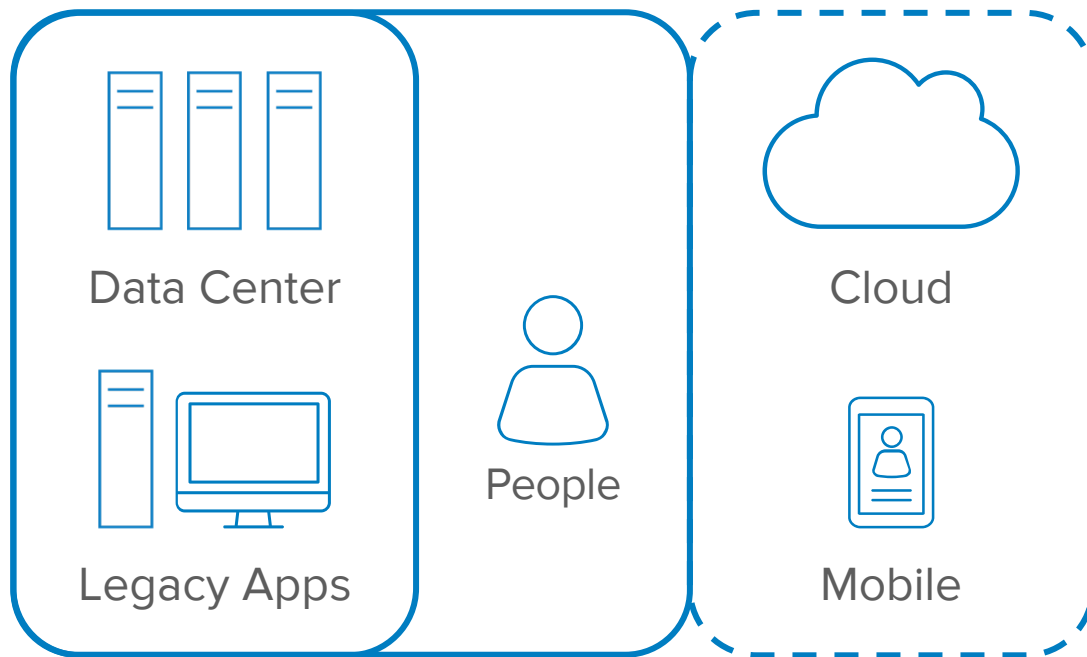




Passwordless + Security

Sami Laine
Director, Product Marketing

Transformation of IT Delivery



Traditional perimeter is disappearing – fast



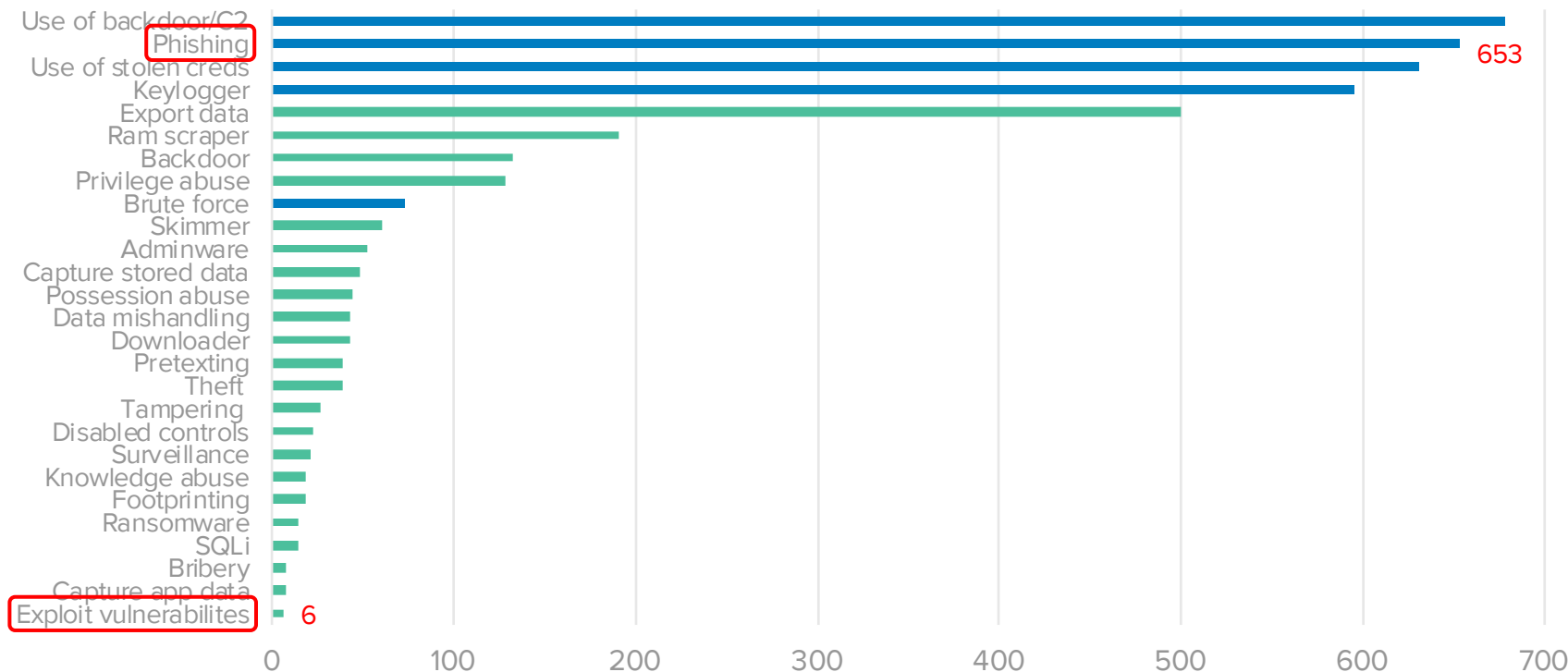
Transformation of IT Delivery



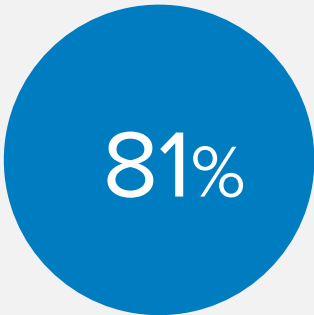
Identity is the new perimeter



Cause of data breaches

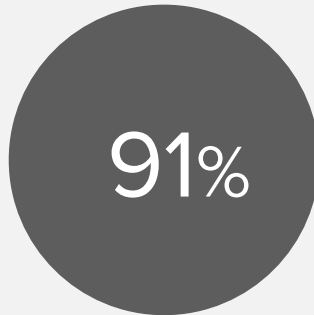


Cloud Risk: Identity Attacks



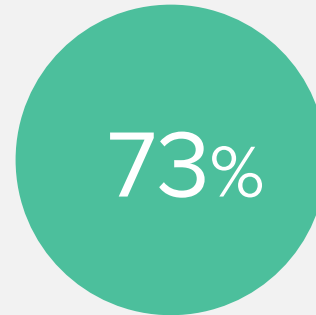
of data breaches involve
stolen/weak credentials

