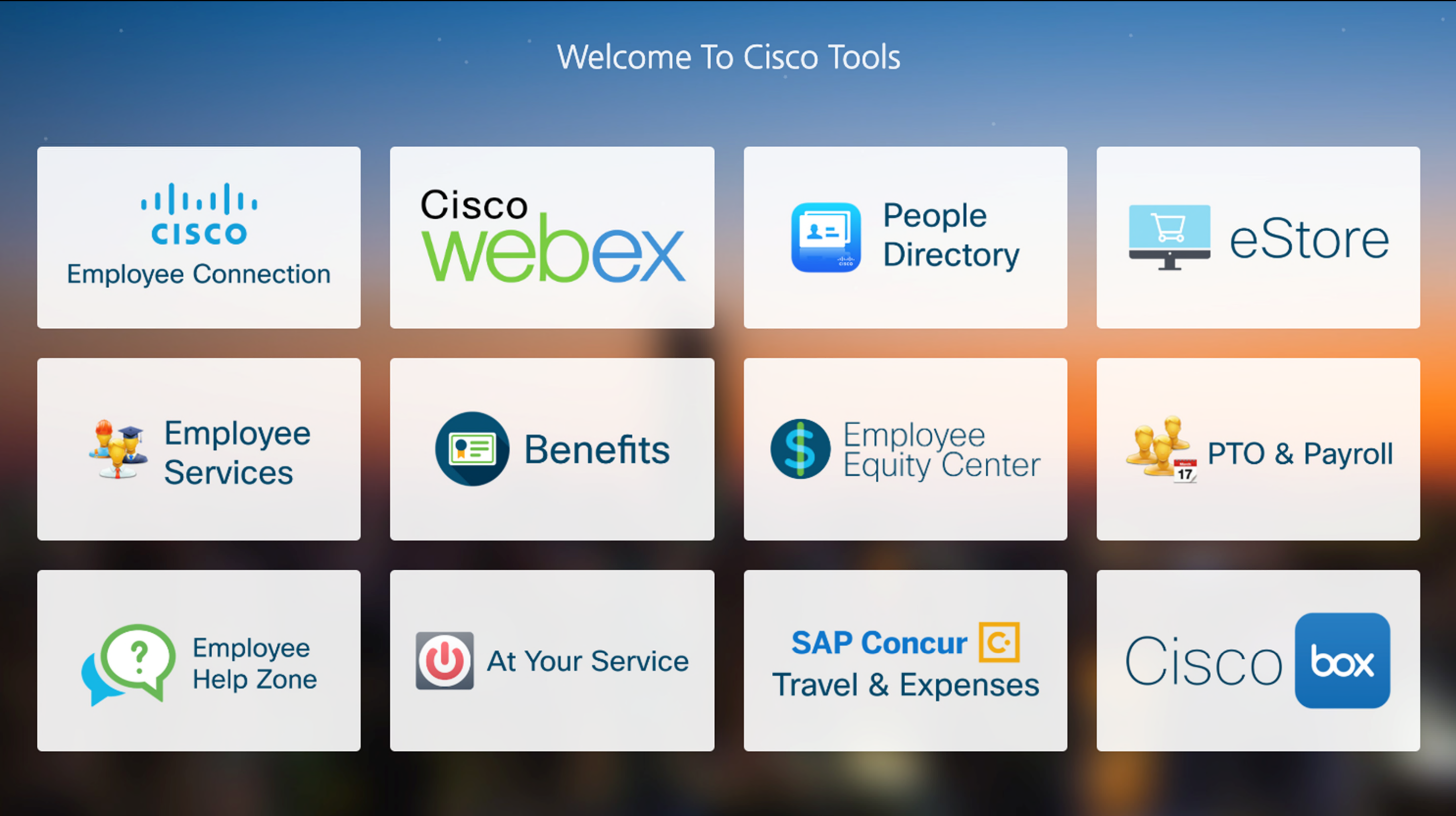
identity

data

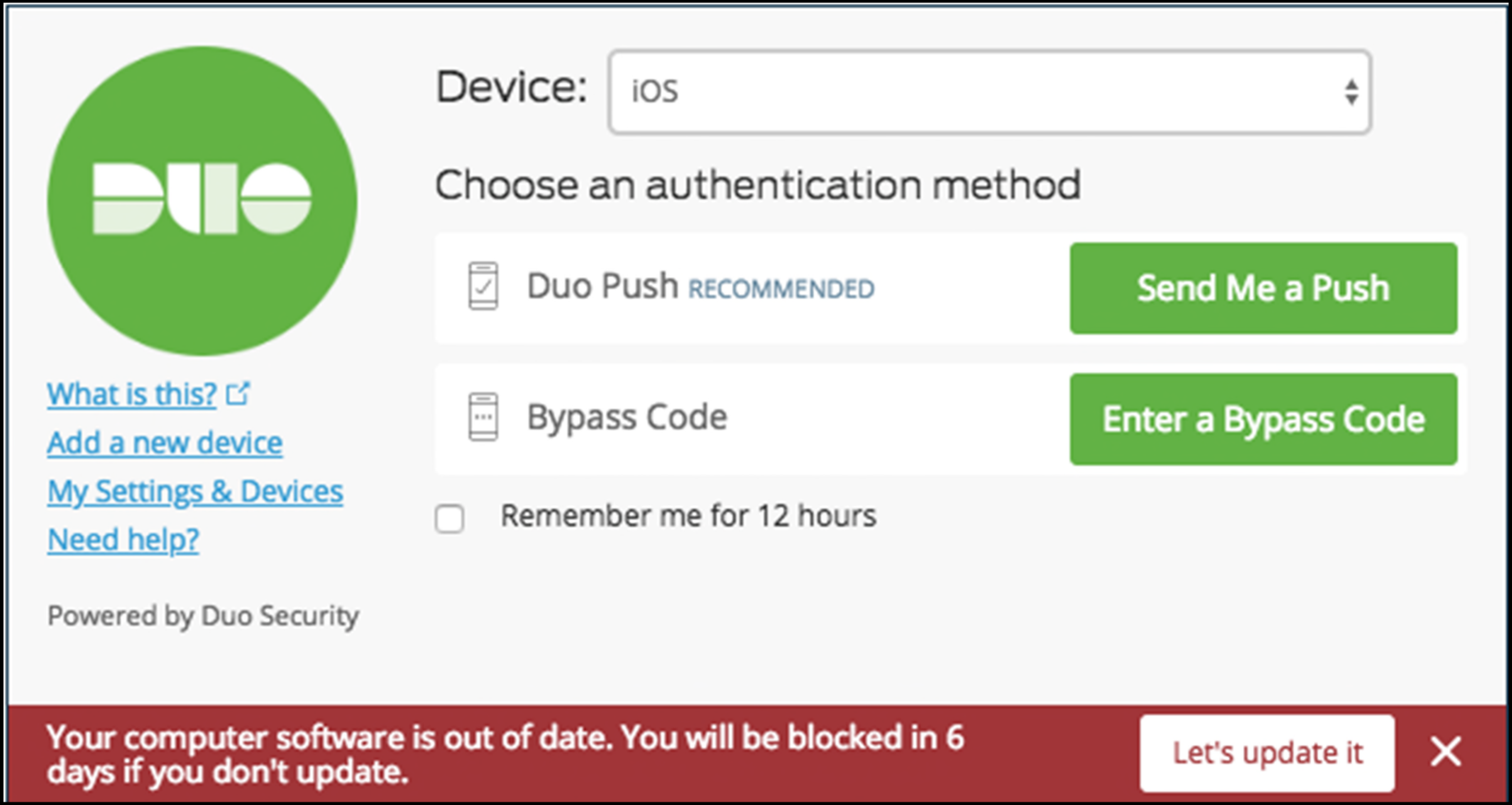
ZT



Welcome To Cisco Tools



