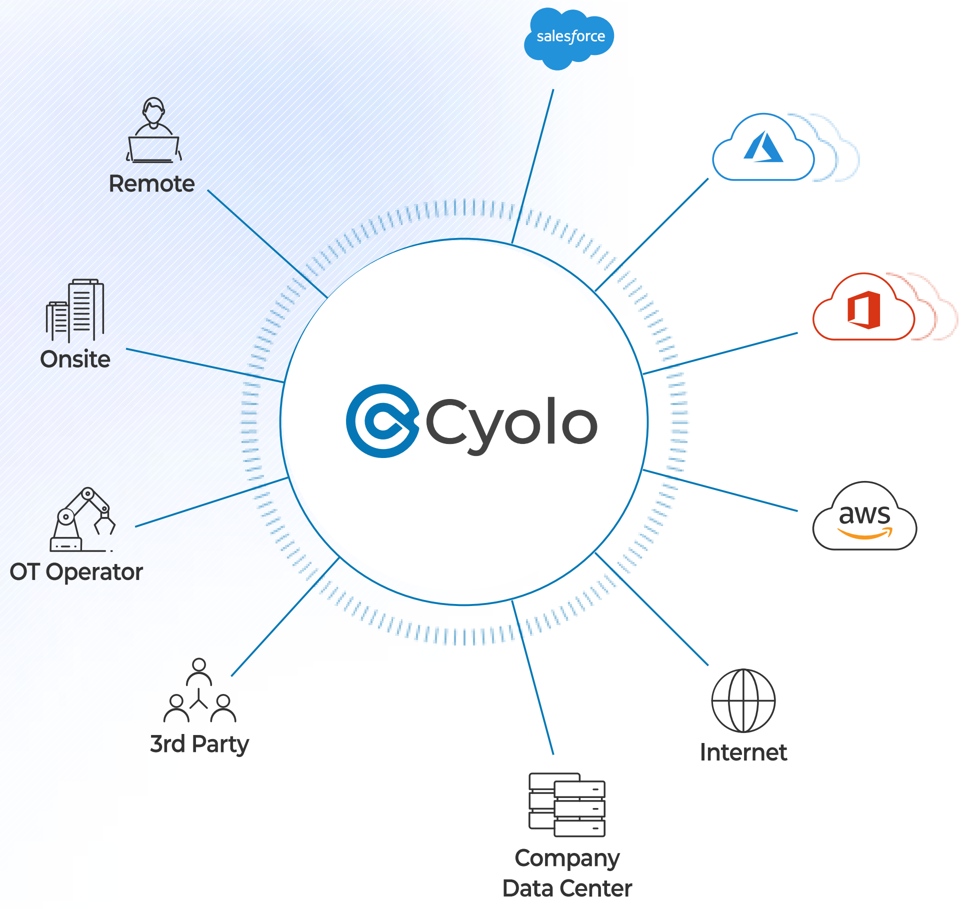
Cyolo

Implementing a Zero Trust Architecture (ZTA) for Highly Regulated Domains

Quickly and securely connect workers to their environments and resources



Kevin Kumpf and Josh Martin

Chief Strategist and Technical Marketing Lead

Kevin.Kumpf@cyolo.io

josh@cyolo.io

August 30th, 2022

Presentation Overview

- Defining NIST SP-800-207, M-22-09, M-21-31
- Evolution of ZTA and the need to reduce complexity
- Real World ZTA - Cyolo’s approach to ZTA and Identity-Based Connectivity
- Implementing Cyolo for ZTA and Identity-Based Connectivity
  - Identity Modernization
  - Identity Federation
  - User Experience Architecture Overview
- Accomplishing ZTA Goals (per NIST SP 800-207, M-22-09 and M-21-31)

Cyolo

NIST 800-207 – The “Official” ZTA Standard

- All data sources and computing services are considered resources
- All communication is secured regardless of network location
- Access to individual computational resources is granted on a per-session basis
- Access to resources is determined by dynamic policy and may include other attributes
- The organization monitors and measures the integrity and security posture of all owned and associated assets
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed
- The organization collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture

