LESS
WORRYING
**MORE
BANKING®**

2021 Cybersecurity Outlook

Brendan McGowan

Chief Technology Officer

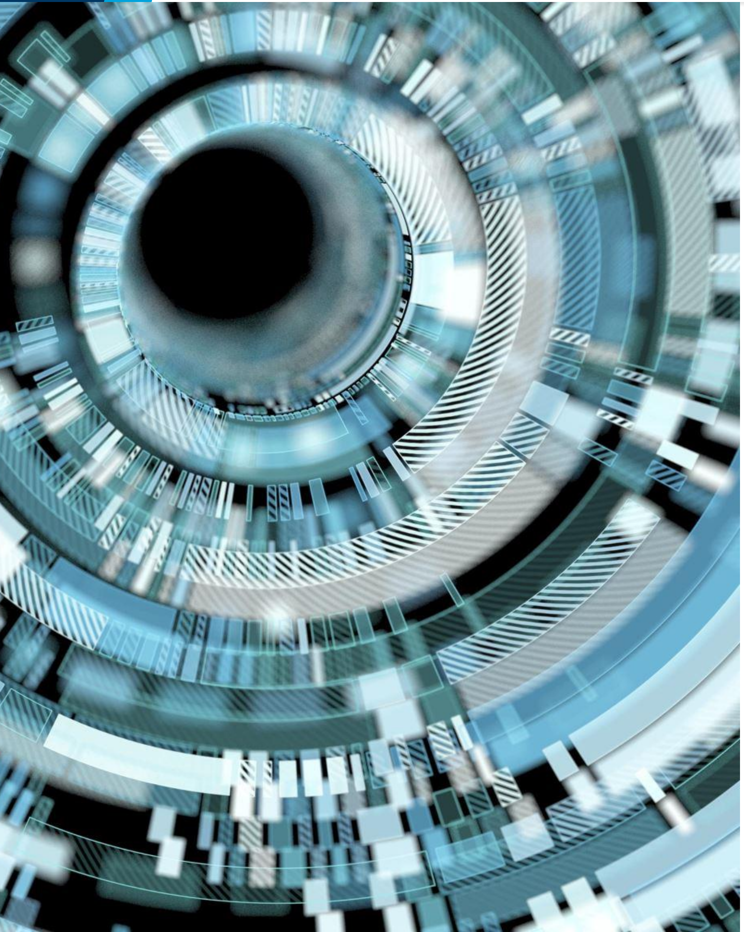
Key Points

- Top concerns
  - Ransomware
  - Remote Worker Security
  - Cyber Insurance
- Recurring themes
  - Multifactor authentication
  - Adopting a Zero Trust mentality

Popular Annual Cybersecurity Reports

- https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
- http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf
- https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf
- https://www.cisco.com/c/en/us/products/security/security-reports.html
- https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

Industry Summary



- The banking industry has fewer breaches than healthcare or general business, but when it happens, banks have the most expensive breaches.

- The 3 biggest topics for 2021 are:
  1. Ransomware
  2. Remote Worker Security
  3. Cybersecurity Insurance

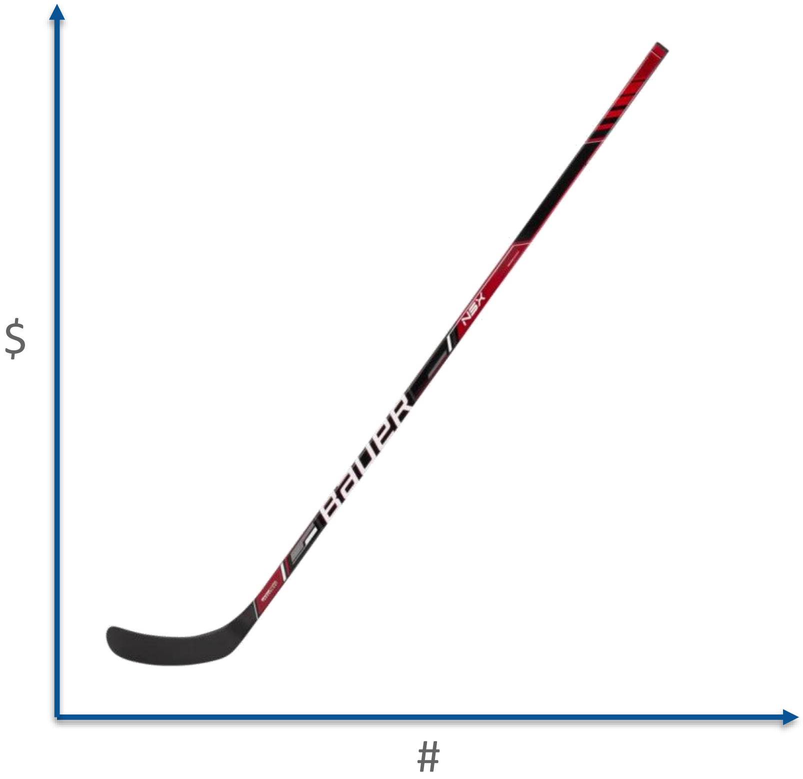
Ransomware

Ransomware

US Department of Justice

- 2020 was "the worst year to date for ransomware attacks.“
- Launching new ransomware task force
  - “…will target the ransomware ecosystem as a whole.”

Colonial Pipeline Company



Ransomware

openIDEO

IN PARTNERSHIP WITH

WILLIAM + FLORA
Hewlett
Foundation

Let's reimagine the visual language of cybersecurity by elevating more representative imagery.

https://www.openideo.com/challenge-briefs/cybersecurity-visuals

Hello John,
I would like to
tell you that
ENCRYPT
bCF74@Sa<B
fJFN^ebCF74
@Sa<BfJFN^e

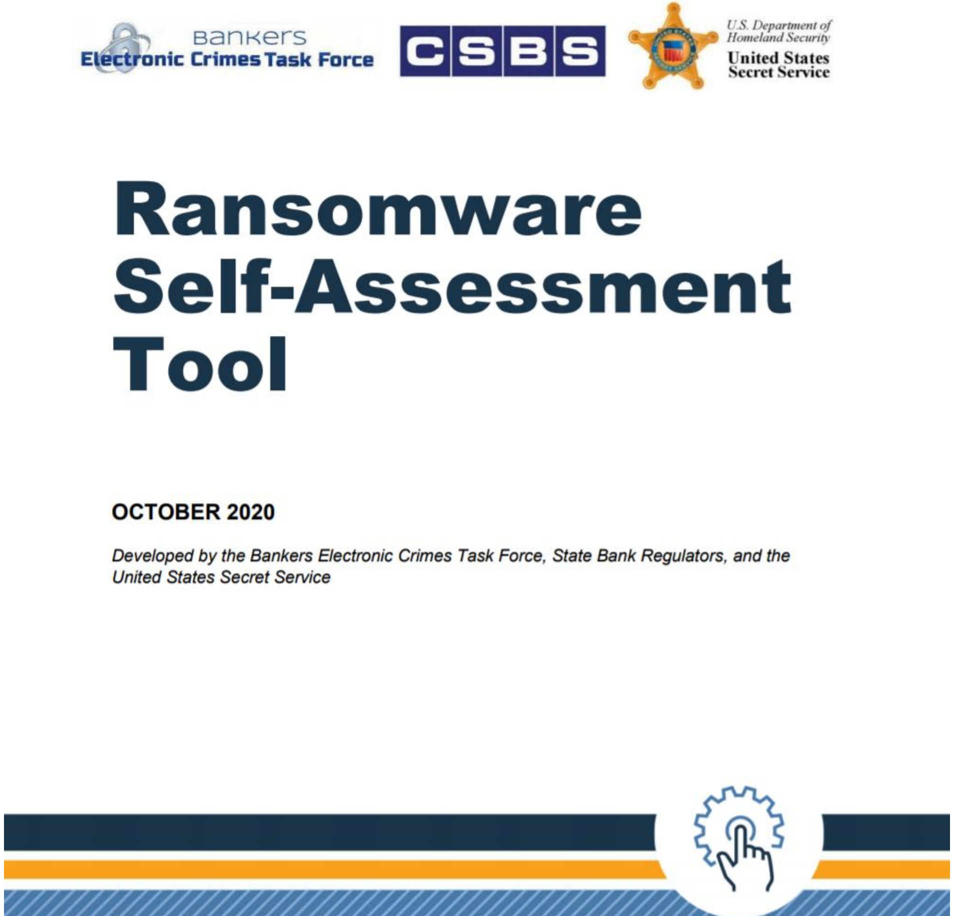
MY OTHER
COMPUTER IS
YOUR
SERVER !

Ransomware

- Big surges, as predicted.
- No signs of slowing.

Ransomware Self Assessment Tool

- 14-page primer
- Not guidance per-se
  - (maybe in Alabama)



Bankers Electronic Crimes Task Force

CSBS

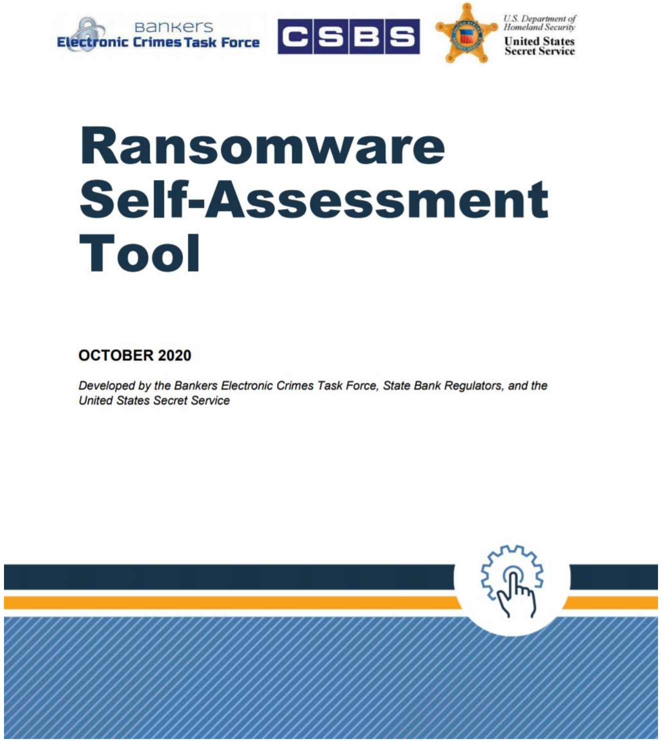
U.S. Department of Homeland Security
United States Secret Service

Ransomware Self-Assessment Tool

OCTOBER 2020

Developed by the Bankers Electronic Crimes Task Force, State Bank Regulators, and the United States Secret Service

Ransomware Self Assessment Tool



Bankers Electronic Crimes Task Force

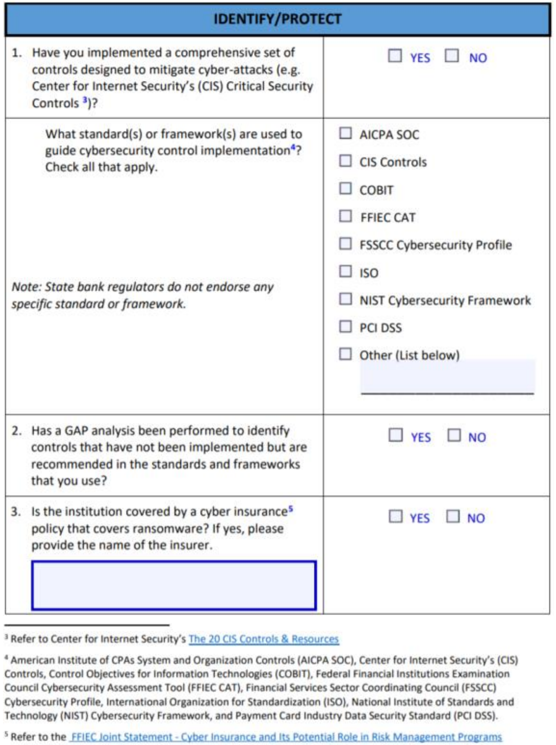
CSBS

U.S. Department of Homeland Security
United States Secret Service

Ransomware Self-Assessment Tool

OCTOBER 2020

Developed by the Bankers Electronic Crimes Task Force, State Bank Regulators, and the United States Secret Service



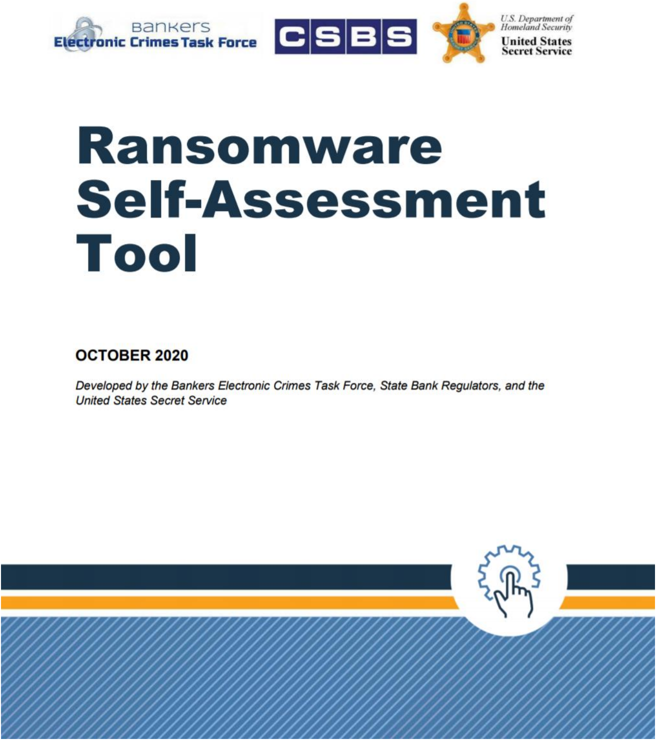
IDENTIFY/PROTECT	
1. Have you implemented a comprehensive set of controls designed to mitigate cyber-attacks (e.g. Center for Internet Security's (CIS) Critical Security Controls [3])?	□ YES □ NO
What standard(s) or framework(s) are used to guide cybersecurity control implementation[4]? Check all that apply. *Note: State bank regulators do not endorse any specific standard or framework.*	□ AICPA SOC □ CIS Controls □ COBIT □ FFIEC CAT □ FSSCC Cybersecurity Profile □ ISO □ NIST Cybersecurity Framework □ PCI DSS □ Other (List below) ________________
2. Has a GAP analysis been performed to identify controls that have not been implemented but are recommended in the standards and frameworks that you use?	□ YES □ NO
3. Is the institution covered by a cyber insurance[5] policy that covers ransomware? If yes, please provide the name of the insurer.	□ YES □ NO

[3] Refer to Center for Internet Security's The 20 CIS Controls & Resources

[4] American Institute of CPAs System and Organization Controls (AICPA SOC), Center for Internet Security's (CIS) Controls, Control Objectives for Information Technologies (COBIT), Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC CAT), Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile, International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST) Cybersecurity Framework, and Payment Card Industry Data Security Standard (PCI DSS).

