



KARL MCGUINNESS

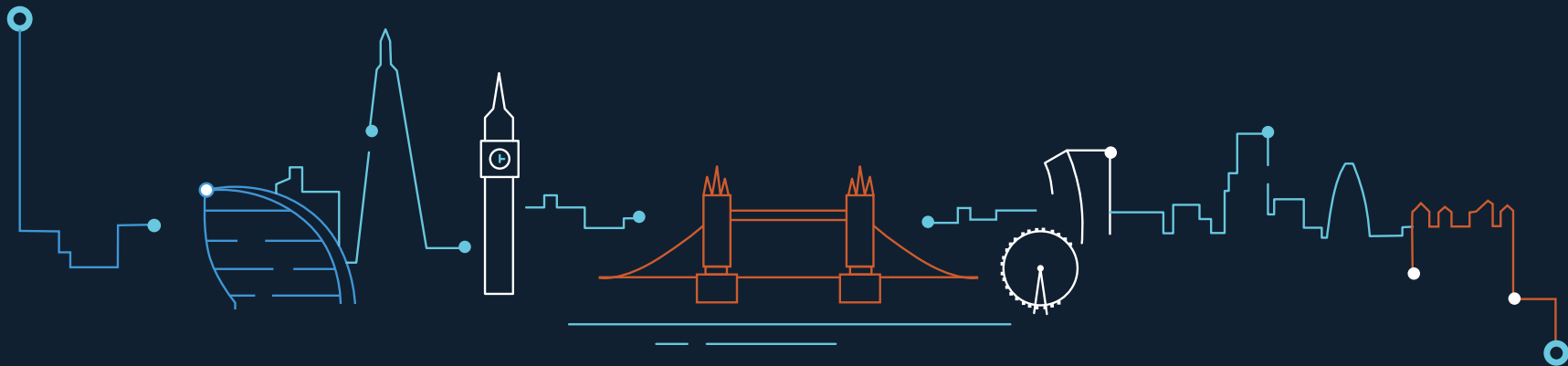
Senior Director, Identity, Okta





Future of Identity and Security

KARL MCGUINNESS, SENIOR DIRECTOR, IDENTITY



Disclaimer

This presentation contains “forward-looking statements” within the meaning of the “safe harbor” provisions of the Private Securities Litigation Reform Act of 1995, which may include, but are not limited to, statements regarding our financial outlook, product development and market positioning. These forward-looking statements are based on current expectations estimates forecasts and projections. Words such as “expect” “anticipate” “should” “believe” “hope” “target” “project” “goals” “estimate” “potential” “predict” “may” “will” “might” “could” “intend” “shall” and variations of these terms or the negative of these terms and similar expressions are intended to identify these forward-looking statements. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that beyond Okta’s Control.

The market for our products may develop more slowly than expected or than it has in the past; quarterly and annual operating results may fluctuate more than expected variations related to our revenue recognition may cause significant fluctuations in our results of operations and cash flows; assertions by third parties that we violate their intellectual property rights could substantially harm our business; a network or data or our security incident that allows unauthorized access to our network or data or our customers data could harm our reputation, create additional liability and adversely impact our financial results; the risk of interruptions or performance problems, including a service outage, associated with our technology; we face intense competition in our market, weakened global economic conditions may adversely affect our industry; the risk of losing key employees; changes in foreign exchange rates; general political or destabilizing events, including war, conflict or acts of terrorism; and other risk and uncertainties. Past performance is not necessarily indicative of future results.

Further information on potential factors that could affect our financial results is included in our Annual report on form 10-K for the year ended January 31, 2018 and other filings or reports filed with the securities and exchange commission that are posted at investor.okta.com

Any unreleased products, features or functionality referenced in this other presentations, press releases or public statements are not currently available and may not be deliver any product, feature or functionality. Customers who purchase our products should make their purchase decisions based upon features that are currently generally available.

The forward-looking statements contained in this presentation represent the company’s estimates and assumptions only as of the date of this presentation. Okta assumes no obligation and does not intend to update these forward-looking statements whether as a result of new information, future events or otherwise.

This presentation contains estimates and other statistical data that we obtained from industry publications and reports generated by third parties. These data involve a number of assumptions and limitations, and you are cautioned not to give undue weight to such estimates. Okta cannot guarantee their accuracy or completeness.

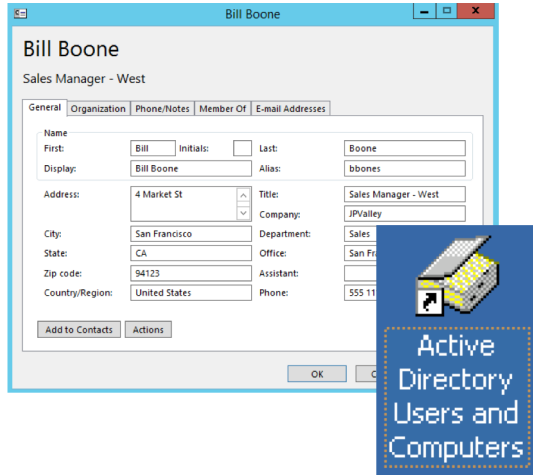
Expectations, estimates, forecasts and projections are subject to a high degree of uncertainty and risk. Many factors, including those that are beyond Okta’s control, could cause results or outcomes to differ materially from those expressed in the estimates made by the independent parties and by Okta.



BACK
TO THE FUTURE™



AD = Center of Gravity for Identity



The screenshot shows a contact record for Bill Boone in a Windows XP application. The window title is "Bill Boone". The record is categorized as "Sales Manager - West". The "General" tab is selected, showing fields for Name (First: Bill, Last: Boone), Display (Bill Boone), Alias (bboone), Address (4 Market St), City (San Francisco), State (CA), Zip code (94123), and Country/Region (United States). There are also fields for Title (Sales Manager - West), Company (JPValley), Department (Sales), Office (San Fr), Assistant, and Phone (555 11). Buttons for "Add to Contacts" and "Actions" are at the bottom left, and "OK" and "Cancel" are at the bottom right. A blue box with a yellow icon and the text "Active Directory Users and Computers" is overlaid on the bottom right of the contact record.

Bill Boone
Sales Manager - West

General Organization Phone/Notes Member Of E-mail Addresses

Name
First: Bill Initials: Last: Boone
Display: Bill Boone Alias: bboone

Address: 4 Market St Title: Sales Manager - West
City: San Francisco Company: JPValley
State: CA Department: Sales
Zip code: 94123 Office: San Fr
Country/Region: United States Assistant: Phone: 555 11

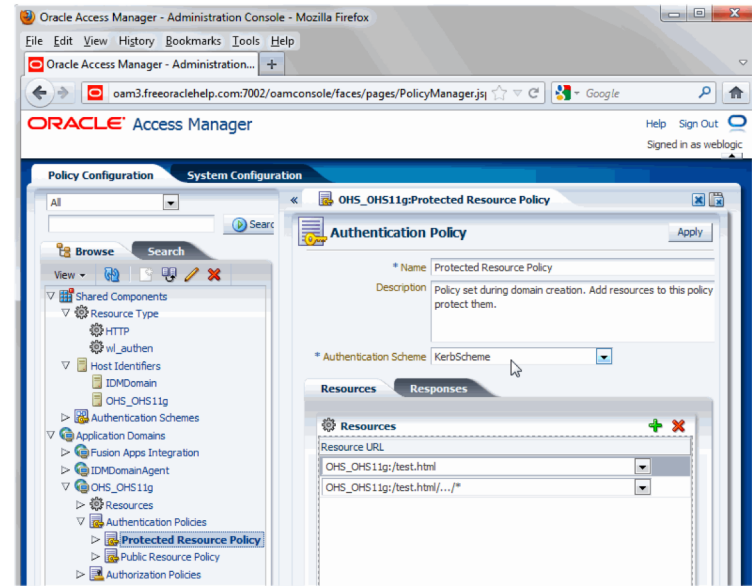
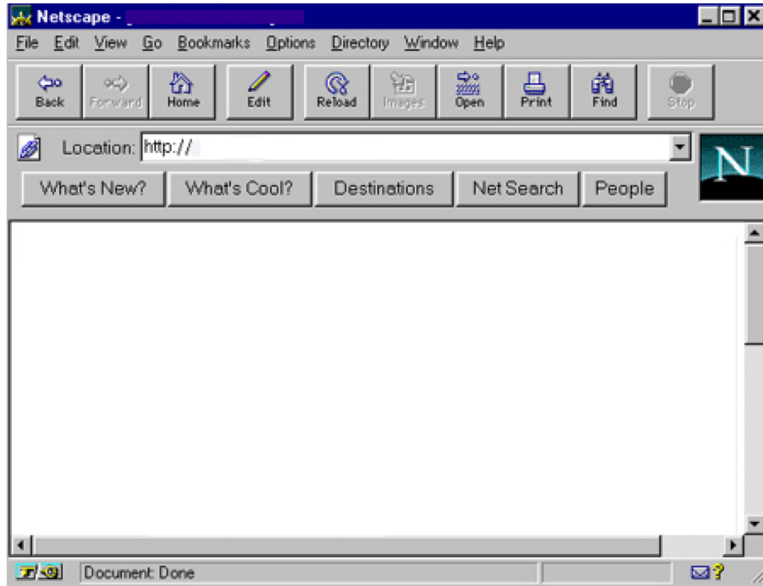
Add to Contacts Actions