Cyolo

Memorandum M-22-09 / EO 14028

Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

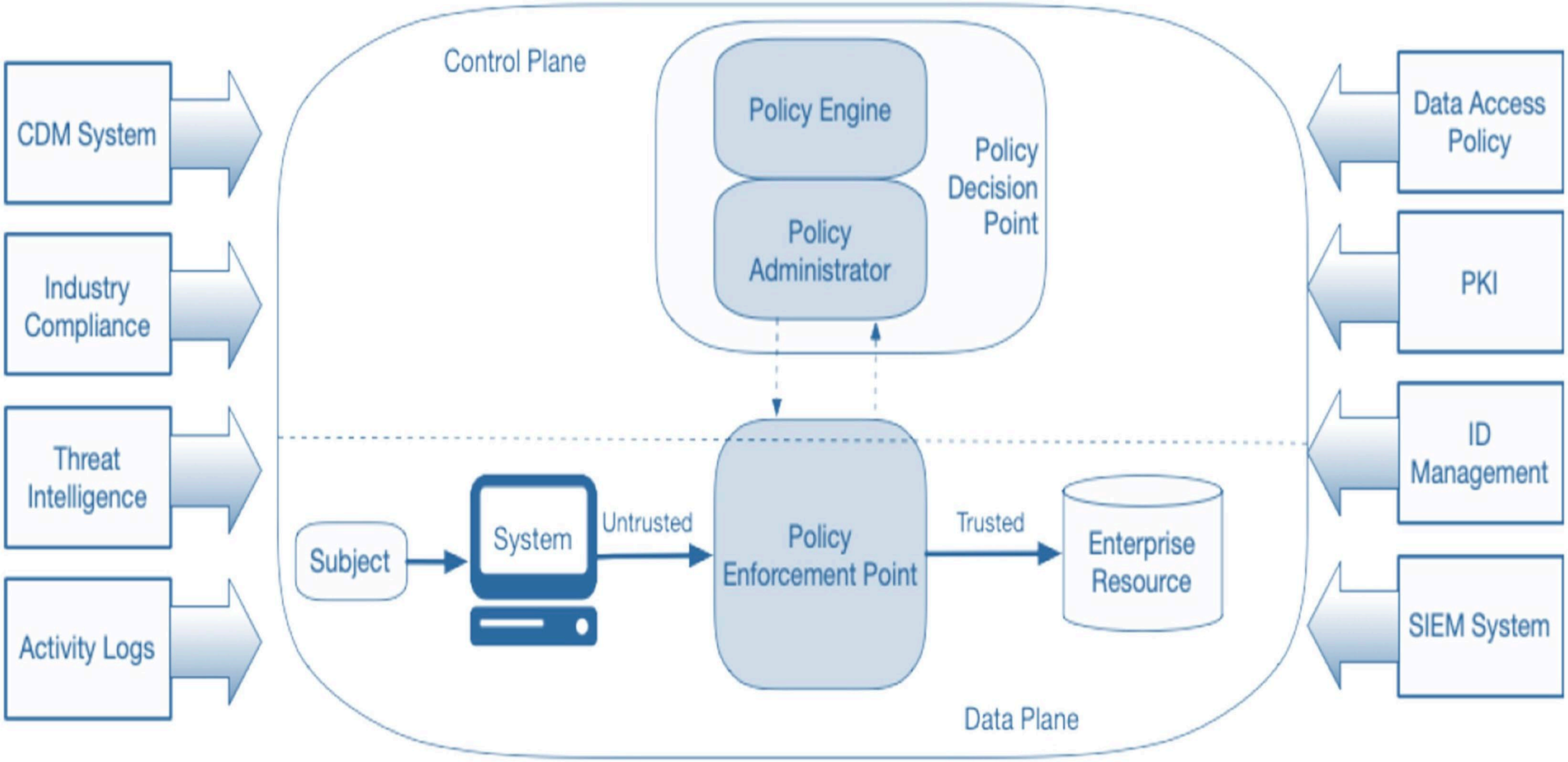
- Federal staff have enterprise-managed accounts, allowing them to access ***everything*** they need to do their job while remaining reliably protected from even targeted, sophisticated phishing attacks.
- The devices that Federal staff use to do their jobs are consistently tracked and monitored, and the security posture of those devices is taken into account when granting access to internal resources.
- Agency systems are isolated from each other, and the network traffic flowing between and within them is reliably encrypted.
- Enterprise applications are tested internally and externally and can be made available to staff securely over the internet.
- Federal security teams and data teams work together to develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information.
- This strategy places significant emphasis on stronger enterprise **identity** and **access** controls, including multi-factor authentication (**MFA**). Without secure, enterprise-managed **identity** systems, adversaries can take over user accounts and gain a foothold in an agency to steal data or launch attacks.

Memorandum M-21-31 / EO 14028

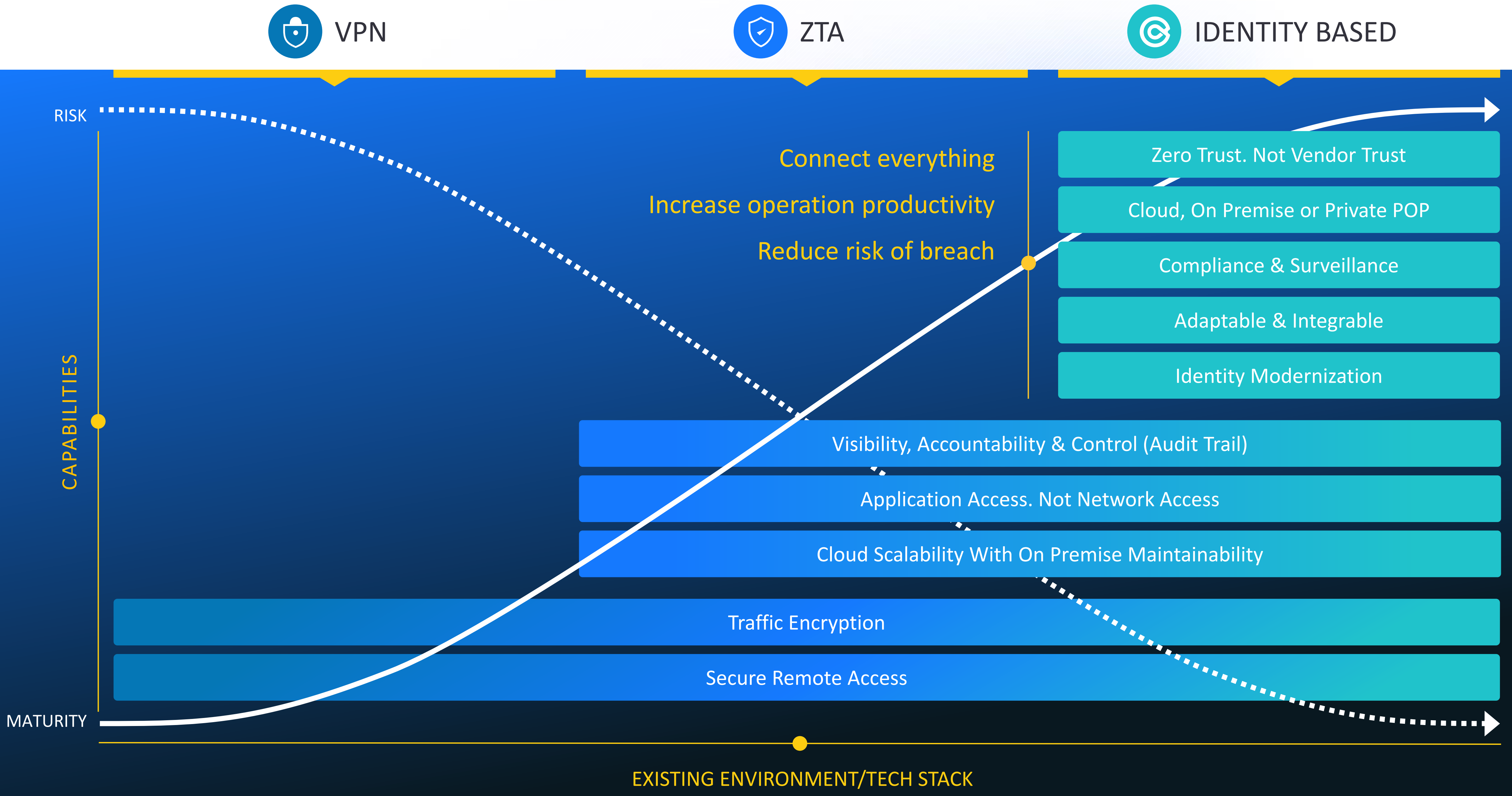
Improving Investigative & Remediation Capabilities Related to Cybersecurity Incidents

