Securing Your Remote Workforce

#RemoteWorkingChallenge

A New World

- Millions of people working remotely now
  - In 2018 3.9 Million Americans or 2.9% of Workforce
  - Predicted by to double by 2020
  - COVID-19 accelerated the adoption
- Now is the time to re-focus on protection
- How are you protecting your company assets
- This is what we'll cover today:
  - Today’s COVID-19 Infused Cyberthreat Landscape
  - Top internal threats
  - Top IT security tasks to incorporate now
  - What should you do next?

Our Expertise…

empowering PEOPLE

Engaged

Innovative

Productive

common PROCESS

Understood

Measurable

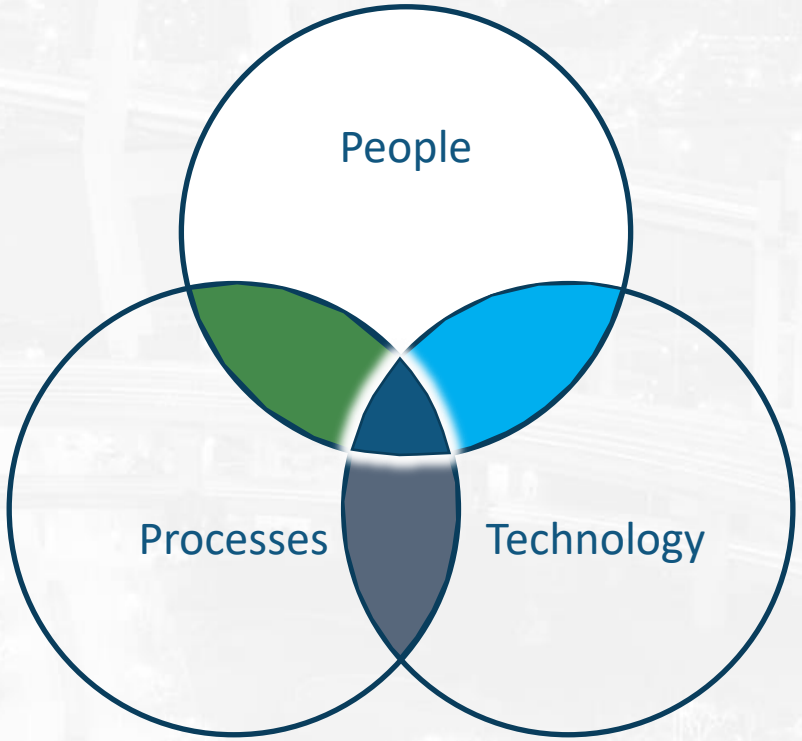
Secured

technology TOOLS

Facilitate

Inspire

Accelerate



Who is Accuvise

#RemoteWorkingChallenge

Accuvise Overview

- Who are we?
  - Full-service consulting firm
    - Operational, Management, & Technology Consulting
    - Services dedicated to SMB or Enterprise organizations
    - Private equity funds and related portfolio companies
- What we do?
  - Deliver measurable value by empowering people through process and technology to grow outside the four-walls of your business
  - Accurately Advise you throughout your transformation journey
  - Connect our clients to a unique collection of expert ecosystem partners
  - Methodology to provide results while protecting economics

Accuvise Services

People

- Office 365 Training
- Security Awareness Training
- System Use Training
- Workload optimization
- Strategic Staffing
- Fractional CX0 Services
- Employee Enrichment

Process

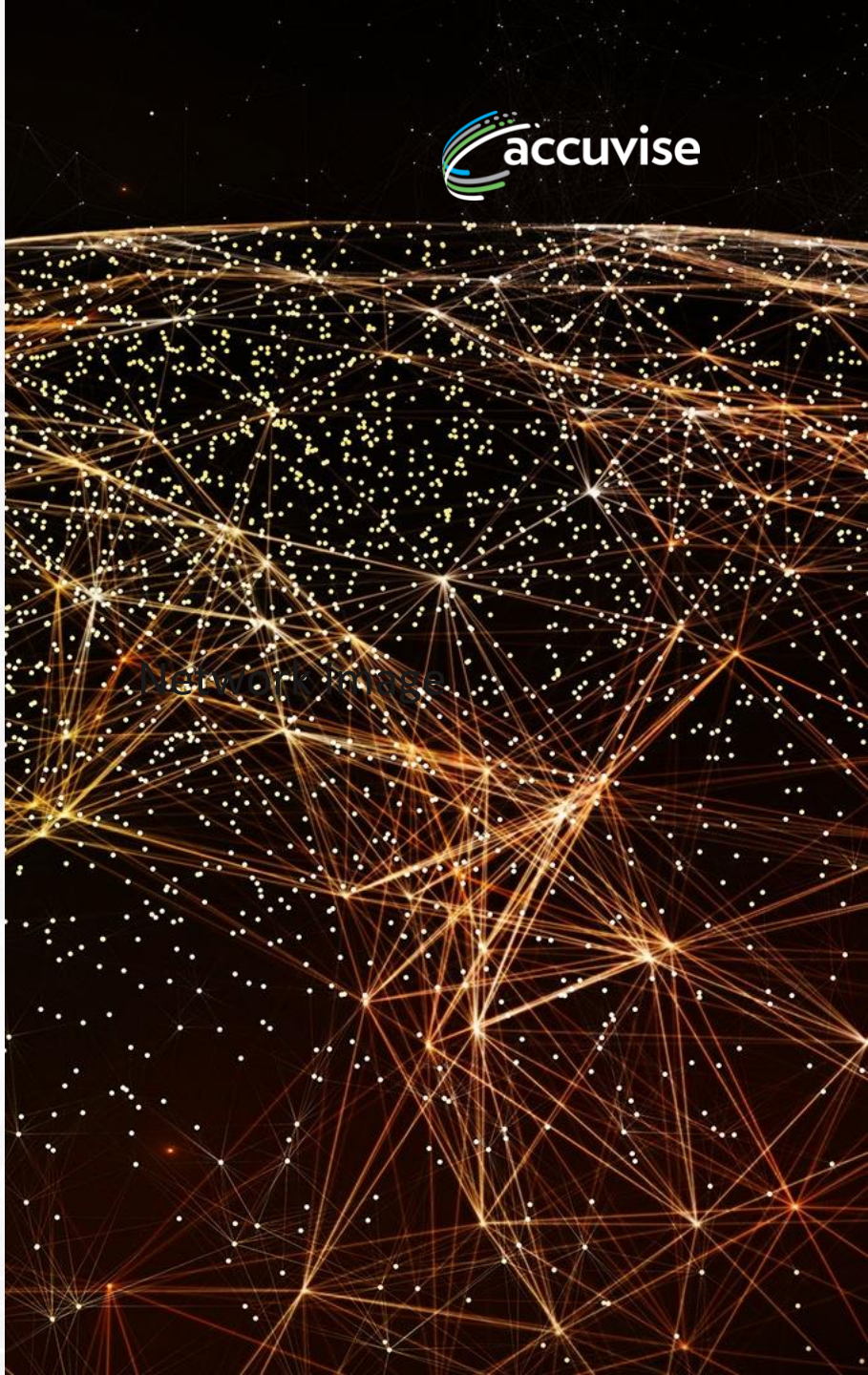
- Current State Assessments
- Business Process Consulting
- Transformation Consulting
- Micro/Marco Process Creation
- ERP/CRM Feature Adoption
- Quality of Implementation Assessment
- Business Requirement Documentation
- Vendor Selection & Oversight
- Unavailability Cost Assessments