OK Cancel

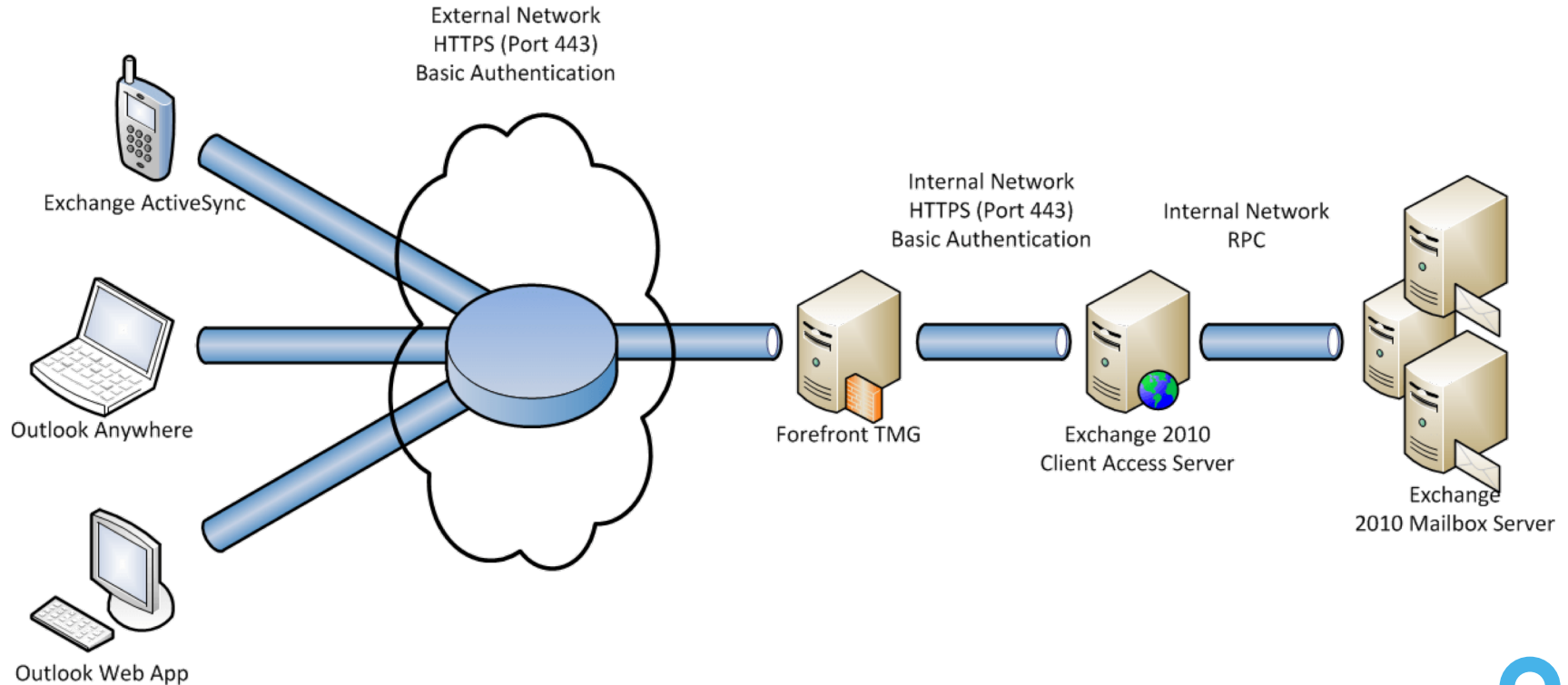
Active Directory Users and Computers



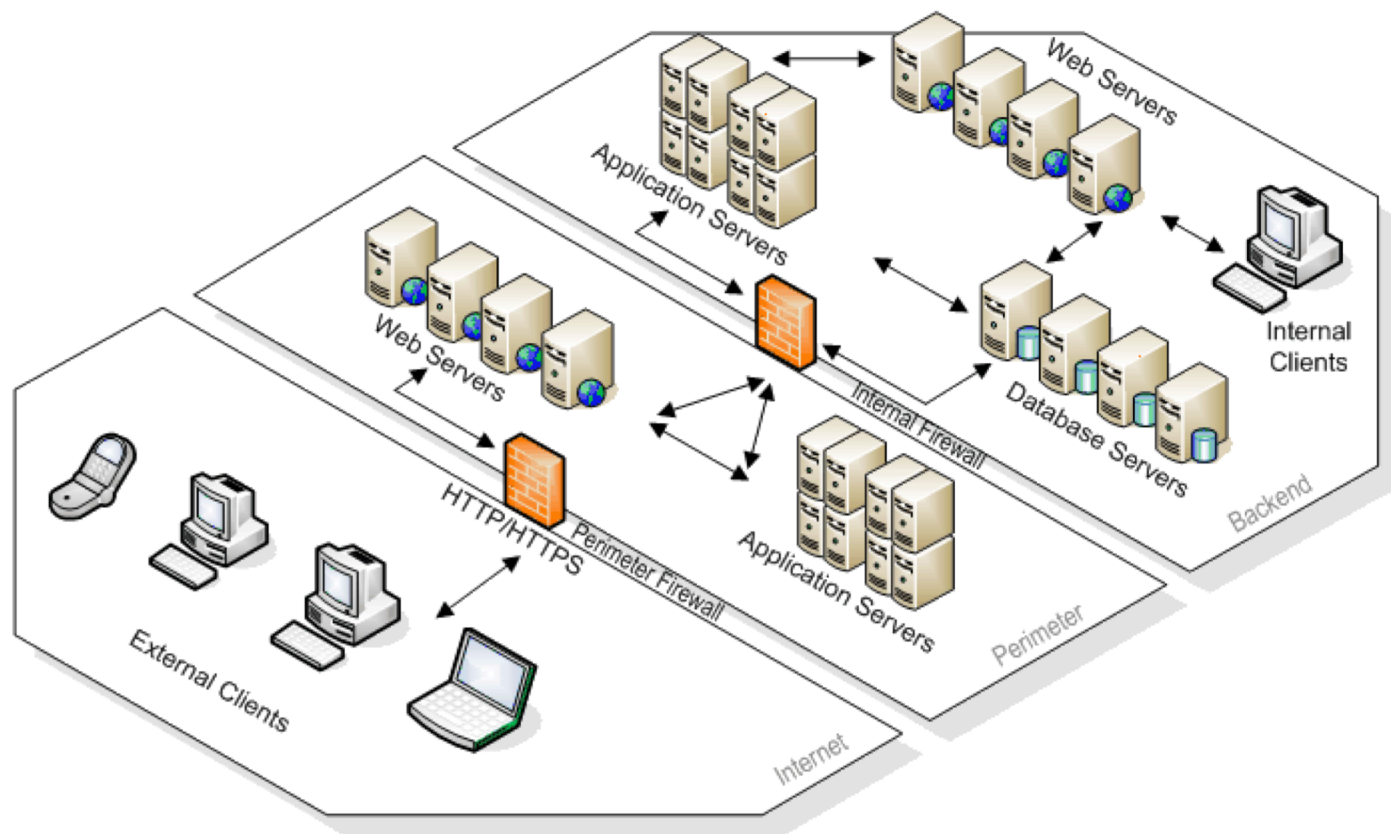
Web Applications = WAM



Device Management = EAS



The DMZ was the Perimeter



The World is Changing

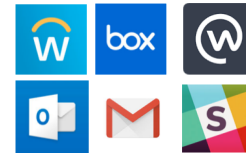
THE WORLD BEFORE



Software is One Industry

CIOs are Technology Operators

THE WORLD TODAY



Contractors



Employees



Customers



Partners



Software is Eating the World

CIOs are Business Enablers

Enterprise Datacenter to Services



IaaS

PaaS

SaaS



New Use Cases & Client Types



Multiple Identity Providers



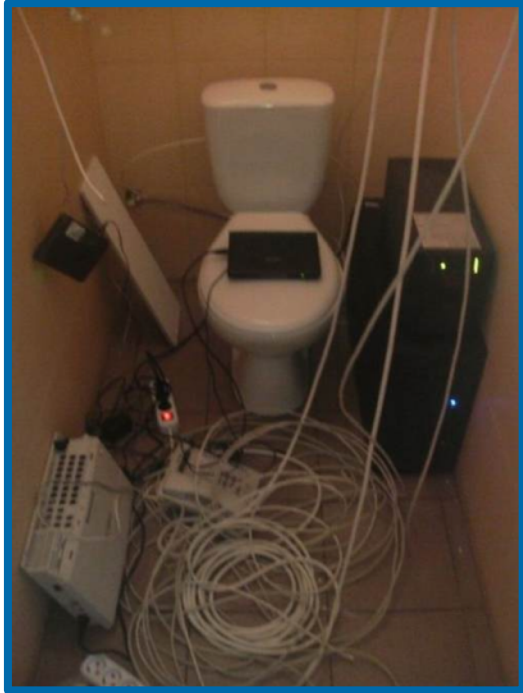
Mobile is the center of gravity for identity



Consumerization of IT (CoIT)



Shadow IT



10x
More
SaaS
Apps



CorpNet: The crown jewels for insider attacks



got root?



Identity is the New Perimeter

3:21 pm ET
May 11, 2015

SECURITY

Google Moves Its Corporate Applications to the Internet

ARTICLE

COMMENTS (20)

AUTHENTICATION

BEYONDCORP

CORPORATE NETWORK

CYBERSECURITY

GOOGLE

Email

Print

Facebook 820

Twitter 1.3k

Google+

LinkedIn

By RACHAEL KING