*Source: 2017 Verizon Data Breach
Investigations Report*



of phishing attacks
target credentials

*Source: 2016 Verizon Data Breach
Investigations Report*



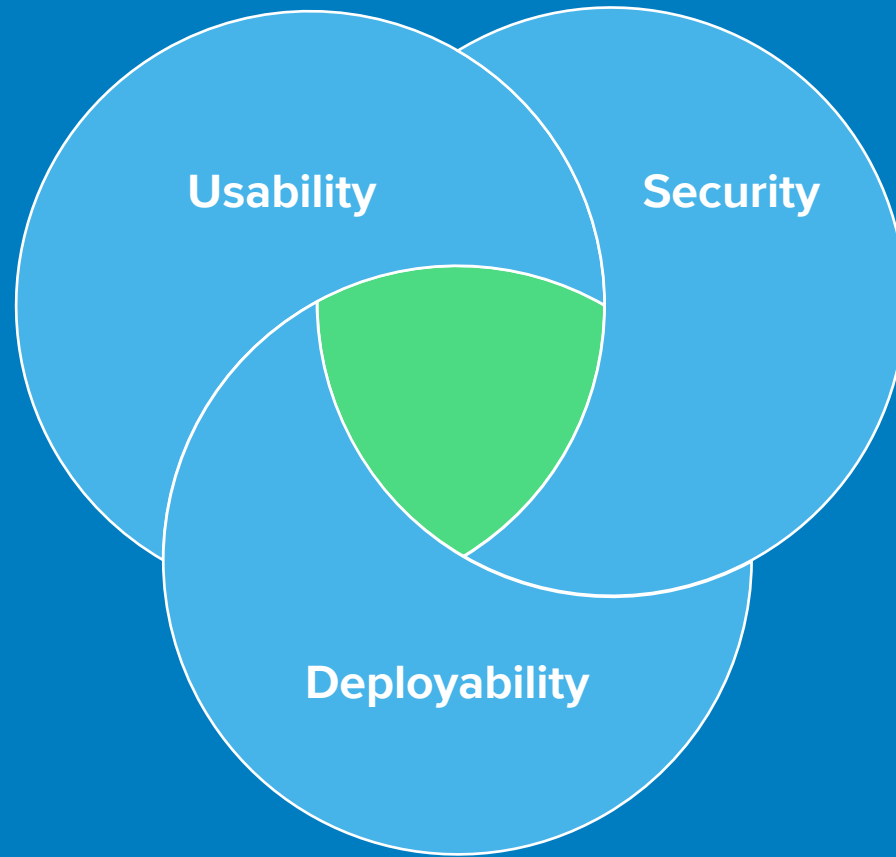
of passwords
are duplicates

*Source: TeleSign 2016 Consumer
Account Security Report*



**In the cloud,
bad guys don't hack in
– they log in**

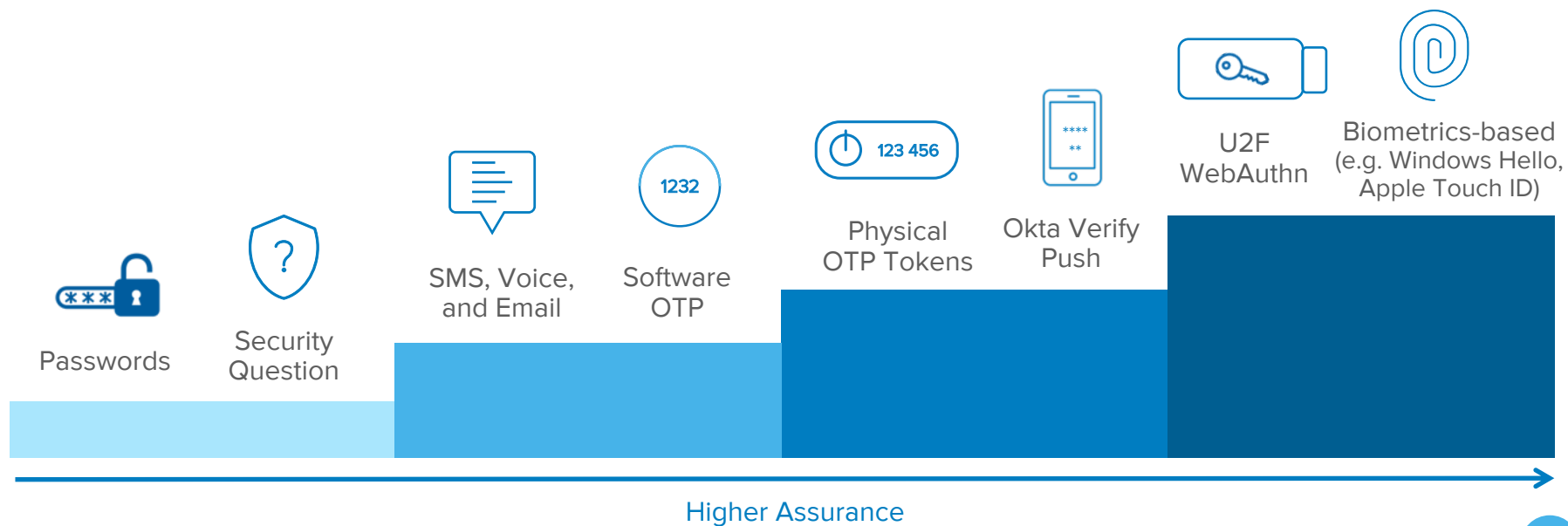




Security Versus Usability

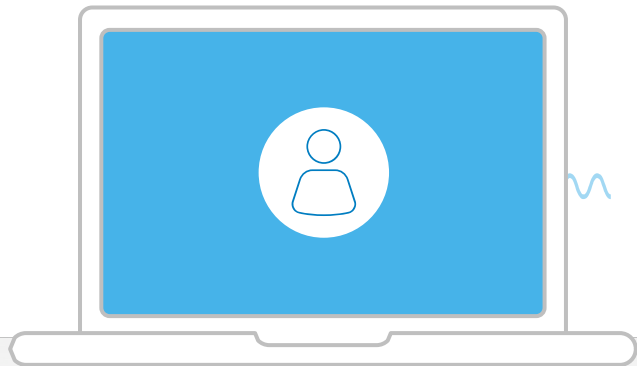


Organizations Must Balance Security with Usability



Enhanced device context

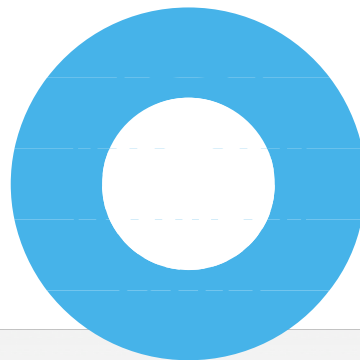
Device



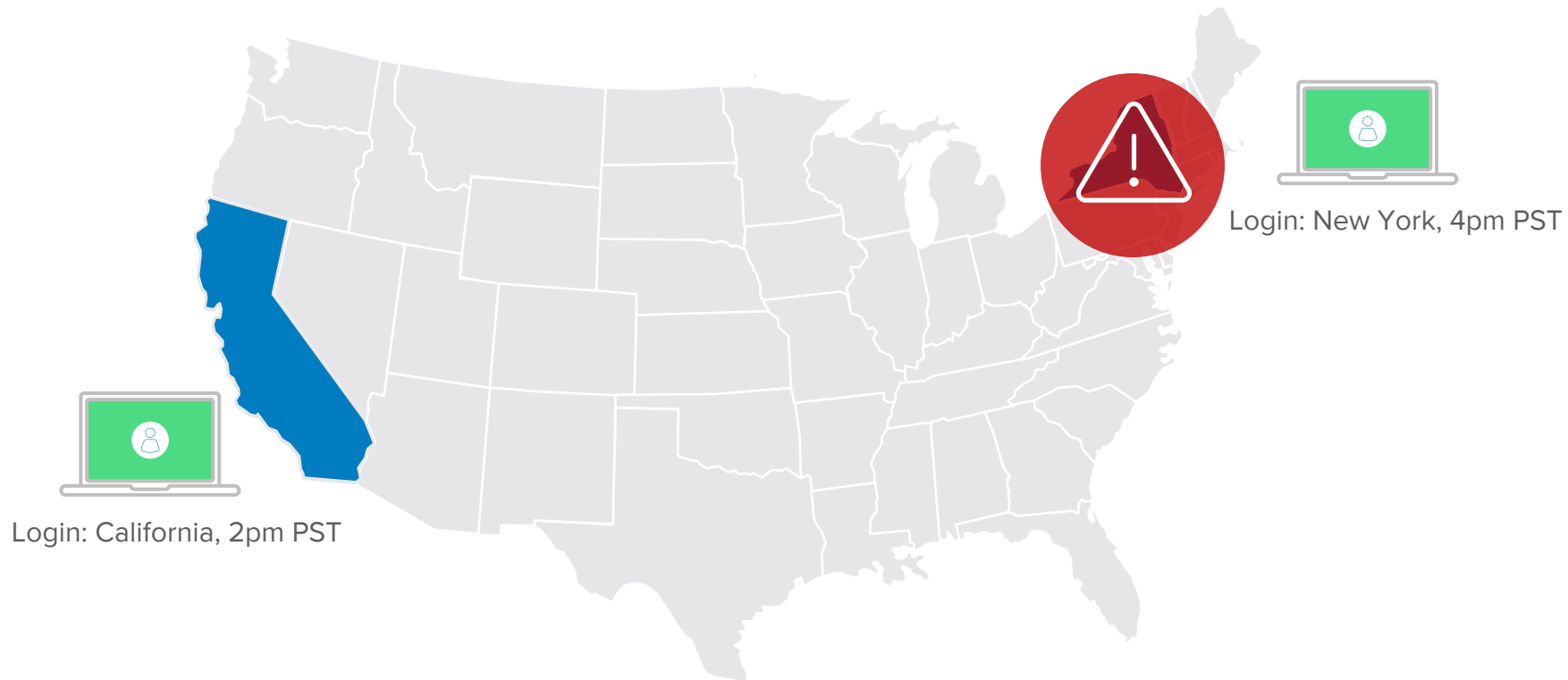
Device attributes

OS version
CPU architecture
Screen resolution
Time zone
Language settings
Color depth
and more...