Welcome To Cisco Tools

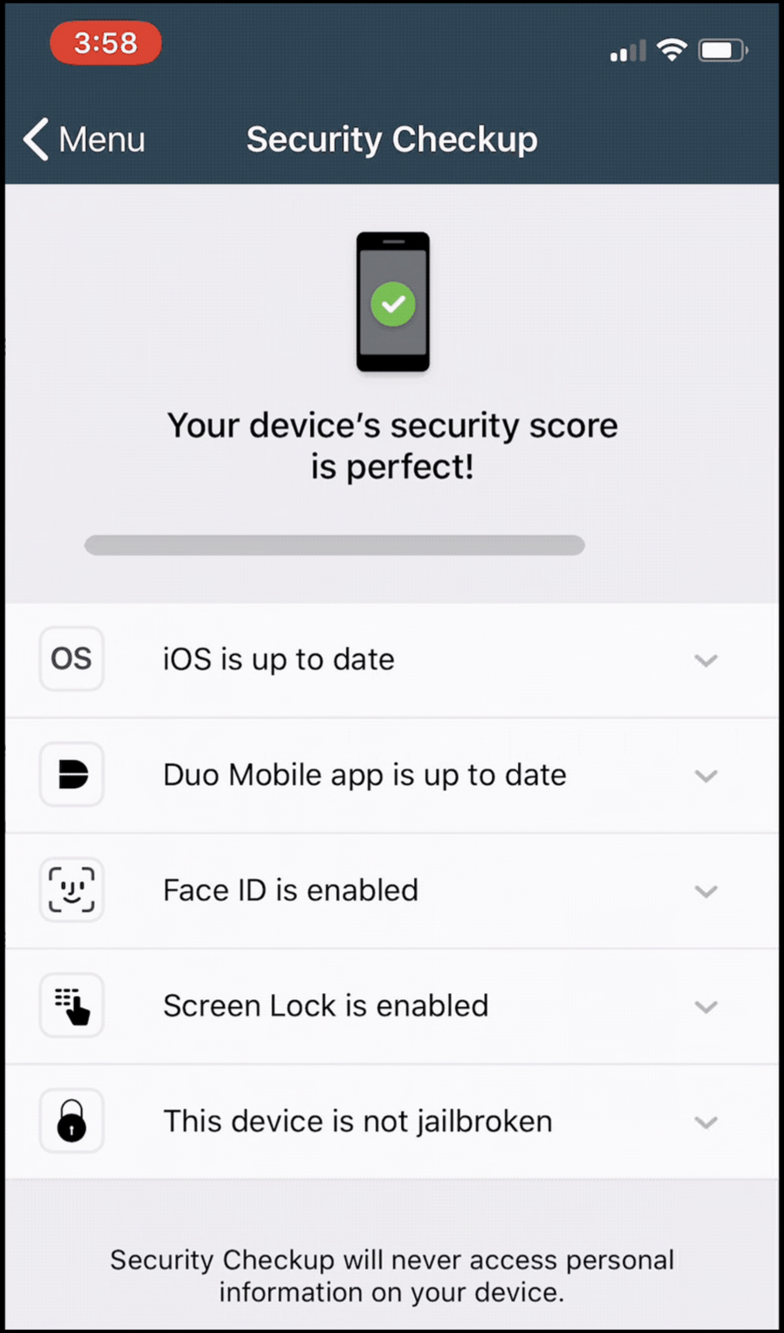


Device: iOS

Choose an authentication method

□ Remember me for 12 hours

Your computer software is out of date. You will be blocked in 6 days if you don't update.