Google Inc. GOOGL -1.42%, taking a new approach to enterprise security, is moving its corporate applications to the Internet. In doing so, the Internet giant is flipping common corporate security practice on its head, shifting away from the idea of a trusted internal corporate network secured by perimeter devices such as firewalls, in favor of a model where corporate data can be accessed from anywhere with the right device and user credentials.

The new model — called the BeyondCorp initiative — **assumes that the internal network is as dangerous as the Internet**. Access depends on the employee's device and user credentials. Using authentication, authorization and encryption, the model grants employees fine-grained access to different enterprise resources, wrote Google's Rory Ward and Betsy Beyer **in a paper published in December**.

“assumes that the internal network is as dangerous as the Internet”

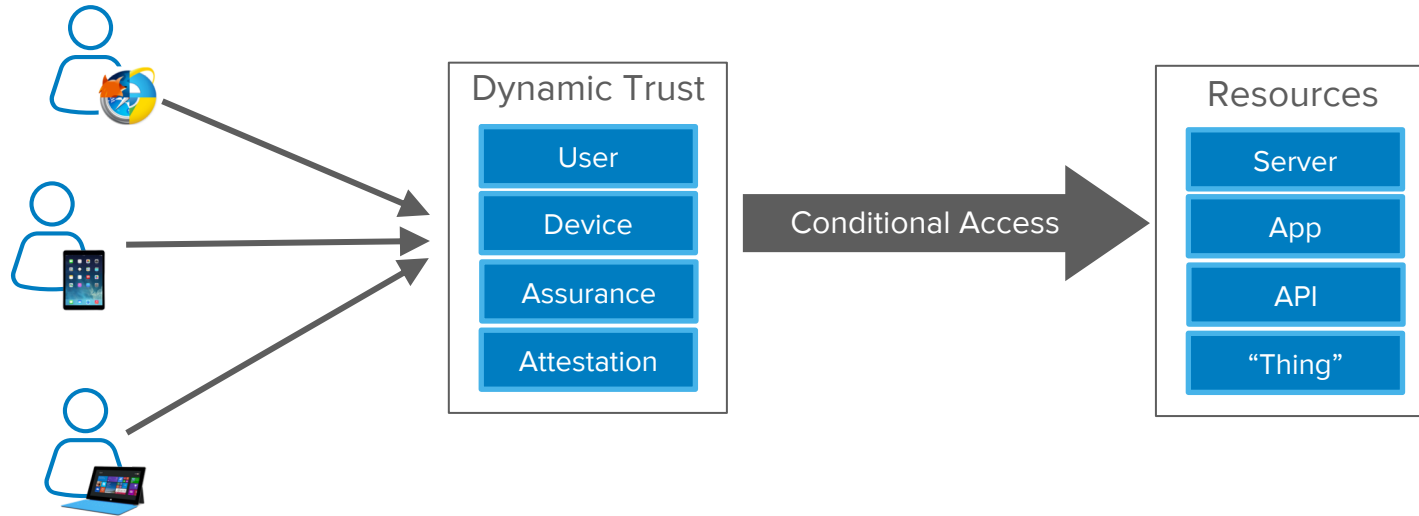


Access is a Layer 7 problem

“connect first, authorize second”



“authorize first, connect second”



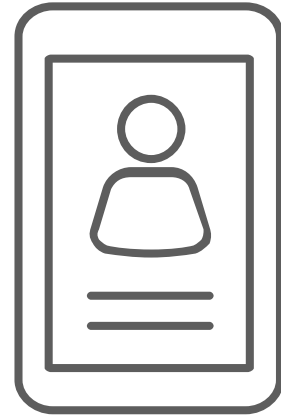
The future of identity + security

Attribute Attestation & Governance

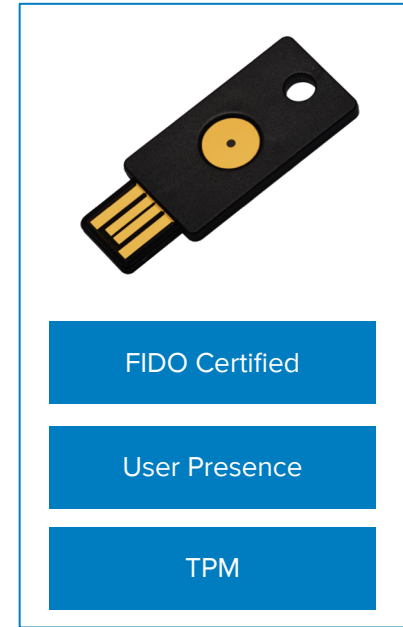
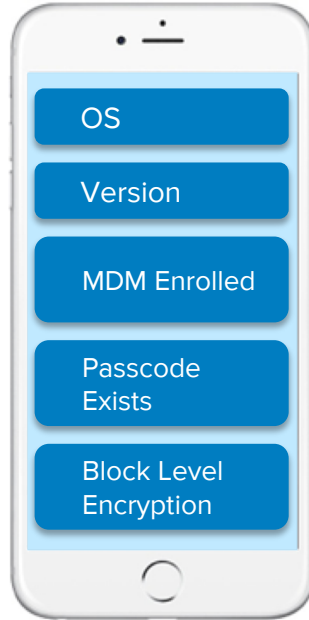
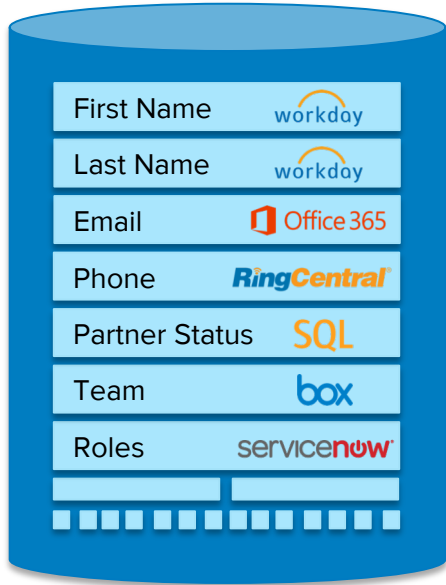
Continuous Authentication