- Information from logs on Federal information systems(for both on-premises systems and connections hosted by third parties, such as cloud services providers (CSPs)) is invaluable in the detection, investigation, and remediation of cyber threats.
- This memorandum was developed in accordance with and addresses the requirements in section 8 of the Executive Order for logging, log retention, and log management, with a focus on ensuring centralized access and visibility for the highest-level enterprise security operations center (SOC) of each agency.
- In addition, this memorandum establishes requirements for agencies to increase the sharing of such information, as needed and appropriate, to accelerate incident response efforts and to enable more effective defense of Federal information in and executive branch departments and agencies.
- This memo establishes a maturity model to guide the implementation of requirements across four Event Logging (EL) tiers (EL 0 – EL 3).
- CYOLO, while not a SIEM, does retain required ZTA Logs for our platform, in acceptable formats for specified timeframes and can forward them to any specified event retention, logging or monitoring platform.

Core ZTA Logical Components



The Cyolo Vision of ZTA



VPN

ZTA

IDENTITY BASED

RISK

CAPABILITIES

MATURITY

Connect everything

Increase operation productivity

Reduce risk of breach

Zero Trust. Not Vendor Trust

Cloud, On Premise or Private POP

Compliance & Surveillance

Adaptable & Integrable

Identity Modernization

Visibility, Accountability & Control (Audit Trail)

Application Access. Not Network Access

Cloud Scalability With On Premise Maintainability

Traffic Encryption

Secure Remote Access

EXISTING ENVIRONMENT/TECH STACK

The Real-World Driver for ZTA Capabilities - Increasingly Complex Environments

More Hybrid Users

Employees

R&D

3rd parties

Executives

More Applications

SaaS Apps

slack

salesforce

On-Prem Data Centers

Internal Networks

Cloud Data Centers

aws

More Locations

Offices (Carpeted floor)

Industrial (Grated Floor)

Remote (In the field)

