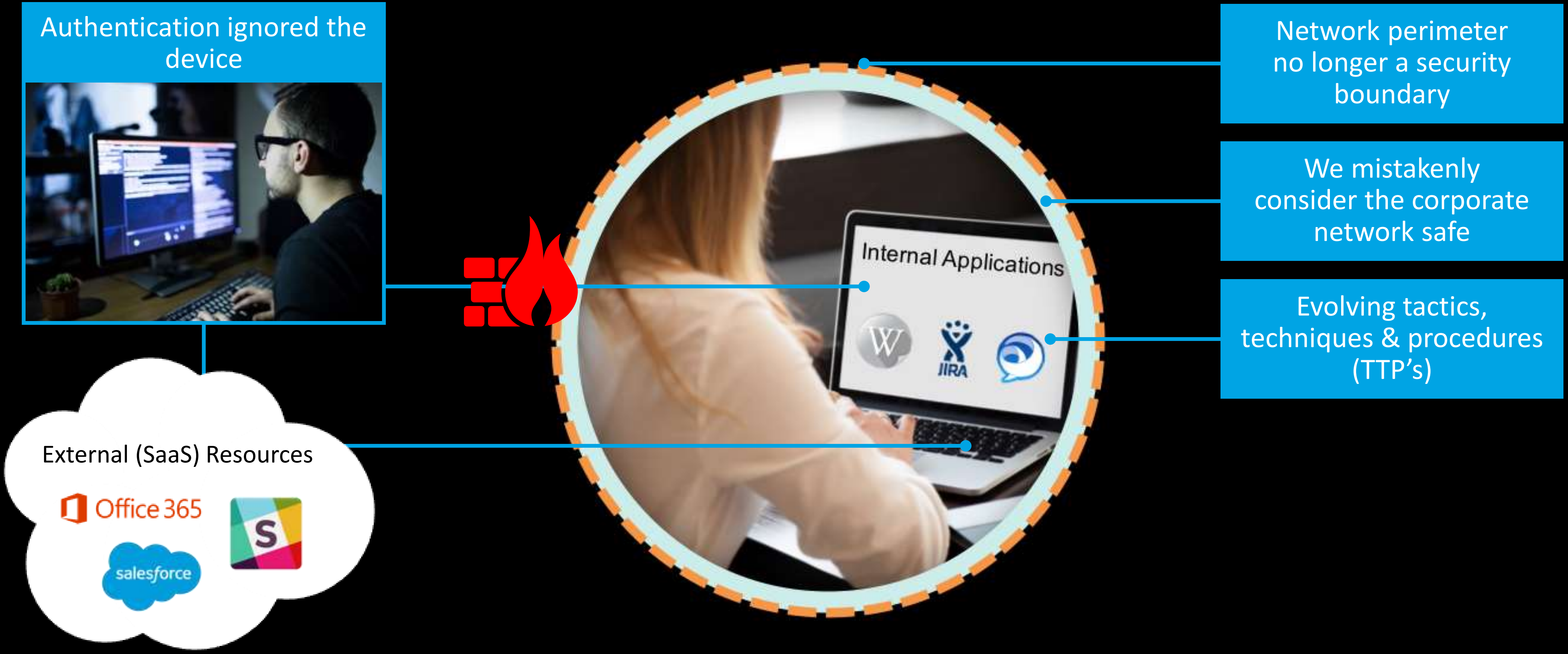
Project ZEN

Eric Anderson | Enterprise Security @ Adobe

#AdobeRemix
Vasjen Katro / Baugasm

Zero-Trust: Why Do We Need It?