Technology

- Cloud Migrations
- App Development
- Workflow Automation
- Security Solutions Implementations
- Security Management, Detection, and Response
- Managed Services Suite
- Endpoint lifecycle services
- Technology Selection Assistance

Things to Consider

- ✓ Are you securing user identities against current and emerging threats?
- ✓ Do you have control over who can access your information?
- ✓ Do you know where employees are storing data?
- ✓ Do you know what applications are being used by your users?
- ✓ Can you quickly remediate advanced threats?



Changing Threat Landscape

#RemoteWorkingChallenge

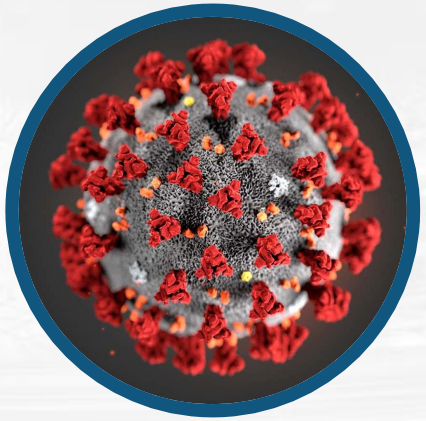
Rapidly Changing Threat Landscape

Cyberspace is the new battlefield

Virtually anything can be attacked

Security skills are in short supply

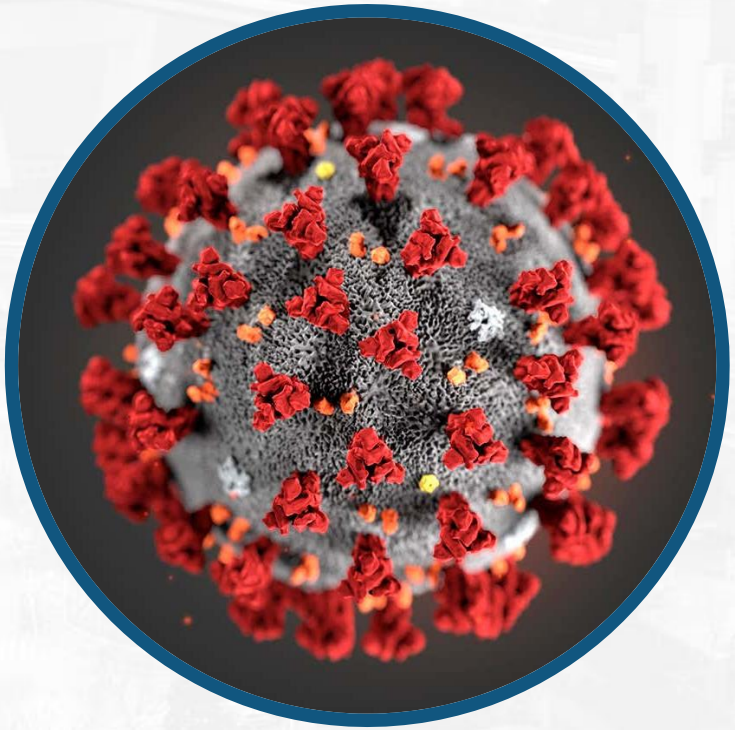
X Factor Provided by COVID-19



Rapidly Changing Threat Landscape

- X Factor by COVID-19
  - Phishing Attacks Increased 350%
  - 149,195 active phishing websites in January
  - 100% increase in February to 293,235 phishing websites
  - Up 350% from January to March to 522,495 websites
  - 300,000 suspicious COVID-19 emails between March 9 and March 23

- Common Tactics
  - Fake Charites
  - Fake CDC Emails
  - Phishing Emails
  - Counterfeit Treatments or Equipment
  - Fake eCommerce sites & social stores



What Criminals Want

- Monetary Gain
  - Extorsion
  - Old fashion theft
- What are they after?
  - Information
  - Economic damage
  - Look for bigger targets

Current Stories From IT Managers at SMB's

"Someone was fooled by the email from the CEO, and used his corp card to send the iTunes gift cards. We lost about $5,000."