[5] Refer to the FFIEC Joint Statement - Cyber Insurance and Its Potential Role in Risk Management Programs

Ransomware Self Assessment Tool



Bankers Electronic Crimes Task Force

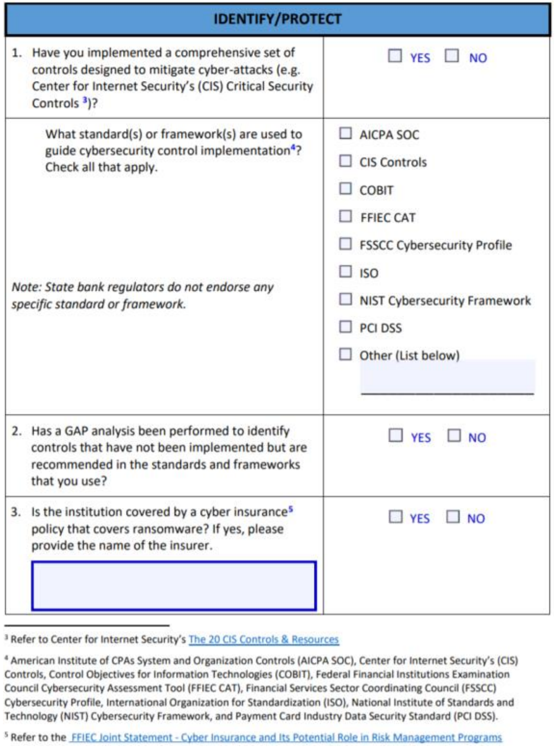
CSBS

U.S. Department of Homeland Security
United States Secret Service

Ransomware Self-Assessment Tool

OCTOBER 2020

Developed by the Bankers Electronic Crimes Task Force, State Bank Regulators, and the United States Secret Service

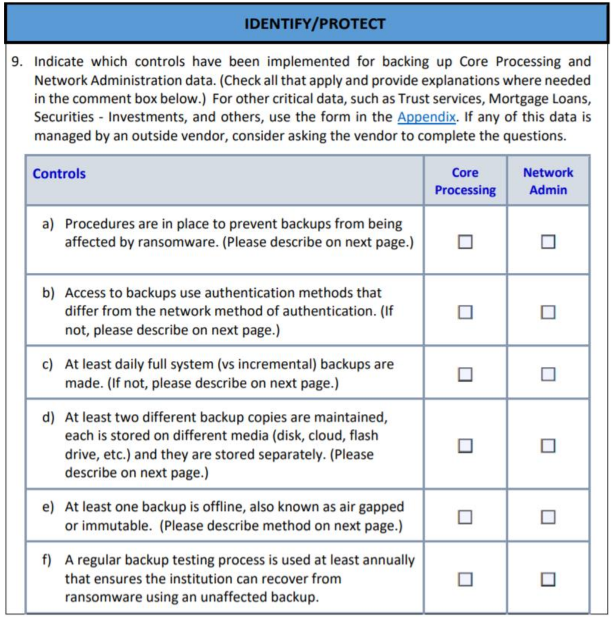


IDENTIFY/PROTECT	
1. Have you implemented a comprehensive set of controls designed to mitigate cyber-attacks (e.g. Center for Internet Security's (CIS) Critical Security Controls [3])?	□ YES □ NO
What standard(s) or framework(s) are used to guide cybersecurity control implementation[4]? Check all that apply. *Note: State bank regulators do not endorse any specific standard or framework.*	□ AICPA SOC □ CIS Controls □ COBIT □ FFIEC CAT □ FSSCC Cybersecurity Profile □ ISO □ NIST Cybersecurity Framework □ PCI DSS □ Other (List below)
2. Has a GAP analysis been performed to identify controls that have not been implemented but are recommended in the standards and frameworks that you use?	□ YES □ NO
3. Is the institution covered by a cyber insurance[5] policy that covers ransomware? If yes, please provide the name of the insurer.	□ YES □ NO

[3] Refer to Center for Internet Security's The 20 CIS Controls & Resources

[4] American Institute of CPAs System and Organization Controls (AICPA SOC), Center for Internet Security's (CIS) Controls, Control Objectives for Information Technologies (COBIT), Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC CAT), Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile, International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST) Cybersecurity Framework, and Payment Card Industry Data Security Standard (PCI DSS).

[5] Refer to the FFIEC Joint Statement - Cyber Insurance and Its Potential Role in Risk Management Programs

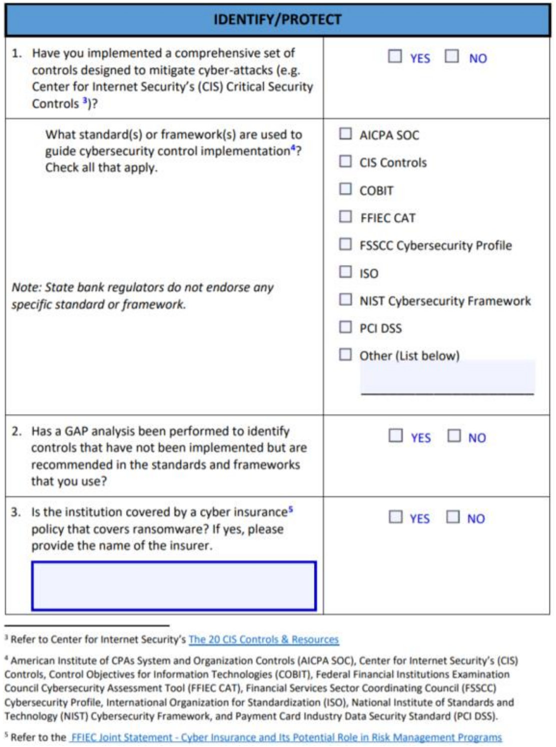


IDENTIFY/PROTECT

9. Indicate which controls have been implemented for backing up Core Processing and Network Administration data. (Check all that apply and provide explanations where needed in the comment box below.) For other critical data, such as Trust services, Mortgage Loans, Securities - Investments, and others, use the form in the Appendix. If any of this data is managed by an outside vendor, consider asking the vendor to complete the questions.

Controls	Core Processing	Network Admin
a) Procedures are in place to prevent backups from being affected by ransomware. (Please describe on next page.)	□	□
b) Access to backups use authentication methods that differ from the network method of authentication. (If not, please describe on next page.)	□	□
c) At least daily full system (vs incremental) backups are made. (If not, please describe on next page.)	□	□
d) At least two different backup copies are maintained, each is stored on different media (disk, cloud, flash drive, etc.) and they are stored separately. (Please describe on next page.)	□	□
e) At least one backup is offline, also known as air gapped or immutable. (Please describe method on next page.)	□	□
f) A regular backup testing process is used at least annually that ensures the institution can recover from ransomware using an unaffected backup.	□	□

Ransomware Self Assessment Tool

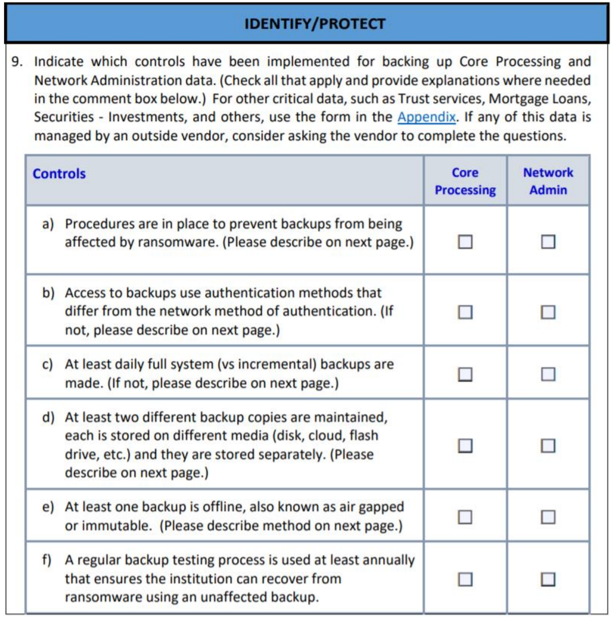


IDENTIFY/PROTECT	
1. Have you implemented a comprehensive set of controls designed to mitigate cyber-attacks (e.g. Center for Internet Security's (CIS) Critical Security Controls [3])?	☐ YES ☐ NO
What standard(s) or framework(s) are used to guide cybersecurity control implementation[4]? Check all that apply. *Note: State bank regulators do not endorse any specific standard or framework.*	☐ AICPA SOC ☐ CIS Controls ☐ COBIT ☐ FFIEC CAT ☐ FSSCC Cybersecurity Profile ☐ ISO ☐ NIST Cybersecurity Framework ☐ PCI DSS ☐ Other (List below)
2. Has a GAP analysis been performed to identify controls that have not been implemented but are recommended in the standards and frameworks that you use?	☐ YES ☐ NO
3. Is the institution covered by a cyber insurance[5] policy that covers ransomware? If yes, please provide the name of the insurer.	☐ YES ☐ NO

[3] Refer to Center for Internet Security's The 20 CIS Controls & Resources

[4] American Institute of CPAs System and Organization Controls (AICPA SOC), Center for Internet Security's (CIS) Controls, Control Objectives for Information Technologies (COBIT), Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC CAT), Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile, International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST) Cybersecurity Framework, and Payment Card Industry Data Security Standard (PCI DSS).

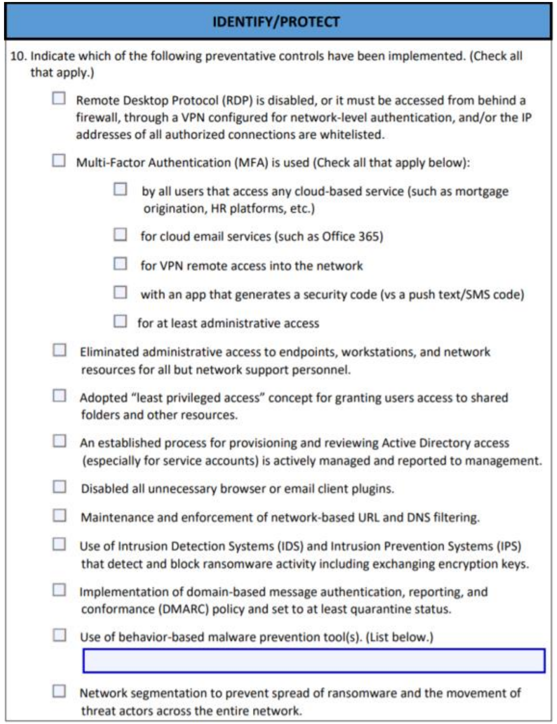
[5] Refer to the FFIEC Joint Statement - Cyber Insurance and Its Potential Role in Risk Management Programs



IDENTIFY/PROTECT

9. Indicate which controls have been implemented for backing up Core Processing and Network Administration data. (Check all that apply and provide explanations where needed in the comment box below.) For other critical data, such as Trust services, Mortgage Loans, Securities - Investments, and others, use the form in the Appendix. If any of this data is managed by an outside vendor, consider asking the vendor to complete the questions.

