An Evolutionary Tale of Identity and Access Management (IAM)

Kent Goodrow - Account Manager

SYSTEMS engineering

Kent Goodrow | Systems Engineering

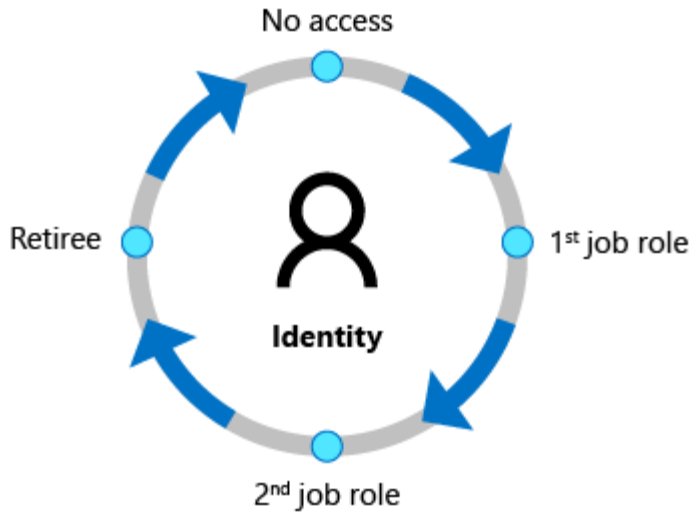
Account Manager

- 17 years experience in Information Technology management and security execution
- Roles: Systems Admin, Senior Engineer, Manager, and Account Manager
- Currently works with Systems Engineering clients to enable the exceptional within their IT environments
- Verticals Supported: Banking/Finance, Legal, Healthcare, Manufacturing, Professional Services

SYSTEMS engineering

Evolution and Response

- Traditional user access and protection scenario
- Current user and data access landscape
- Proliferation of Software as a Service (SaaS)
- Security models and methodologies
- Identity and Access Management (IAM) hurdles
- Where do I start?
- Real-world comparative scenarios
- Q&A



Traditional IAM Processes

- Applications and data live on-premises
- Users access data in-office or via Client VPN/RDS
- Firewall(s) configured to keep bad actors out
- MFA enabled for Client VPN/RDS access for remote workers
- File and application-level permissions to silo data access
- Active Directory drives security

Today's Application and Data Landscape

- Cloud-first, access-anywhere model
- Multiple cloud IaaS/SaaS hosting solutions
- Users working from anything, anywhere, anytime
  - Mobile devices and tablets
  - Home computers
  - Hotels, workspaces, airports, living rooms, etc.
- Rising zero-day vulnerabilities and breaches
  - Microsoft Exchange
  - SolarWinds Orion
  - Mimecast

Proliferation of IaaS and SaaS

- Cloud application platform providers
  - Microsoft 365 - Exchange, SharePoint, OneDrive, Teams
  - Microsoft Azure – IaaS, SaaS, PaaS
  - Google Apps – email, data storage, collaboration
  - Amazon Web Services – application delivery, data storage
- VDI and Hosted Desktop as a Service
  - Azure WVD, SaaS via RDS/VDI/Citrix
- Line of Business (LoB) application providers
  - Salesforce, Highradius, Intralinks, nCino, Stripe, etc.

Zero Trust Security Model

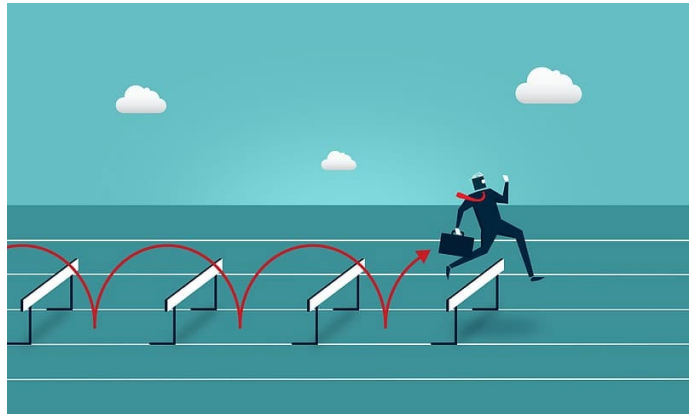
- Do *not* trust anything inside or outside your network
- Verify, verify, verify again – then allow access
  - Who is attempting to access this app/data?
  - What device is the attempt coming from?
  - Where in the world is this device located?
- Change the way users think about security
  - Historically, internal resources were implicitly trusted (firewall conundrum)
  - Bad actors can (and do) live within your computing solutions
  - Gone are the days of “set it and forget it” within your security solutions
- Addresses mobile access, cloud migration, and risk mitigation