Shared Signals

Risk-based Dynamic Access Control



Attribute Authorities



Attribute Attestation

Centralize

Centralized

Attribute Facts	
Pricing	Transactional
Confidence Level	1 - High
Data Type	1 - Authoritative
Availability	1 - Real-Time
Date Last Refreshed	10/23/2012
Refresh Rate	7 - Variable
Geographic Coverage	2 - National
Coverage Amount	2 - Partial
Verification Method	2 - Verified by 3 rd Party
OpenIdentityExchange.org	



duplicity



sensitivity



veracity



liability



real-time



Governance of data and privacy

Different users often have different claims to data

IoT Data	Actor	Claim Holders	Data Claims
• GPS location • Speed • Mileage • Acceleration • Battery • Radar • Temperature	 Driver	Do not track my location	Discard
		Track Battery Usage	Encrypt
	 Owner	Publish Battery for Statistics	Anonymize





GDPR

EU General Data
Protected Regulation



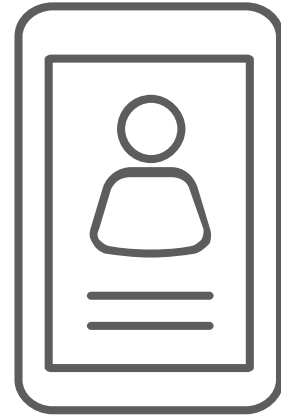
The future of identity + security

Attribute Attestation & Governance

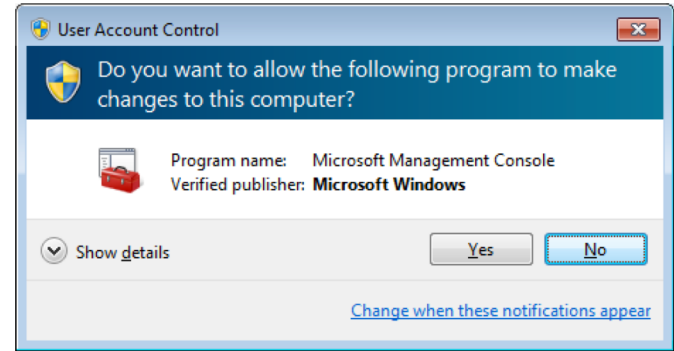
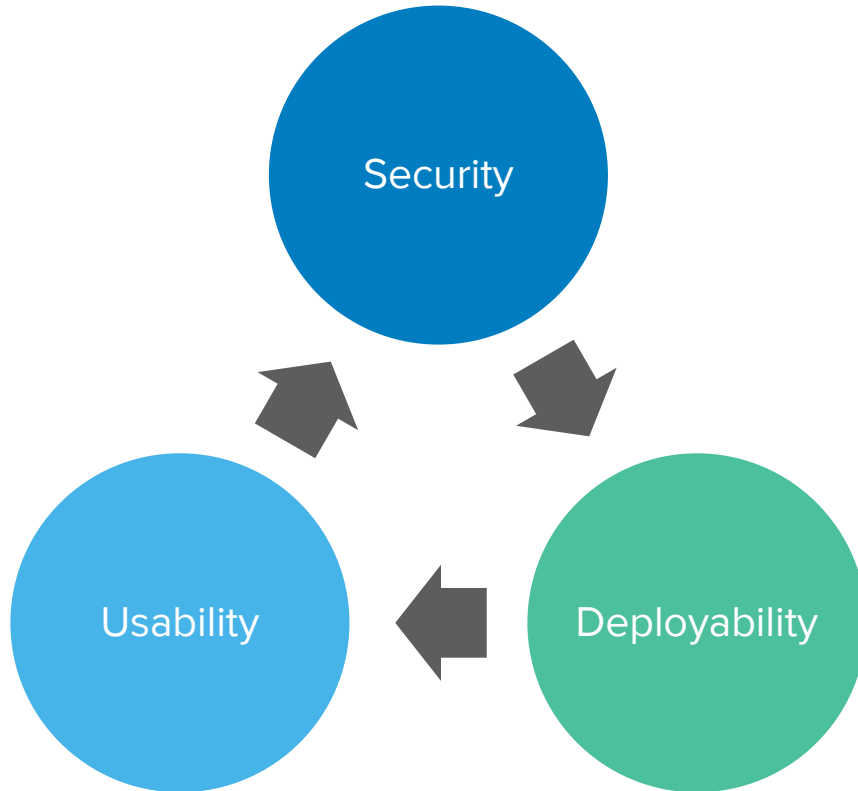
Continuous Authentication

Shared Signals

Risk-based Dynamic Access Control



The Security Challenge



Many Attempts at Strong Authentication



Killing the Password is Hard

Category	Scheme	Described in section	Reference	Usability					Deployability					Security					
				Memorywise-Effortless Scalable-for-Users Nothing-to-Carry	Physically-Effortless Easy-to-Learn Efficient-to-Use	Infrequent-Errors Easy-Recovery-from-Loss	Accessible Negligible-Cost-per-User Server-Compatible Browser-Compatible	Mature Non-Proprietary	Resilient-to-Physical-Observation Resilient-to-Targeted-Impersonation Resilient-to-Throttled-Guessing Resilient-to-Unthrottled-Guessing Resilient-to-Internal-Observation Resilient-to-Leaks-from-Other-Verifiers Resilient-to-Phishing	Resilient-to-Theft No-Trusted-Third-Party Requiring-Explicit-Consent Unlinkable									
(Incumbent)	Web passwords	III	[13]	●	●	●	●	●	●	●	●	●	○				●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			●	●	○	●	■	■	■	●	●	●	●	●	■	●
	Yubikey		[53]			●	●	○	●	■	■	■	●	○	●	●	●	■	●
	Ironkey		[54]	●		○	●	○	■	■	■	■	○	○	●	●	●	■	●
	CAP reader		[55]	●		●	●	○	■	■	■	■	●	●	●	●	●	■	●
	Pico		[8]	●	●	●	■	○	■	■	■	■	●	●	●	●	○	■	●
Phone-based	Phoolproof	IV-H	[36]		○	●	○	○	○	■	■	■	●	●	●	●	●	■	●
	Cronto		[56]		○	●	○	○	○	■	■	■	●	○	●	●	●	■	●
	MP-Auth		[6]		○	●	○	○	○	■	■	■	○	○	●	●	●	■	●
	OTP over SMS			●	●	●	■	○	○	■	■	■	●	●	○	●	○	■	●
	Google 2-Step		[57]		○	●	○	○	○	■	■	■	○	○	●	●	●	■	●
Biometric	Fingerprint	IV-I	[38]	●	●	○	○	○	○	■	■	■	○	●	●		■	■	■
	Iris		[39]	●	●	○	○	○	○	■	■	■	●	●			■	■	■
	Voice		[40]	●	●	○	○	○	○	■	■	■	○	○	●		■	■	■

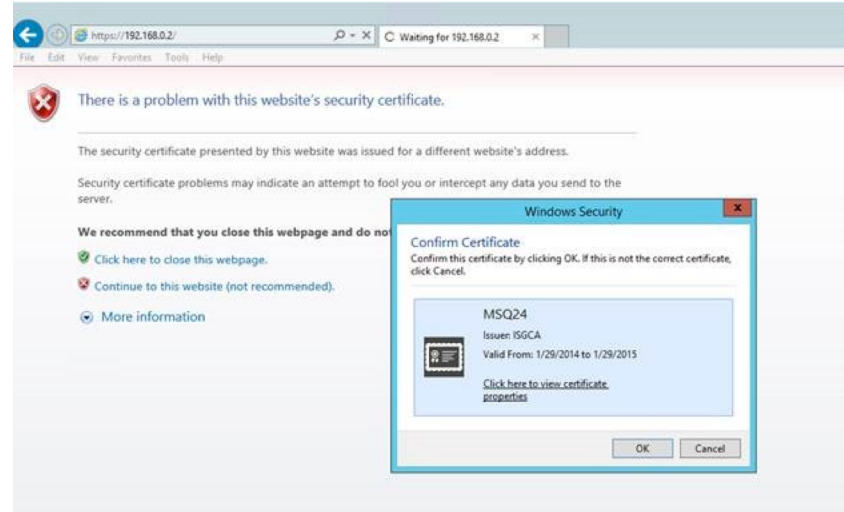
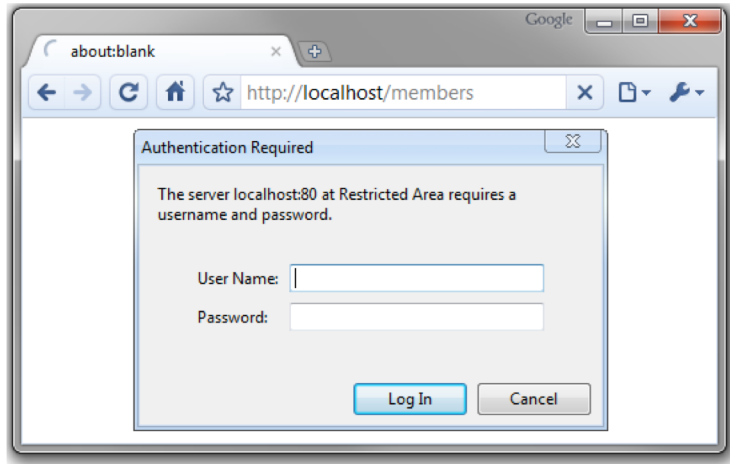
● = offers the benefit; ○ = almost offers the benefit; no circle = does not offer the benefit.