Authentication ignored the device

External (SaaS) Resources

Network perimeter no longer a security boundary

We mistakenly consider the corporate network safe

Evolving tactics, techniques & procedures (TTP’s)

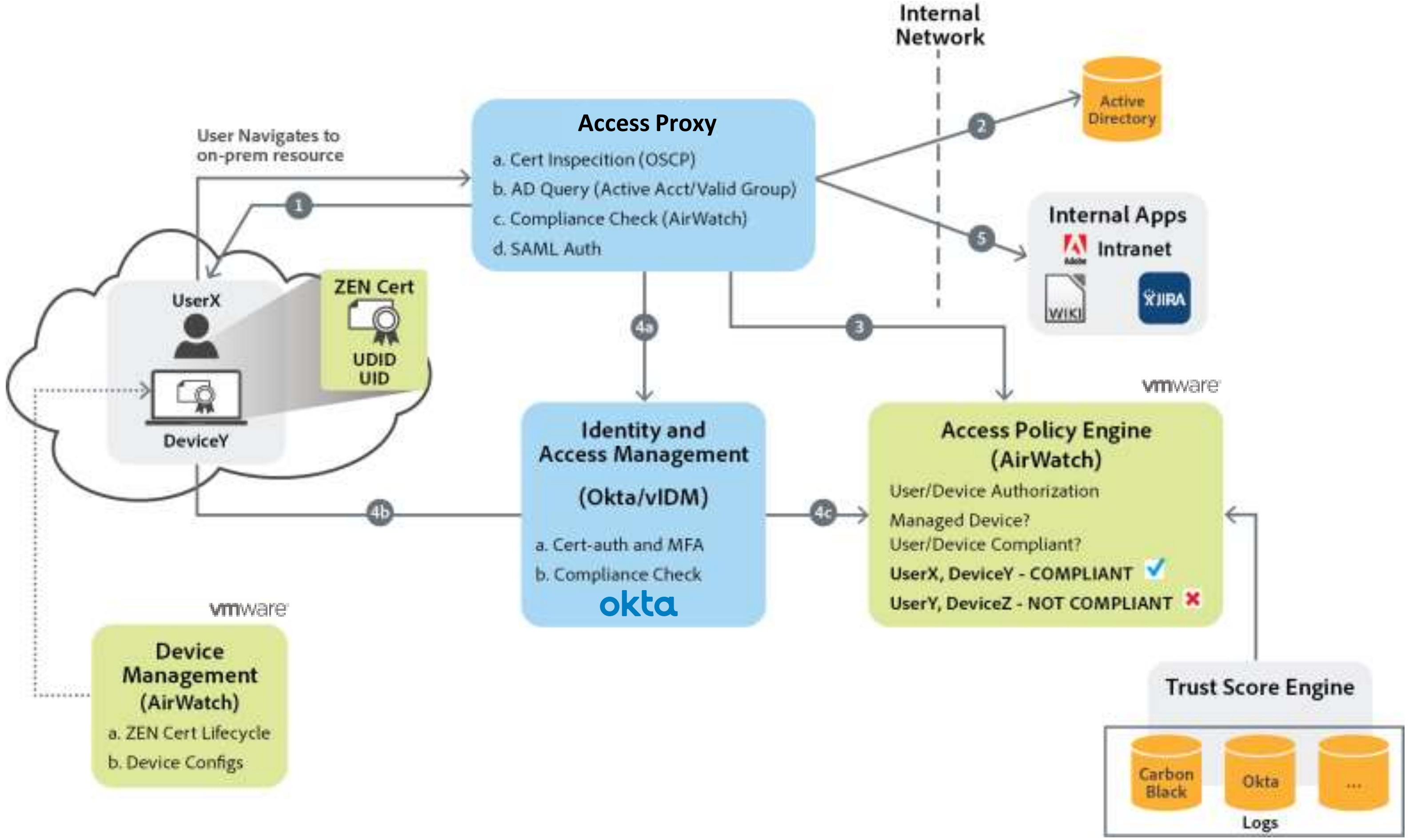
© 2019 Adobe. All Rights Reserved.

Leverages Existing Investments In…

- Authentication
- Network Access Control
- Logging
- Endpoint Detection & Response
- Device Management

© 2019 Adobe. All Rights Reserved.