Zero Trust Principles

- Verify explicitly
  - Use *all* available data points to the best of your ability
  - Includes both user/device data and the access request
- Least privileged access
  - Just-In-Time (JIT) or Just-Enough-Access (JEA) permissions
  - Risk-based policies to drive conditional access
- Assume breach
  - Treat each authentication attempt as though it is malicious
  - Utilize analytics to drive visibility, detection, and continuous improvement

IAM Business Hurdles

- Strategy
  - Where do we start?
  - Which application(s) and solution(s) do we need to worry about?
  - Which platform covers most of our needs?
- Productivity
  - Are all required stakeholders part of the conversation?
  - How will IAM implementation affect day-to-day business?
- Ongoing Management
  - How do we manage IAM once deployed?
  - How do I know my IAM solution/strategy is effective?



Where do we start?

- Define your maturity model
  - Traditional > Advanced > Optimal
  - How/Where do we manage our users' identities?
  - How do we manage our users' devices?
  - How are our applications accessed and where do they live?
  - How do we manage changes to infrastructure?
  - What is my network topology today?
  - How do I classify and protect my data today?

- Next, align the answers to these questions with Zero Trust…

Zero Trust Organization Needs

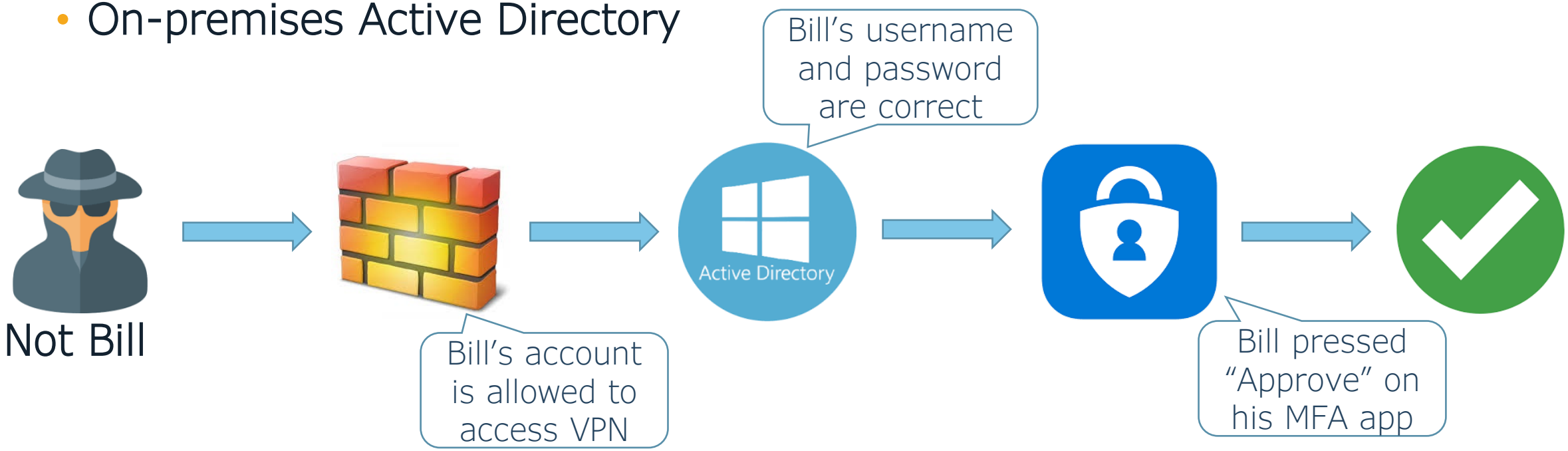
- Identity platform (Azure or on-premises AD)
- Multifactor Authentication (MFA)
- Single Sign-On (mileage may vary depending on apps)
- Mobile Device (MDM) and Application Management (MAM)
- Data discovery and classification
- Shadow IT management
- Conditional Access

Scenario: Client VPN Remote Access

- Bill's account is being used to access Client VPN
- Device being used is a non-domain tablet
- Login location is Aruba
  - Bill's account last logged into Office 365 one hour ago from Rumford, Maine
- Bill tends to quickly accept notifications on his phone
- In Bill's role as COO, he has extensive access to internal data once authenticated