■ = better than passwords; ■ = worse than passwords; no background pattern = no change.

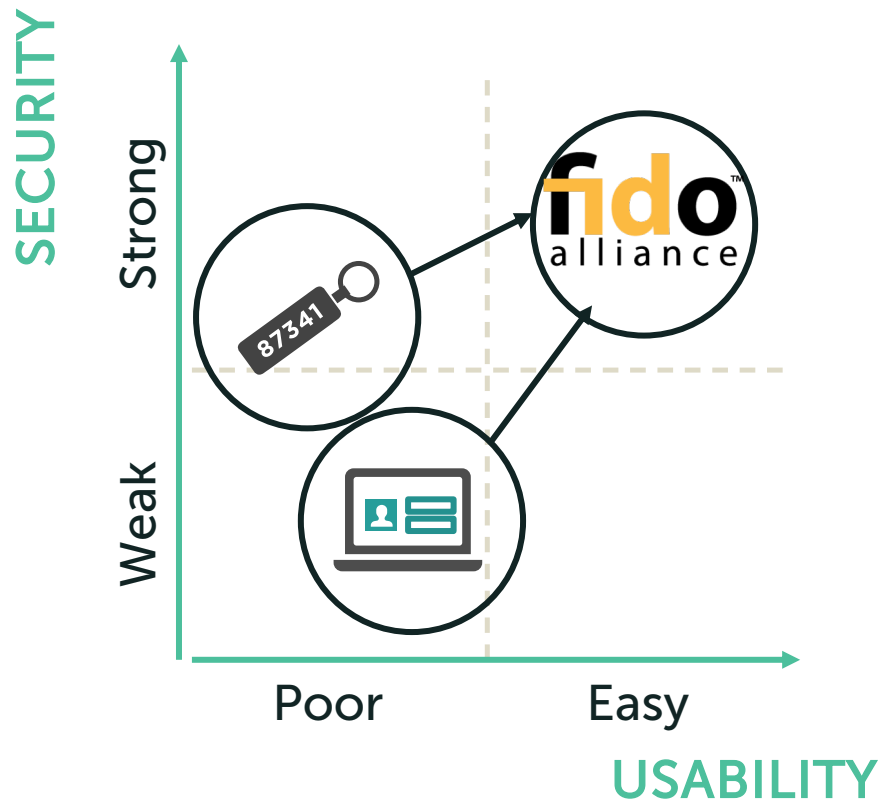
- More Accessible & Efficient to Use
- Easier to Recover
- Negligible Cost per-User
- Server/Browser Compatible



Browser-based authentication was stuck in the 90's



FIDO & Web Authentication



Leading browser vendors are implementing new W3C standards for FIDO Authentication, opening a new era of ubiquitous, hardware-backed protection for everyone using the internet

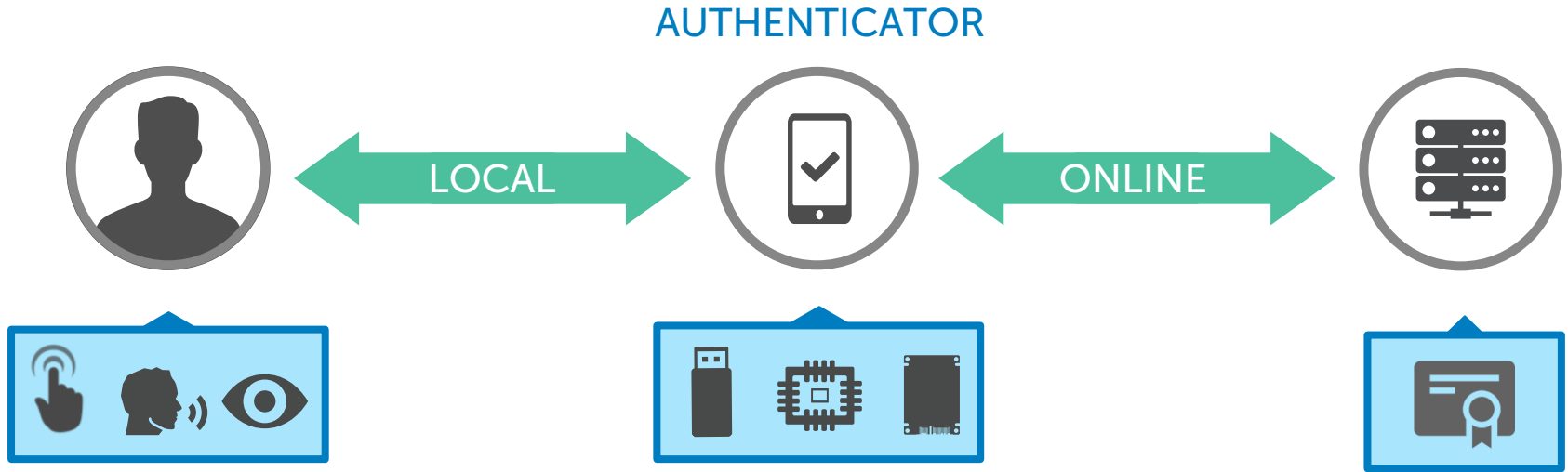


300+ FIDO CERTIFIED SOLUTIONS

1.5 AVAILABLE TO BILLION PEOPLE



Modern Passwordless Authentication



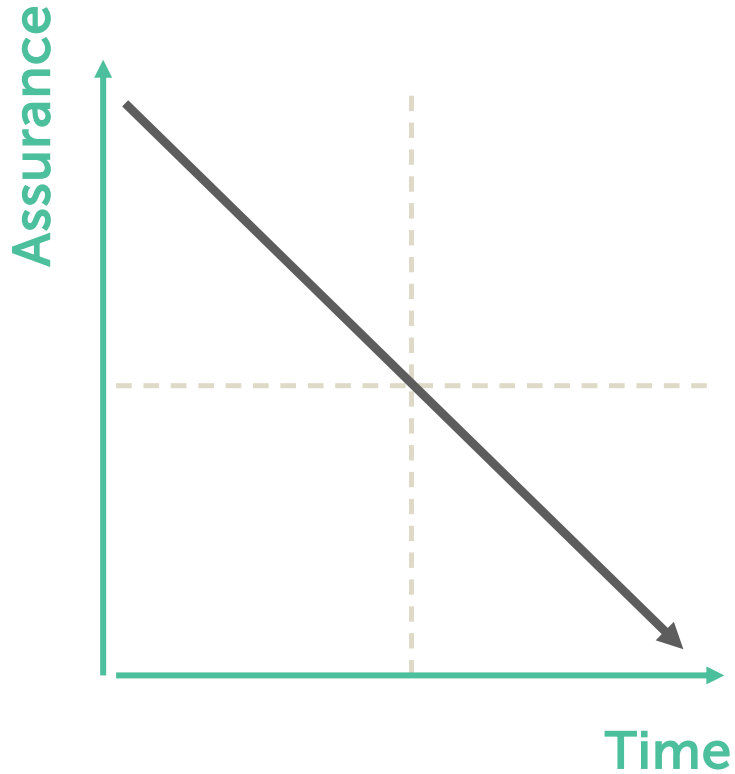
Assurance



How sure am I that you are
who you say you are?