Adam A., video game rentals, 150 employees

"We saw that it was moving through the network drives, encrypting files, starting with Z: drive and moving down"

Jerry K, import/export, 250 employees

"The only reason we caught it was that it was a 6 digit sales order and our sales orders are a 7 digit."

Joe B, food distribution, 250 employees

"They got someone's password, and sent an email to our CFO, who sent the $40,000 wire transfer."

Bob K., property management, 150 employees

Small & Midsized Business

58%
Breaches took place at small businesses[1]

$120k
Average cost of a SMB data breach[2]

62%
Lack the skills in-house to deal with security issues [3]

[1] Verizon 2018 Data Breach Investigations Report

[2] Kapersky Lab study, 2018

[3] Underserved and Unprepared: The State of SMB Cyber Security in 2019, Vanson Bourne for Continuum

Help your employees to minimize internal threats

- **Be Skeptical** of emails from unusual senders
- **Don’t click** on link or open attachments from unusual sources
- **Don’t forward** suspicious emails to all your co-workers
- **Note grammar issues** in the text of the email often a sign of fraud

- **Validate senders' email**
  - Inspect addresses
  - Look for slight charter differences
- **Report suspicious emails** to the IT or Security departments
- **Require verbal confirmation** on financial wires or adjusted payment requests

Top Security Measures to Implement Now

#RemoteWorkingChallenge

Top Security Measures

Identity &
Access Management

Threat Protection

Device Management

Application Management

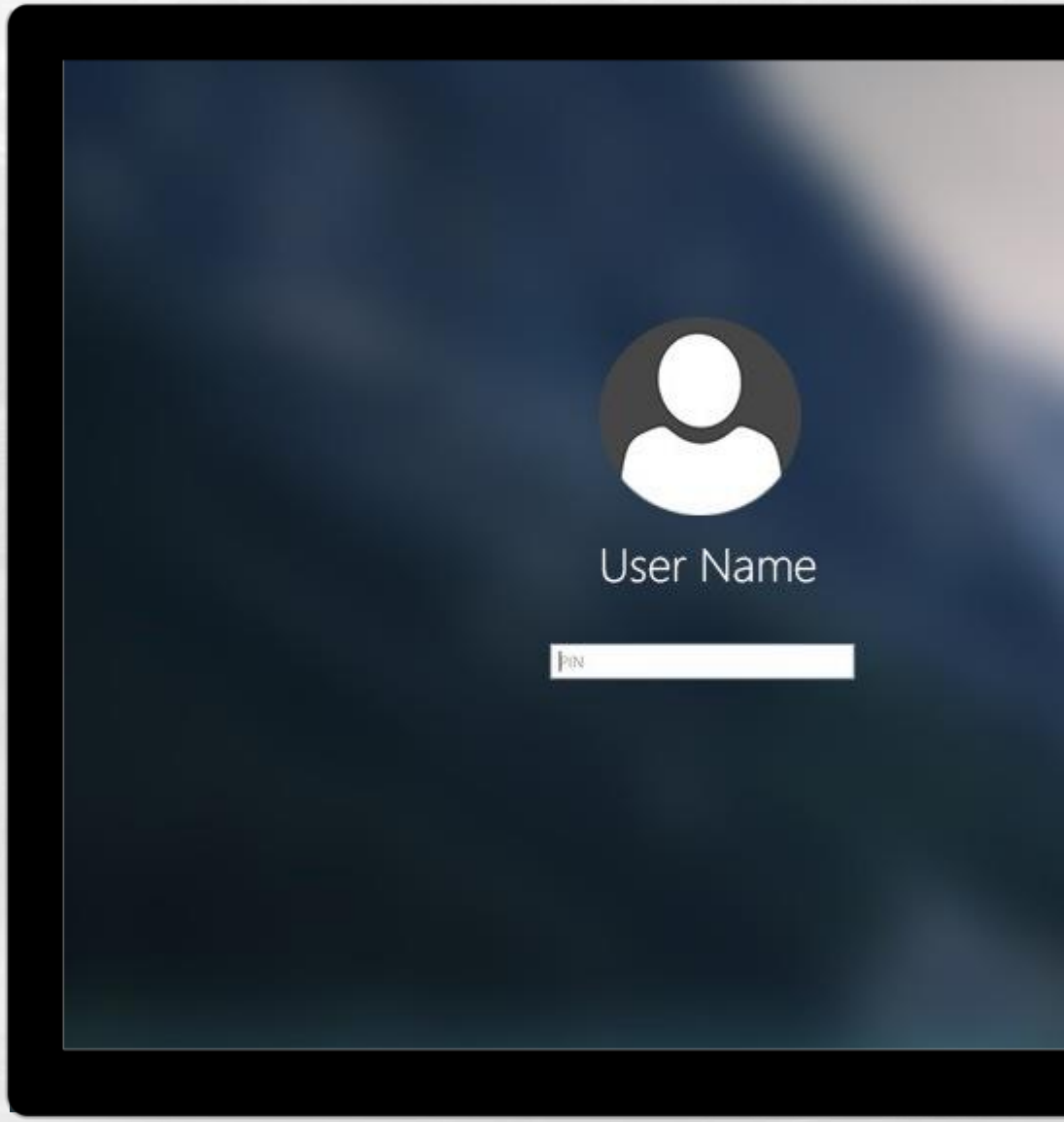
Information Protection

Conditional Access Policies

Security is a <u>Journey</u>, not a <u>Destination</u>
Accuvise is the Guide

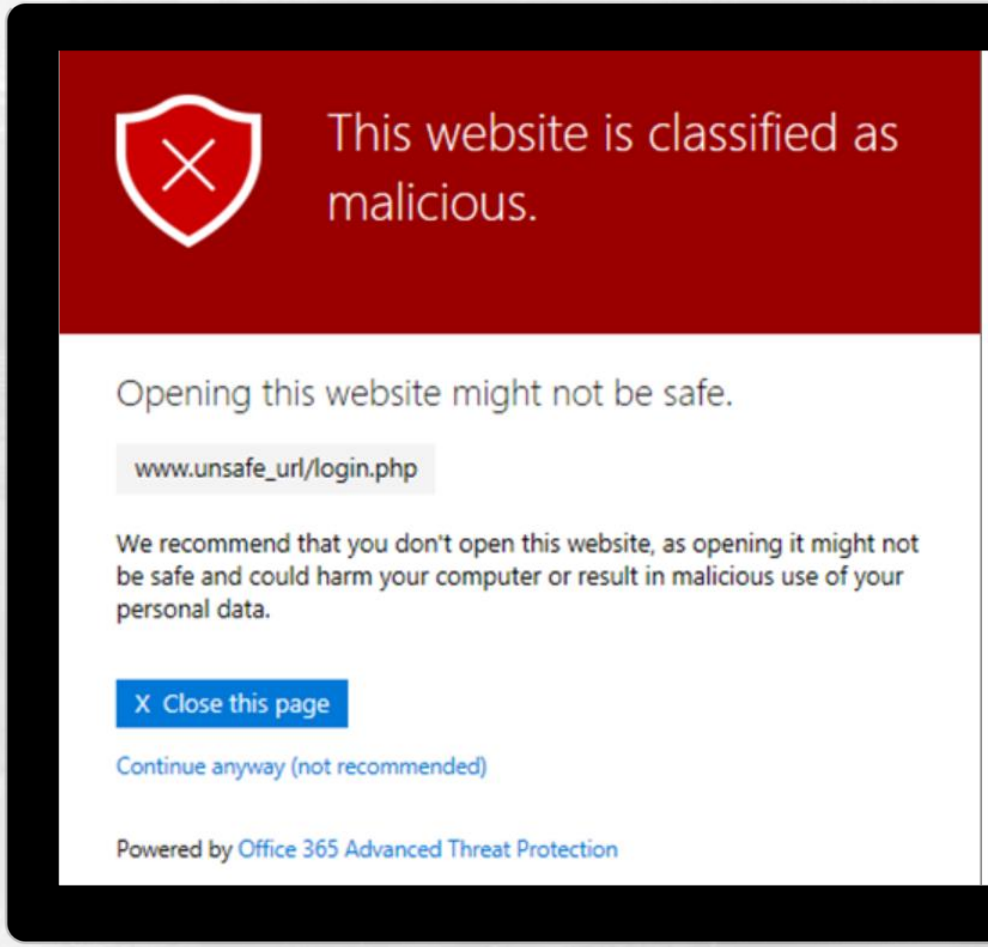
Identity and Access Management

- Simplify user access with single sign-on (SSO)
- Strengthen your credentials with Multi-Factor Authentication (MFA)
- Block common passwords
- Self Service Password Reset (SSPR)
- Risk-based conditional access policies
- Privileged Access Management (PAM)