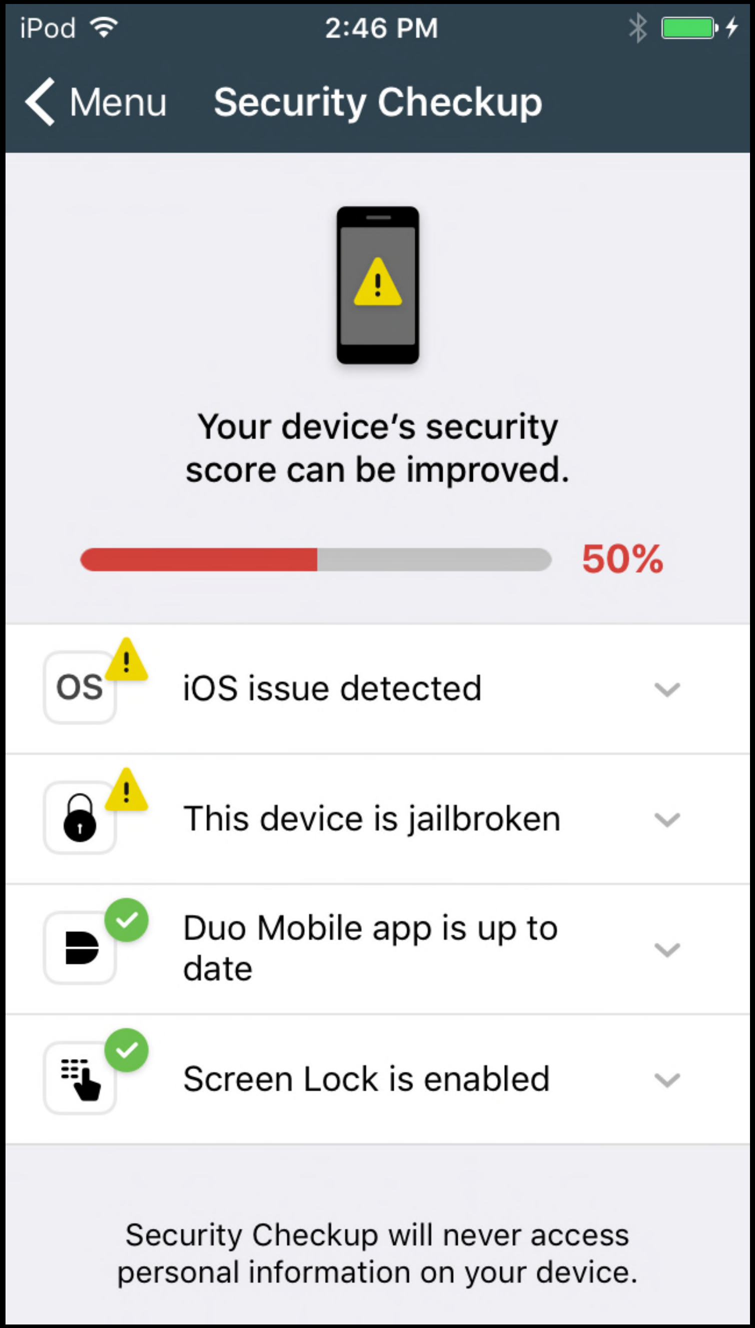


Security Checkup

Your device's security score is perfect!

- OS iOS is up to date
- Duo Mobile app is up to date
- Face ID is enabled
- Screen Lock is enabled
- This device is not jailbroken

Security Checkup will never access personal information on your device.