ZEN Overview



Internal Network

User Navigates to on-prem resource

Access Proxy

a. Cert Inspection (OSCP)

b. AD Query (Active Acct/Valid Group)

c. Compliance Check (AirWatch)

d. SAML Auth

Active Directory

Internal Apps

Intranet

WIKI

JIRA

UserX

DeviceY

ZEN Cert

UDID

UID

1

2

3

4a

4b

4c

5

Identity and Access Management

(Okta/vIDM)

a. Cert-auth and MFA

b. Compliance Check

okta

vmware

Access Policy Engine (AirWatch)

User/Device Authorization

Managed Device?

User/Device Compliant?

UserX, DeviceY - COMPLIANT ✓

UserY, DeviceZ - NOT COMPLIANT ✗

vmware

Device Management (AirWatch)

a. ZEN Cert Lifecycle

b. Device Configs

Trust Score Engine

Carbon Black

Okta

...

Logs

LEGEND

1 Client challenged for certificate

2 Active Directory

3 Compliance check to Access Policy Engine

4a AuthN request to IdP

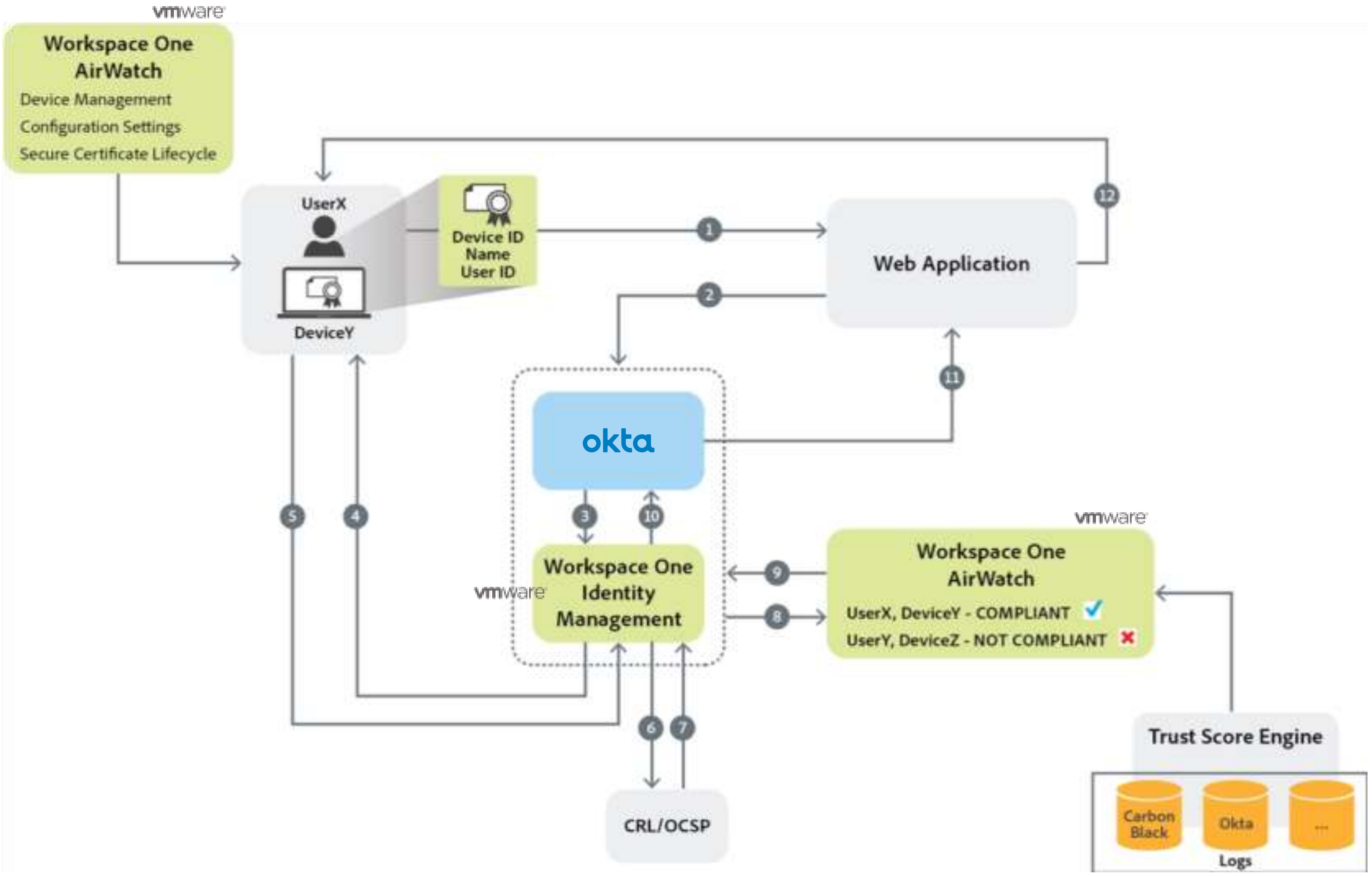
4b Client challenged for certificate

4c Compliance check to Access Policy Engine

5 Allow access if all conditions met

© 2019 Adobe. All Rights Reserved.

ZEN Overview



LEGEND

1 Request goes to web app

2 App makes AuthN request to Okta

3 Okta delegates AuthN request to vIDM

4 vIDM challenges client for certificate

5 Certificate sent for authentication

6 CRL/OCSP Check

7 CRL/OCSP Response

8 Compliance Check

9 Response (Compliant)

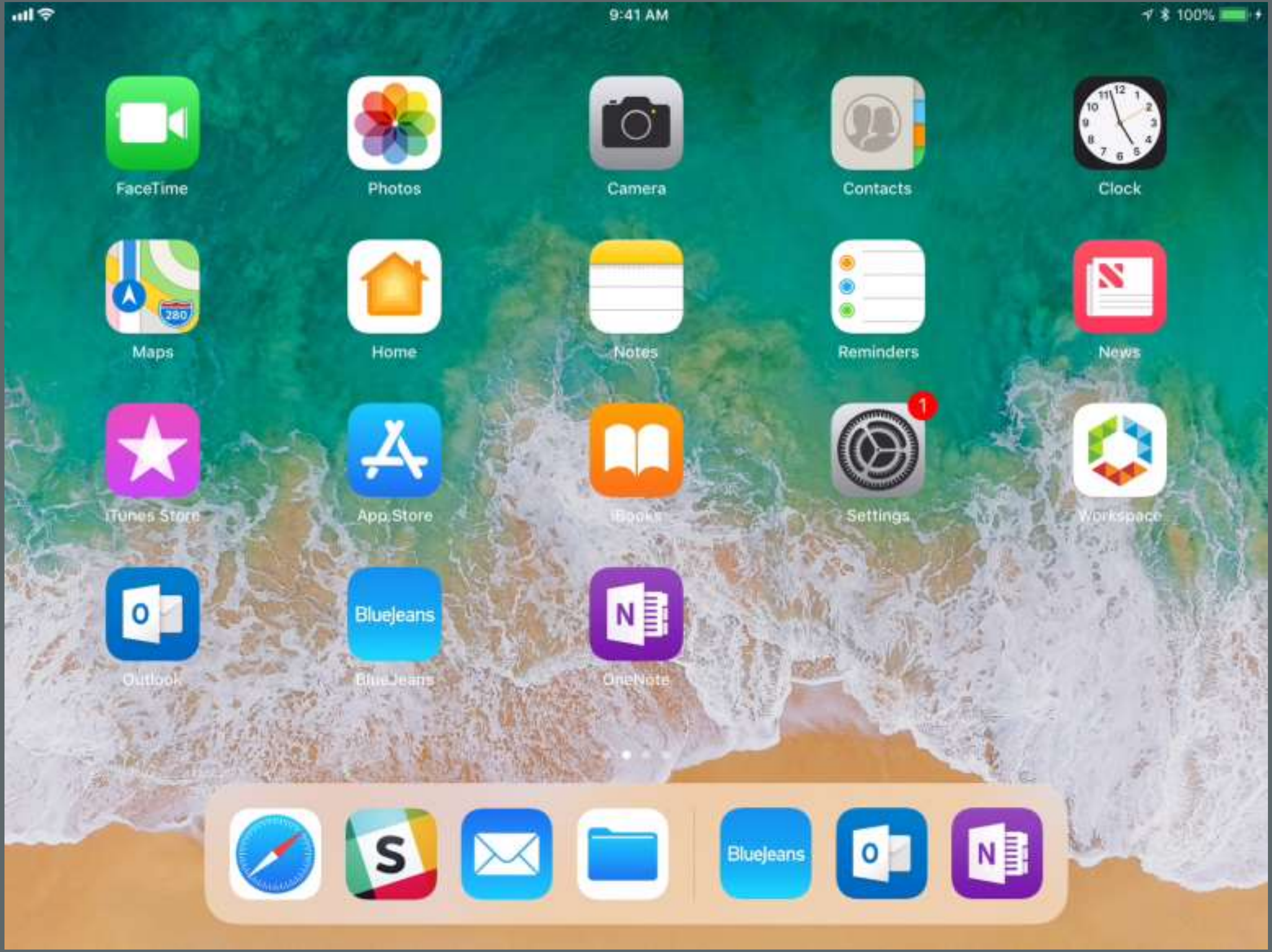
10 If cert valid, vIDM generates SAML response and send to Okta