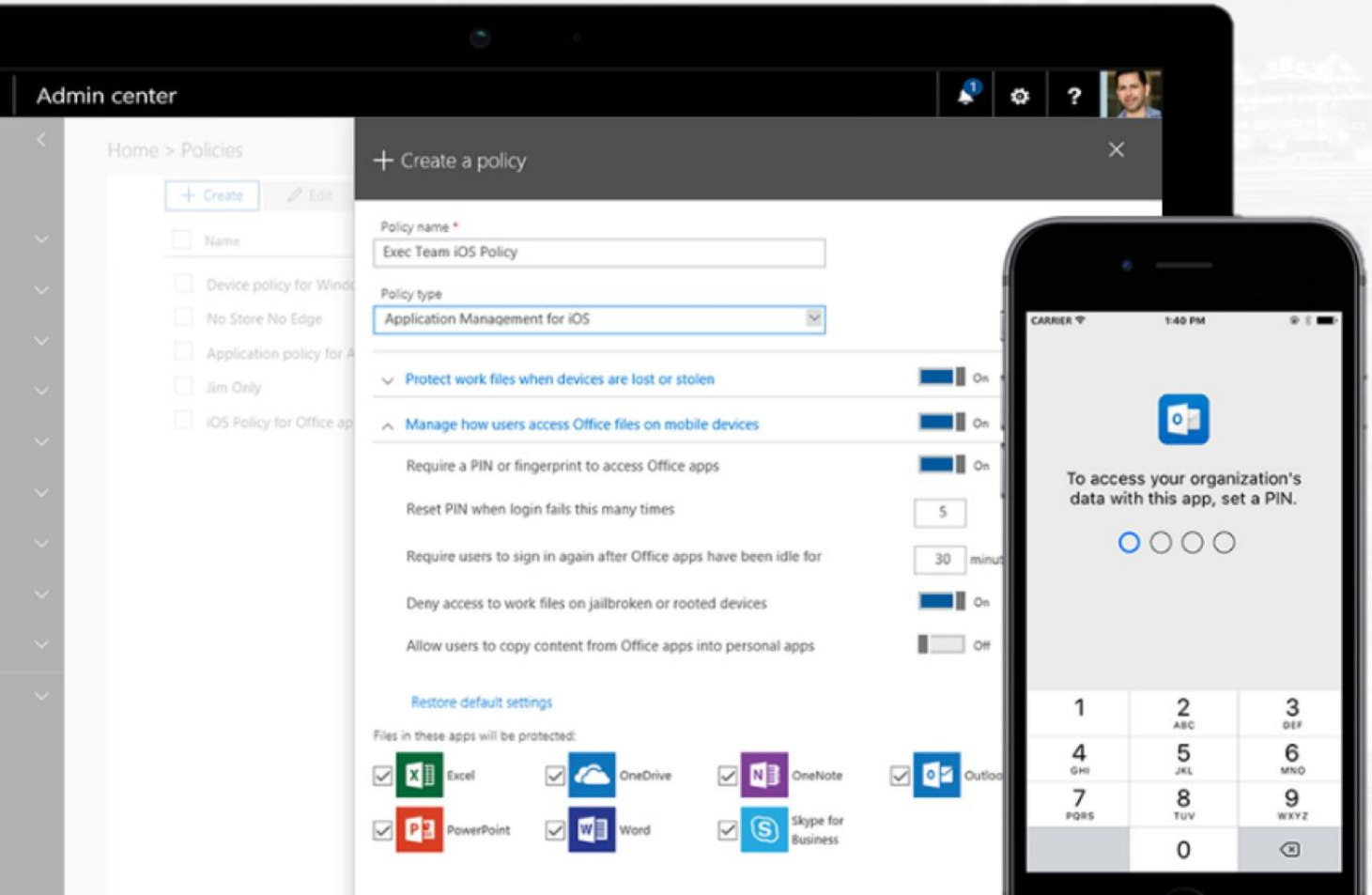
Threat Protection

- Protect against phishing, ransomware, malware, and other advanced threats
- Links are checked in real time to warn you if the destination is a malicious site
- Attachment scanning detects malware previously not seen
- Users are protected from increasingly sophisticated cyberattacks, including spoofing
- Devices are protected against for suspicious processes like ransomware



Device Management

Manage the security of the devices that access your business information



Control the devices and users that access Office 365 data

Apply security policies that **protect business data** on devices

Keep documents, emails, and other data **within approved Office mobile apps**

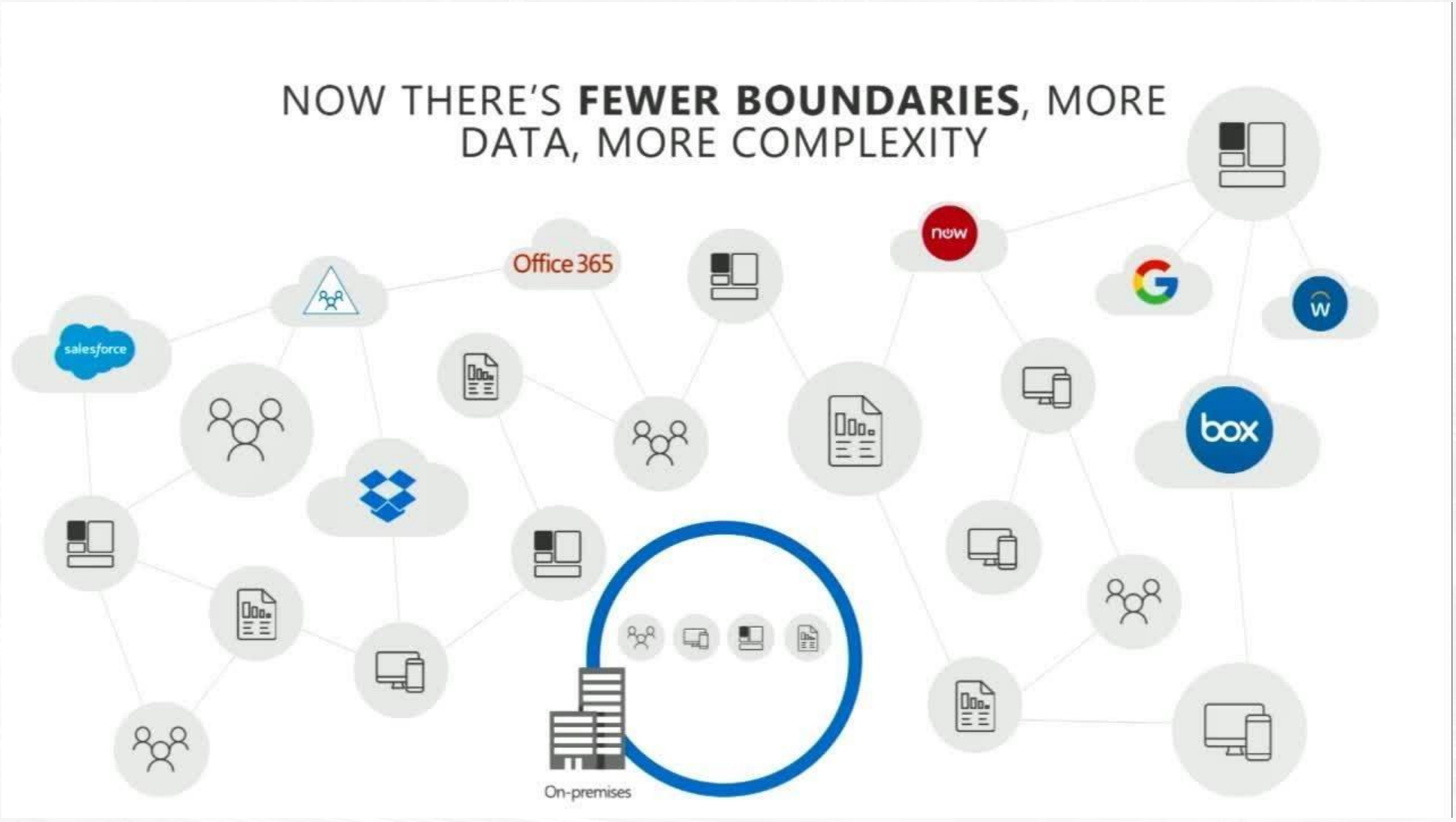
Remotely wipe business data **without affecting personal information**

