



Adobe

Project ZEN

Eric Anderson | Enterprise Security @ Adobe



#AdobeRemix
Vasjen Katro / Baugasm

Zero-Trust: Why Do We Need It?

Authentication ignored the device



Network perimeter no longer a security boundary

We mistakenly consider the corporate network safe

Evolving tactics, techniques & procedures (TTP's)

External (SaaS) Resources



Leverages Existing Investments In...



Authentication



Network Access Control



Logging

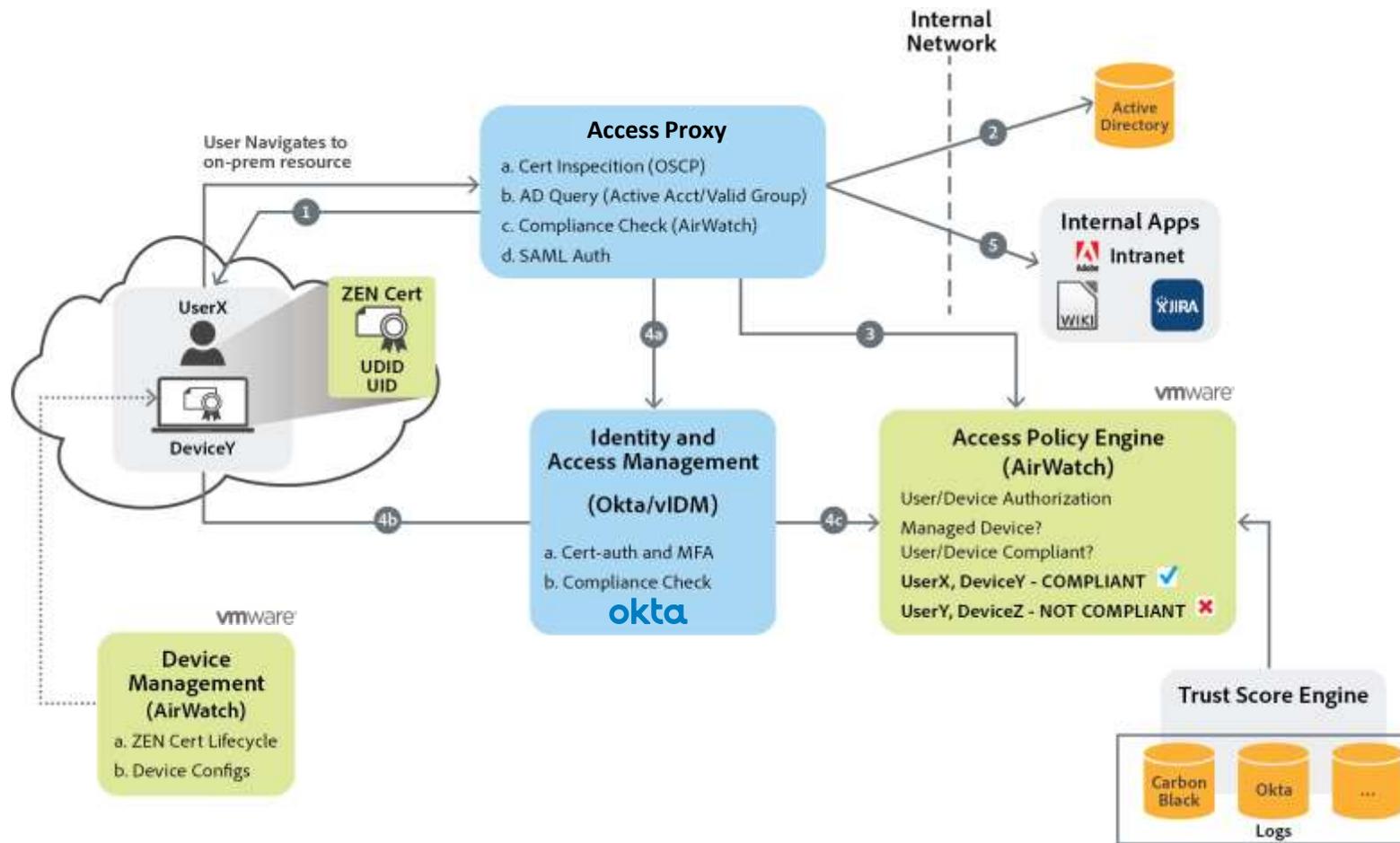


Endpoint Detection & Response



Device Management

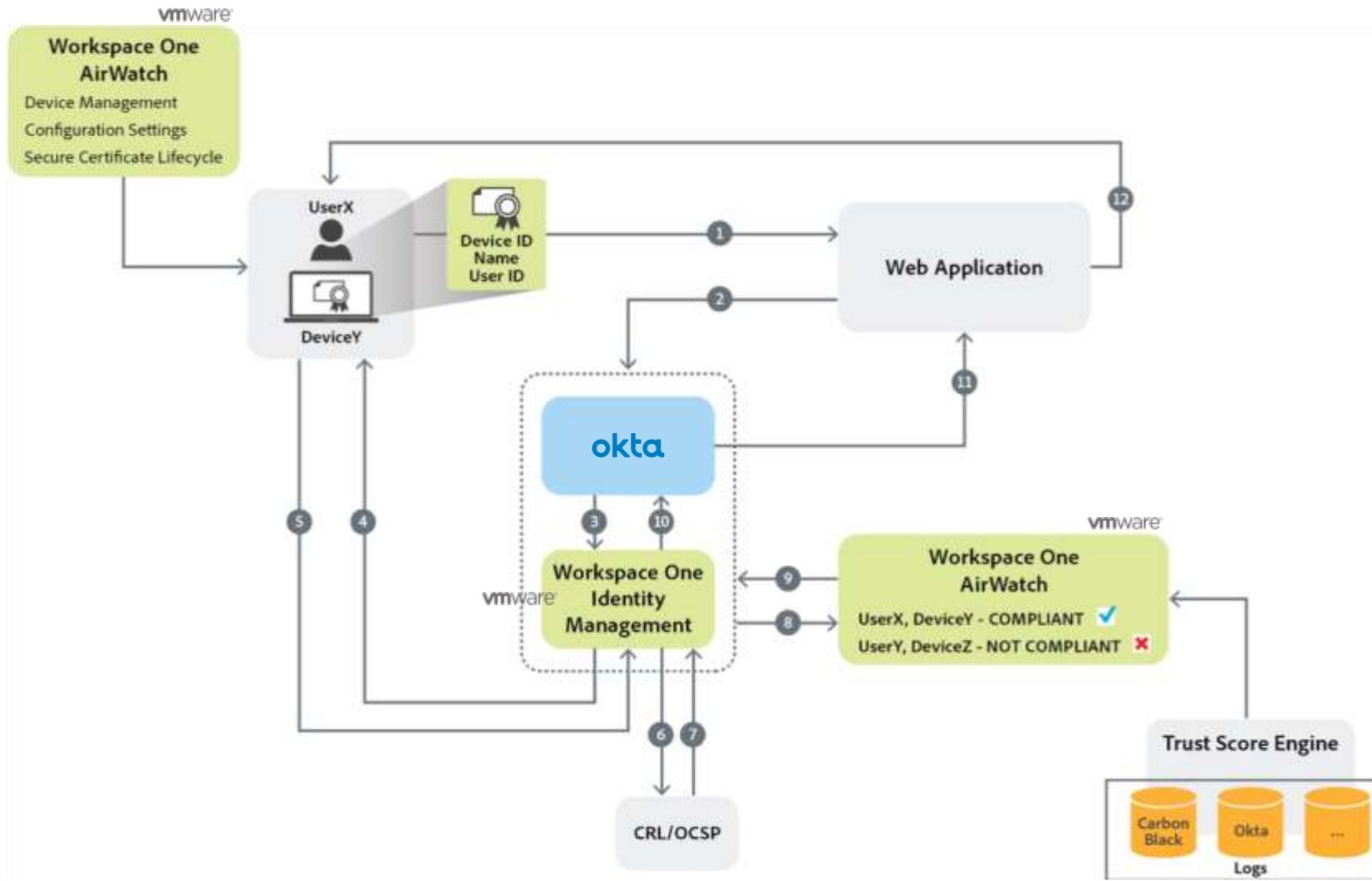
ZEN Overview



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

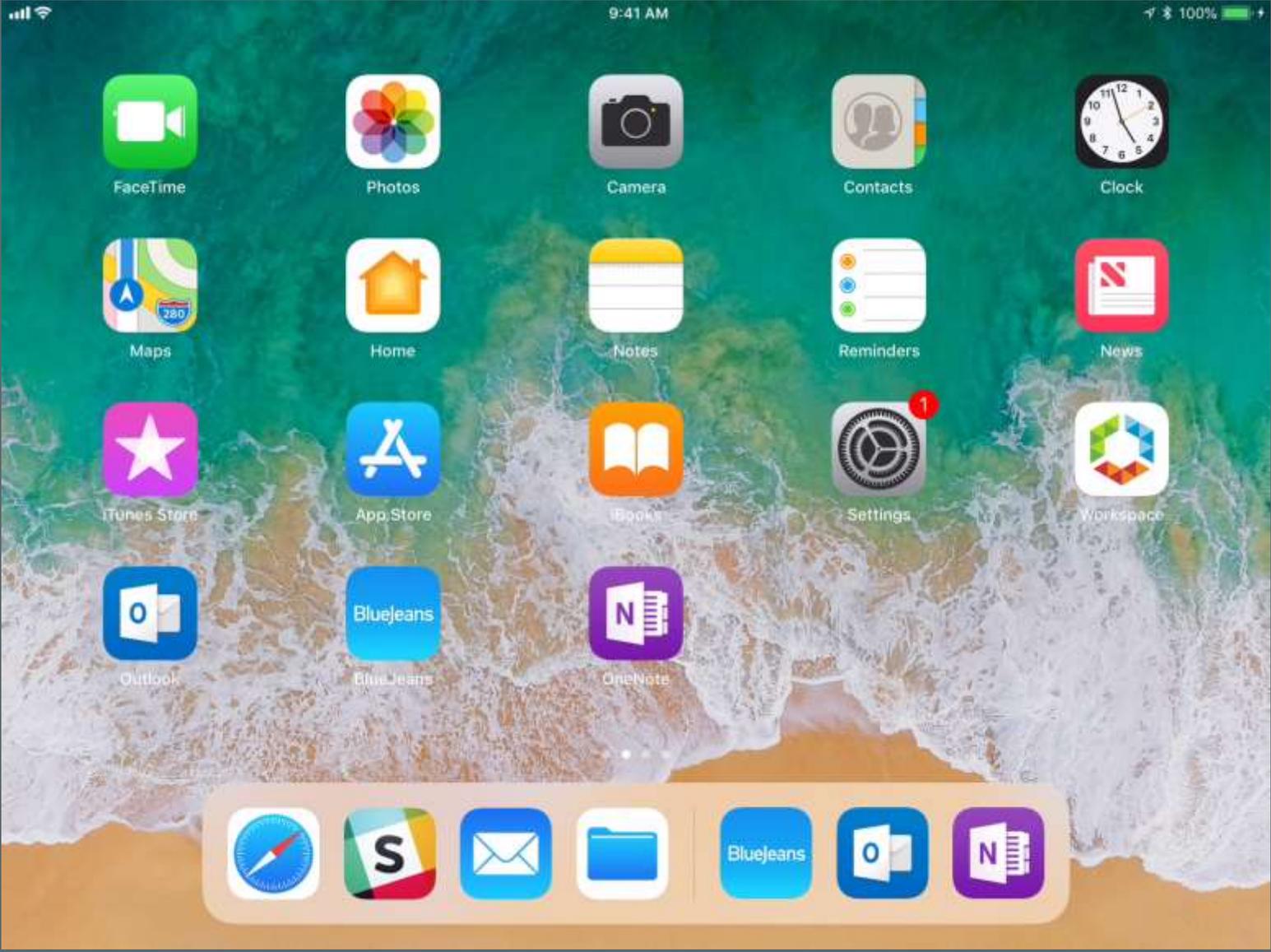
ZEN Overview



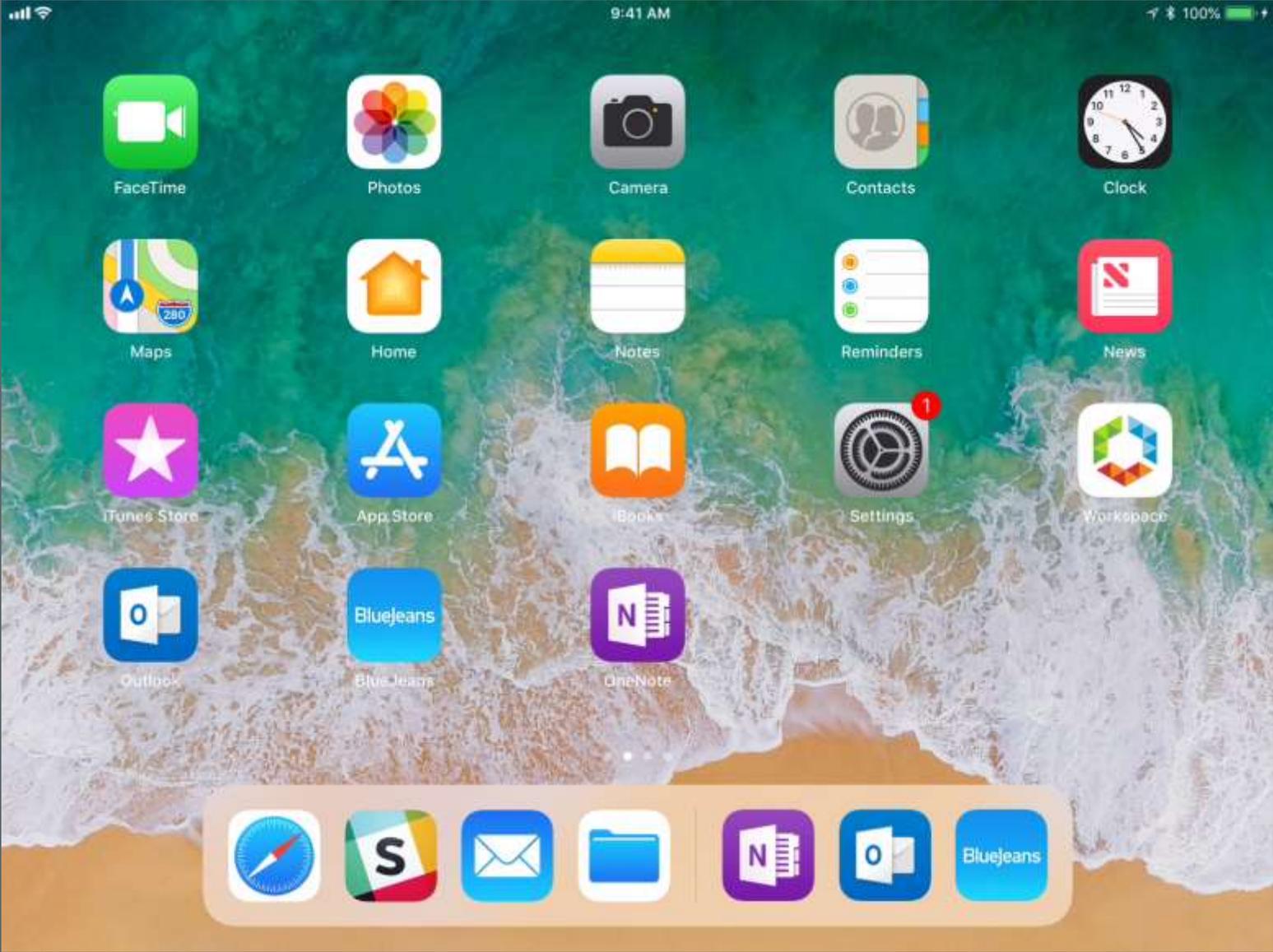
LEGEND

- 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