11 Okta validates SAML, challenges for MFA generates new SAML response and sends to app

12 App validates SAML and if valid, redirects user to protected application content

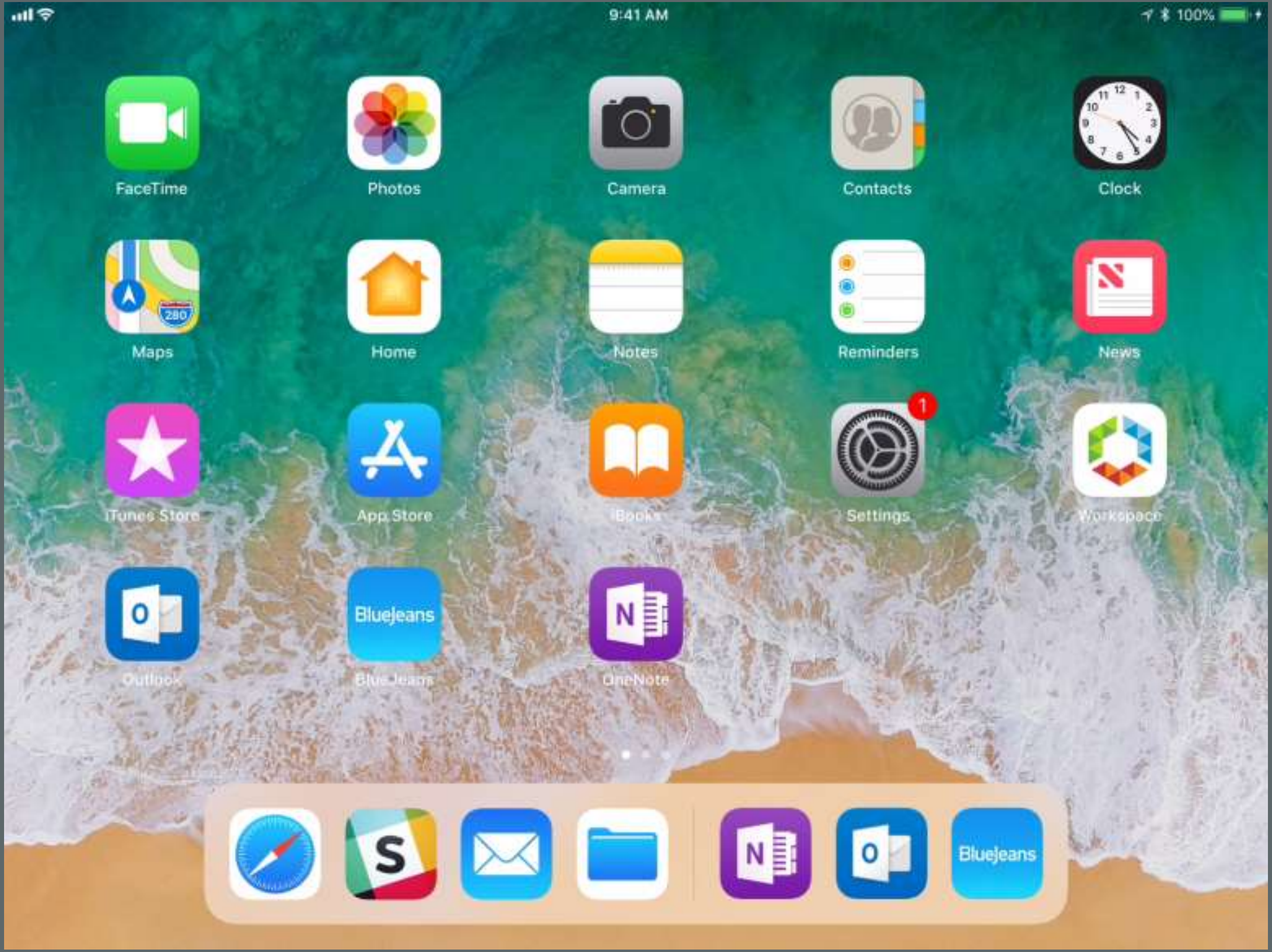
© 2019 Adobe. All Rights Reserved.