Virtual

More Managed and Unmanaged Devices

More Resources

IT/OT Resources

Remote

Files & Data

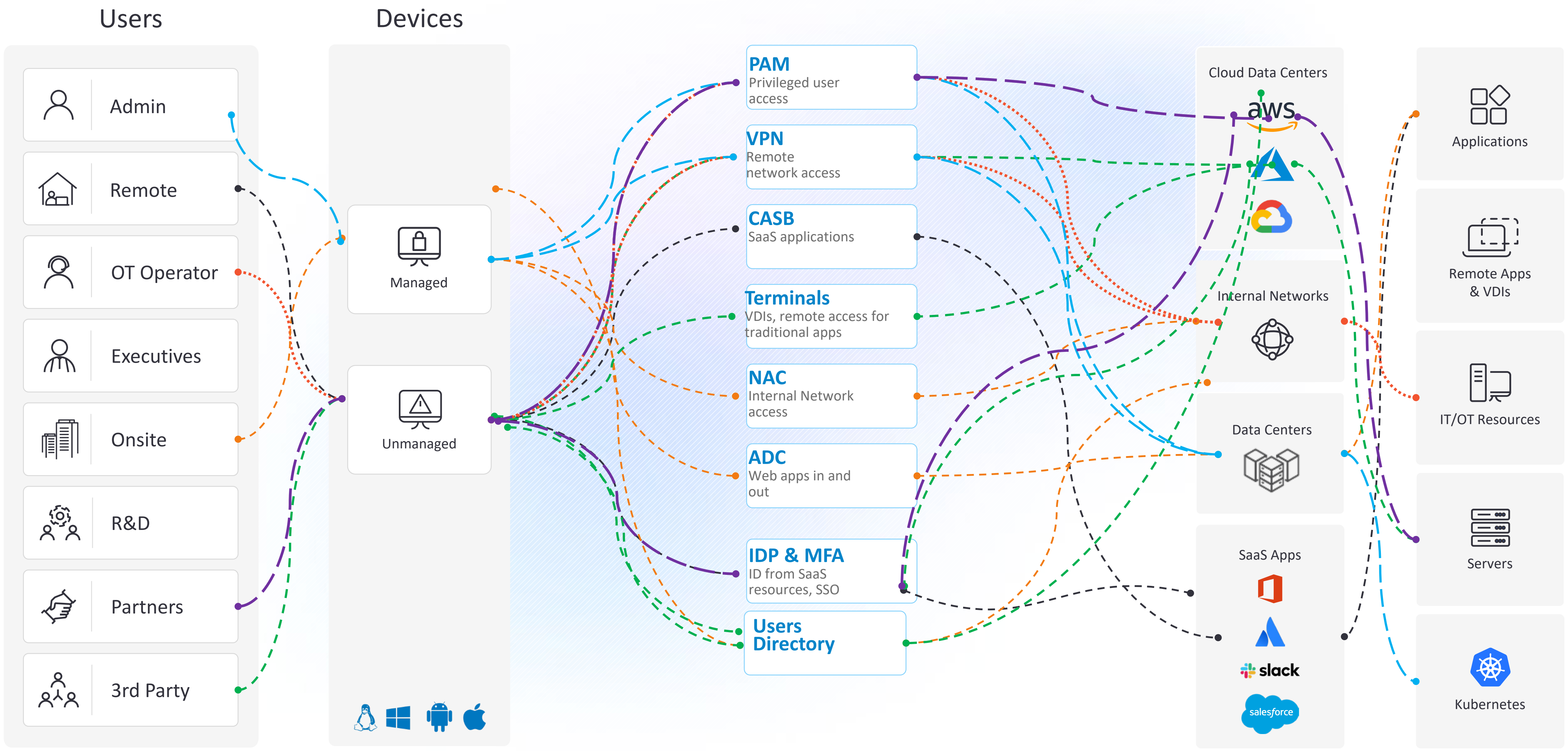
Legacy

Internal

Servers

Cyolo

Connecting People To Their Work Has Gotten **Much Harder**



Users

Admin

Remote

OT Operator

Executives

Onsite

R&D

Partners

3rd Party

Devices

Managed

Unmanaged

PAM
Privileged user access

VPN
Remote network access

CASB
SaaS applications

Terminals
VDIs, remote access for traditional apps

NAC
Internal Network access

ADC
Web apps in and out

IDP & MFA
ID from SaaS resources, SSO

Users Directory

Cloud Data Centers

aws

Internal Networks

Data Centers

SaaS Apps

slack

salesforce

Applications

Remote Apps & VDIs

IT/OT Resources

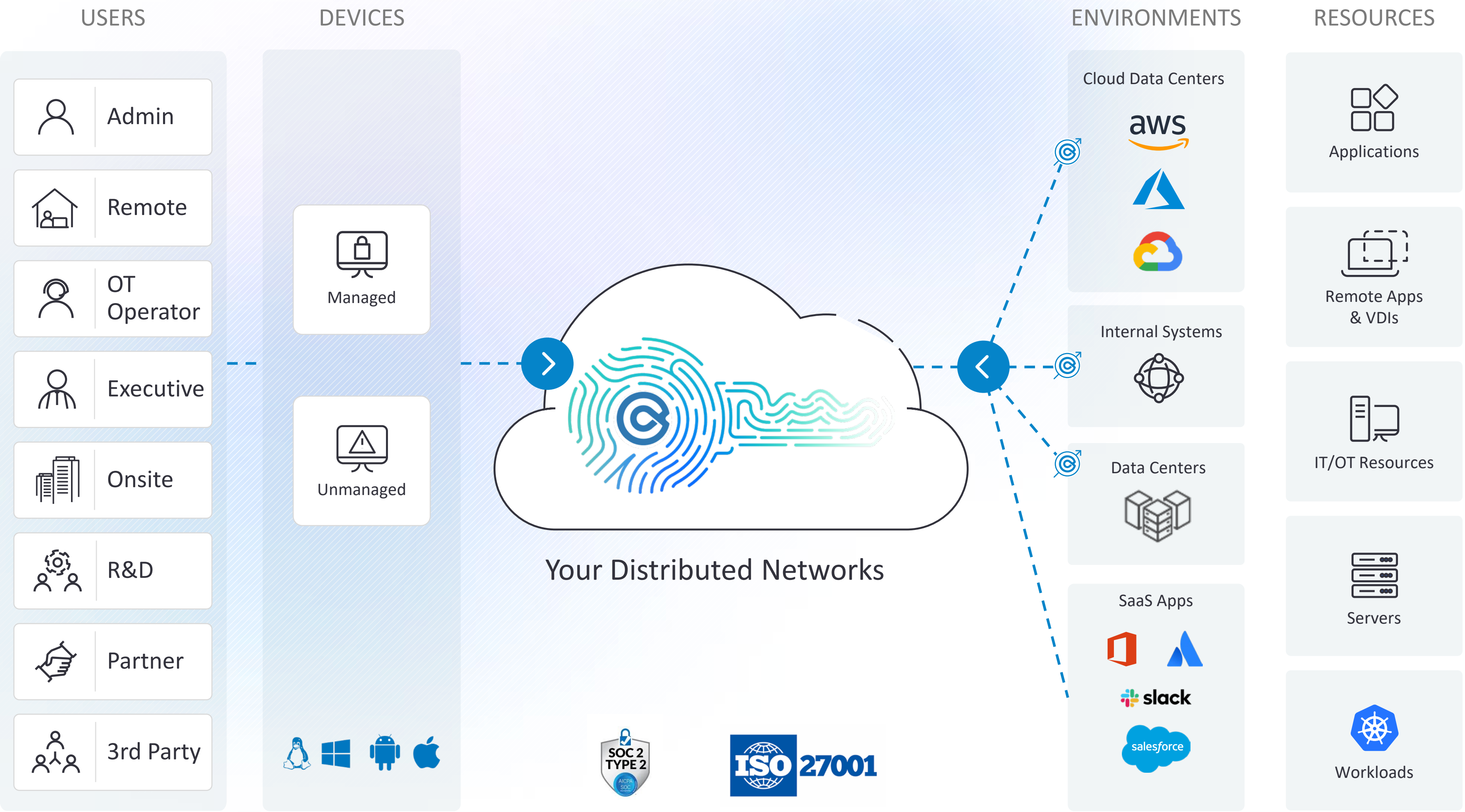
Servers

Kubernetes

Cyolo

Identity Based Connectivity