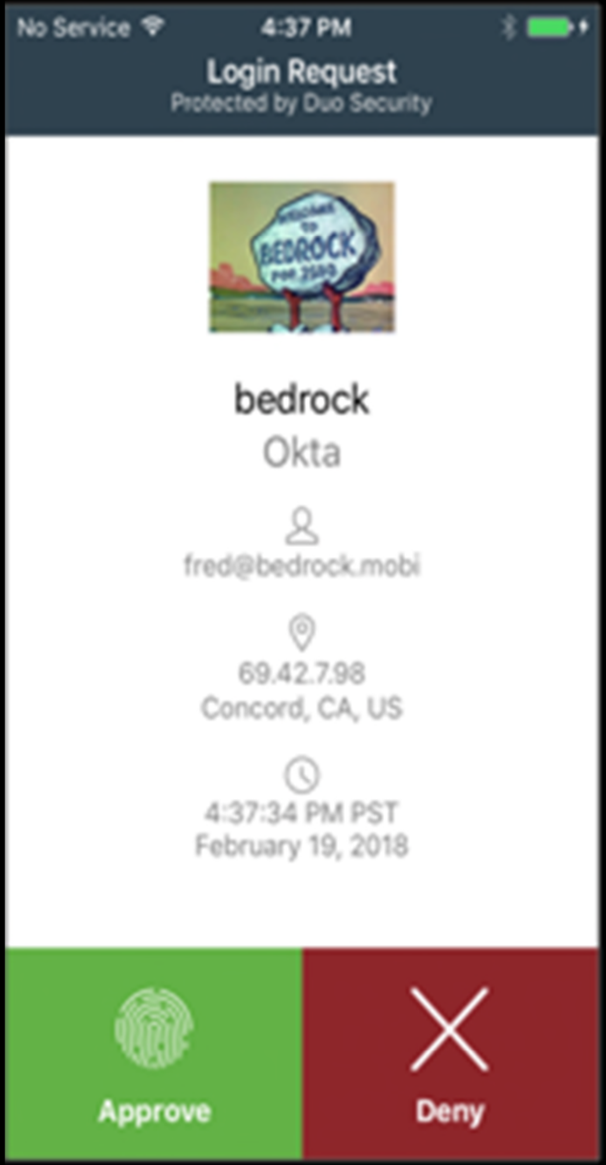
Security Checkup

Your device's security score can be improved.

50%

- OS iOS issue detected
- This device is jailbroken
- Duo Mobile app is up to date
- Screen Lock is enabled

Security Checkup will never access personal information on your device.