Device fingerprint



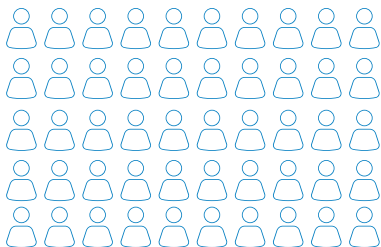
Enhanced location context



Okta ThreatInsight

4,700+ Customers

5,500+ Partners



Add Rule

Rule Name
Operations Team Sign On Policy

Exclude Users
Exclude users

If user's IP is
Anywhere
[Manage configurations for Network](#)

And authenticates via
Any method

And threat suspected ⓘ ☒ Yes

Then access is
Allowed

☒ Prompt for factor
[Manage configuration for Multifactor Authentication](#)

☒ Per device
☐ Every time
☐ Per session

Session duration
4 Hours

Add Rule Cancel

No Threat

Factor Challenge

BLOCKED



Okta Contextual Access Management



Risk Context: Okta Threat Insight, Risk Scoring



Okta Contextual Access Management



Risk Context: Okta Threat Insight, Risk Scoring



Response: Use Authentication Factors of Choice

Add Rule

Rule Name

Trusted Company Networks

Exclude Users

Exclude users

PRE - AUTHENTICATION

If user's IP is

In zone

Manage configurations

☐ All zones

Select zone

Then access is

Allowed

Select your criteria

AUTHENTICATION

Password

Required additional authentication

Okta Verify

OR

Google Authenticator

OR

SMS Authentication

Security strength

Password + Okta Verify

Strong

Password + Google Auth

Strong

Password + SMS

Moderate

Add

Okta Verify

Required additional authentication

None

Security strength

Okta Verify Only

Strong

Add

Add authentication chain

SESSION LIFETIME

Session lifetime

☒ Per device

☐ Every time



- Select your method of authentication(s)



- Choose factors other than password



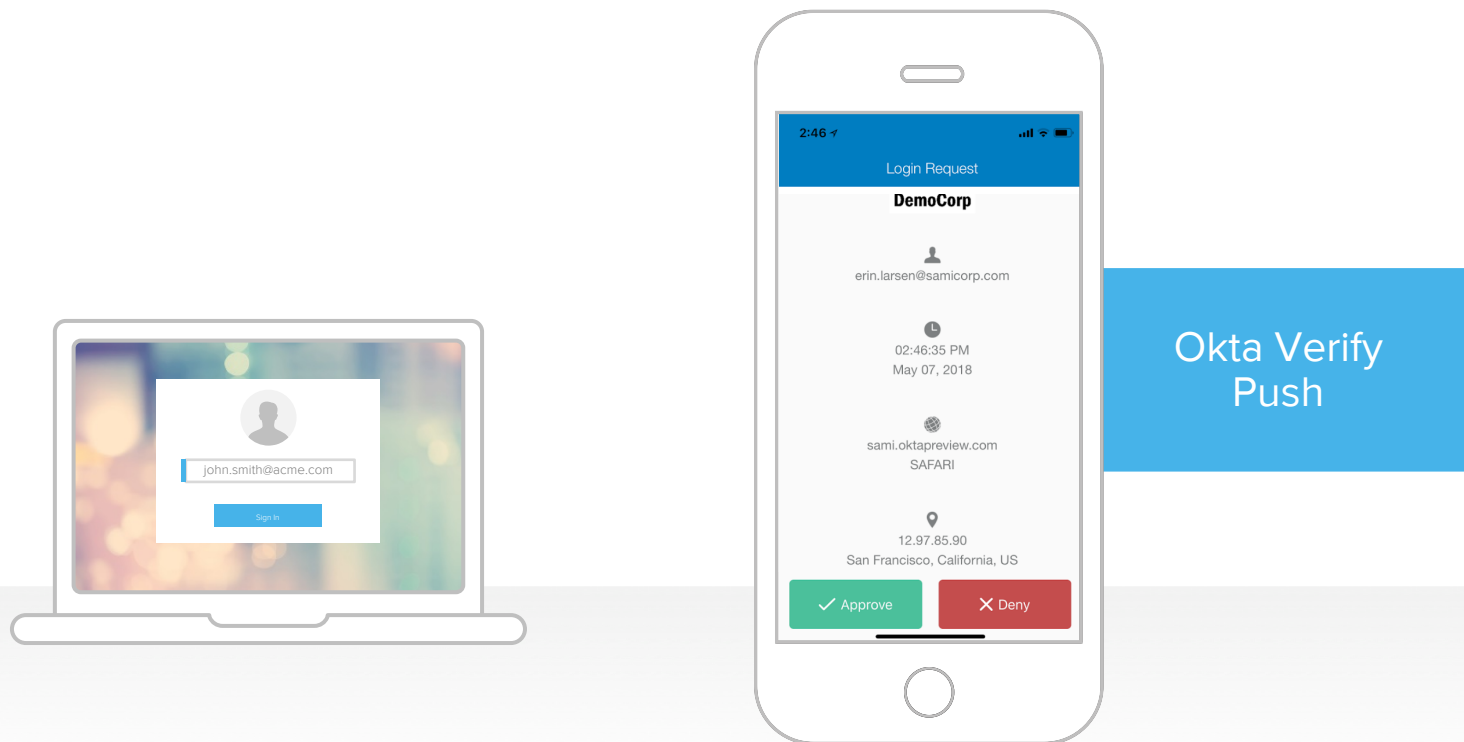
- Flexibility to prompt for stronger authentication factors for high risk use cases