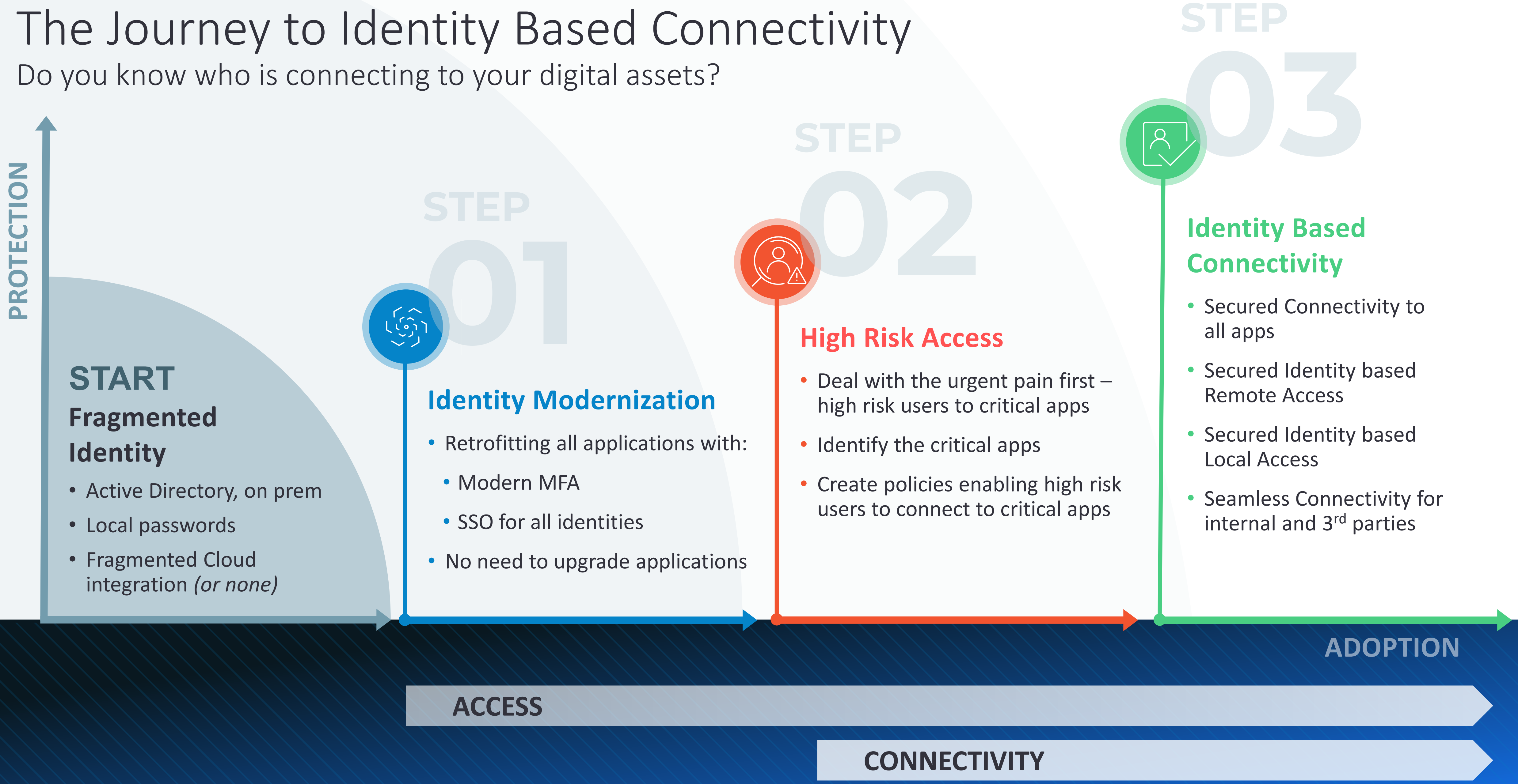
The Key to Secure Connectivity for ZTA



Cyolo

The Journey to Identity Based Connectivity

Do you know who is connecting to your digital assets?



START

Fragmented Identity

- Active Directory, on prem
- Local passwords
- Fragmented Cloud integration *(or none)*

Identity Modernization

- Retrofitting all applications with:
  - Modern MFA
  - SSO for all identities
- No need to upgrade applications

High Risk Access

- Deal with the urgent pain first – high risk users to critical apps
- Identify the critical apps
- Create policies enabling high risk users to connect to critical apps

Identity Based Connectivity

- Secured Connectivity to all apps
- Secured Identity based Remote Access
- Secured Identity based Local Access
- Seamless Connectivity for internal and 3rd parties