Enforce polices like **BitLocker encryption** to protect data if a computer is lost or stolen

Application Management

- Compliance Policies
- Protect sensitive data within apps
- Protect customer data on unmanaged devices
- Use detect rogue applications
  - Your users are in the cloud—even if you aren't

Information Protection



Information Protection

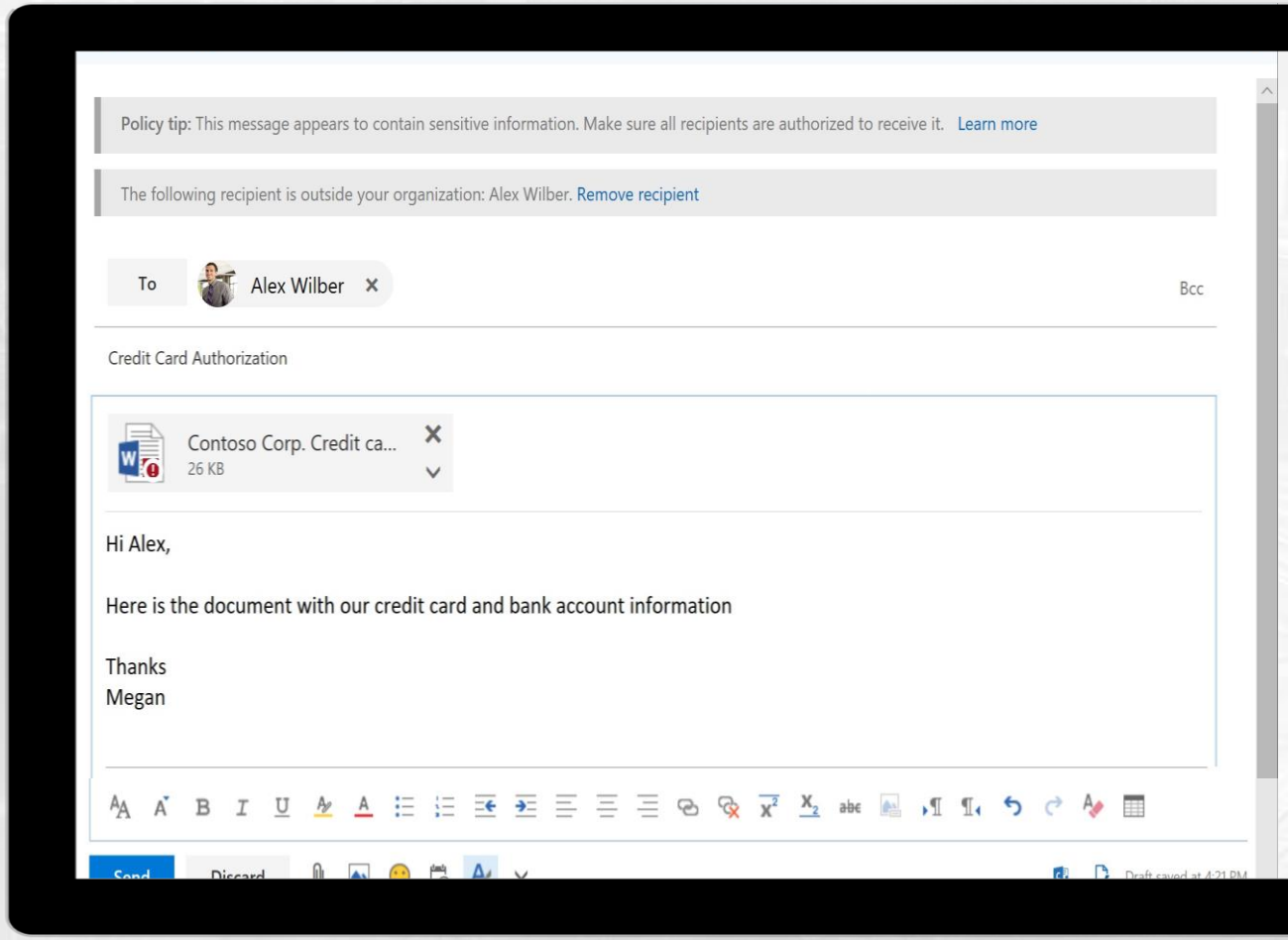
Control who has access to sensitive information

Apply encryption and restrictions like do not forward to emails and documents

Control access to your data and documents even after they have left the four walls of your business

Apply data loss prevention policies to help keep sensitive information from falling into the wrong hands

Use long-term archiving to meet legal and regulatory requirements



Bringing it all together…

Conditional Access Policies in Microsoft 365

accuvise

User attributes
Group membership

Devices
Domain Joined
compliant
Platform type
(Windows, iOS, Android)

Application
Per app policy
Type of client
(Web, Rich, mobile)