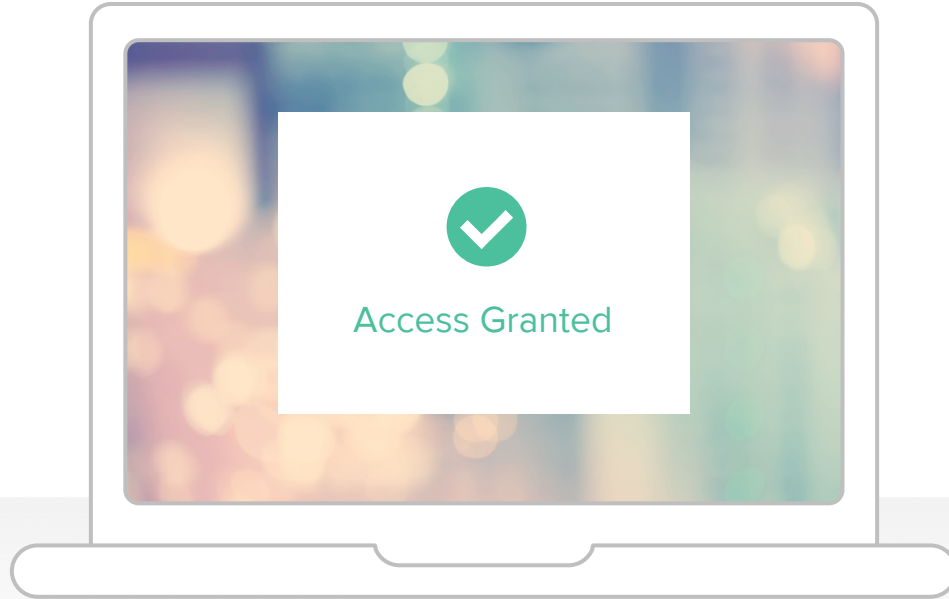
Secure Passwordless Experience



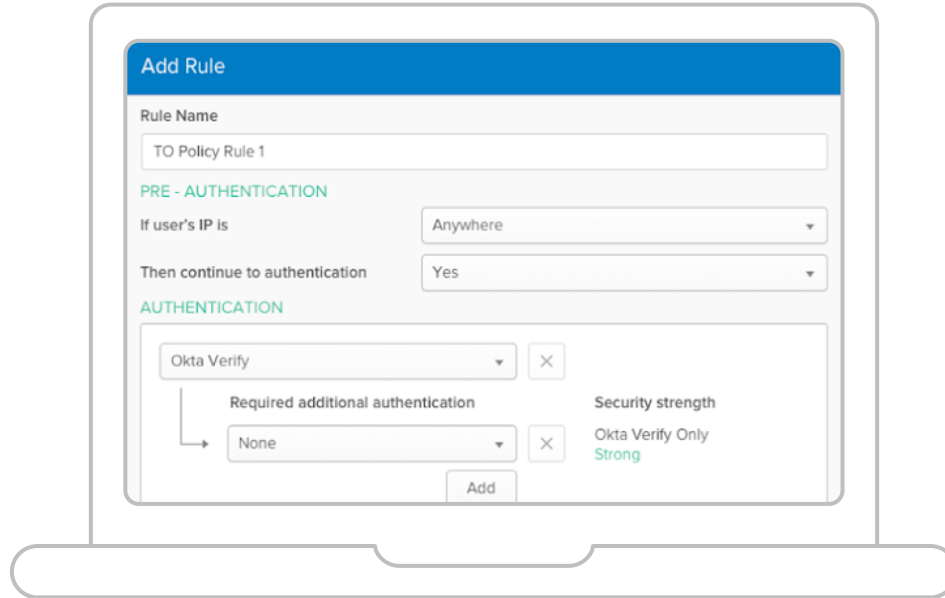
Secure Passwordless Experience



Secure Passwordless Experience



Secure Passwordless Experience



The screenshot shows the 'Add Rule' interface in the Okta Admin console. It features a blue header bar with the title 'Add Rule'. Below the header, there is a 'Rule Name' field containing 'TO Policy Rule 1'. The interface is divided into two main sections: 'PRE - AUTHENTICATION' and 'AUTHENTICATION'. In the 'PRE - AUTHENTICATION' section, there are two dropdown menus: 'If user's IP is' set to 'Anywhere' and 'Then continue to authentication' set to 'Yes'. The 'AUTHENTICATION' section contains a list of authentication methods, with 'Okta Verify' selected. To the right of the list, there is a 'Security strength' dropdown set to 'Okta Verify Only Strong'. An 'Add' button is located at the bottom right of the authentication methods list.

Add Rule

Rule Name
TO Policy Rule 1

PRE - AUTHENTICATION

If user's IP is: Anywhere

Then continue to authentication: Yes

AUTHENTICATION

Okta Verify

Required additional authentication: None

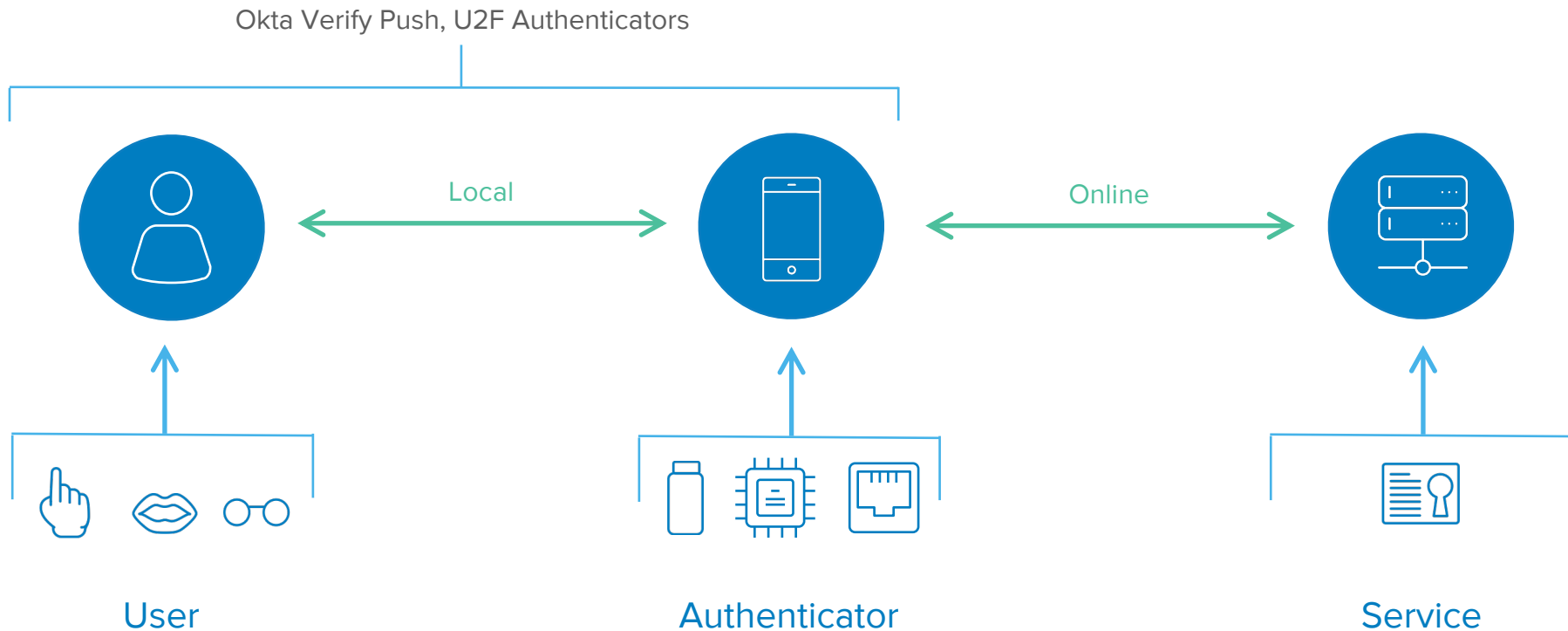
Security strength: Okta Verify Only Strong