Demo – compliant device



Demo – non-compliant device



Progress To Date

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

What's Coming

LEGEND



Access Proxy – Expansion

Continuous Access Enforcement

Supporting New Use Cases



ZEN Control Plane – Enhancements

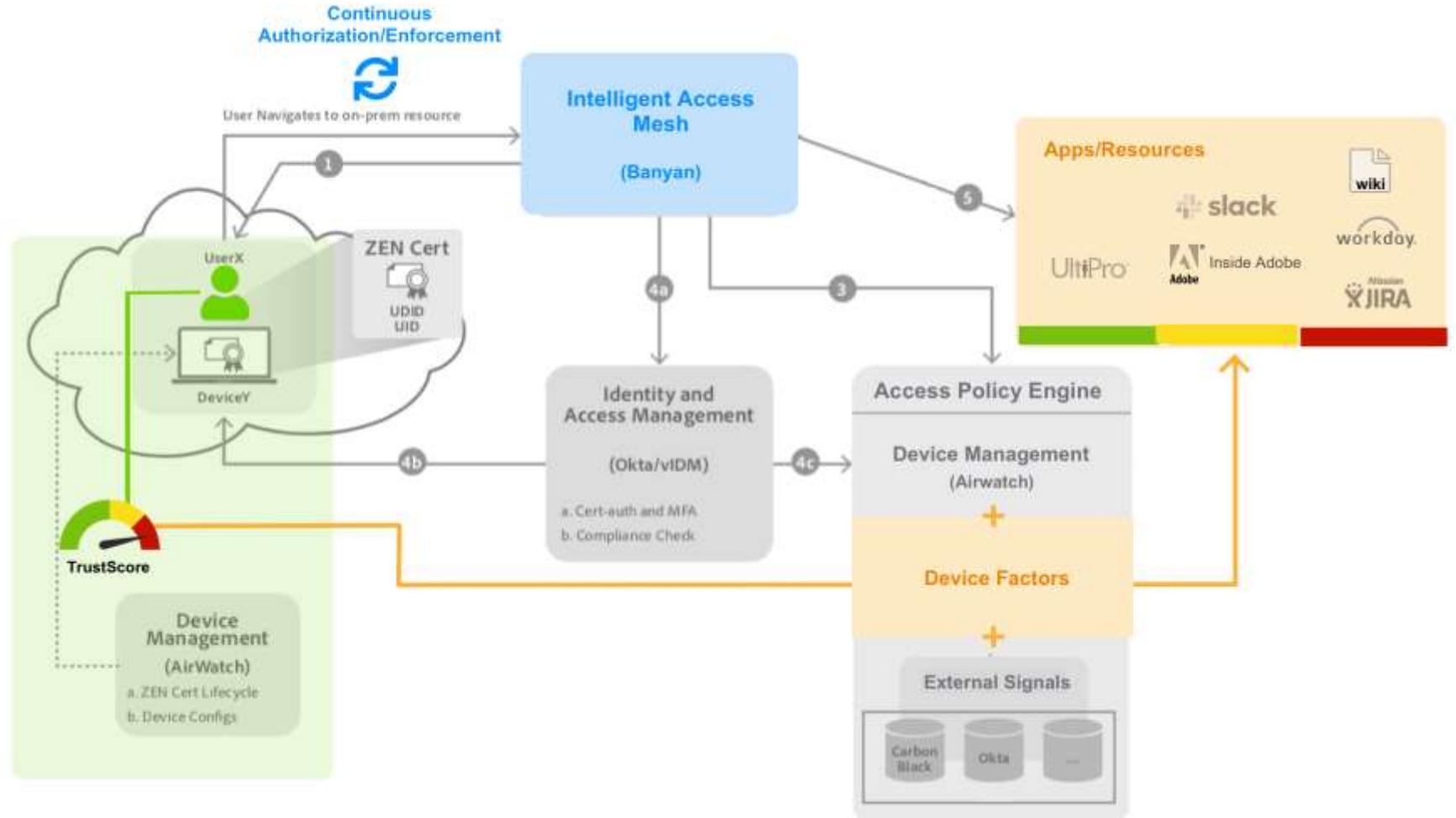
Granular Authorization to resources



Endpoint Improvements

Empowering Employees

Security 'Credit Score'



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>

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



Customer Advisory Board



IDS Alliance Resources

- ⑩ Whitepaper: Identity Defined Security Framework
- ⑩ Whitepaper: The Path To Zero Trust Starts with Identity
- ⑩ Customer Story: LogRhythm's Journey to Zero Trust