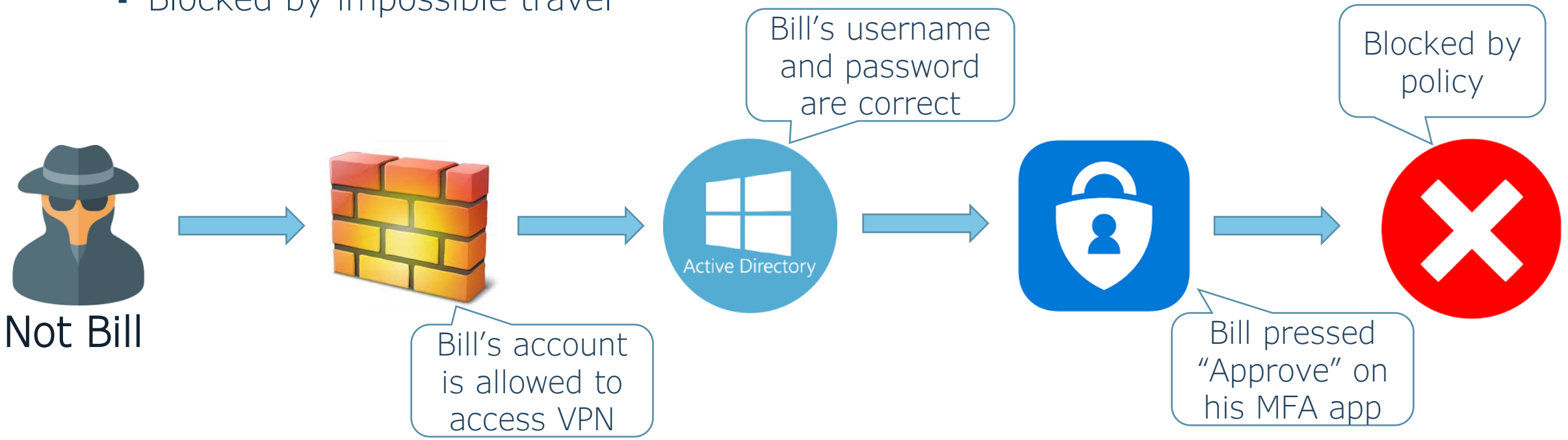
Traditional Identity and Access

- Cisco AnyConnect VPN
- MFA with Push Notification to Mobile App
- On-premises Active Directory



Zero Trust Identity and Access

- Optional scenarios:
  - Blocked by conditional access policy blocking international login
  - Blocked by impossible travel