Add

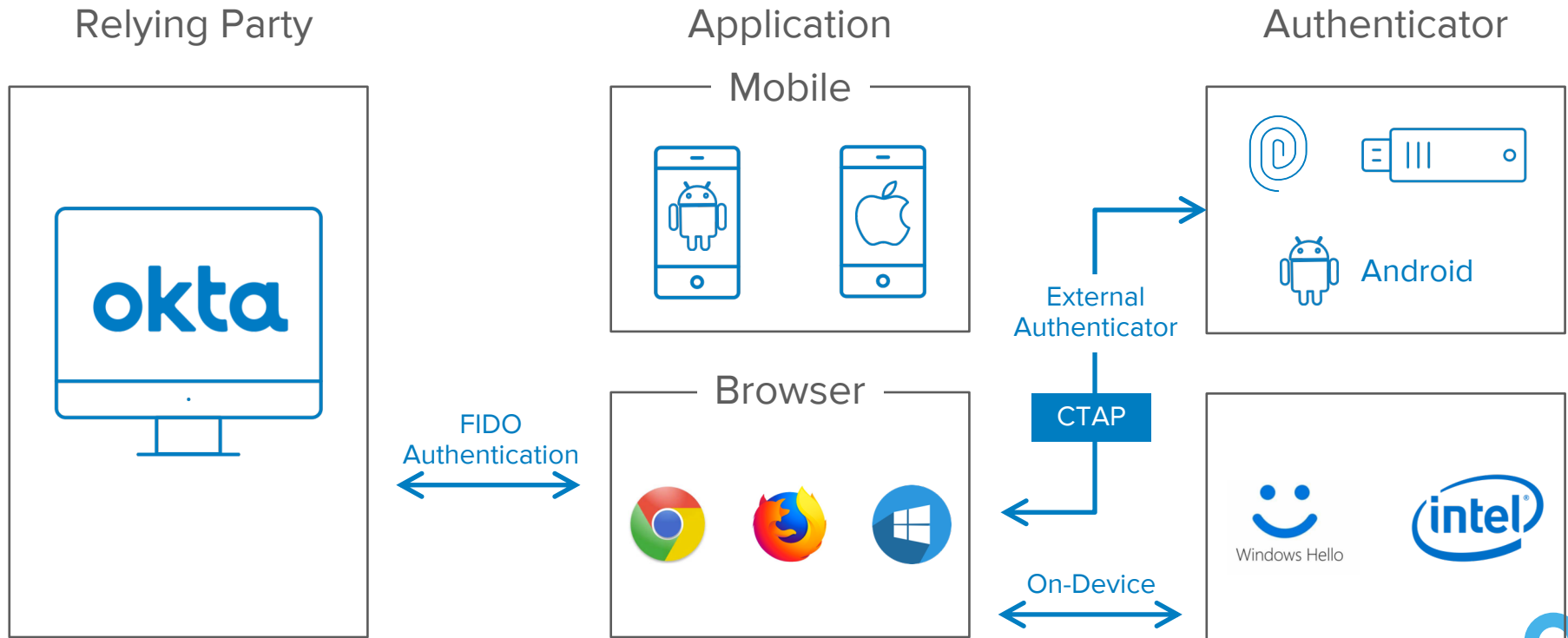
Admin console



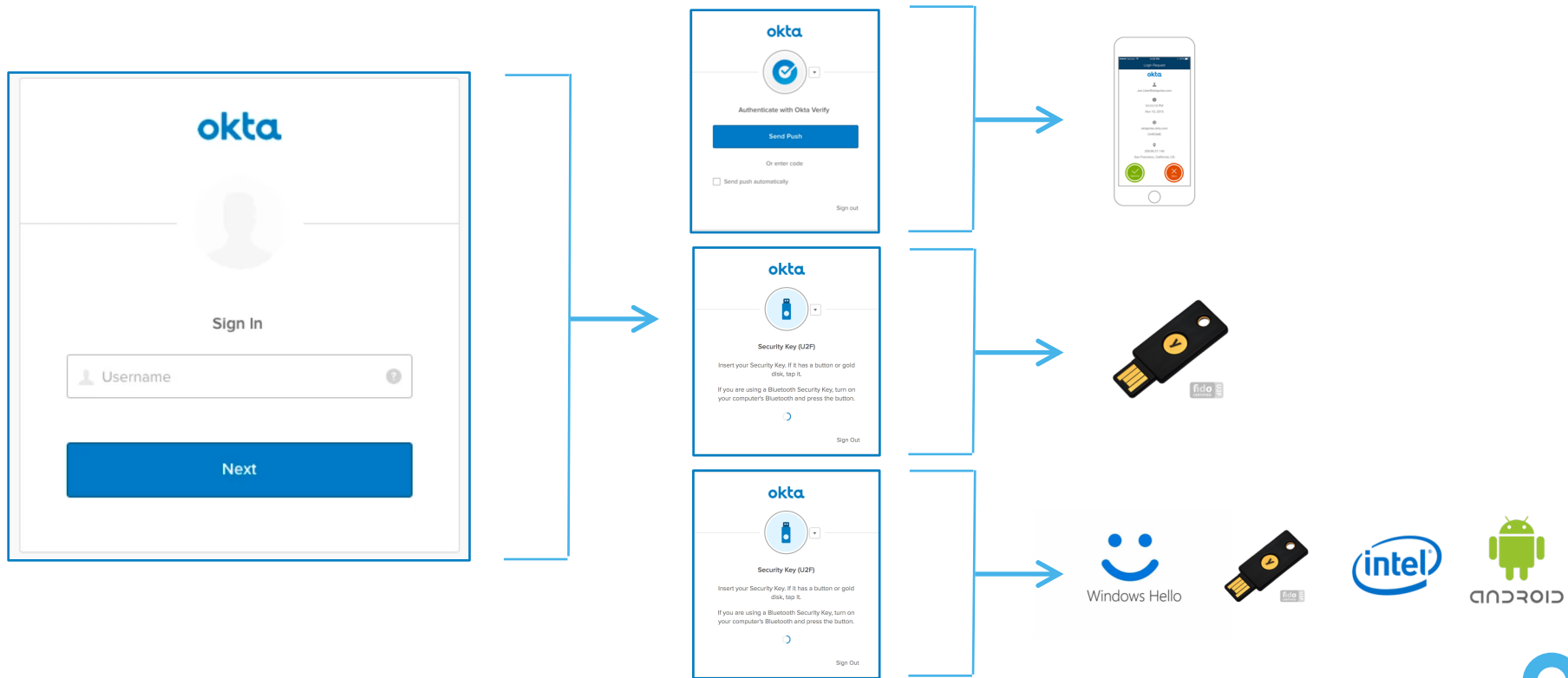
Modern Passwordless Authentication



Modern Passwordless Authentication



Modern Passwordless Authentication



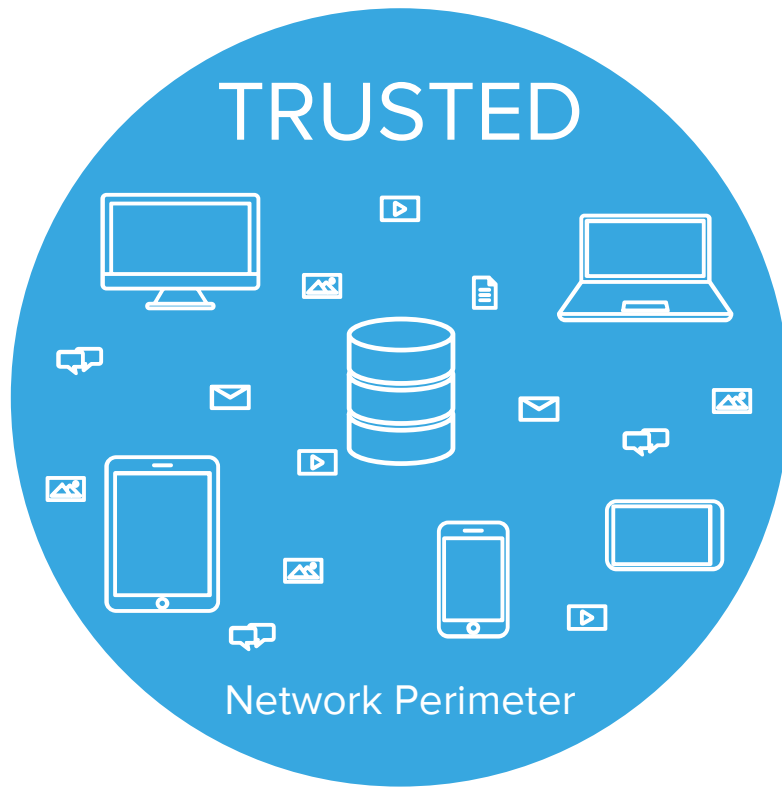
Okta Contextual Access Management



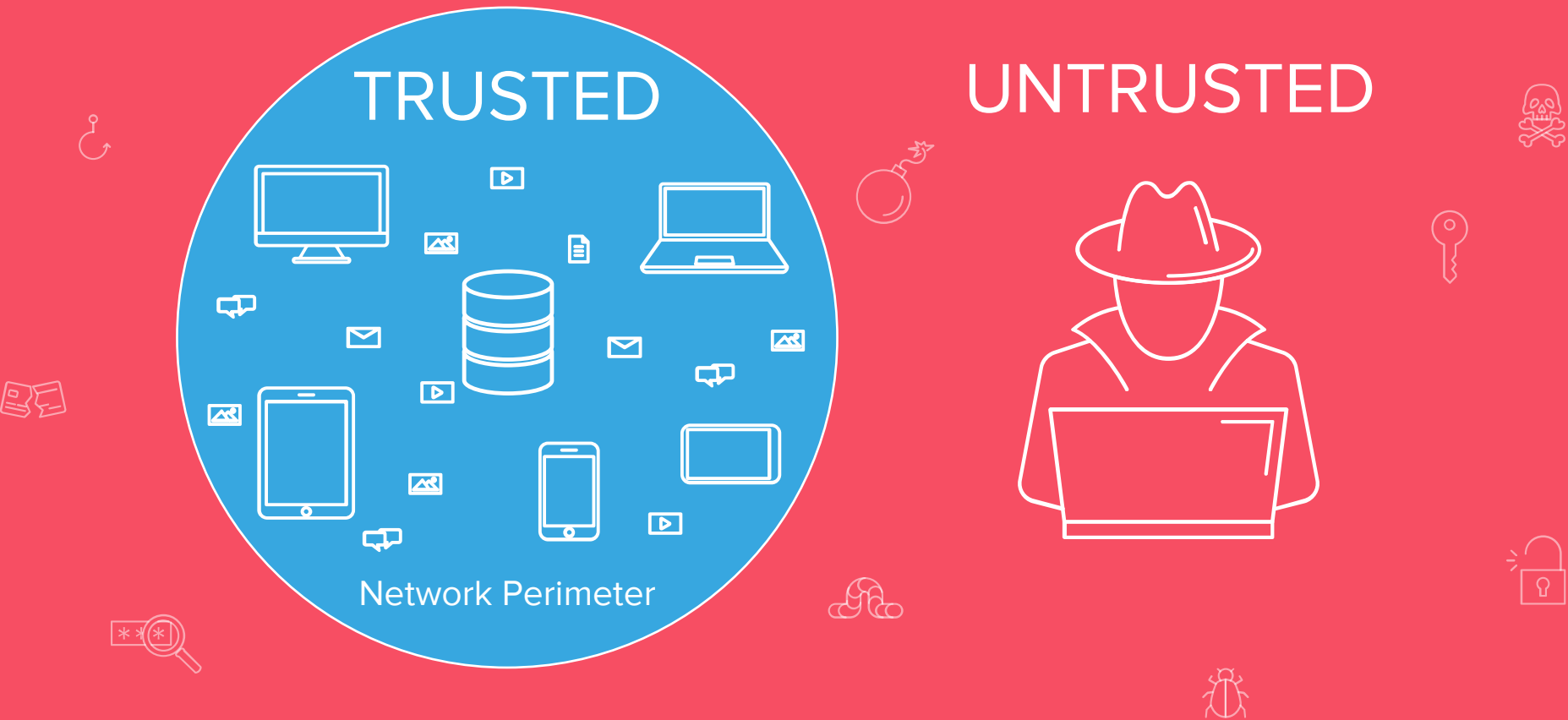
Risk Context: Okta Threat Insight, Risk Scoring