Cyolo

Identity Modernization

Existing Infrastructure

Identity Modernization

OPTION 1

Rip and replace with modern infrastructure

DIFFICULT EXPENSIVE TIME CONSUMING

Identity Modernization

OPTION 1

Rip and replace with modern infrastructure

DIFFICULT EXPENSIVE INEFFICIENT

OPTION 2

Retrofit to enable modern infrastructure

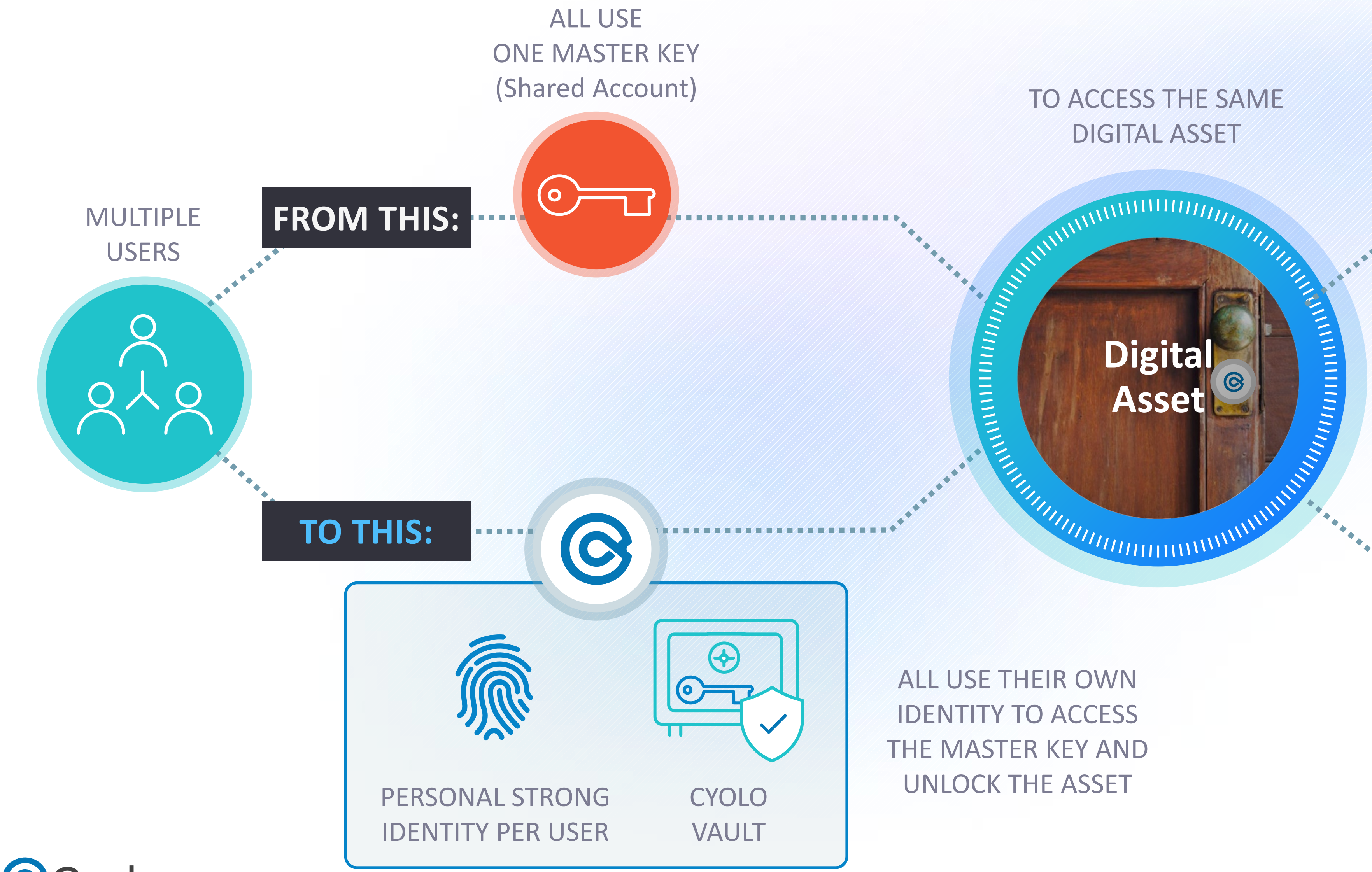
Identity is the new key

SEAMLESS FASTER EASIER

30x

Cyolo

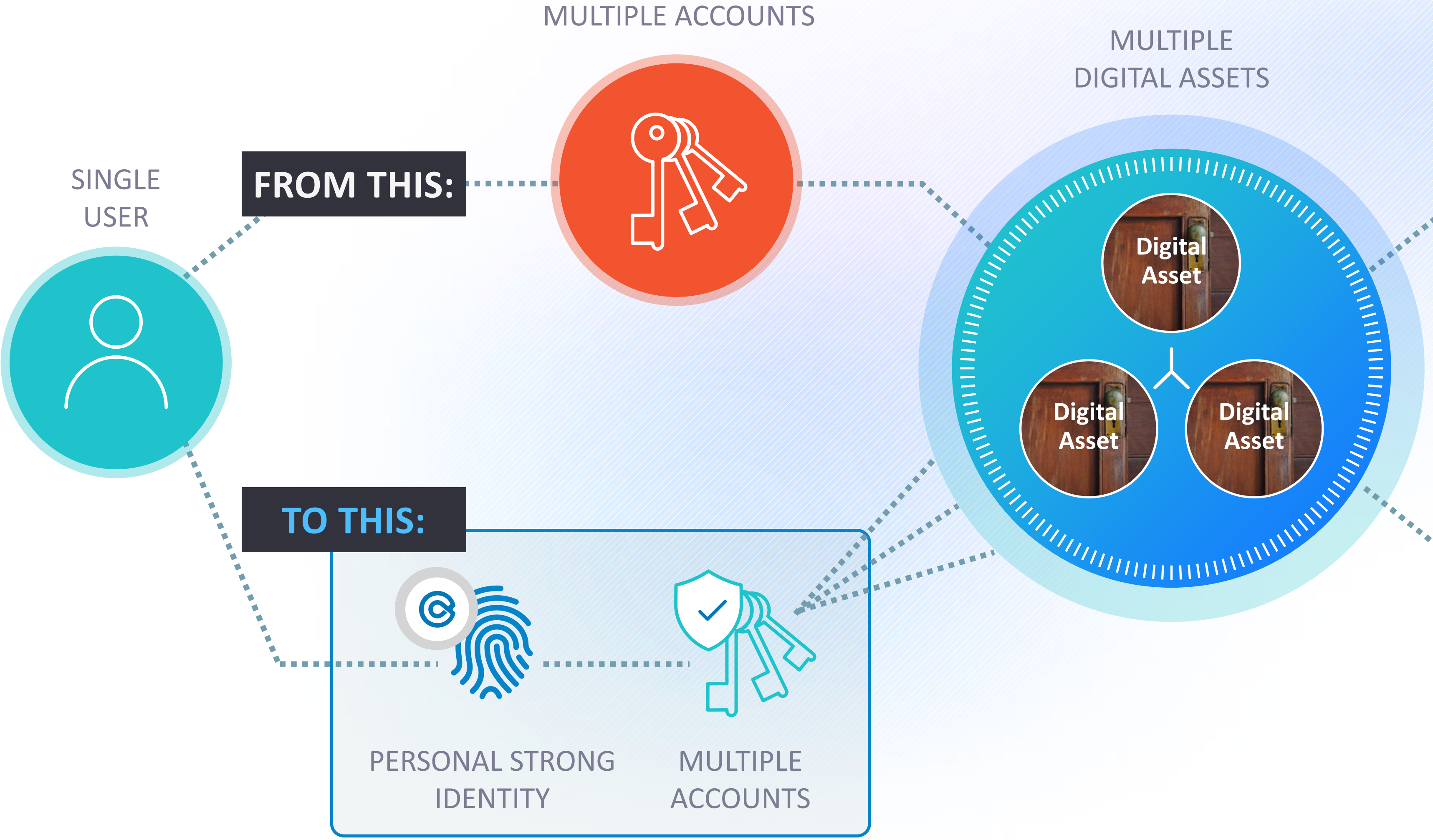
Generic Accounts / Shared Account



- No traceability or audit trail
- Prone to attack
- Cannot pass security assessment
- Cannot adhere to regulation

- No need to upgrade digital assets
- No lift and shift
- Seamless Modern Identity
- Full access trail

Identity Federation



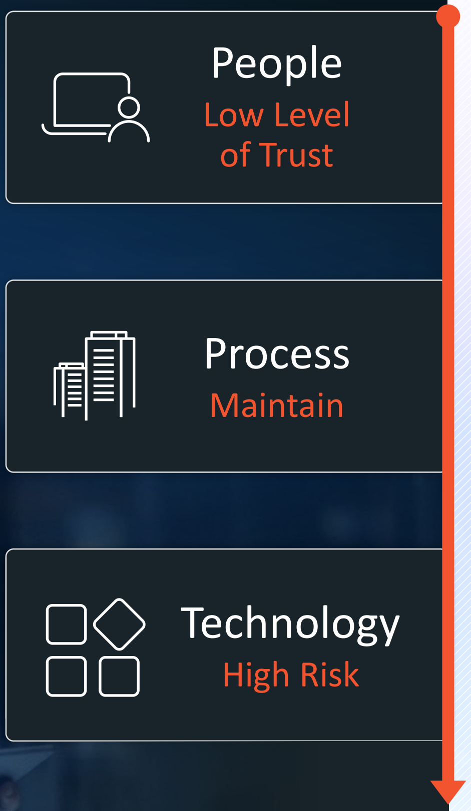
- Complex management
- No single point for audit trailing
- Complex user experience

- No change in digital assets
- No configuration changes on IDPs or assets
- Single strong identity
- Superior User Experience
- Full audit trail