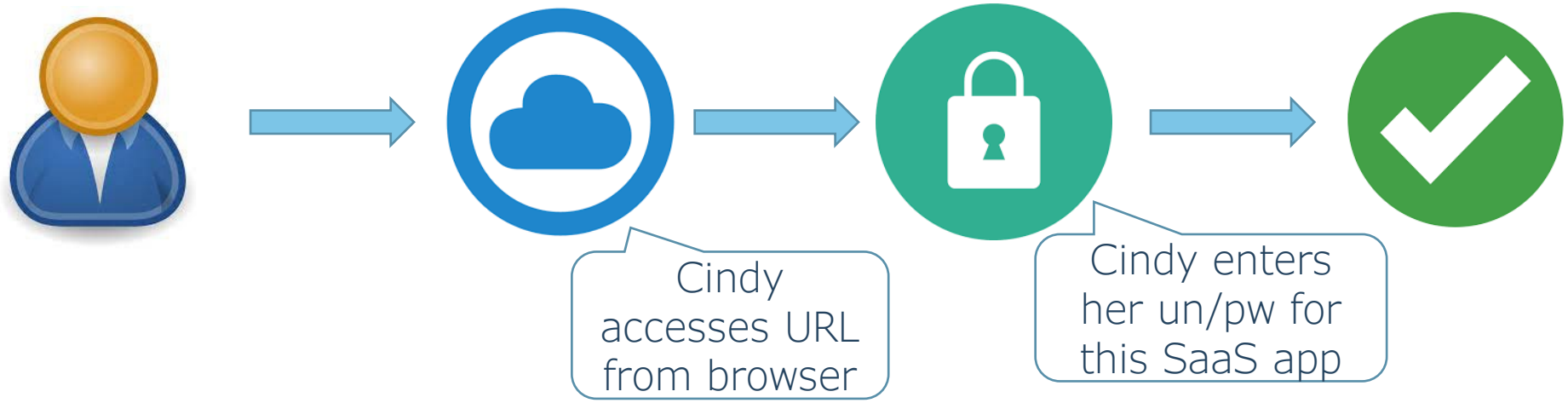


Scenario: Application Access

- Cindy is accessing a SaaS application remotely
- This application houses highly sensitive customer data
- Device being used is Cindy's home computer
- YourBank's internal use policy does not allow access to this application from non-domain computers due to security risks
- As this application lives in the cloud, users do not technically need to be on-site or connected to Client VPN to access it

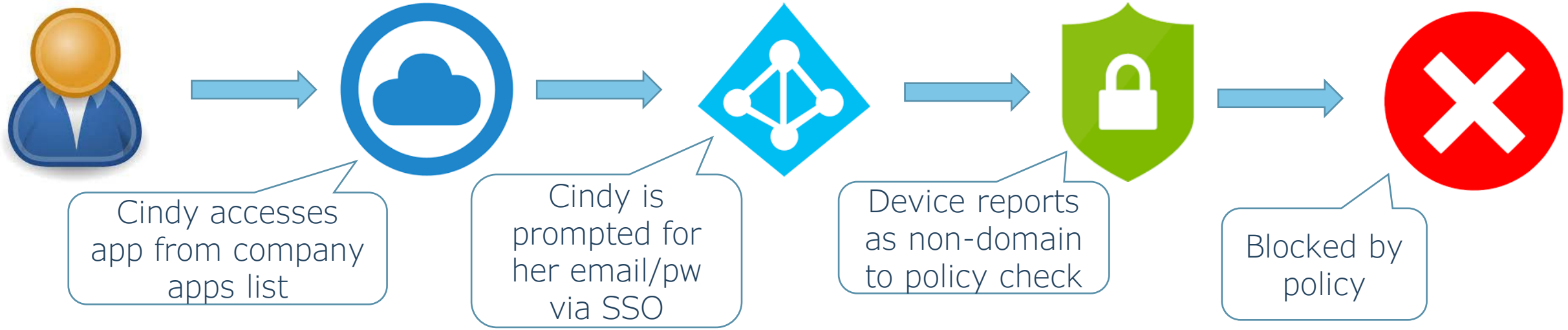
Traditional Identity and Access

- SaaS application accessible via the internet
- Cindy utilizes a separate username and password
- On-premises IAM is not part of the authentication workflow



Zero Trust Identity and Access

- SaaS application accessible via the internet
- Single Sign-On enabled app with Azure Active Directory
- Conditional access policy denies access to non-domain devices