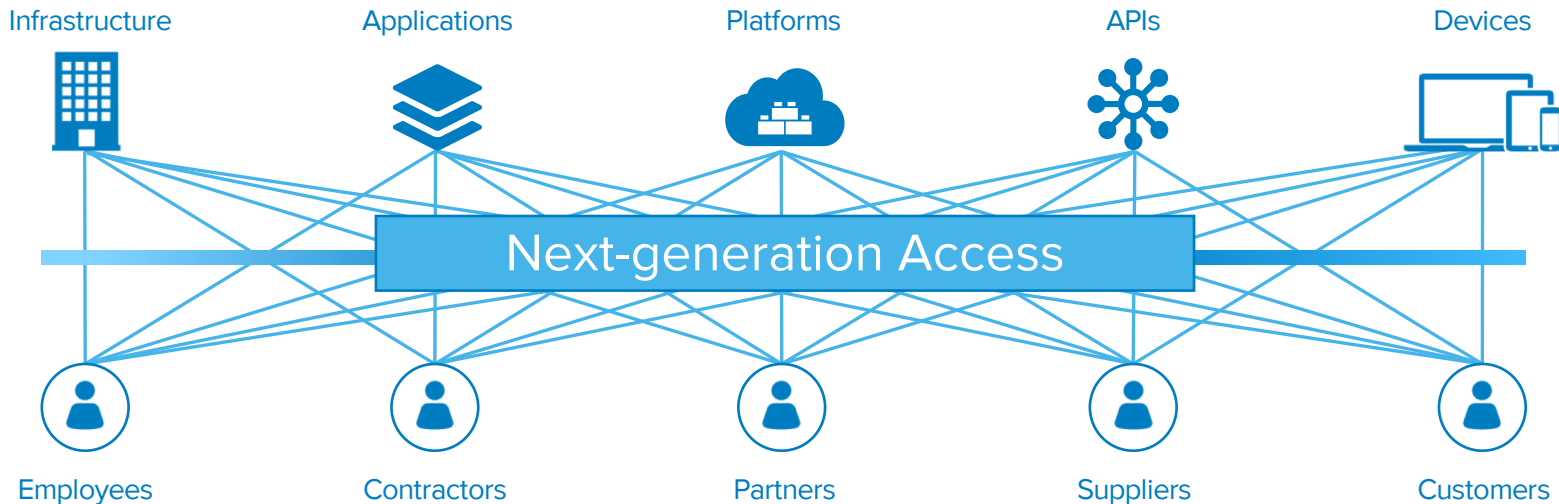


The “Old Way” of Viewing the Corporate Network



The “Old Way” of Viewing the Corporate Network



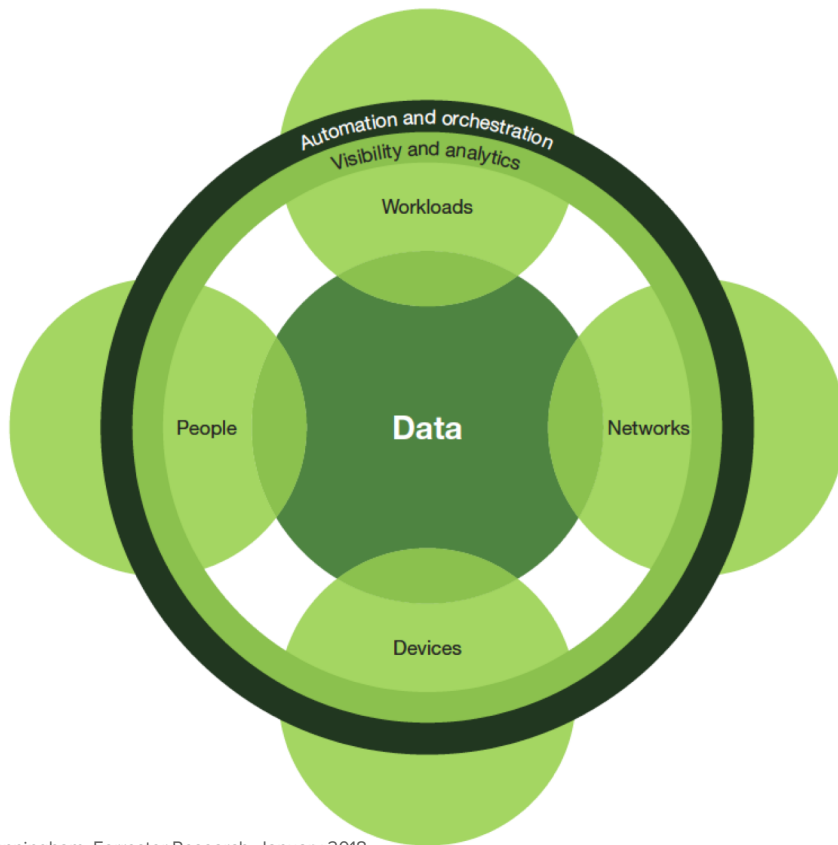


With Traditional Network Moat Disappearing,
People Are The New Perimeter





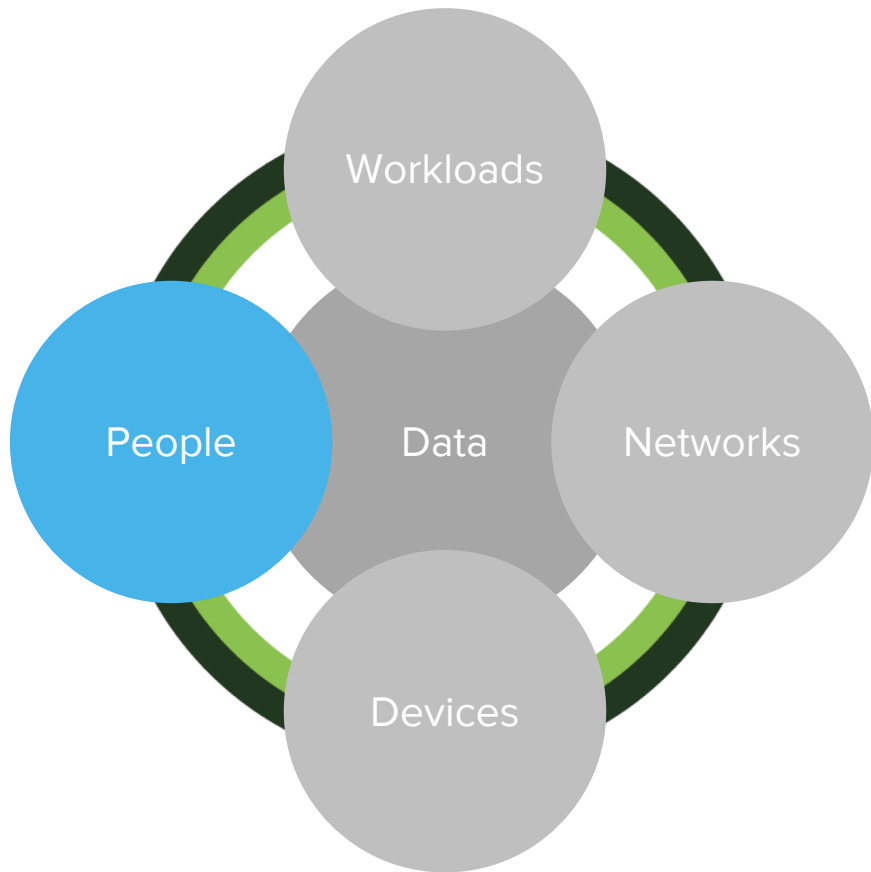
Making Identity The Foundation for Zero Trust