Controls	Core Processing	Network Admin
a) Procedures are in place to prevent backups from being affected by ransomware. (Please describe on next page.)	☐	☐
b) Access to backups use authentication methods that differ from the network method of authentication. (If not, please describe on next page.)	☐	☐
c) At least daily full system (vs incremental) backups are made. (If not, please describe on next page.)	☐	☐
d) At least two different backup copies are maintained, each is stored on different media (disk, cloud, flash drive, etc.) and they are stored separately. (Please describe on next page.)	☐	☐
e) At least one backup is offline, also known as air gapped or immutable. (Please describe method on next page.)	☐	☐
f) A regular backup testing process is used at least annually that ensures the institution can recover from ransomware using an unaffected backup.	☐	☐



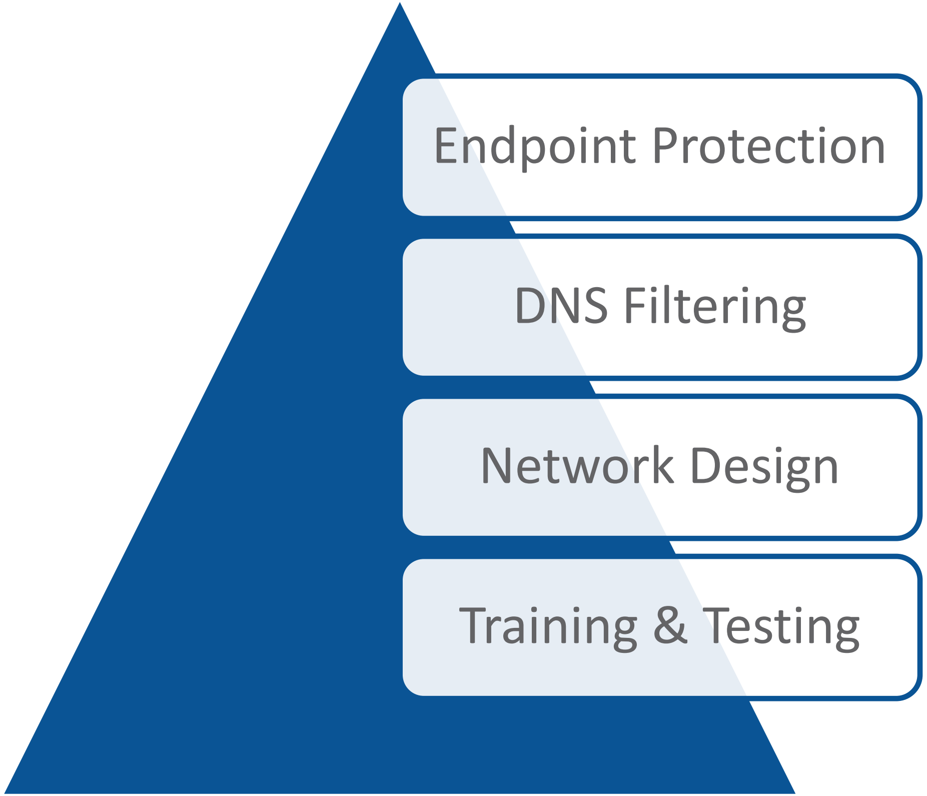
IDENTIFY/PROTECT

10. Indicate which of the following preventative controls have been implemented. (Check all that apply.)

- ☐ Remote Desktop Protocol (RDP) is disabled, or it must be accessed from behind a firewall, through a VPN configured for network-level authentication, and/or the IP addresses of all authorized connections are whitelisted.
- ☐ Multi-Factor Authentication (MFA) is used (Check all that apply below):
  - ☐ by all users that access any cloud-based service (such as mortgage origination, HR platforms, etc.)
  - ☐ for cloud email services (such as Office 365)
  - ☐ for VPN remote access into the network
  - ☐ with an app that generates a security code (vs a push text/SMS code)
  - ☐ for at least administrative access
- ☐ Eliminated administrative access to endpoints, workstations, and network resources for all but network support personnel.
- ☐ Adopted "least privileged access" concept for granting users access to shared folders and other resources.
- ☐ An established process for provisioning and reviewing Active Directory access (especially for service accounts) is actively managed and reported to management.
- ☐ Disabled all unnecessary browser or email client plugins.
- ☐ Maintenance and enforcement of network-based URL and DNS filtering.
- ☐ Use of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) that detect and block ransomware activity including exchanging encryption keys.
- ☐ Implementation of domain-based message authentication, reporting, and conformance (DMARC) policy and set to at least quarantine status.
- ☐ Use of behavior-based malware prevention tool(s). (List below.)
- ☐ Network segmentation to prevent spread of ransomware and the movement of threat actors across the entire network.

Ransomware Response - Objective

Ransomware Response - Prevention



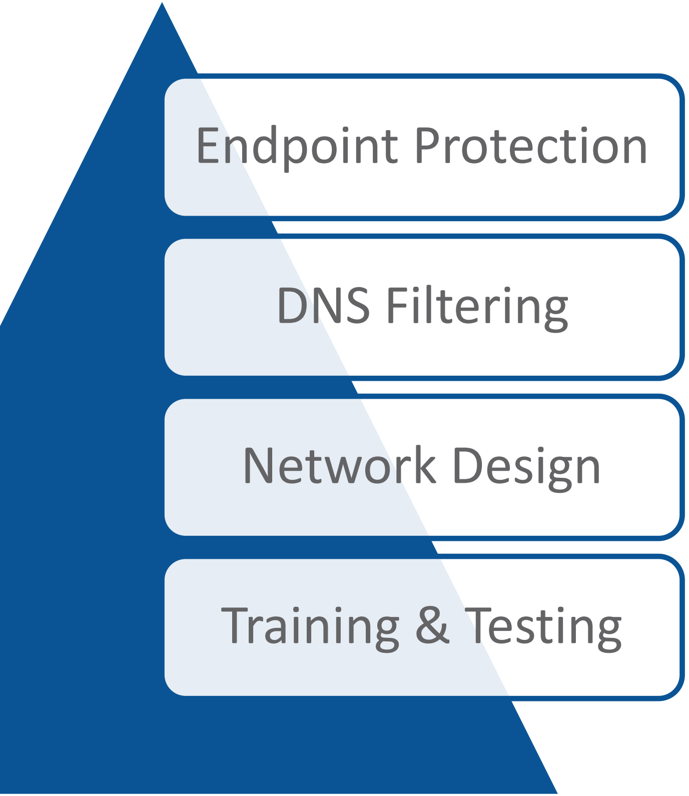
Endpoint Protection

DNS Filtering

Network Design

Training & Testing

Ransomware Response - Prevention



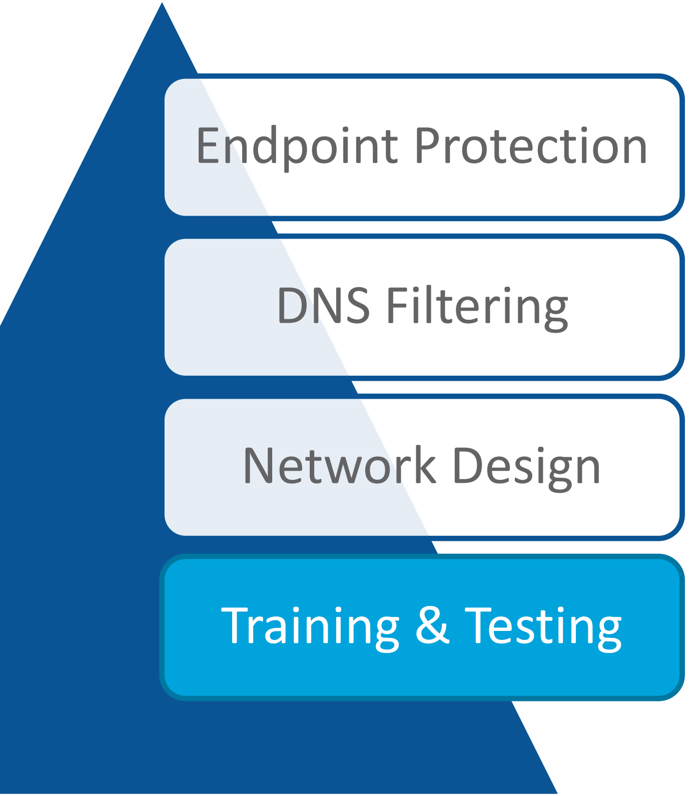
Endpoint Protection

DNS Filtering

Network Design

Training & Testing

Ransomware Response - Prevention



Endpoint Protection

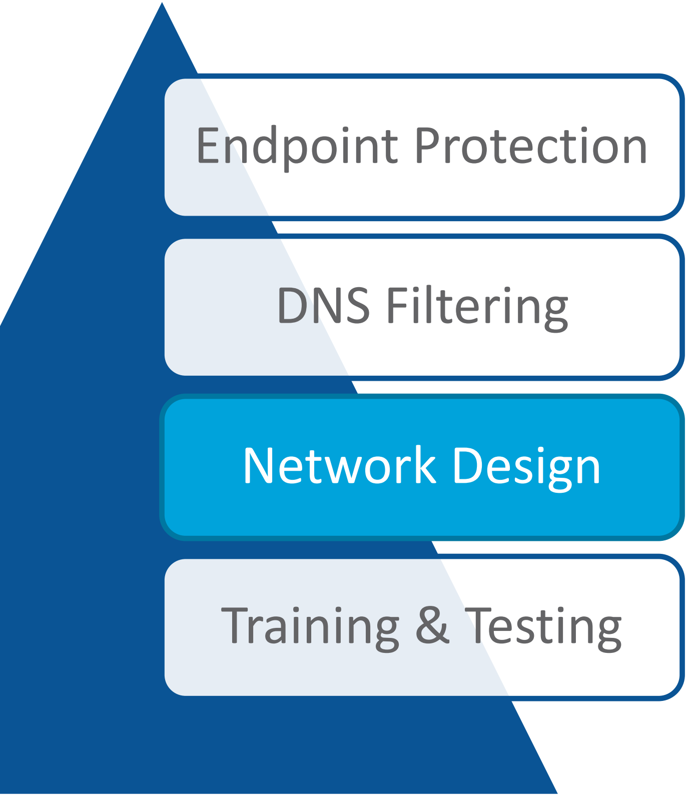
DNS Filtering

Network Design

Training & Testing

KnowBe4

Ransomware Response - Prevention

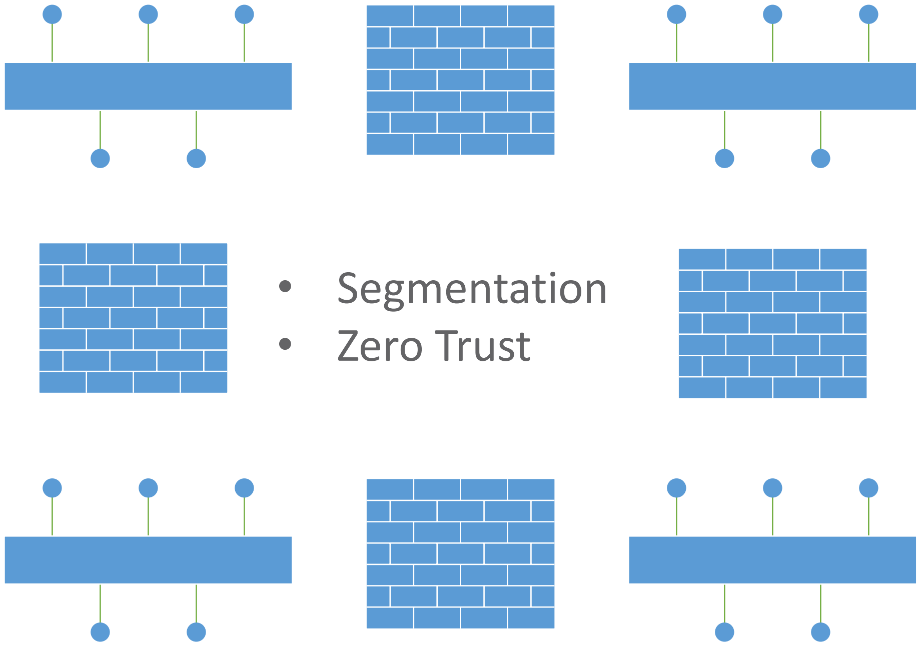


Endpoint Protection

DNS Filtering

Network Design

Training & Testing

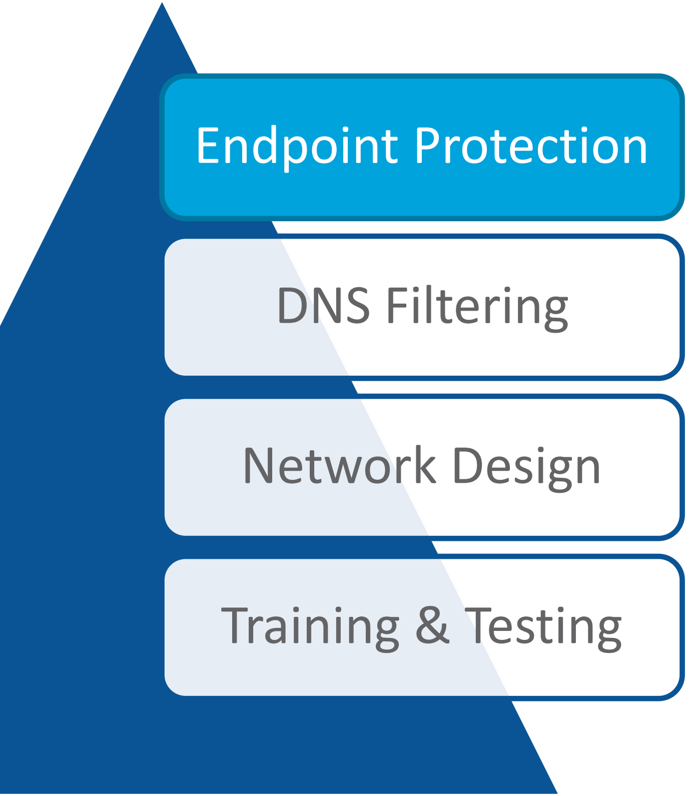


- Segmentation
- Zero Trust

Ransomware Response - Prevention

- Endpoint Protection
- DNS Filtering
- Network Design
- Training & Testing

Ransomware Response - Prevention



Endpoint Protection

DNS Filtering

Network Design

Training & Testing

Bitdefender

Symantec.