Demo – compliant device



© 2019 Adobe. All Rights Reserved.

Demo – non-compliant device



© 2019 Adobe. All Rights Reserved.

Progress To Date

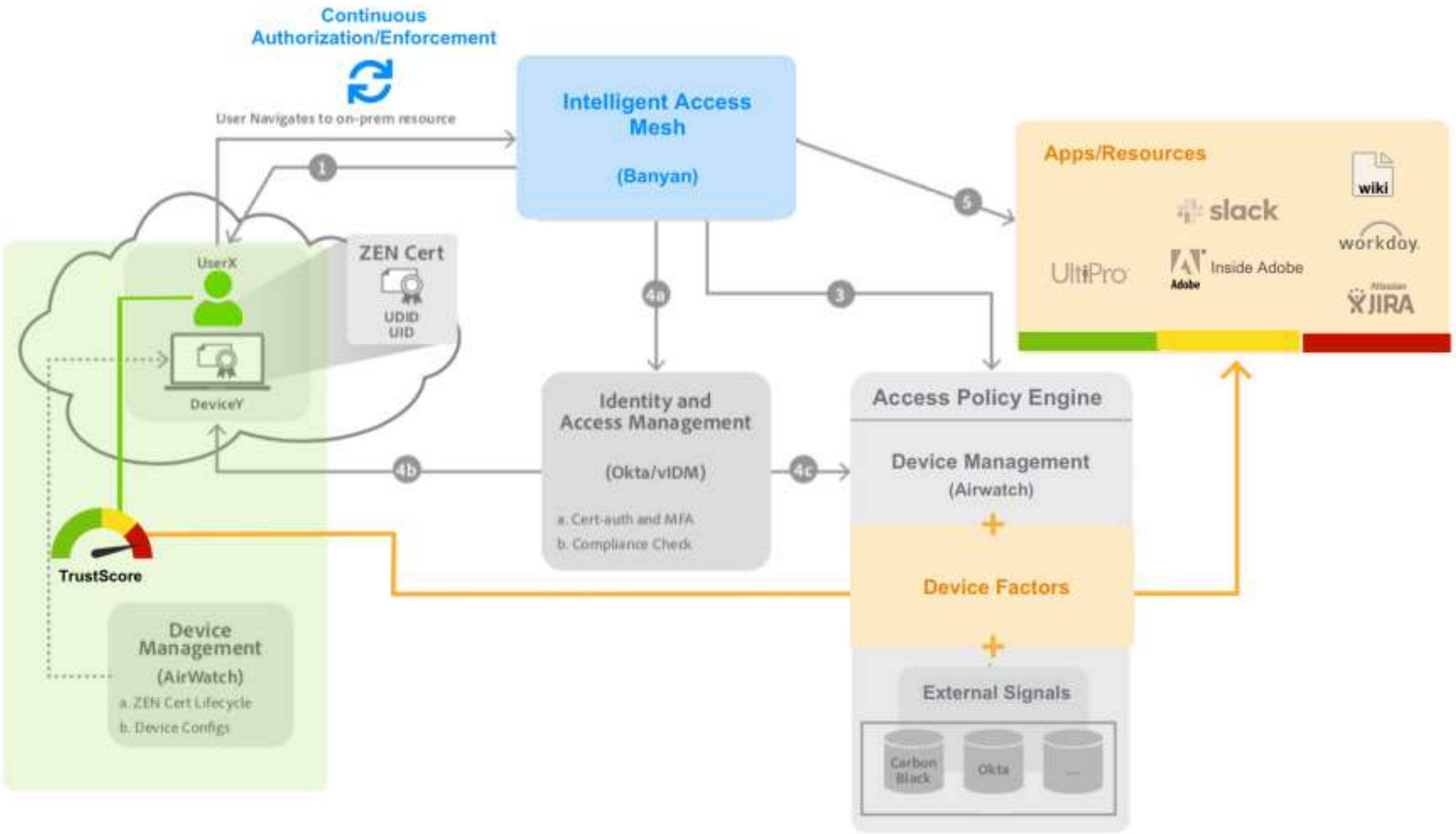
- Certificates deployed to over 45,000 devices
- 2000+ ZEN-enabled applications
  - 12,000 authentications per hour
- 20+ applications available via proxy