Cyolo

High Risk Access

Solve the High-Risk Problems First

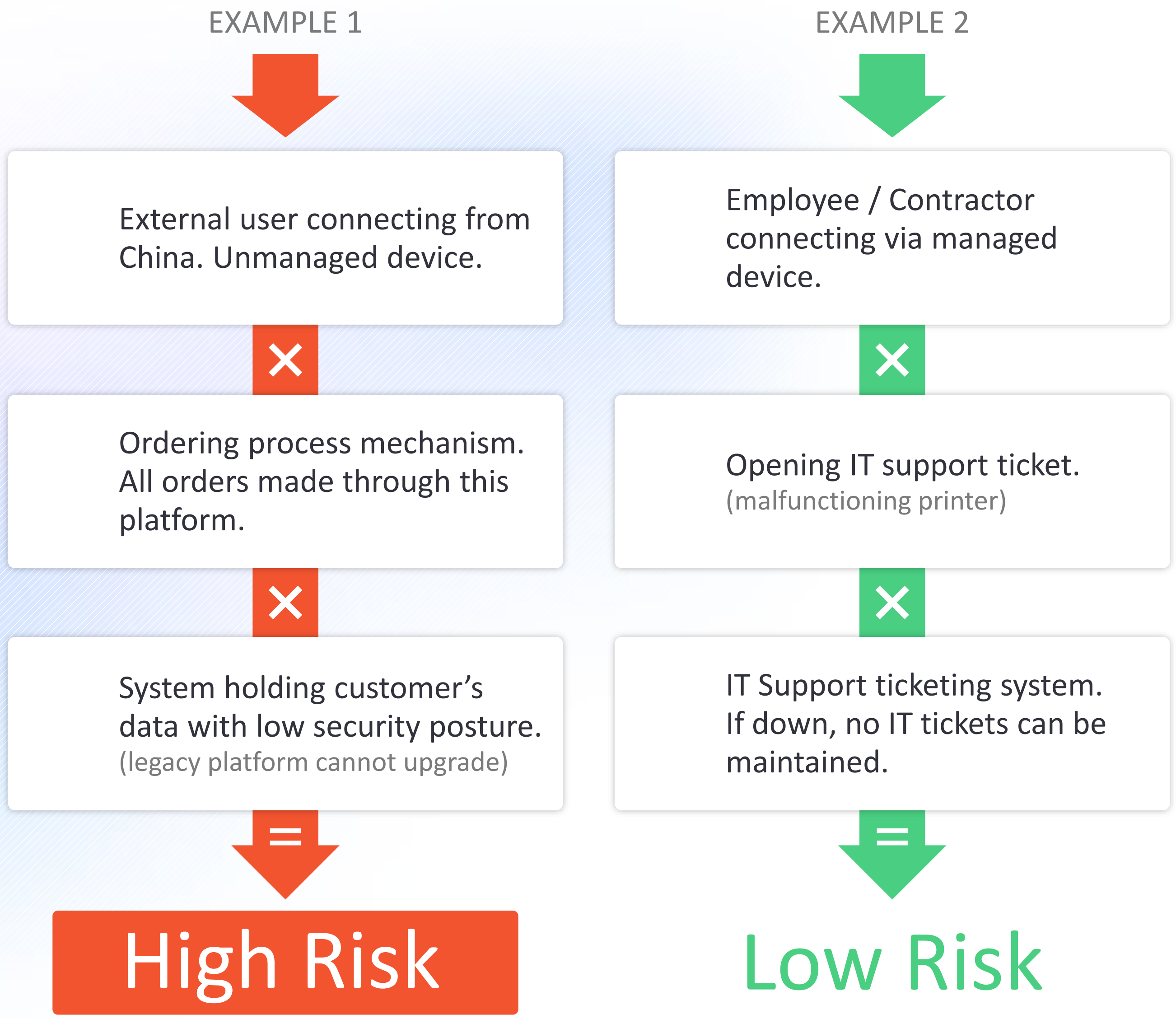


People
Low Level of Trust

Process
Maintain

Technology
High Risk

IT and OT systems holding **sensitive data** or running **critical missions**



EXAMPLE 1

External user connecting from China. Unmanaged device.

×

Ordering process mechanism. All orders made through this platform.

×

System holding customer's data with low security posture. (legacy platform cannot upgrade)

=

High Risk

EXAMPLE 2

Employee / Contractor connecting via managed device.

×

Opening IT support ticket. (malfunctioning printer)