McAfee™

TREND MICRO

Ransomware Response - Recovery

Backups

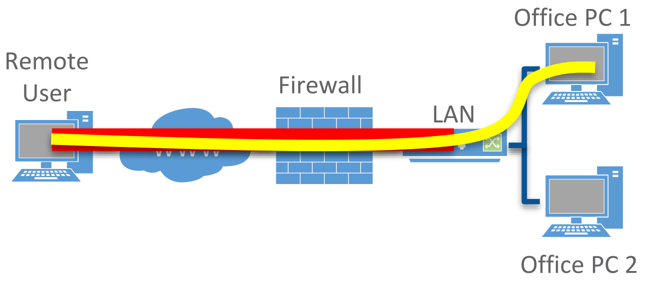
- Reliable
- Out of reach of ransomware

Remote Worker Security

Remote Access Models

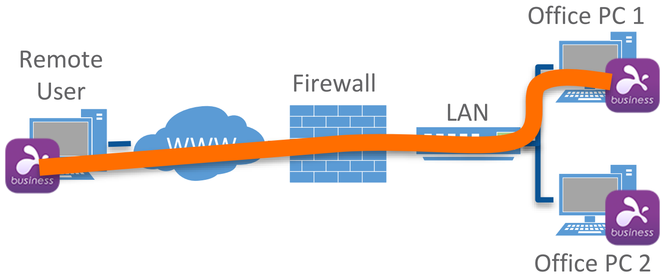
VPN

1. Connect to network
   - Example: NetExtender
2. Launch control software
   - Example: Windows Remote Desktop



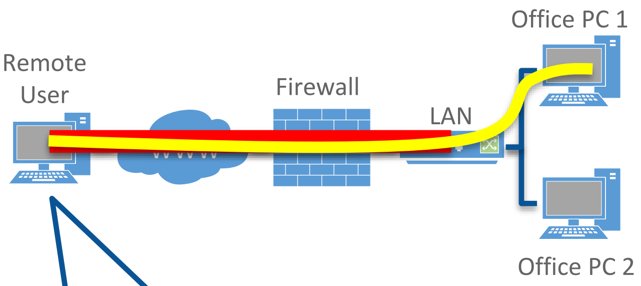
Remote Access Applications

- Examples: GoToMyPC, Splashtop
- Connect and Control in one app



Which is Safer?

VPN



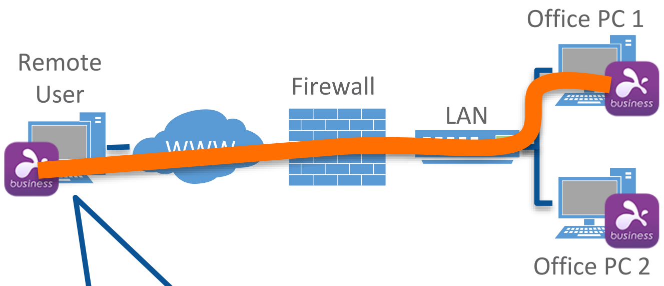
Who's device?

👍 Bank laptop →

- Patches
- AV
- DNS filter
- Etc.

✗ Home PC

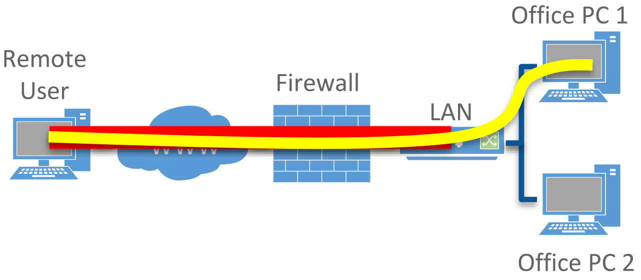
Remote Access Applications



Opened the door for emergency use of home PC's

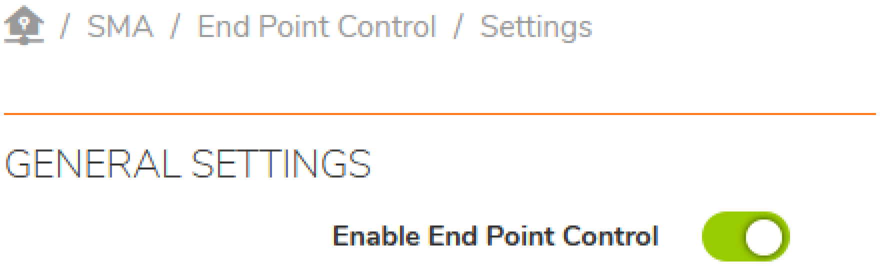
Look into endpoint control features

VPN



Examples

- Require certain OS attributes
- Require certain AV product

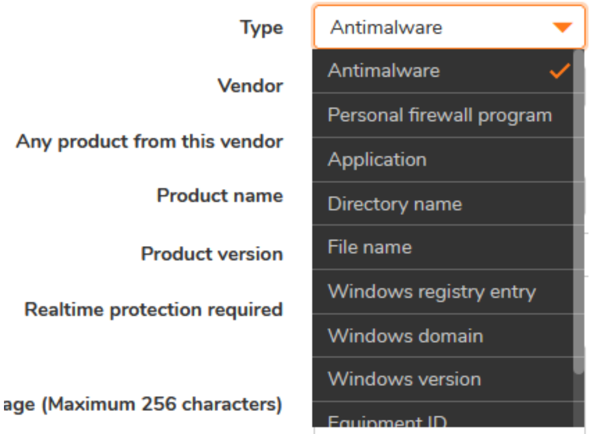

/ SMA / End Point Control / Settings

GENERAL SETTINGS

Enable End Point Control ●

Sonicwall SMA Endpoint Control

Possible Attributes



Type: Antimalware

Vendor

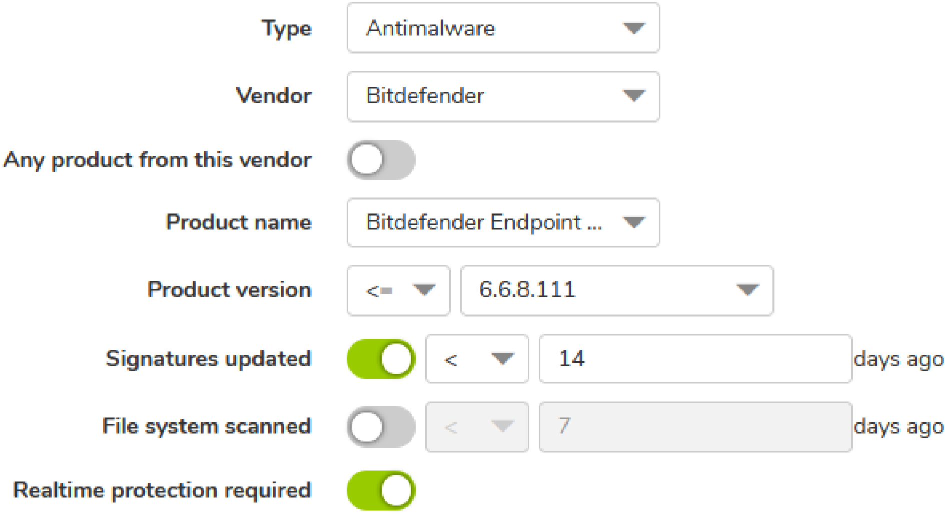
Any product from this vendor

Product name

Product version

Realtime protection required

age (Maximum 256 characters)



Type: Antimalware

Vendor: Bitdefender

Any product from this vendor: ○ off

Product name: Bitdefender Endpoint ...

Product version: <= 6.6.8.111

Signatures updated: ● on < 14 days ago

File system scanned: ○ off < 7 days ago

Realtime protection required: ● on

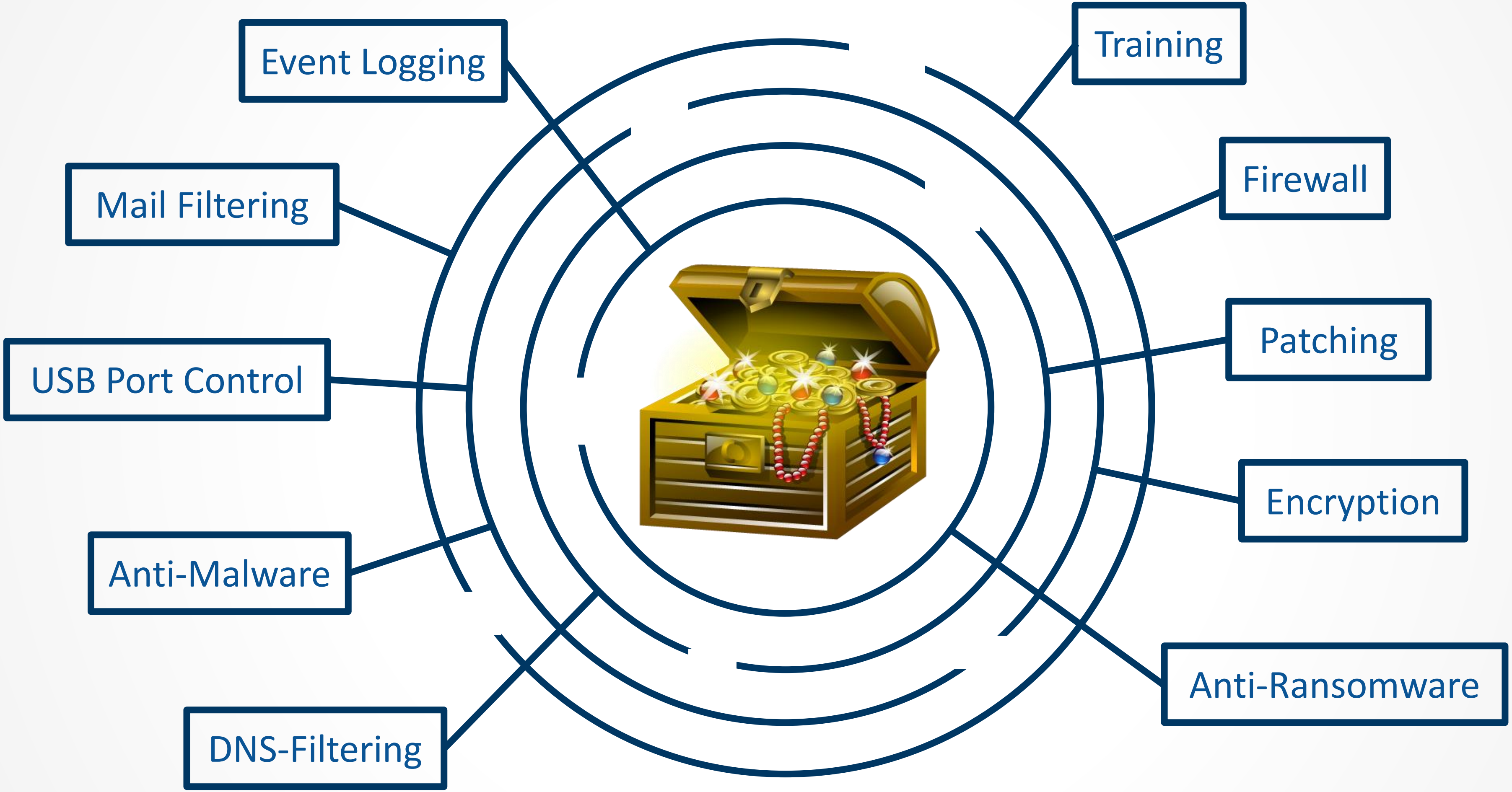
Cyber Insurance

Cyber Insurance

- It’s been a rough year for the insurance carriers
  - Frequent large payouts
  - Underfunded coffers
- Raising the bar
  - To unreachable heights?
  - Maybe just for now
- Biggest hurdle
  - MFA everywhere