Assurance decreases over time



Modular Assurance

	1	2	3	4
same unique user	yes			
user was proofed	no	remote or in person	remote or in person	in person
verified name provided	no	no / yes	yes	yes
authn strength	weak	a bit stronger	stronger still	really strong



Contractors



Employees



Customers



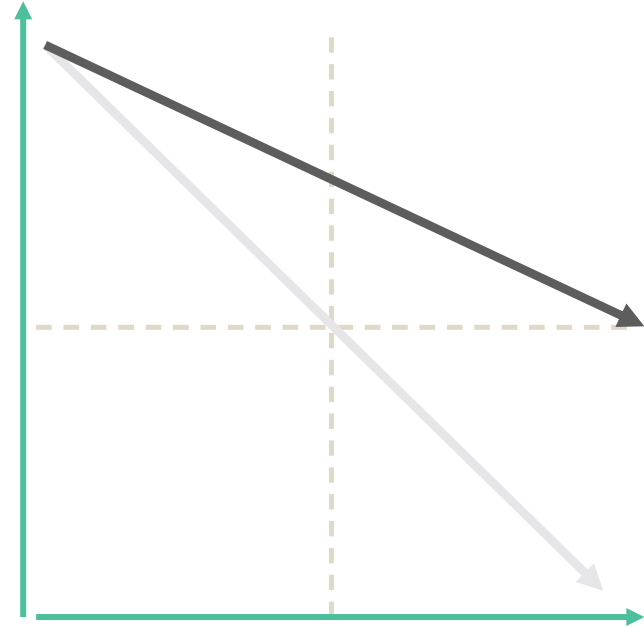
Partners



Continuous Authentication



Assurance



Time

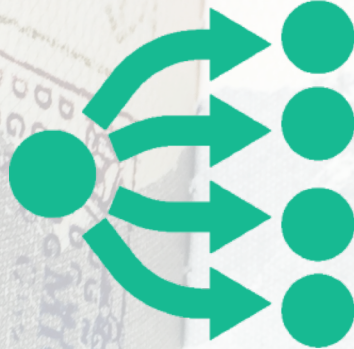


Long-term sessions with continuous authentication



Token Binding

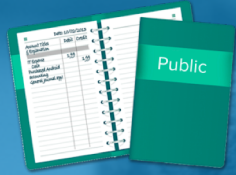




Session Revocation & Logout



Blockchain & Distributed Ledgers



John Hancock



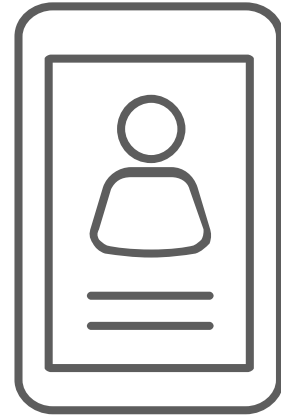
The future of identity + security

Attribute Attestation & Governance

Continuous Authentication

Shared Signals

Risk-based Dynamic Access Control



The challenge of account recovery

MAT HONAN GEAR 08.06.12 8:01 PM

HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING



ADVERTISING/SPEAKING ABOUT THE AUTHOR

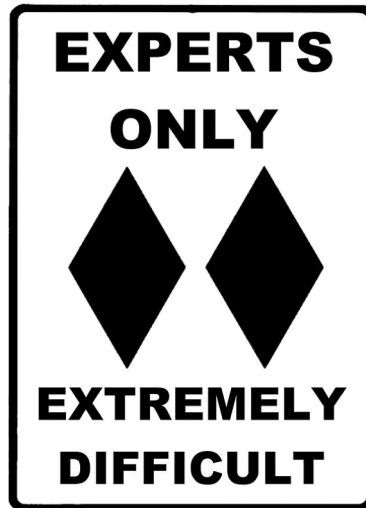
18 T-Mobile Employee Made Unauthorized 'SIM Swap' to Steal Instagram Account

MAY 10

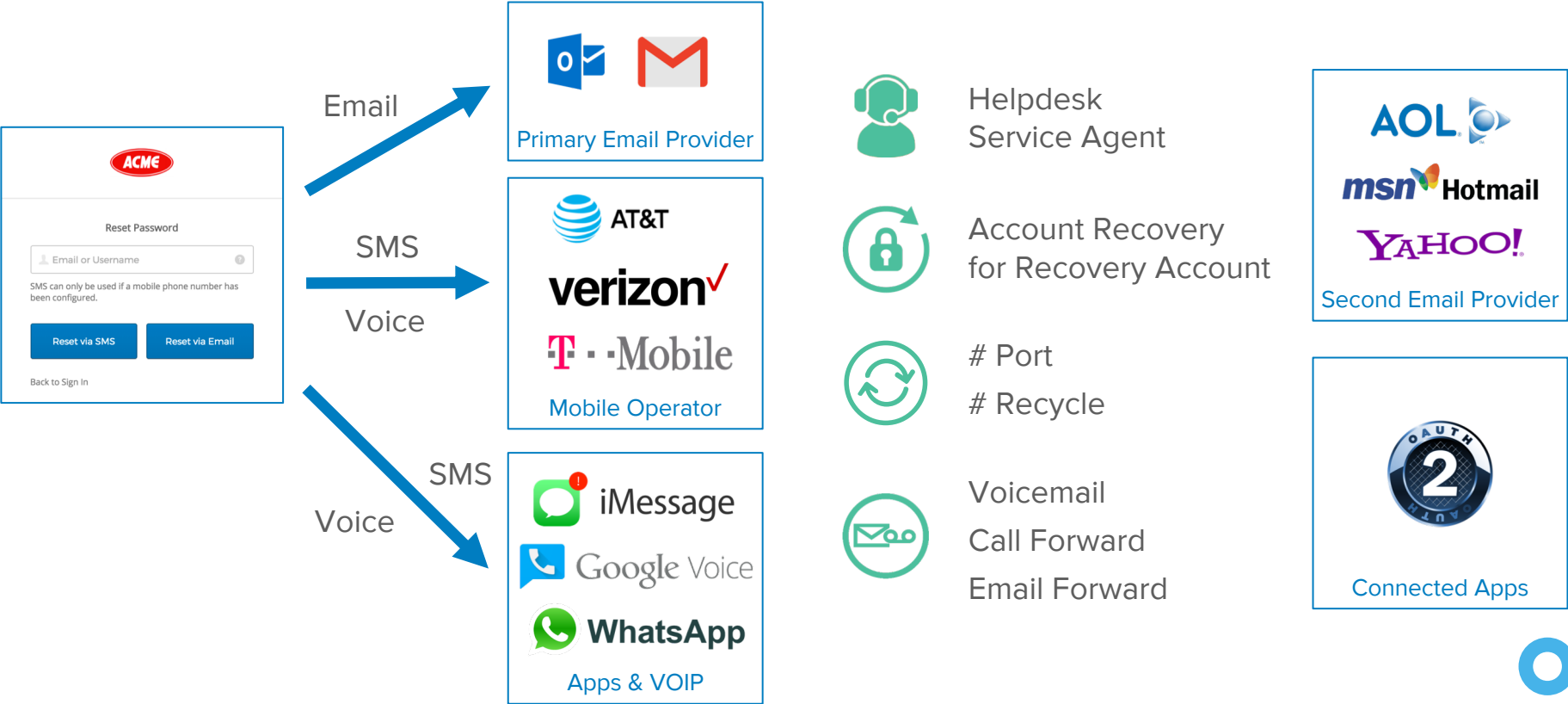
Mark Zuckerberg's Twitter and Pinterest accounts hacked, LinkedIn password dump likely to blame