- ⑩ Customer Story: Adobe Finds ZEN through Identity Centric Security
- ⑩ Zero Trust Blog Series



WHITEPAPER
THE PATH TO ZERO TRUST STARTS WITH IDENTITY

CASE STUDY
LogRhythm's Journey to Identity-Centric Zero Trust

Overview
As a next-generation security information and event management (SIEM) company, LogRhythm is on the cutting edge of security. Documented to helping organizations to reduce risk by rapidly detecting, investigating and neutralizing damaging cyberattacks. But just like every organization, they are also susceptible to a breach, and change in processes and policies—especially when a disruptive threat—is a challenge. When Jason Carbin, CISO and VP of LogRhythm Labs, joined the organization, he recognized he had an opportunity to not only improve the security of a security organization, but to also design and engineer an architecture based on Zero Trust that could be used as a model for organizations of similar size and/or threat vectors.

Fortunately for the LogRhythm team, the existing IT environment was built with a cloud-first approach, reducing the complexity of their IT infrastructure while enabling a distributed workforce. The transition to a Zero Trust architecture would need to prioritize scope and existing technology, allowing it to integrate with the current infrastructure in a way that enables simplicity and budget build support.

Solution
Jason has been a supporter of Zero Trust since its concept was introduced in 2009. The Zero Trust model fits well with a single perimeter and covers a lot of many endpoints, apps, applications, and data elements, with the opportunity to live at the corporate threshold. The sharing of identity context through integrated technologies is the basis of identity-centric security. The result focuses on two primary principles:

1. Don't inherently trust anything on or off your network, and
2. Apply appropriate security controls based on the data.

LogRhythm approached the project in phases, making its 2018 target to complete in 2020. This approach involves the following steps:

- Perform data identification and classification of most sensitive data
- Map out and identify the points of data flows and system architecture
- Implement identity and access management (IAM) and multifactor authentication (MFA), addressing user permissions
- Integrate user and entity behavior (UEBA) analysis and issue alerts for digital actions
- Implement micro-segmentation and privileged access management
- Develop access control engine and session posture

Once fully implemented, the team believes they will have the closest thing to a silver bullet to improve their IT organization, improve security and reduce risk of a breach.

Identity Defined Security Alliance
• Risk-based authentication
• Zero Trust architecture
• LogRhythm

Identity of the future of Zero Trust, the identity of your organization's IT systems, the identity of your organization's data, and the identity of your organization's users. All of these elements are the Zero Trust Foundation. All of these elements are the Zero Trust Foundation. All of these elements are the Zero Trust Foundation. All of these elements are the Zero Trust Foundation.

www.idsalliance.org





Adobe