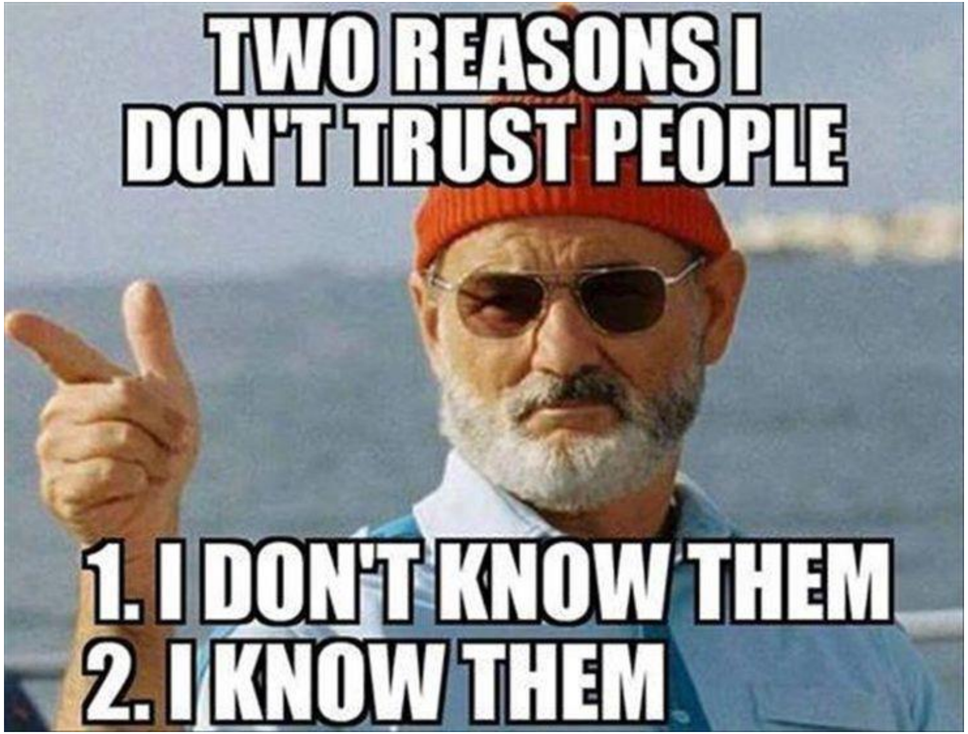
Zero Trust

Castle and Moat Doctrine


Event Logging
Training
Mail Filtering
Firewall
Patching
USB Port Control
Encryption
Anti-Malware
Anti-Ransomware
DNS-Filtering

Zero Trust Doctrine

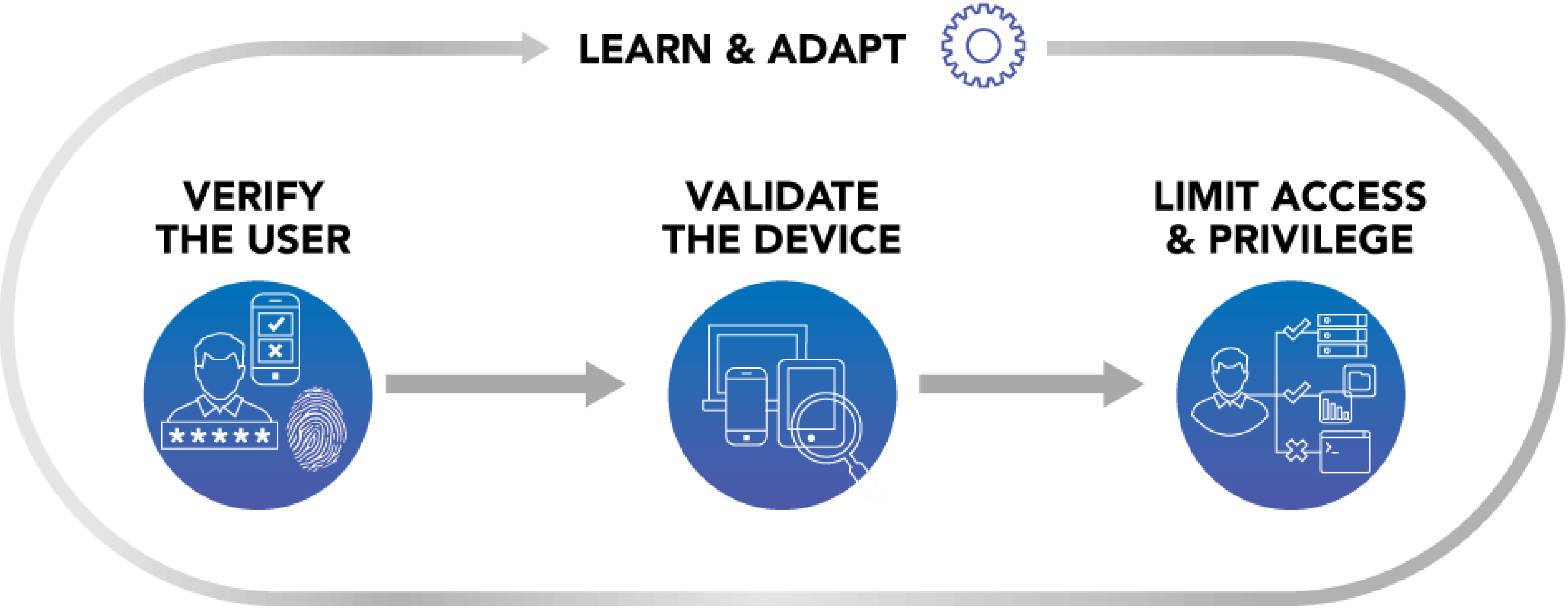
- “The belief that organizations should not automatically trust anything *inside* or *outside* its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.”
- Not a new concept
  - First paper in 2010
- This is not a product nor a technology.



Safe Systems®

https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

Zero Trust Model



LEARN & ADAPT

VERIFY THE USER

VALIDATE THE DEVICE

LIMIT ACCESS & PRIVILEGE

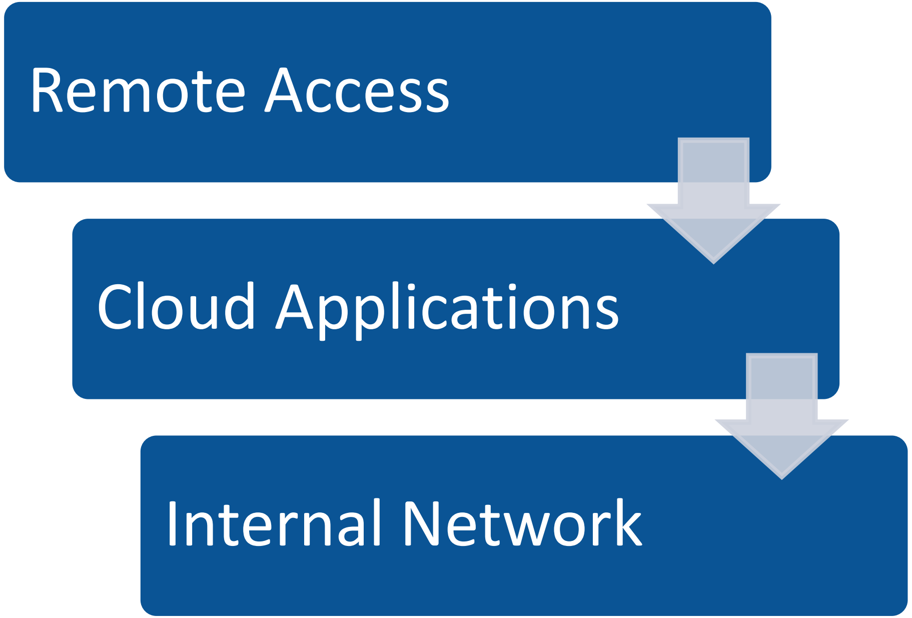
Enabling Technologies

- Big reach for community FI's today
  - Network micro-segmentation through software defined networking ("firewalls" everywhere)
  - Automatic Privilege Management tools
- Leading edge for the community FI today
  - Multifactor Authentication

What is looks like in practice

- A user can plug into a “LAN” switch, WiFi, or VPN and get the same experience.
- They can’t see anything useful until they have been authenticated and their device has been validated
- Then they can only see the specific apps and files to which they have been granted least-privilege access

MFA Adoption Path



Remote Access

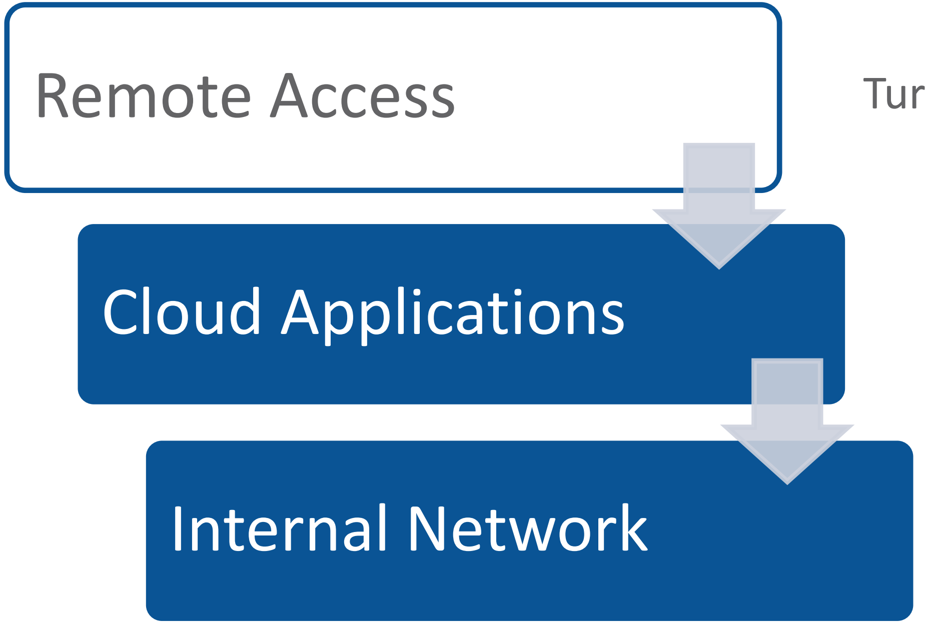
Cloud Applications

Internal Network

- “Zero Trust is incremental. It is built out one protect surface at a time so that it is done in an iterative and non-disruptive manner.”
- Start with MFA

https://www.helpnetsecurity.com/2021/04/06/john-kindervag-zero-trust/

MFA Adoption Path

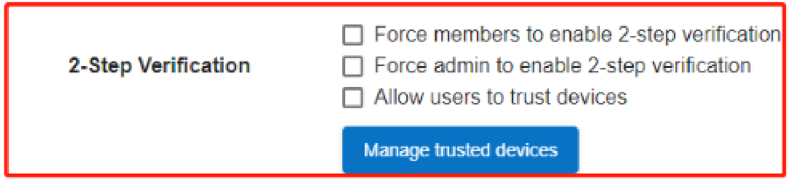


Remote Access

Cloud Applications

Internal Network

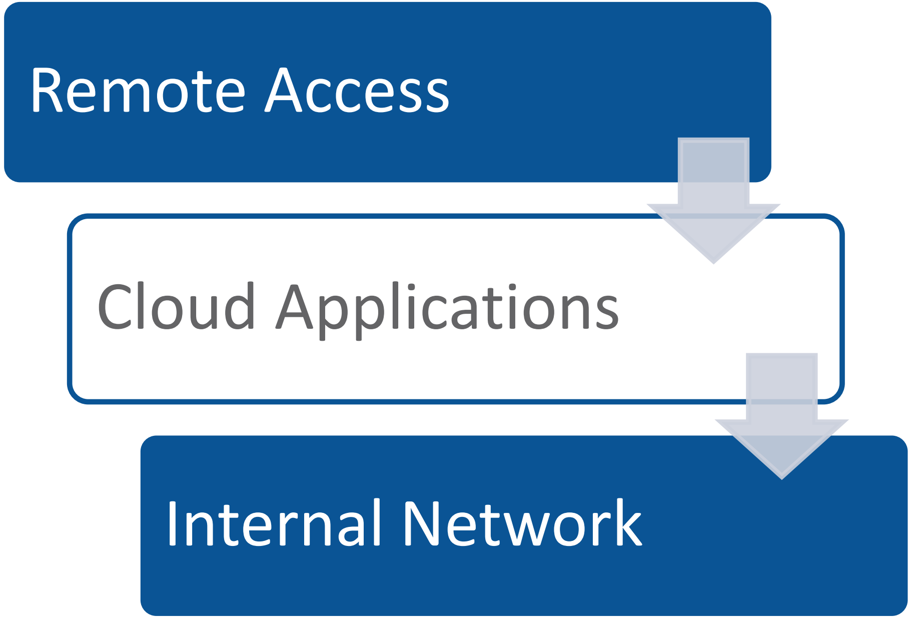
Turn it on in your vpn/remote access product



2-Step Verification

□ Force members to enable 2-step verification
□ Force admin to enable 2-step verification
□ Allow users to trust devices

MFA Adoption Path



Remote Access

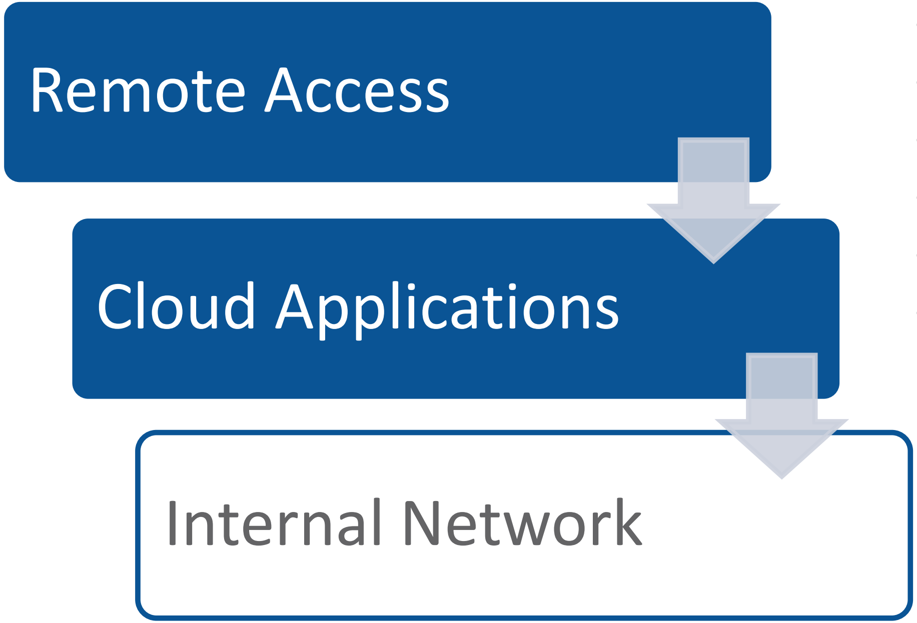
Cloud Applications

Internal Network

Office 365

Multi-factor Authentication

MFA Adoption Path



- Not as easy
- Requires agent installations
- Break-glass-accounts
- Becomes another infrastructure
- This is the new frontier for our industry
- Vendors still being vetted