EMIL PROTALINSKI JUNE 5, 2016 1:15 PM

TAGS: FACEBOOK, LINKEDIN, MARK ZUCKERBERG, PINTEREST, TOP-STORIES, TWITTER



Chain of account recovery



Shared Signals



IdPs often know security risks before the Service Provider

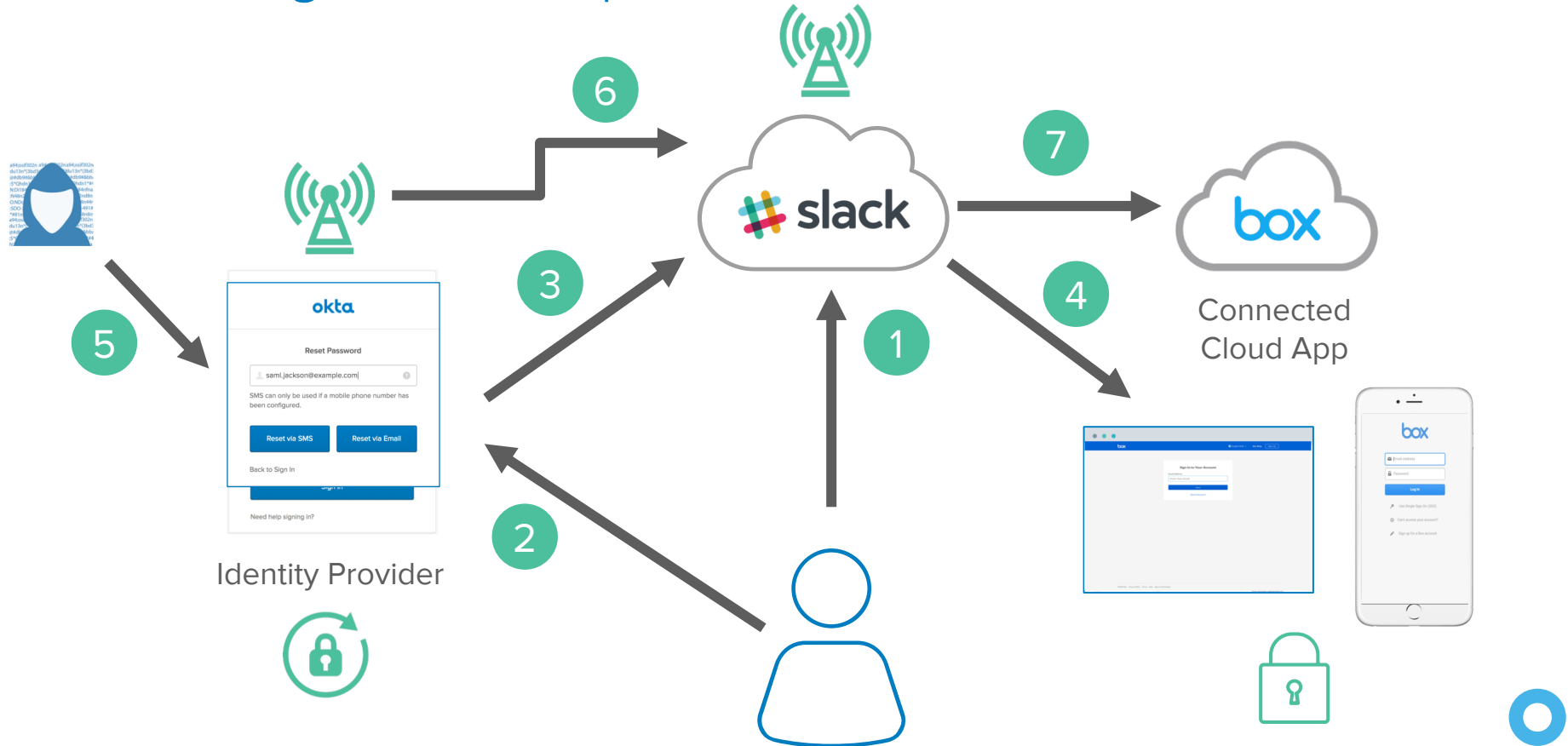
- ✓ Credential theft
- ✓ Unauthorized machine access
- ✓ Account recovery
- ✓ Account is abusive

IdPs can share visibility to key events

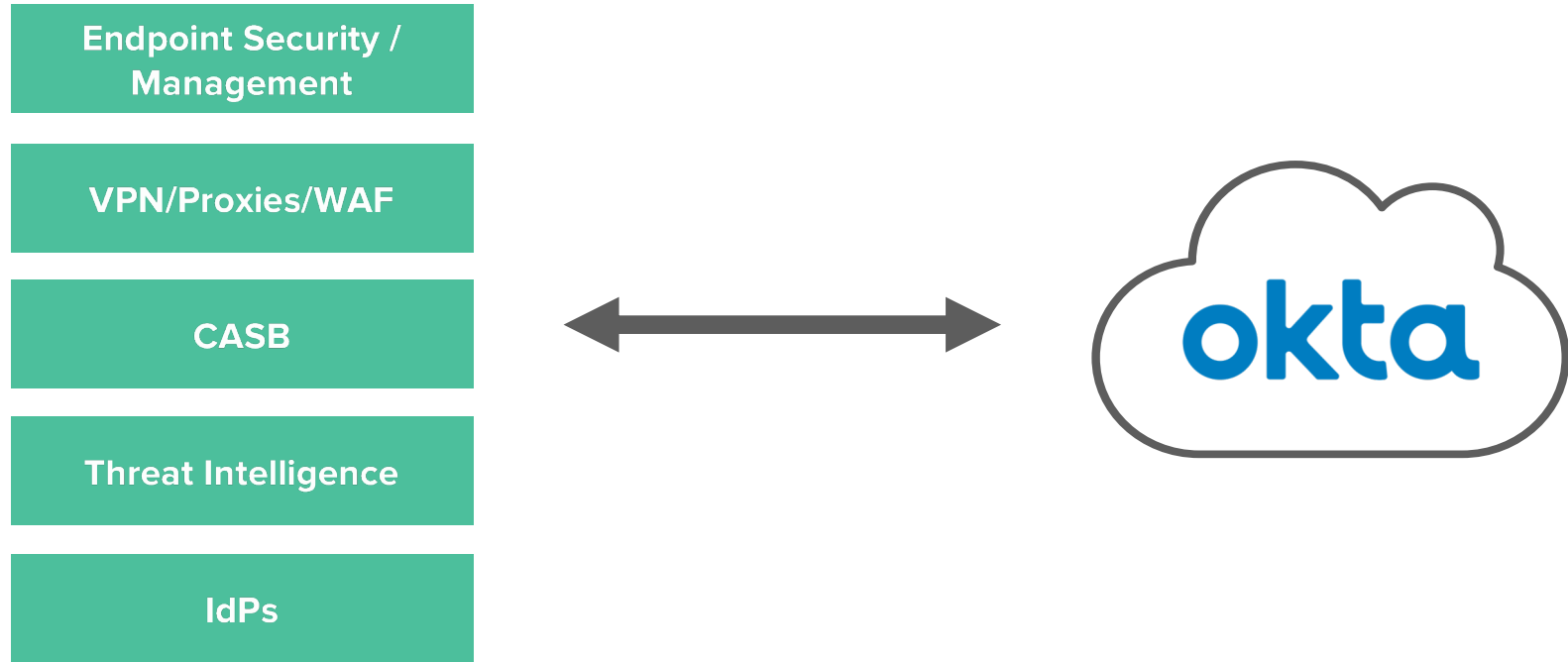
- ✓ Password reset
- ✓ Account recycling
- ✓ Account suspension
- ✓ Token revocation
- ✓ New payment method
- ✓ New shipping address



Shared Signals Example



Takes an ecosystem...



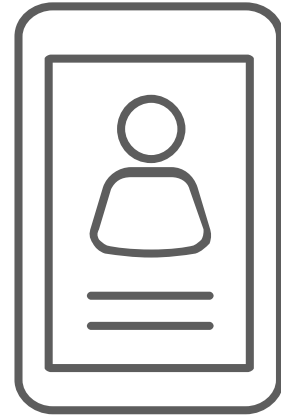
The future of identity + security

Attribute Attestation & Governance

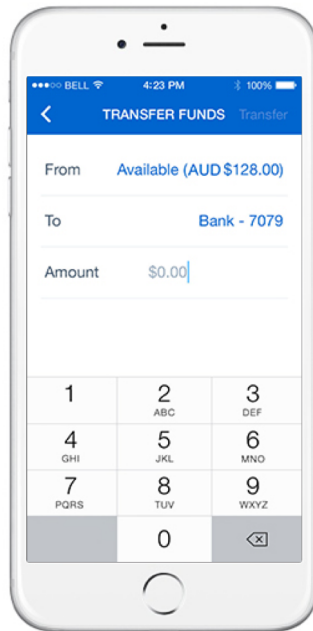
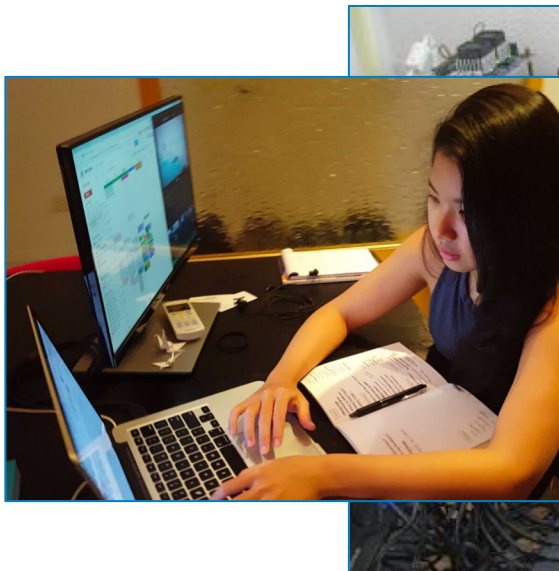
Continuous Authentication