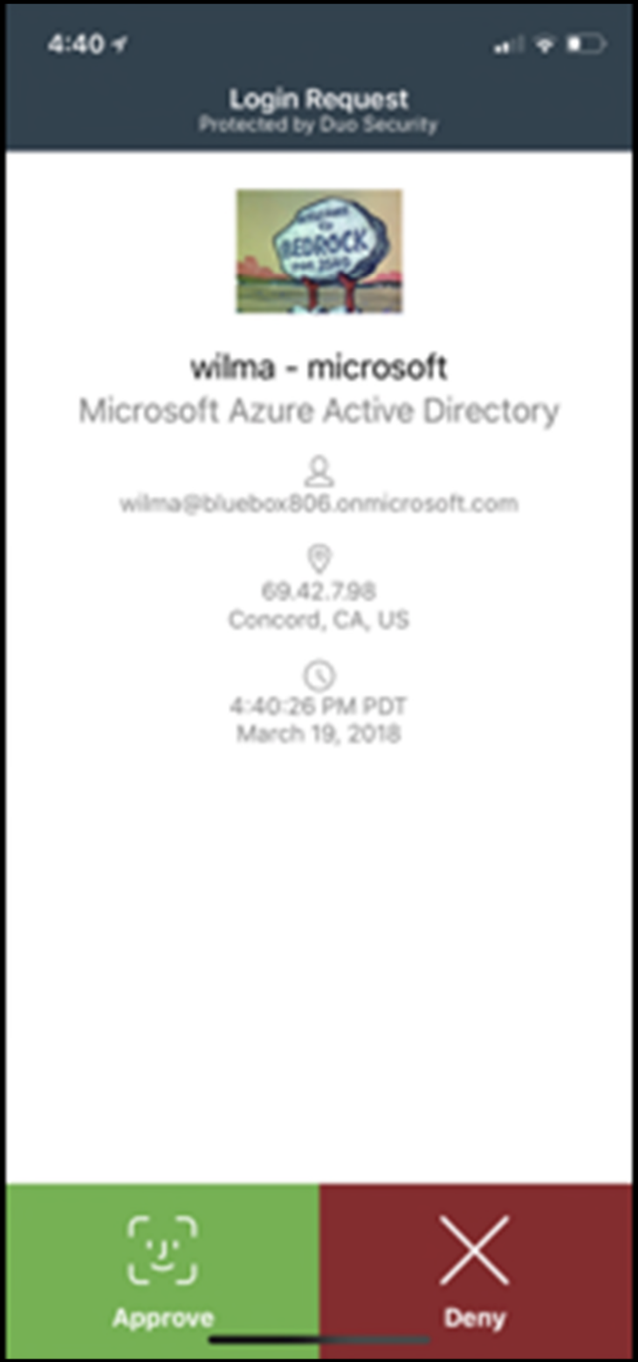
Login Request
Protected by Duo Security

bedrock
Okta

fred@bedrock.mobi

69.42.7.98
Concord, CA, US

4:37:34 PM PST
February 19, 2018



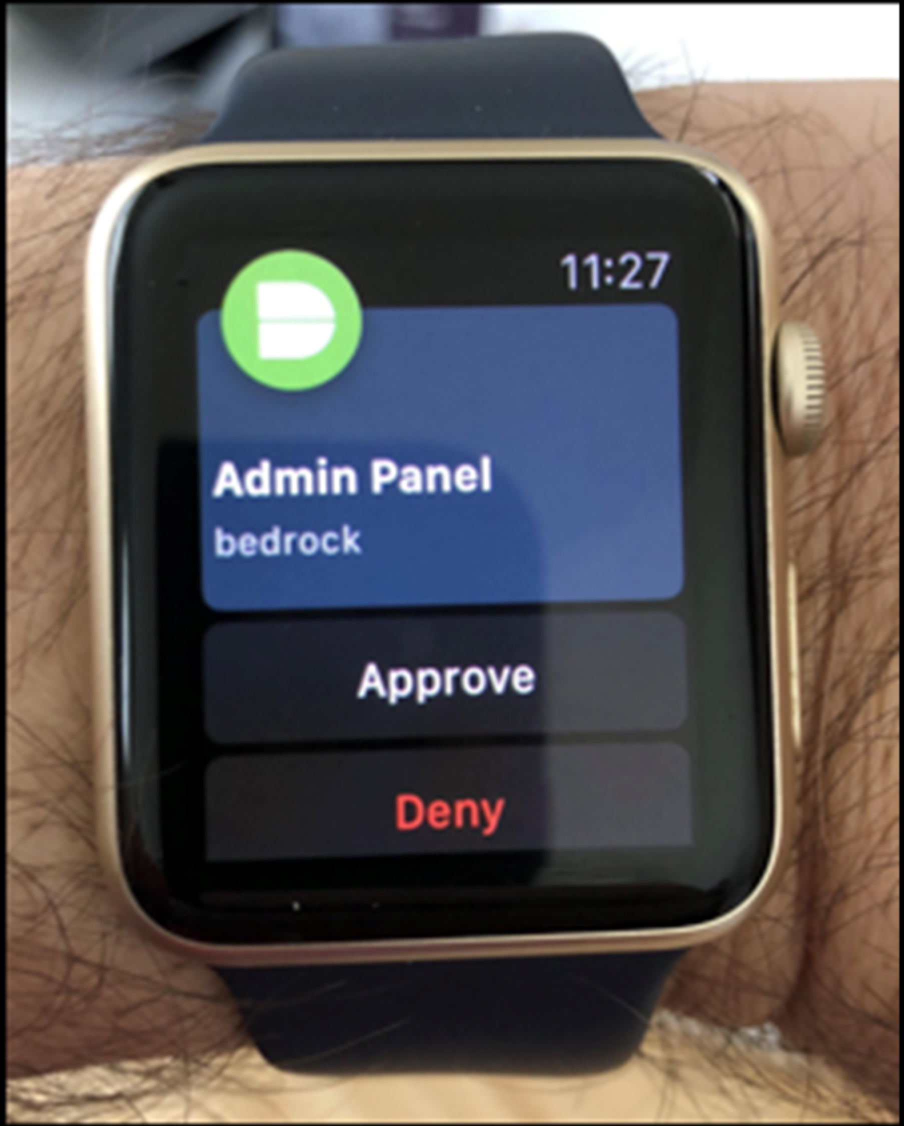
Login Request
Protected by Duo Security

wilma - microsoft
Microsoft Azure Active Directory

wilma@bluebox806.onmicrosoft.com

69.42.7.98
Concord, CA, US

4:40:26 PM PDT
March 19, 2018



DISCO

NIST CYBER

Cybersecurity Considerations for Telework

Cybersecurity Coalition

VENABLE LLP