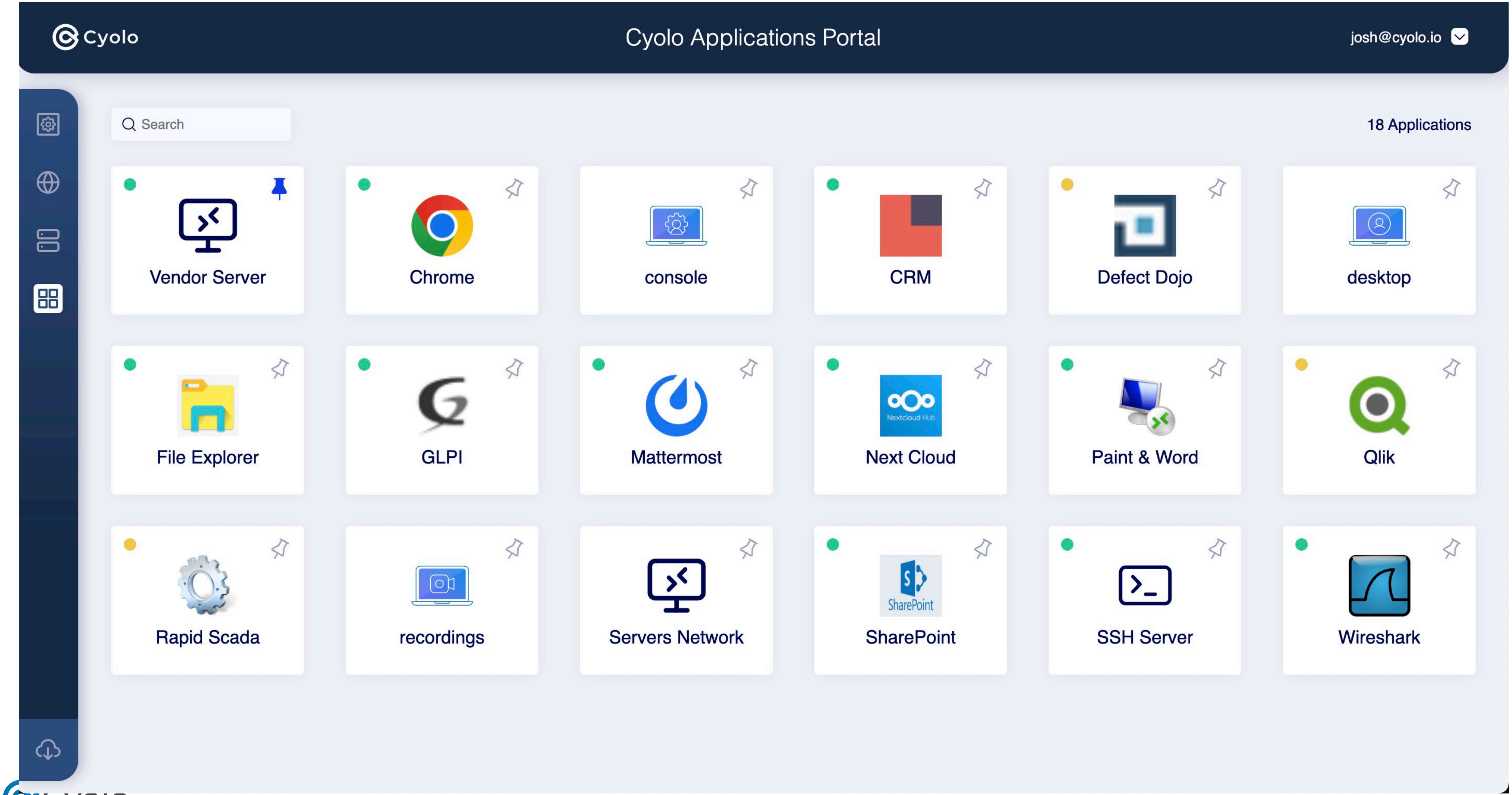
×

IT Support ticketing system. If down, no IT tickets can be maintained.

=

Low Risk

Cyolo


Cyolo
Cyolo Applications Portal
josh@cyolo.io
Search
18 Applications
Vendor Server
Chrome
console
CRM
Defect Dojo
desktop
File Explorer
GLPI
Mattermost
Next Cloud
Paint & Word
Qlik
Rapid Scada
recordings
Servers Network
SharePoint
SSH Server
Wireshark

Achieving ZTA Goals (Functional) using Cyolo

Mitigate / Reduce Risk of an Event / Incident

Decrease TCO
Increase ROI
Improve Process

Seamless Integration Into Existing Resources

Improved Threat Detection and Audit Reporting

Cyolo

Achieving ZTA Goals (Technical) using Cyolo

Mitigate Risk of Breach

- MFA & SSO to any app and resource
- End-to-end encryption & continuous authorization
- Secrets vault
- Application access instead of network access

Increase Operational Productivity

- Just in time access
- Disaster Recovery
- Integrate with all IdPs, support multiple idPs
- Identity federation
- Local IDP
- Work with any device & BYOD

Seamlessly Adapted by End Users

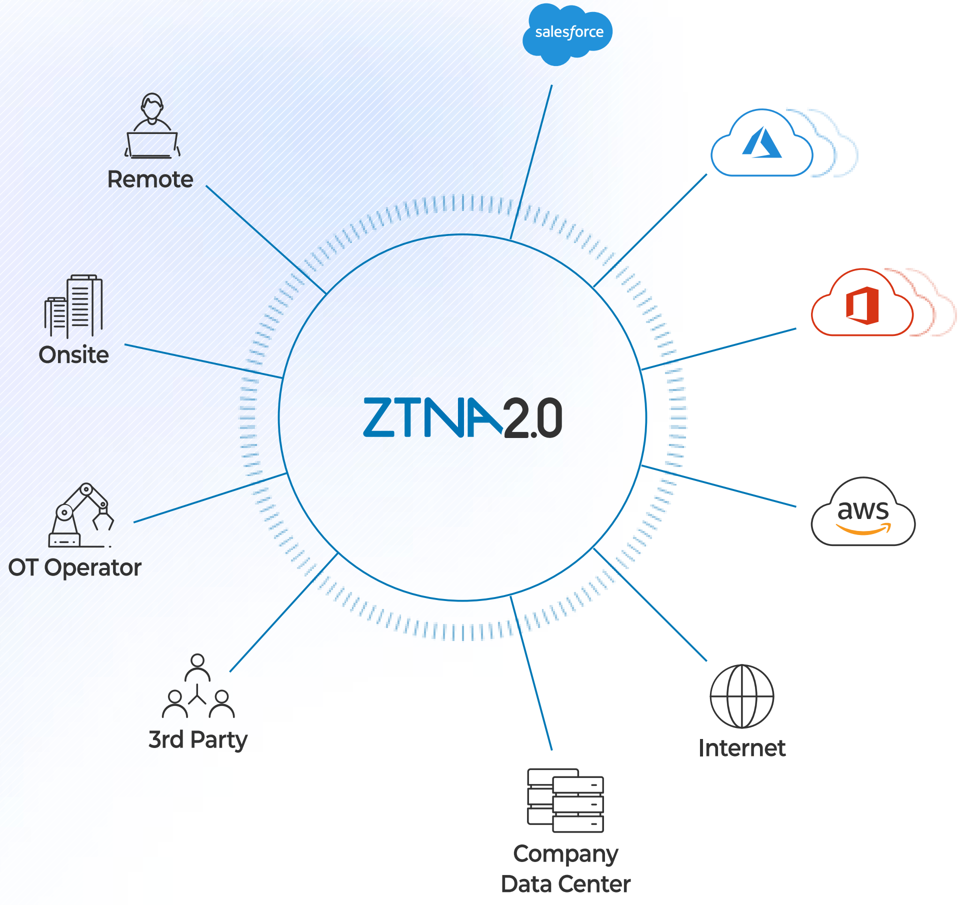
- Web and native application support
- Agentless
- Fastest ZTA by design
- Just in time access
- Android, iOS
- Windows, iOS, Linux

Simplify Compliance Reporting

- Supervised Access
- Session recording
- Cloud, On Premise or Private PoP
- Full audit trail
- Integrate with security tools and SIEMs

Cyolo

Thank You!



Cyolo