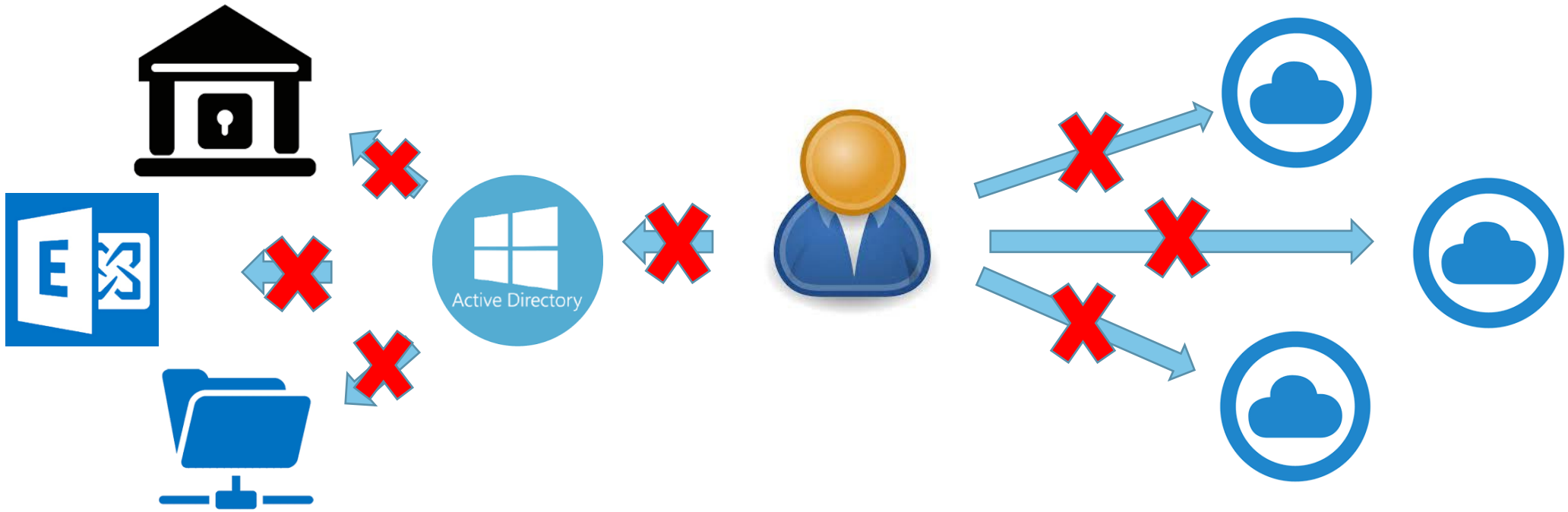


Scenario: User Termination

- David is leaving the organization
- David's job role had access to all on-prem apps
- David's job role had access to all cloud/SaaS apps
- Will need to ensure that access to all on-prem and cloud applications is disabled by 5:00 p.m. on Friday

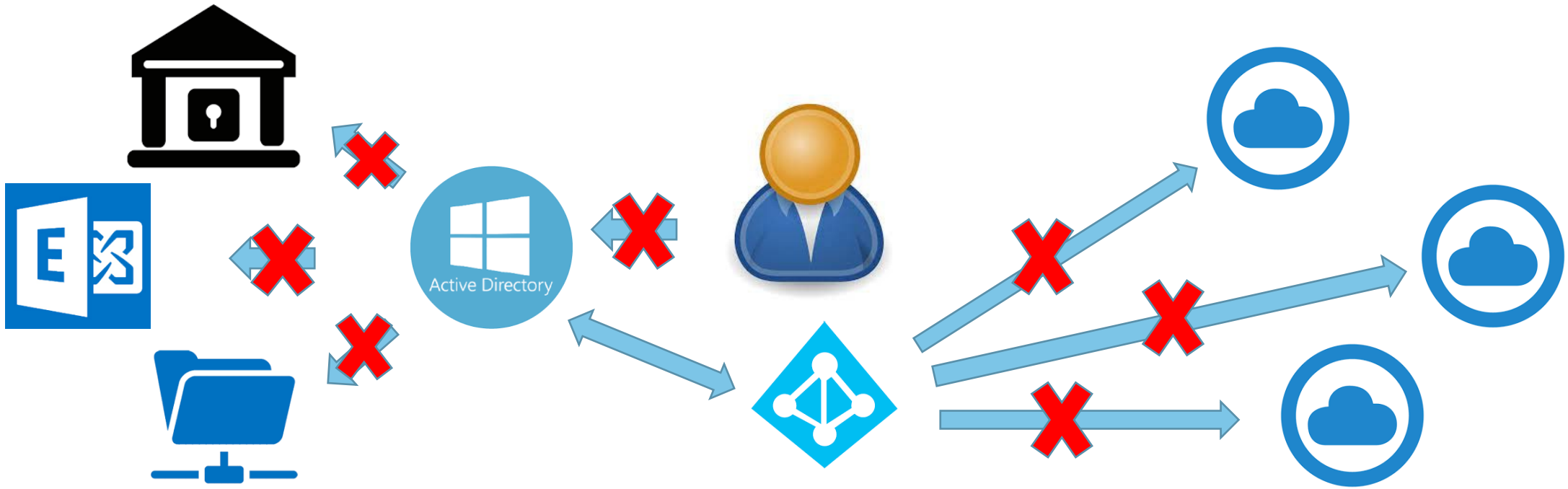
Traditional Identity and Access

- On-premises Active Directory with no SSO
- Separate accounts/credentials for all cloud/SaaS apps



Zero Trust Identity and Access

- Hybrid on-prem/Azure Active Directory with SSO



Zero Trust Recap

- Trust nothing (users or devices) implicitly
- Evaluate all applications and access scenarios
- When in doubt, deny access
- Maximize automation, minimize administrative overhead

Enabling the EXCEPTIONAL

Kent Goodrow - Account Manager
kgoodrow@systemsengineering.com