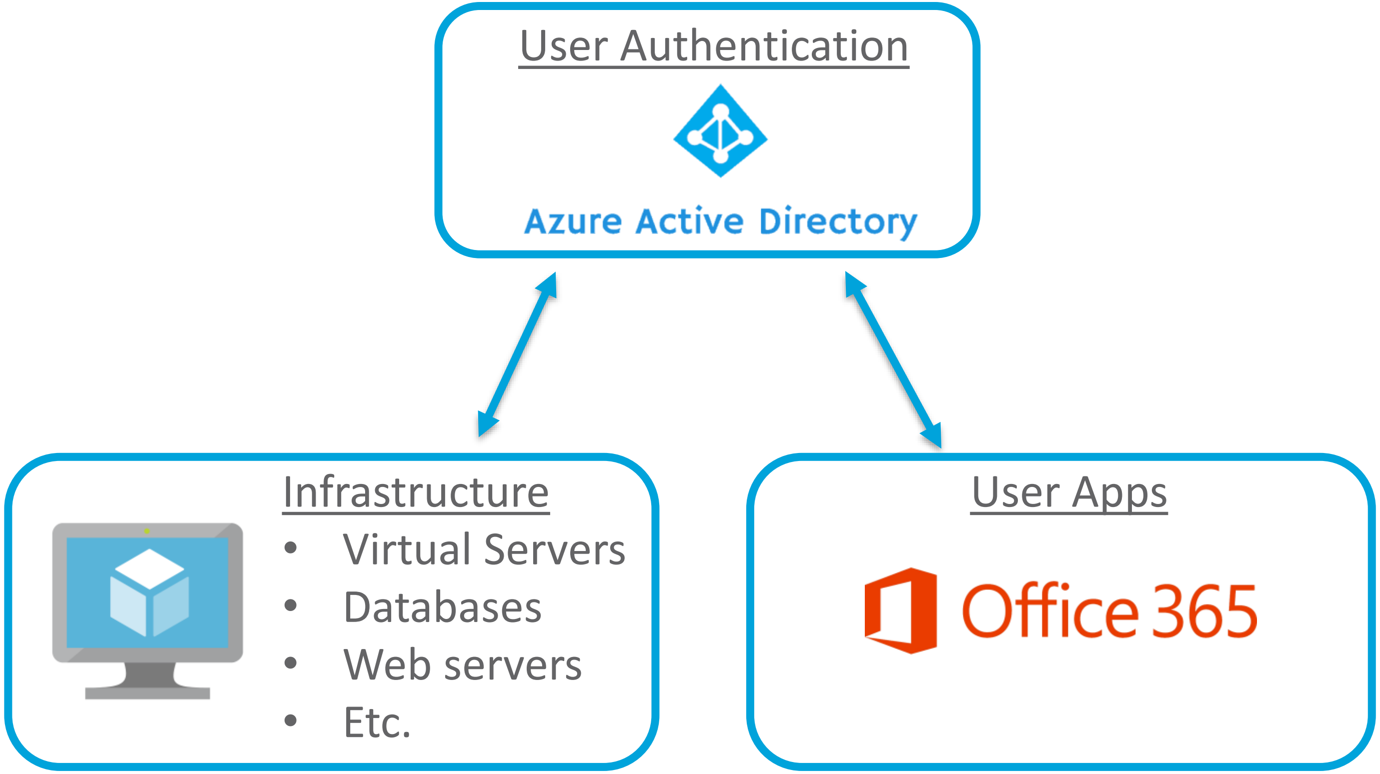
DUO okta

LastPass••• Ping Identity onelogin

RSA SECUREAUTH SECRET DOUBLE OCTOPUS

Azure AD

Microsoft Azure



User Authentication

Azure Active Directory

Infrastructure

- Virtual Servers
- Databases
- Web servers
- Etc.

User Apps

Office 365

Add-On Microsoft Cloud Licensing

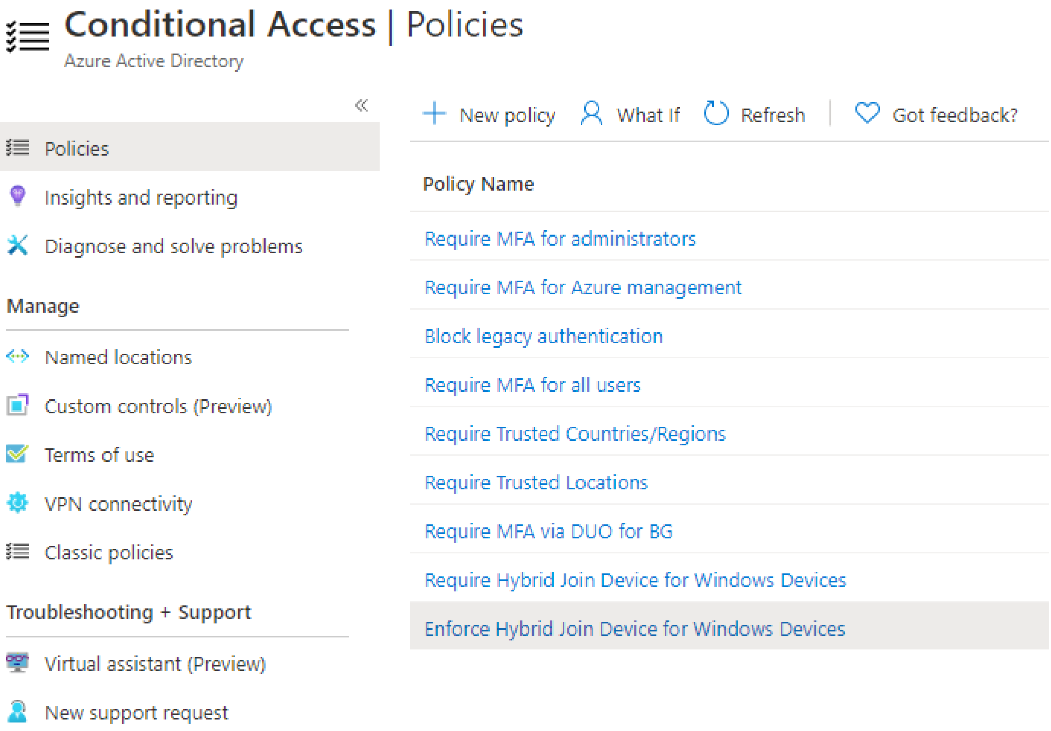
- Feature: Conditional Access Policies
  - “I want MFA for everyone except John when he’s using his bank laptop at the bank.”
  - “I want to block any O365 login attempts from most countries but allow it from the country my CEO is traveling to next week.”
  - “I want to allow O365 login only from PC’s owned by the bank.”

- Available through higher O365 licenses or add-ons like Azure Active Directory Premium P1

Conditional Access Policy Configuration

https://portal.azure.com

- → Azure AD
- → Security
- → Conditional Access



Conditional Access | Policies

Azure Active Directory

Policy Name
Require MFA for administrators
Require MFA for Azure management
Block legacy authentication
Require MFA for all users
Require Trusted Countries/Regions
Require Trusted Locations
Require MFA via DUO for BG
Require Hybrid Join Device for Windows Devices
Enforce Hybrid Join Device for Windows Devices

Safe Systems®

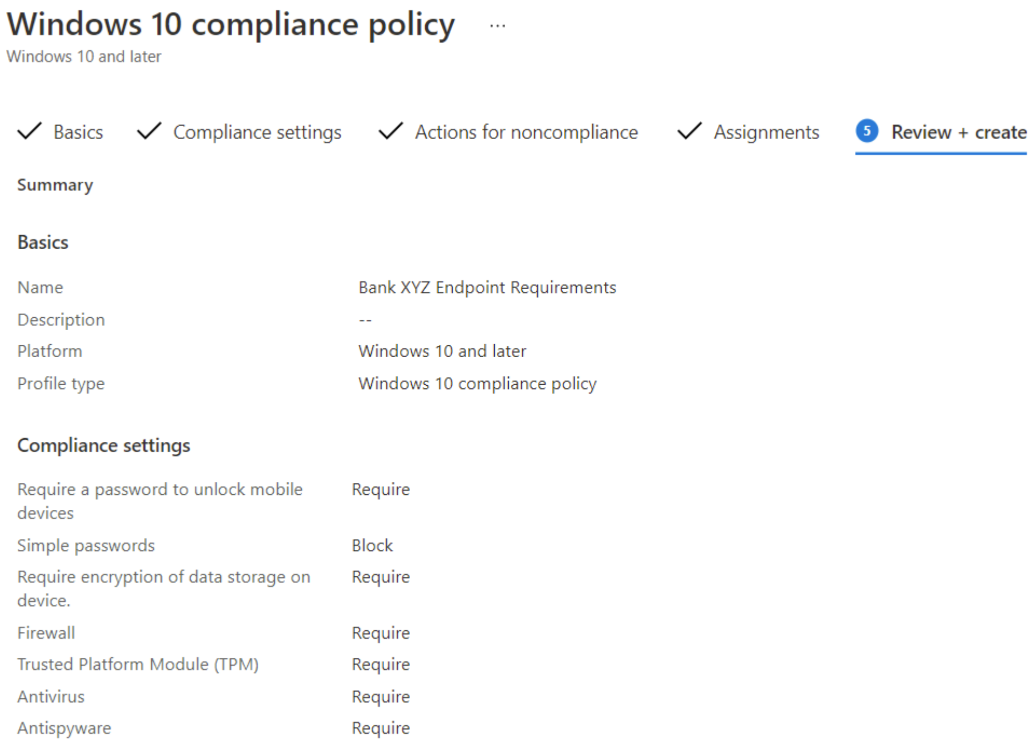
Add-On Microsoft Cloud Licensing

- Feature: Device App Control
  - “I want to make sure certain apps are installed and certain apps are blocked on bank devices.”
  - “I need protection beyond my mailbox settings.”
- Available through higher O365 licenses or add-ons that give you access to Microsoft Intune (Device Management)

Endpoint Security Configuration

https://endpoint.microsoft.com

- → Devices
- → Windows
- → Compliance Policies



Windows 10 compliance policy ···

Windows 10 and later

Summary

Basics

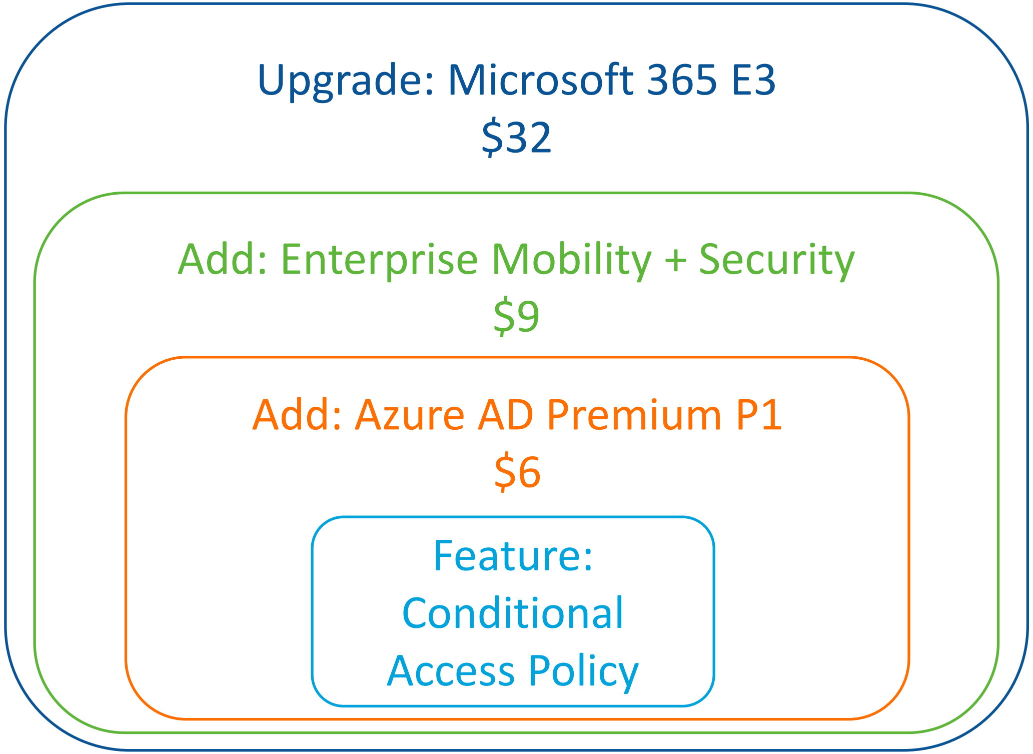
Name	Bank XYZ Endpoint Requirements
Description	--
Platform	Windows 10 and later
Profile type	Windows 10 compliance policy