© 2019 Adobe. All Rights Reserved.

LEGEND

- ● **Access Proxy – Expansion**
  - Continuous Access Enforcement
  - Supporting New Use Cases
- ● **ZEN Control Plane – Enhancements**
  - Granular Authorization to resources
- ● **Endpoint Improvements**
  - Empowering Employees
  - Security ‘Credit Score’

What’s Coming



© 2019 Adobe. All Rights Reserved.

Resources

- **Adobe Zero-Trust Whitepaper**
  https://adobe.com/go/projectZEN

- **Security @ Adobe blog**
  https://blogs.adobe.com/security/

- **Security Jobs @ Adobe**
  https://adobe.com/go/securityjobs

© 2019 Adobe. All Rights Reserved.

Mission

The Identity Defined Security Alliance is a non-profit organization that facilitates community collaboration to develop a framework and practical guidance that helps organizations put identity at the center of their security strategy.

Membership

Atos

BANYAN

BeyondTrust

Centrify ZERO TRUST PRIVILEGE

CYBERARK

Cyxtera

f5

FOCAL POINT DATA RISK

idaptive

iddataweb

IMAGEWARE SYSTEMS

LikeMinds Consulting

LogRhythm The Security Intelligence Company

NEXTLABS

OBSIDIAN

okta

Omada

ONE IDENTITY

OPTIV

Ping Identity

Remediant

SailPoint

SECUREAUTH

SecZetta

STEALTHbits TECHNOLOGIES

THALES

ThreatMetrix

vmware

Customer Advisory Board

Adobe

Brighthouse FINANCIAL

LogRhythm

Huntington

OPTUM

WELLS FARGO

IDSA Resources

- Whitepaper: Identity Defined Security Framework
- Whitepaper: The Path To Zero Trust Starts with Identity
- Customer Story: LogRhythm’s Journey to Zero Trust
- Customer Story: Adobe Finds ZEN through Identity Centric Security
- Zero Trust Blog Series

THE PATH TO ZERO TRUST STARTS WITH IDENTITY

CASE STUDY

LogRhythm's Journey to Identity-Centric Zero Trust

IDENTITY DEFINED SECURITY ALLIANCE

www.idsalliance.org

© 2019 Adobe. All Rights Reserved.

Adobe