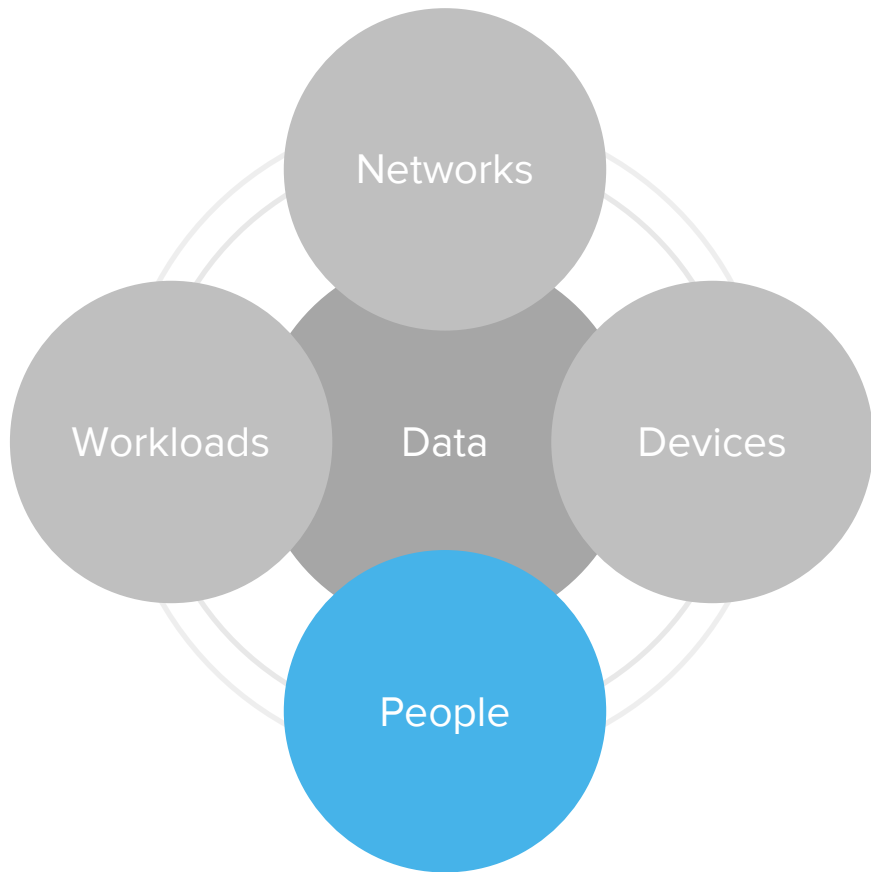
The Zero Trust eXtended (ZTX) Ecosystem, Dr. Chase Cunningham, Forrester Research, January 2018



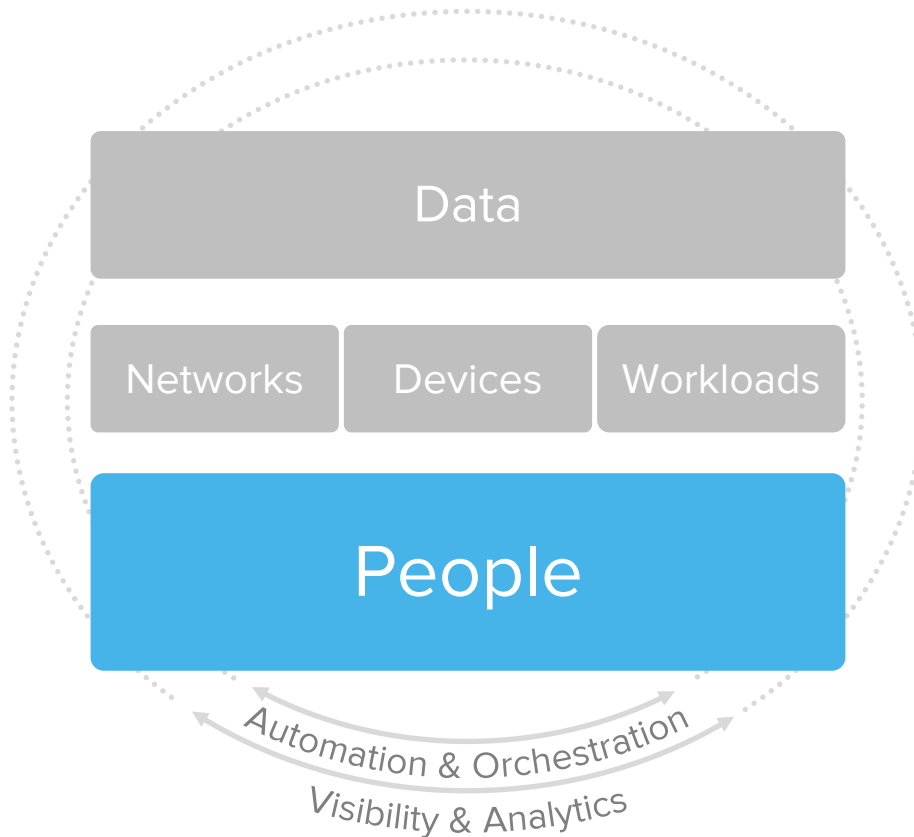
Making Identity The Foundation for Zero Trust



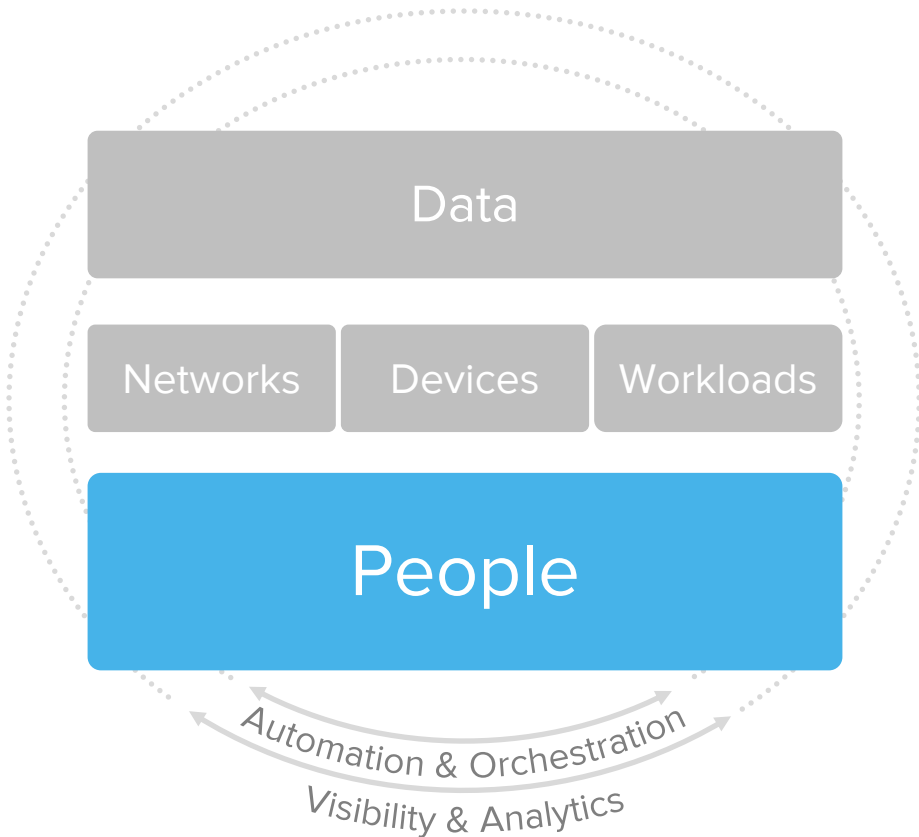
Making Identity The Foundation for Zero Trust