Compliance settings

Require a password to unlock mobile devices	Require
Simple passwords	Block
Require encryption of data storage on device.	Require
Firewall	Require
Trusted Platform Module (TPM)	Require
Antivirus	Require
Antispyware	Require

Safe Systems®

License Nesting



Upgrade: Microsoft 365 E3
$32

Add: Enterprise Mobility + Security
$9

Add: Azure AD Premium P1
$6

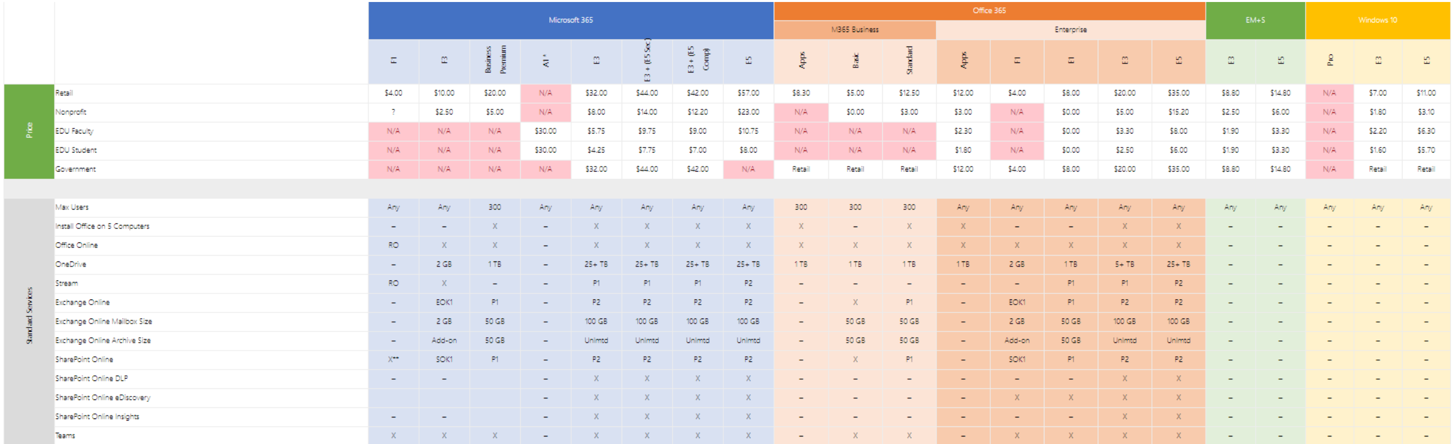
Feature:
Conditional
Access Policy

Many paths to get Conditional Access Policies

Licensing navigation

Third party attempt at mapping out O365 licensing

- Not guaranteed to be accurate nor up to date



		Microsoft 365								Office 365								EM+S		Windows 10		
										M365 Business			Enterprise									
		F1	F3	Business Premium	A1 *	E3	E3 + (E5 Sec)	E3 + (E5 Comp)	E5	Apps	Basic	Standard	Apps	F1	E1	E3	E5	E3	E5	Pro	E3	E5
Price	Retail	$4.00	$10.00	$20.00	N/A	$32.00	$44.00	$42.00	$57.00	$8.30	$5.00	$12.50	$12.00	$4.00	$8.00	$20.00	$35.00	$8.80	$14.80	N/A	$7.00	$11.00
	Nonprofit	?	$2.50	$5.00	N/A	$8.00	$14.00	$12.20	$23.00	N/A	$0.00	$3.00	$3.00	N/A	$0.00	$5.00	$15.20	$2.50	$6.00	N/A	$1.80	$3.10
	EDU Faculty	N/A	N/A	N/A	$30.00	$5.75	$9.75	$9.00	$10.75	N/A	N/A	N/A	$2.30	N/A	$0.00	$3.30	$8.00	$1.90	$3.30	N/A	$2.20	$6.30
	EDU Student	N/A	N/A	N/A	$30.00	$4.25	$7.75	$7.00	$8.00	N/A	N/A	N/A	$1.80	N/A	$0.00	$2.50	$6.00	$1.90	$3.30	N/A	$1.60	$5.70
	Government	N/A	N/A	N/A	N/A	$32.00	$44.00	$42.00	N/A	Retail	Retail	Retail	$12.00	$4.00	$8.00	$20.00	$35.00	$8.80	$14.80	N/A	Retail	Retail
Standard Services	Max Users	Any	Any	300	Any	Any	Any	Any	Any	300	300	300	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any
	Install Office on 5 Computers	–	–	X	–	X	X	X	X	X	–	X	X	–	–	X	X	–	–	–	–	–
	Office Online	RO	X	X	–	X	X	X	X	X	X	X	X	X	X	X	X	–	–	–	–	–
	OneDrive	–	2 GB	1 TB	–	25+ TB	25+ TB	25+ TB	25+ TB	1 TB	1 TB	1 TB	1 TB	2 GB	1 TB	5+ TB	25+ TB	–	–	–	–	–
	Stream	RO	X	–	–	P1	P1	P1	P2	–	–	–	–	–	P1	P1	P2	–	–	–	–	–
	Exchange Online	–	EOK1	P1	–	P2	P2	P2	P2	–	X	P1	–	EOK1	P1	P2	P2	–	–	–	–	–
	Exchange Online Mailbox Size	–	2 GB	50 GB	–	100 GB	100 GB	100 GB	100 GB	–	50 GB	50 GB	–	2 GB	50 GB	100 GB	100 GB	–	–	–	–	–
	Exchange Online Archive Size	–	Add-on	50 GB	–	Unlmtd	Unlmtd	Unlmtd	Unlmtd	–	50 GB	50 GB	–	Add-on	50 GB	Unlmtd	Unlmtd	–	–	–	–	–
	SharePoint Online	X**	SOK1	P1	–	P2	P2	P2	P2	–	X	P1	–	SOK1	P1	P2	P2	–	–	–	–	–
	SharePoint Online DLP	–	–		–	X	X	X	X	–	–	–	–	–	–	X	X	–	–	–	–	–
	SharePoint Online eDiscovery				–	X	X	X	X	–	–	–	–	X	X	X	X	–	–	–	–	–
	SharePoint Online Insights	–	–		–	X	X	X	X	–	–	–	–	–	–	X	X	–	–	–	–	–
	Teams	X	X	X	–	X	X	X	X	–	X	X	–	X	X	X	X	–	–	–	–	–

https://www.infusedinnovations.com/blog/secure-modern-workplace/complete-office-365-and-microsoft-365-licensing-comparison

Internally at Safe Systems

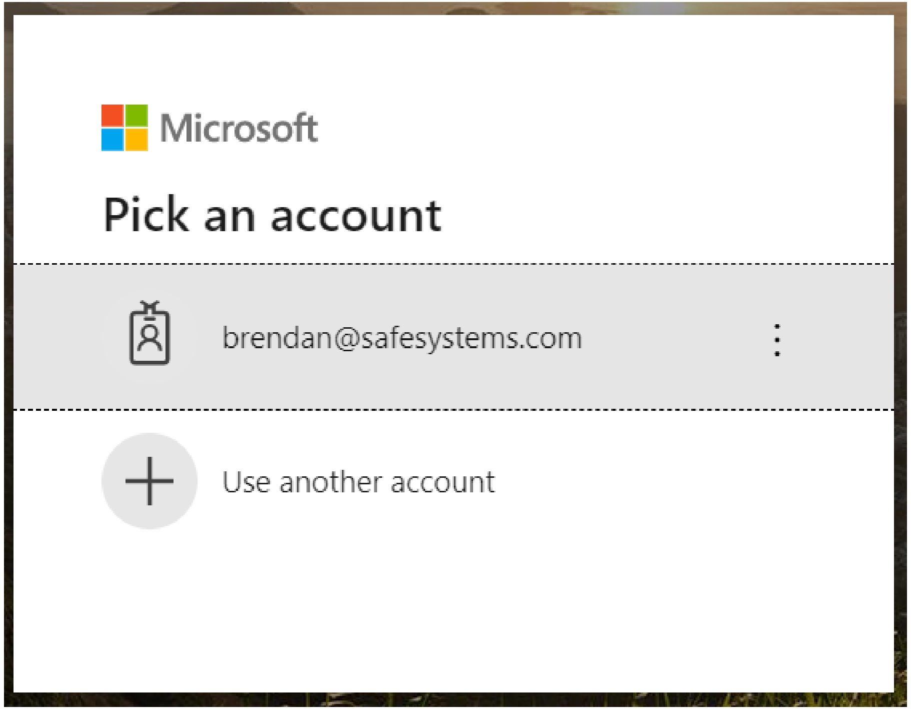
- Azure AD for identity wherever possible
  - O365, Salesforce, Smartsheet, VPN, etc.
- Azure AD Conditional Access Policies per application
  - Role-based access by user group
  - Geographical exclusions
  - Granular exception policies per group/user
- Device policies
  - Must be SS owned PC