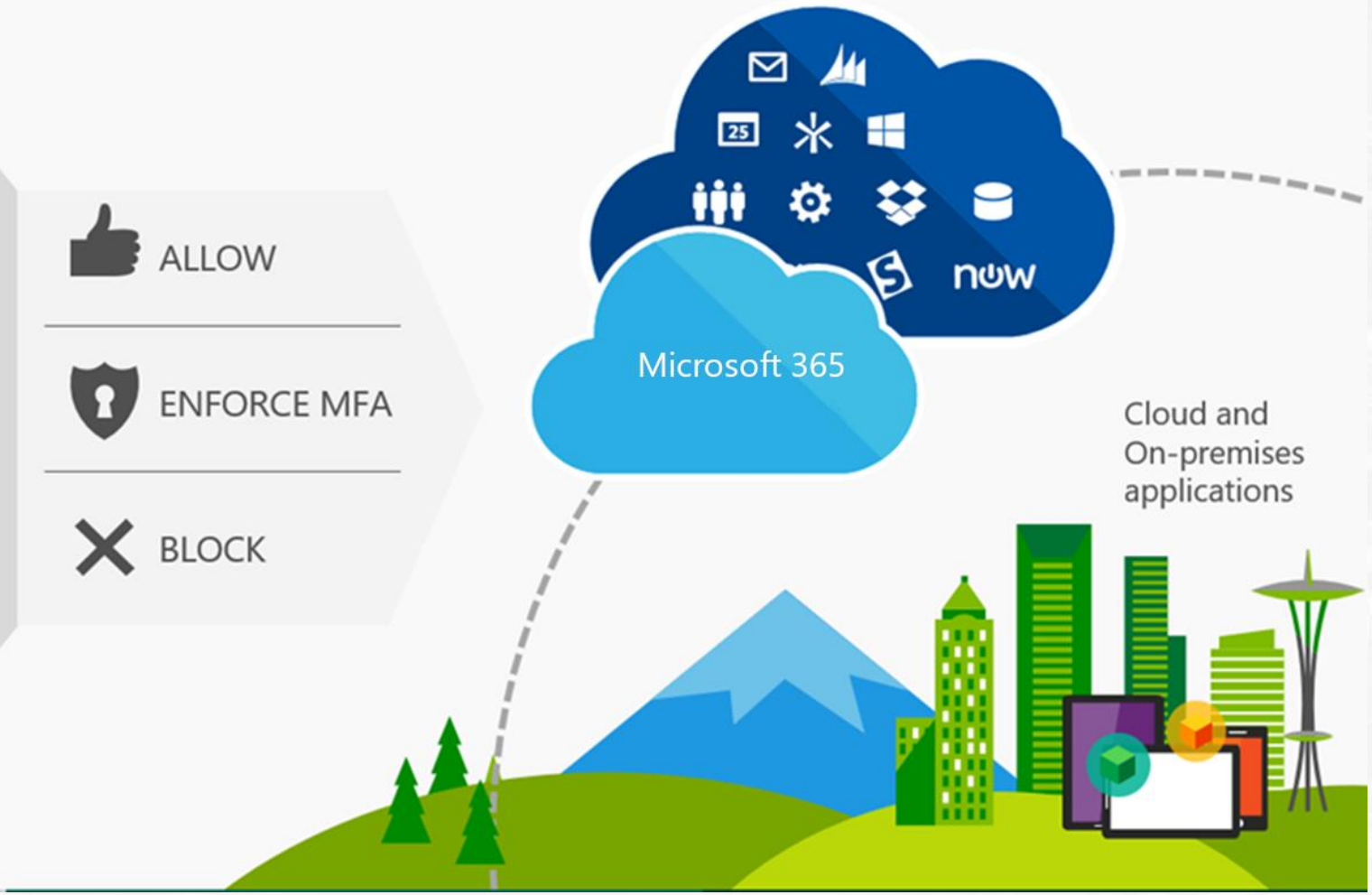
Location
IP Range

Risk
Session risk
User risk

ALLOW

ENFORCE MFA

BLOCK



Security is a Journey, not a Destination

accuvise

Identity &
Access Management

Threat Protection

Device Management

Application Management

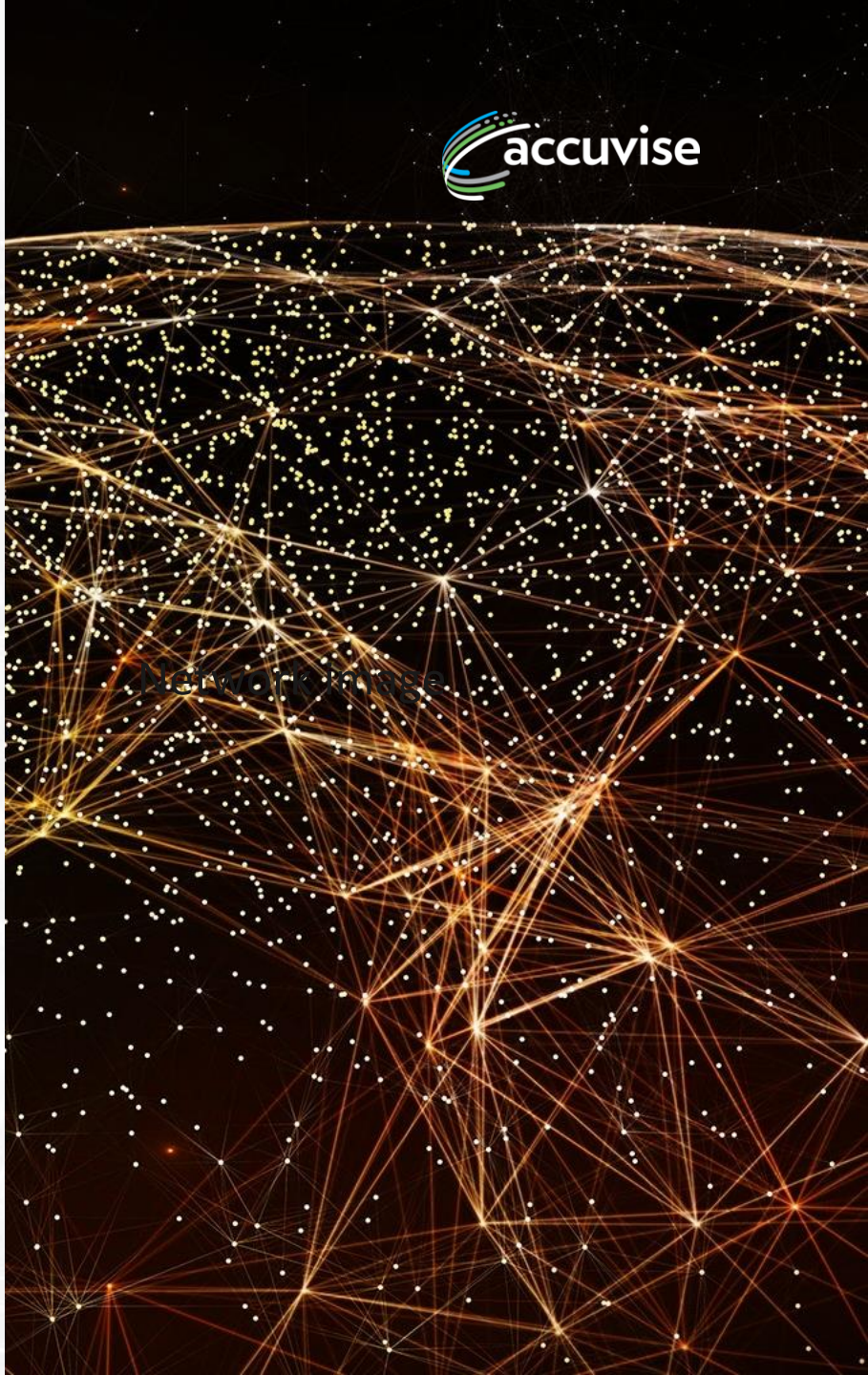
Information Protection

Conditional Access Policies

Call for help
Focus on your business

Self Assessment

- ✓ How do you secure identities against current and emerging threats?
- ✓ How much control do you have over who can access your information?