Shared Signals

Risk-based Dynamic Access Control



Risk Profiles



Real-time Identity Intelligence



Humans are not able to prevent, detect and respond in this new world to **internet scale problems**



Espionage



Crime



Hacktivism



Warfare

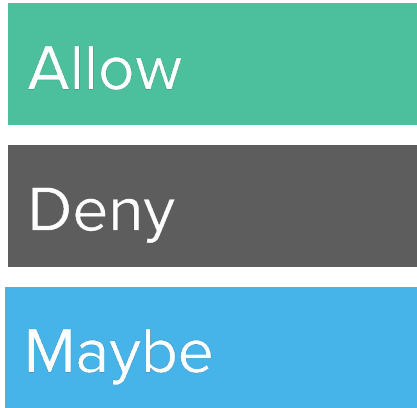


Terrorism



Mischief

Risk-based dynamic access control



CONTEXT MATTERS



**Device
Assurance
Level**



**Identity
Assurance
Level**

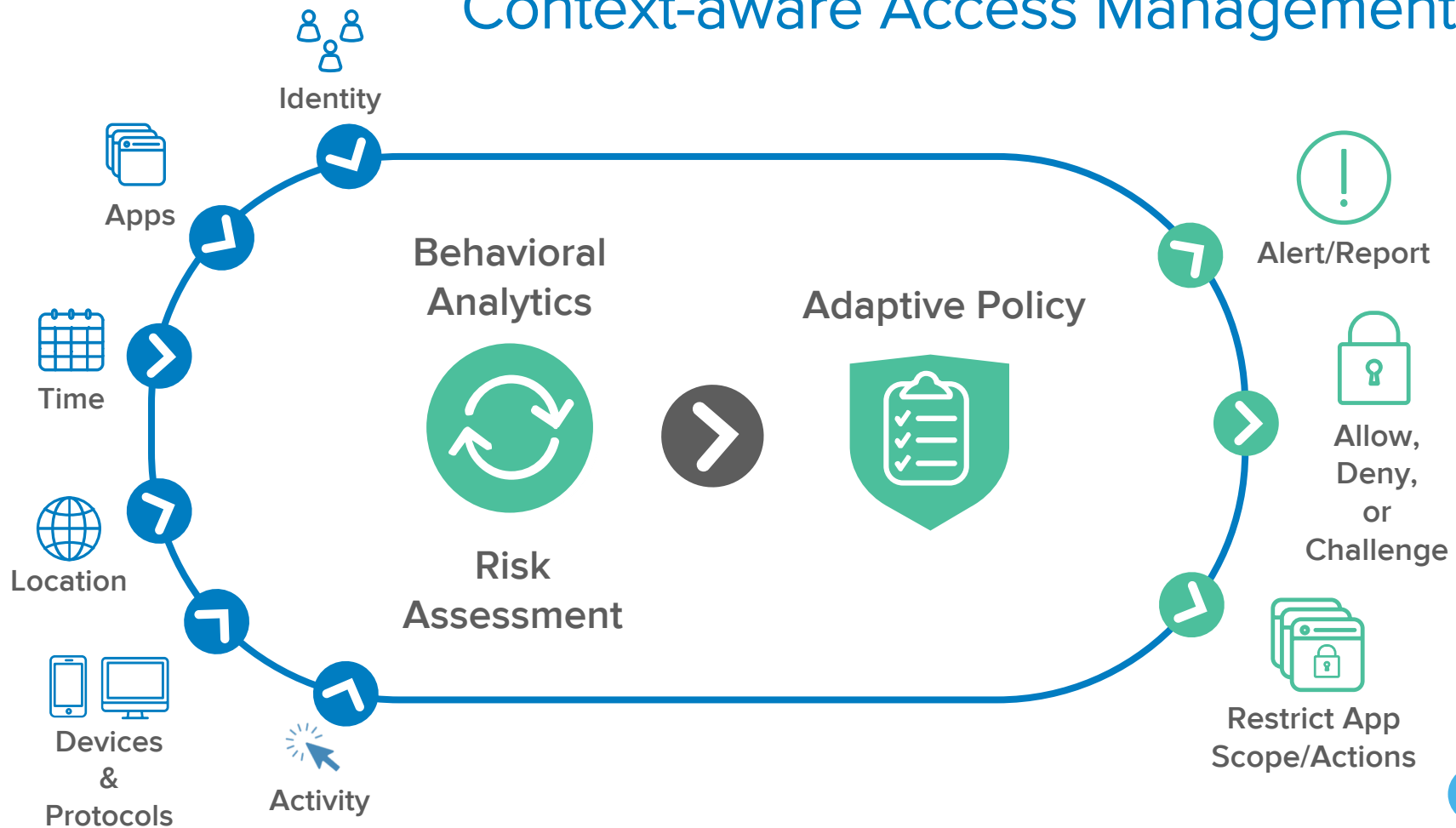


**Authenticator
Assurance
Level**



**Federation
Assurance
Level**

Context-aware Access Management





“

“We have to stop trying to authenticate the person;
instead, we need to authenticate the transaction”

— Bruce Schneier @schneierblog

Right **people** to right **things** for the **shortest time** possible

Risk-based dynamic access control

Sharing settings

Link to share (only accessible by collaborators)

`https://www.okta.com/onenote/d/1kMdQm6aCI7gbSMxWPKDgeoHZvo1odkPIK5bL9A-KoAM/edit?usp=sharing`

Who has access

Private - Only you can access [Change...](#)

	Karl McGuinness (you) kmcguinness@okta.com	Is owner
---	---	----------

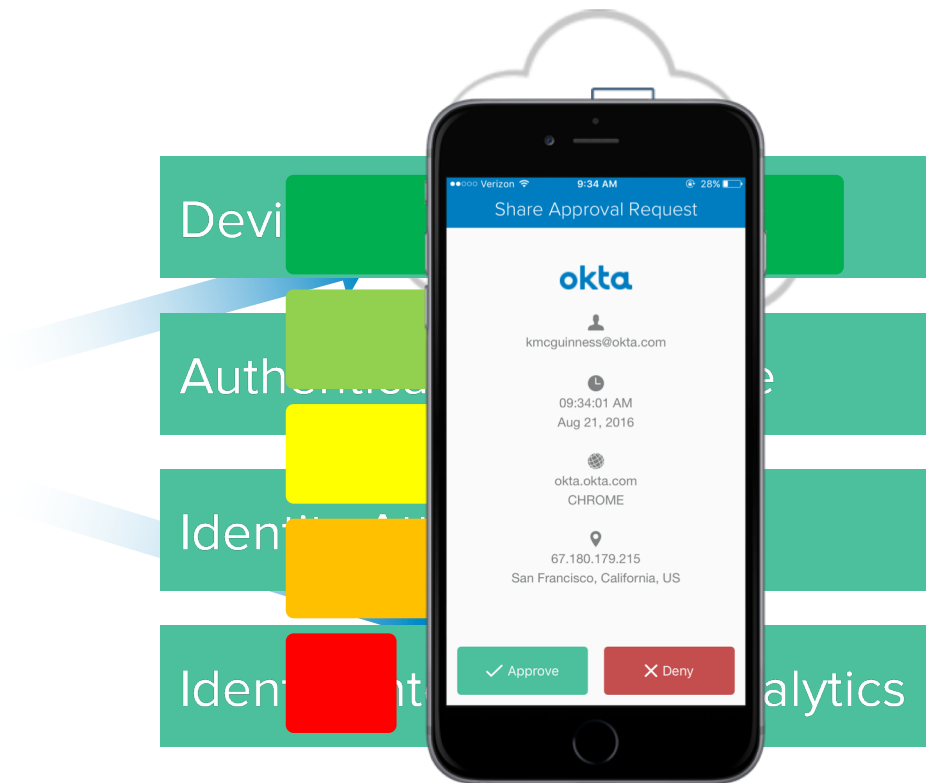
Invite people:

[Can edit](#)

Owner settings [Learn more](#)

- ☐ Prevent editors from changing access and adding new people
- ☐ Disable options to download, print, and copy for commenters and viewers

[Done](#)



The future of identity + security

Single identity system for all your people, devices, services, & things

Attributes with authority, context, and attestation

Continuous authentication that is user-centric

Shared signals across ecosystem & app boundaries

Access control that is dynamic and based on risk





Thank You