Passwordless Experience

Phone Sign-In: In Use

Logging into O365 on PC

On PC



Microsoft

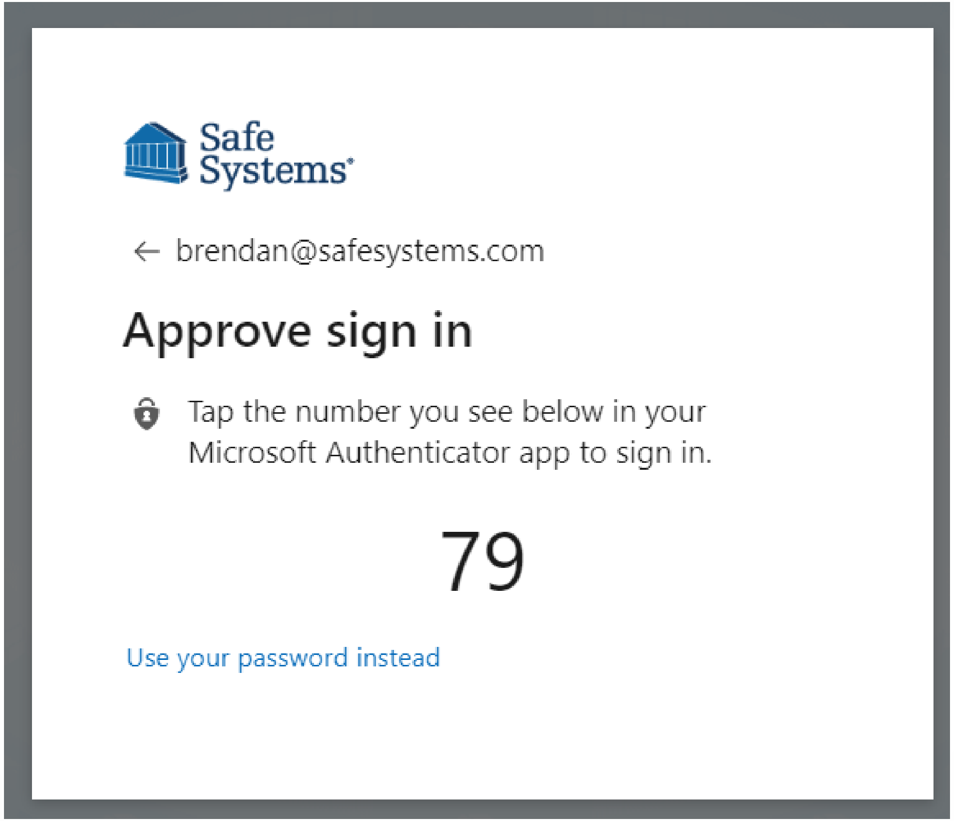
Pick an account

brendan@safesystems.com

Use another account

Phone Sign-In: In Use

On PC



Safe Systems®

← brendan@safesystems.com

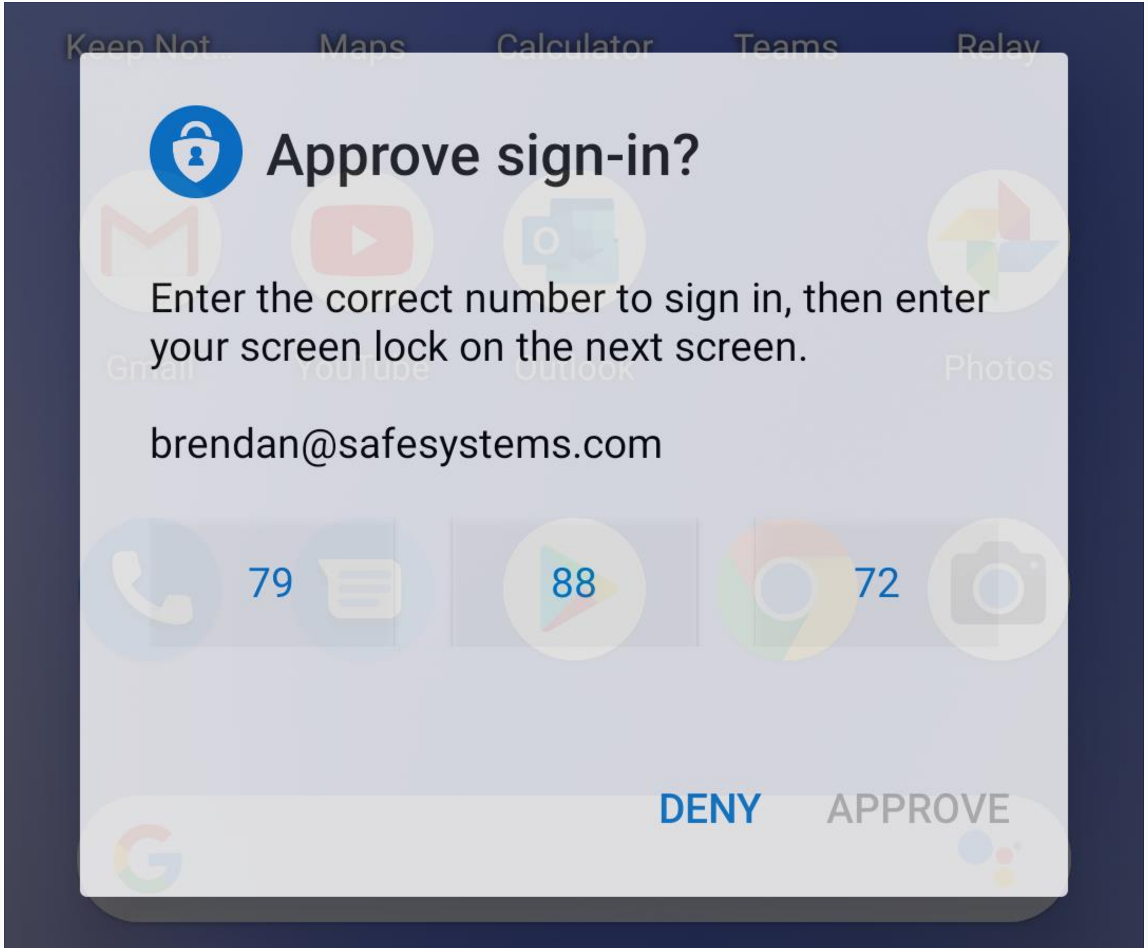
Approve sign in

Tap the number you see below in your Microsoft Authenticator app to sign in.

79

Use your password instead

Phone Sign-In: In Use



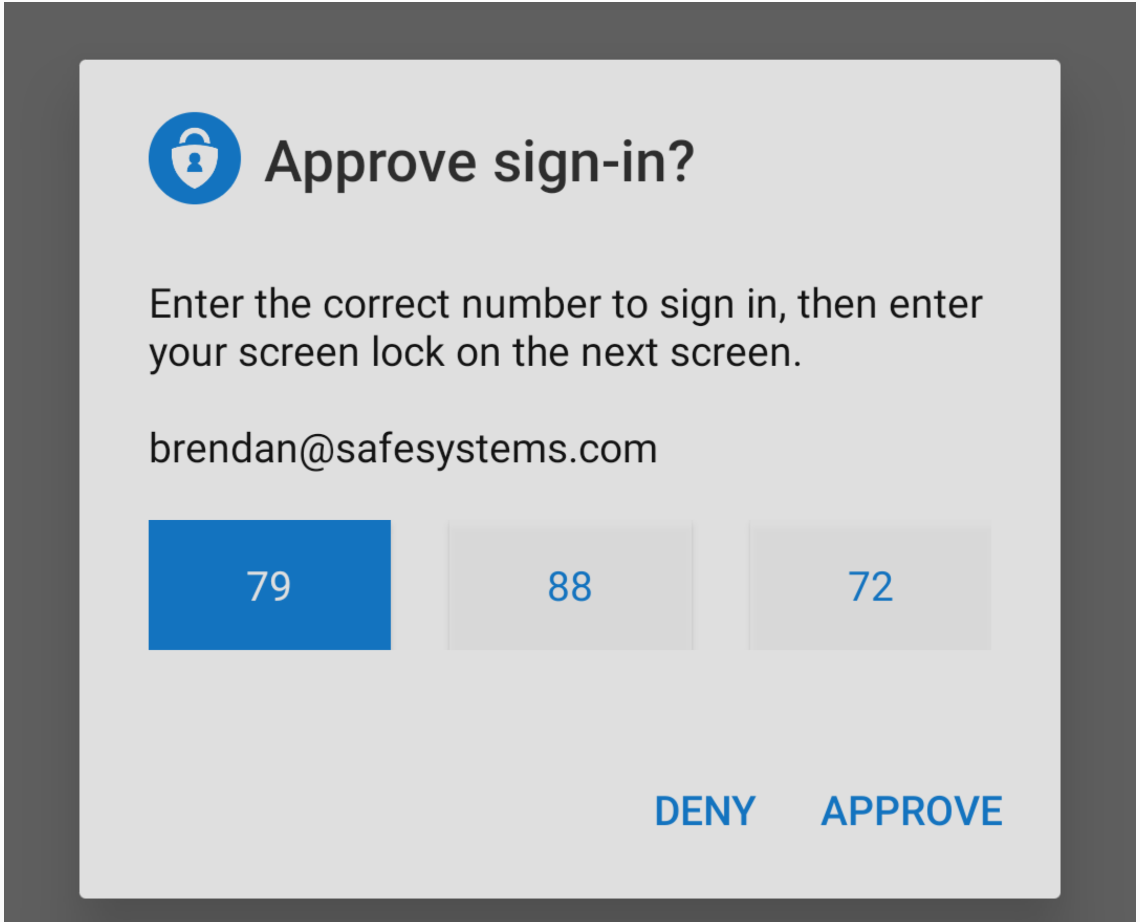
Approve sign-in?

Enter the correct number to sign in, then enter your screen lock on the next screen.

brendan@safesystems.com

On Phone

Phone Sign-In: In Use



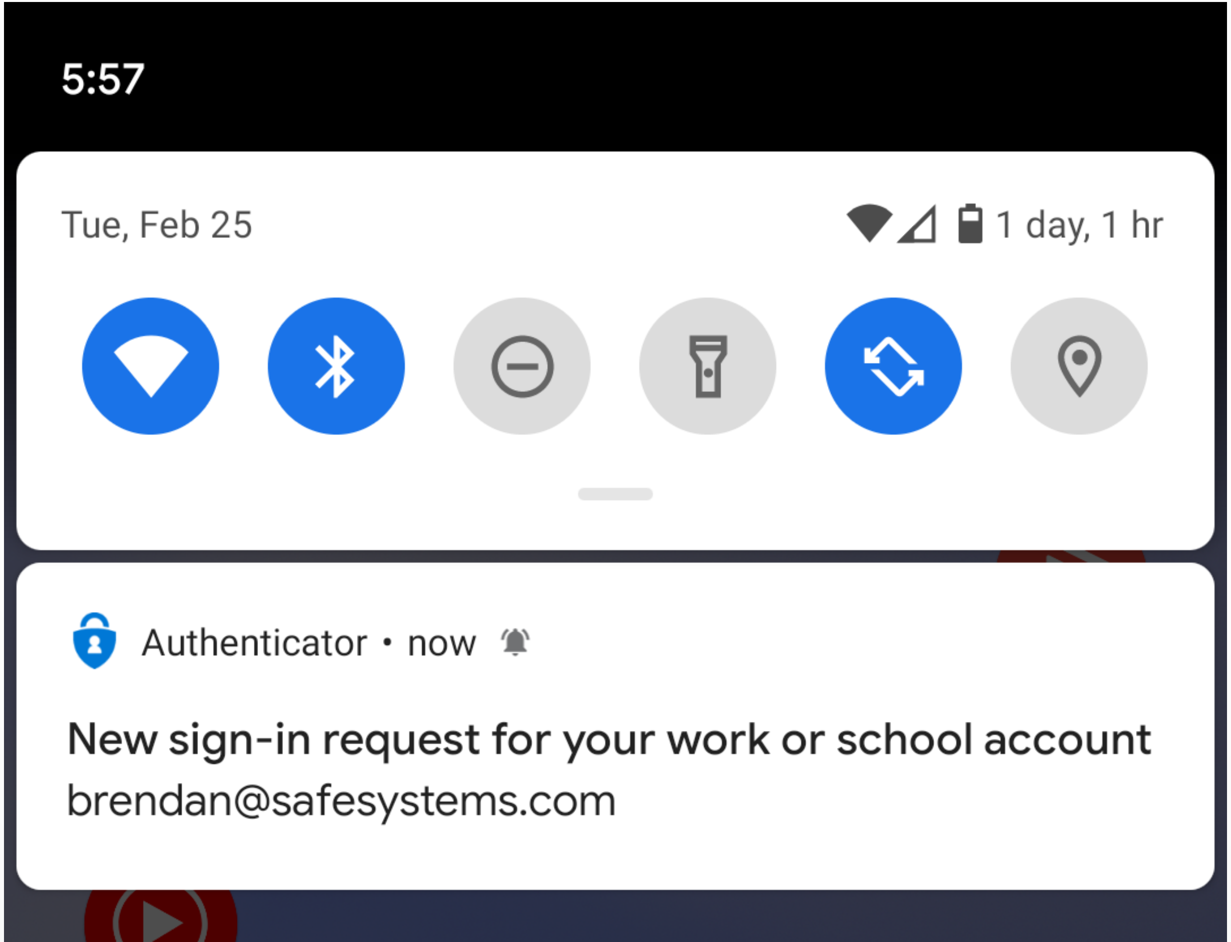
Approve sign-in?

Enter the correct number to sign in, then enter your screen lock on the next screen.

brendan@safesystems.com

On Phone

Phone Sign-In: In Use

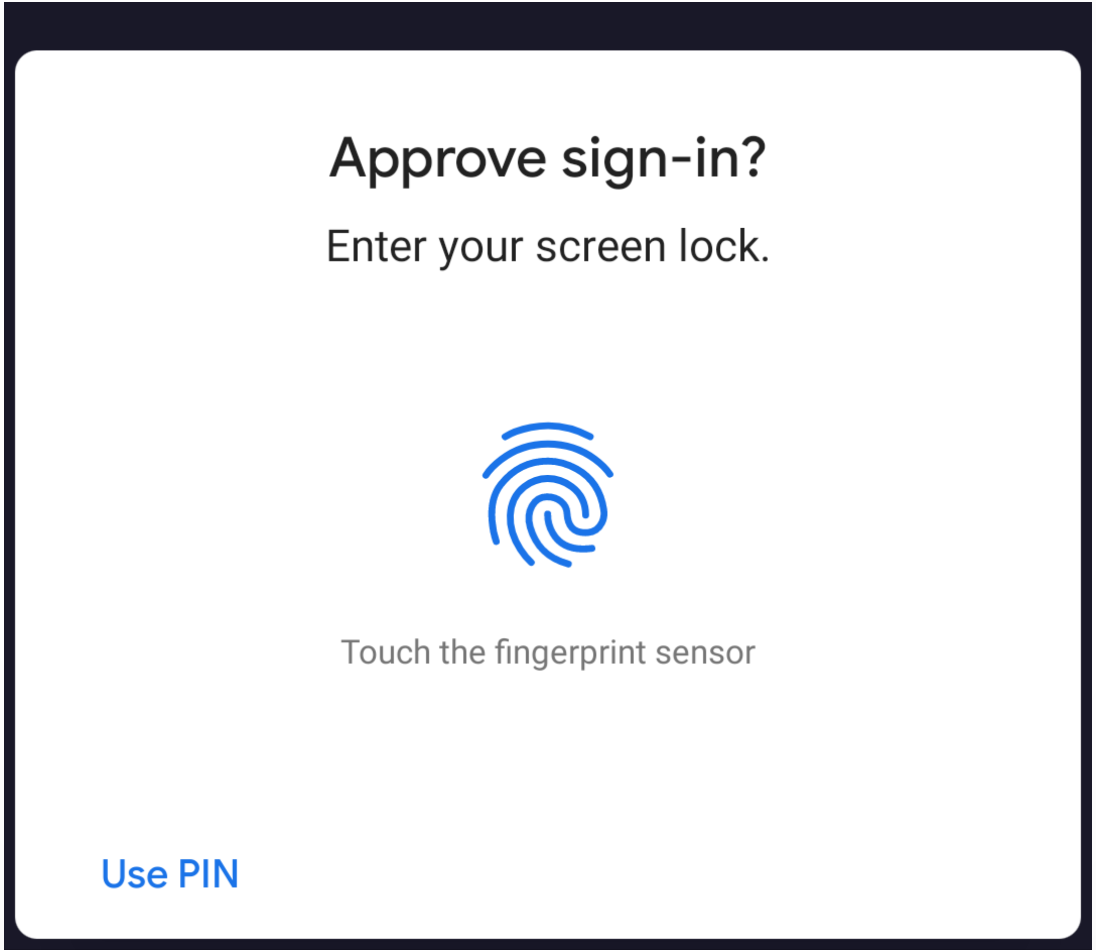


Authenticator • now

New sign-in request for your work or school account
brendan@safesystems.com

On Phone

Phone Sign-In: In Use



Approve sign-in?

Enter your screen lock.

Touch the fingerprint sensor

On Phone

Safe Systems®

LESS WORRYING. **MORE BANKING®**

Thank You!

SEND QUESTIONS OR COMMENTS TO

Brendan McGowan
brendan@safesystems.com

Adam Causey
Adam.Causey@safesystems.com