- ✓ Where are your employees storing data?
- ✓ What applications are being used by your users?
- ✓ **How quickly can you remediate advanced threats?**



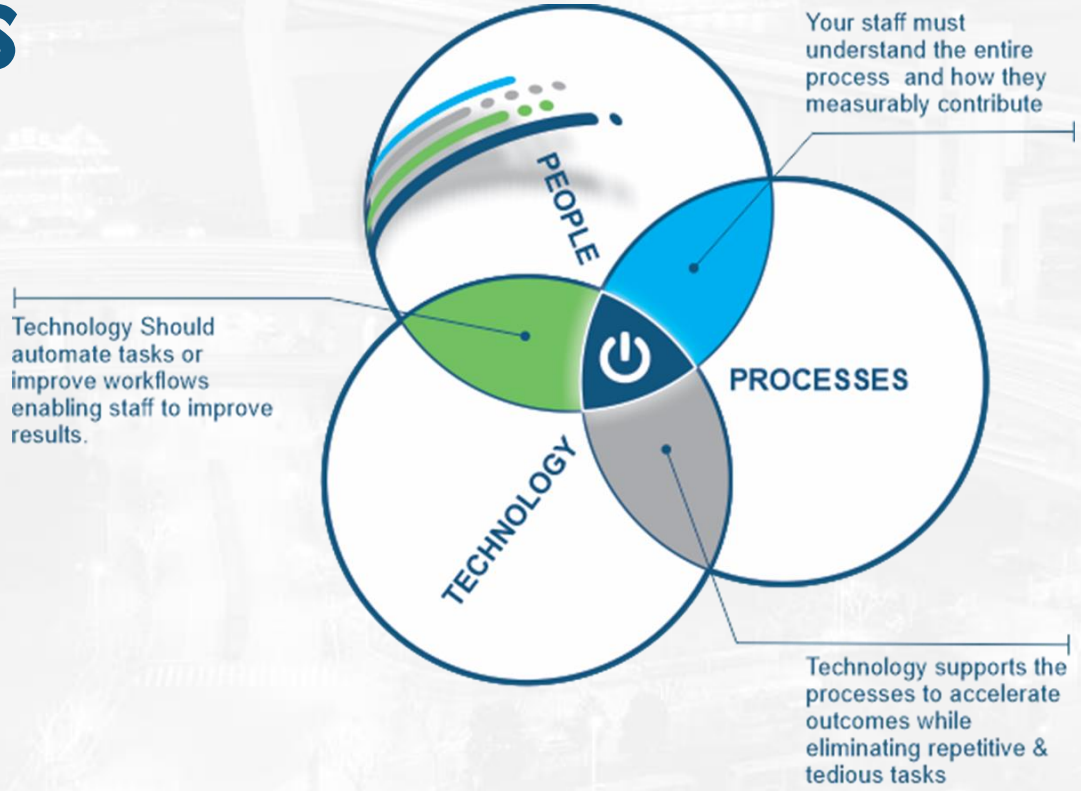
Next steps

- ✓ Conduct a security assessment
- ✓ Focus on your business
- ✓ Let Accuvise help with the rest

Accurately Advise & Consult

Questions & Answers

email: info@accuvise.com
Phone: (561) 910-8100
#RemoteWorkingChallenge



Security is a Journey, not a Destination
Accuvise is the Guide