Making Identity The Foundation for Zero Trust



Making Identity The Foundation for Zero Trust

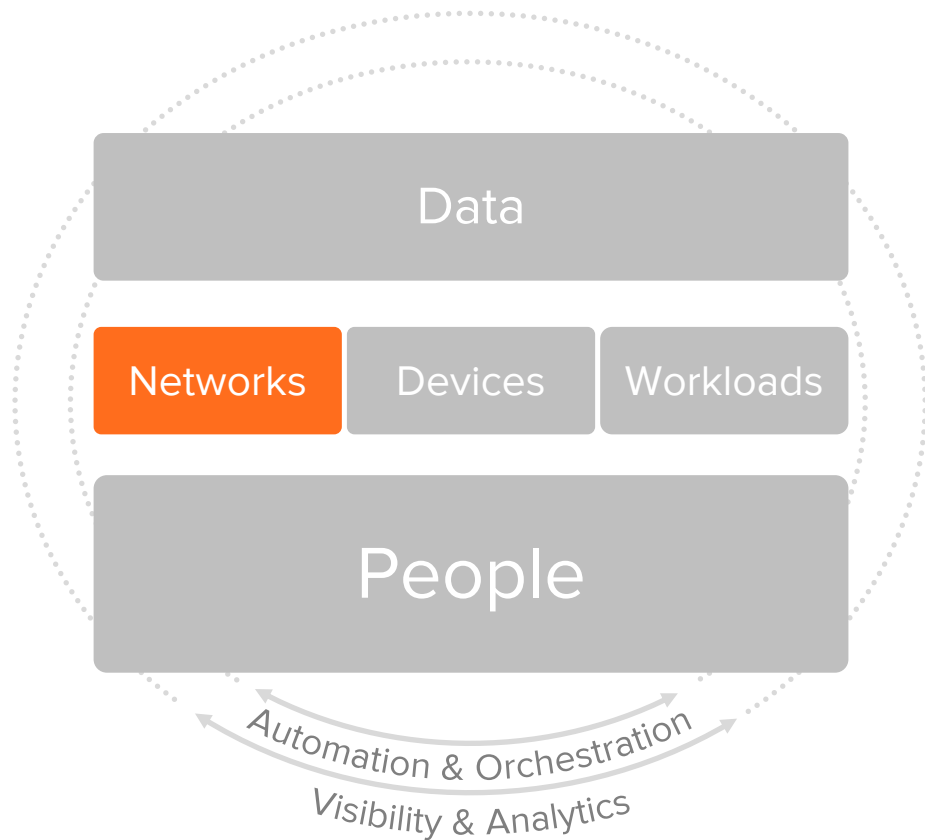


People / Identity solutions

- Single-Sign on
- Adaptive Multi-Factor Authentication
- Lifecycle Management
- API Access Management

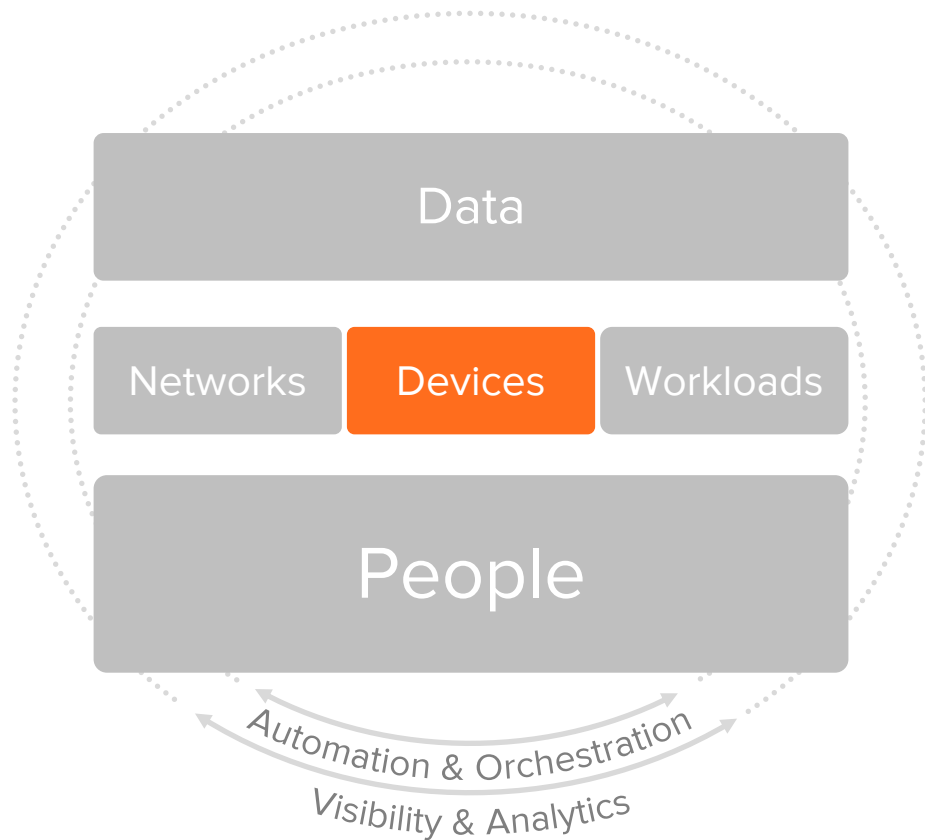


Identity Enables Other Components of the ZTX



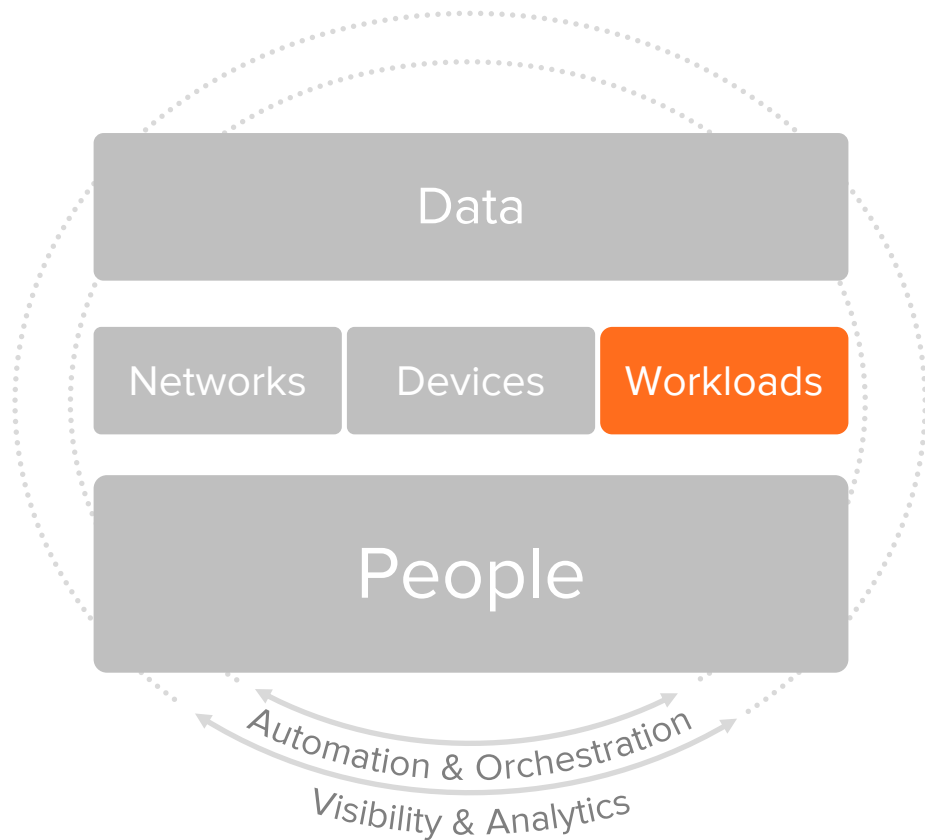
- Use known network zones inform policy
- Enrich network context (proxy anonymizers, Tor)
- Authenticate with IAM solution and seamlessly access on-prem applications
- Leverage existing perimeter and networking infrastructure with identity-driven MFA

Identity Enables Other Components of the ZTX



- Creates fingerprint of device to determine if new device
- Assess device state for access decisions: disk encryption, OS version, & firewall enabled
- Set authentication and access policies in IAM solution based on device state
- Ensure only compliant devices are able to access apps

Identity Enables Other Components of the ZTX



- Secure access to server workloads via SSH/RDP protocols
- Continuous authentication to server workloads using ephemeral credentials
- API Access Management allows admins to centrally manage scopes of OAuth tokens

Modern Identity As Zero Trust Foundation



Assume the network is
untrusted



IDENTITY
is the perimeter



Make decisions based on
user & device context



IDENTITY
drives security



Strong authentication to
services in real-time



IDENTITY
defines the experience





Thank You!