Leveraging Adaptive Auth and Device Trust for Enhanced Security and Compliance

CHRISTOPHER NIGGEL, DIRECTOR OF SECURITY & COMPLIANCE
SWAROOP SHAM, SR PRODUCT MARKETING MANAGER, SECURITY
CHRIS NIGGEL
Director of Security & Compliance, Okta
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 are beyond Okta’s control.

In particular, the following factors, among others, could cause results to differ materially from those expressed or implied by such forward-looking statements: 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 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 risks 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 or other presentations, press releases or public statements are not currently available and may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation or promise to 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 has not independently verified the statistical and other industry data generated by independent parties and contained in this presentation and, accordingly, 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.
Privacy by design

Trust is our number one value

Okta was born in the cloud

Our approach to data privacy is simple:

- Customers own their data
- Okta only uses data to provide our service
- We keep our customers’ data safe and secure
Our approach to security

- Offensive security
- Defensive security
- Trust and compliance
Offensive Security

- Peer code reviews
- Security Research
- 65,000+ automated unit, acceptance, and security tests
  - OWASP Top 10 and SANS Top 20
- Internal and external penetration testing teams
- Secure code training
Defensive Security

- Organization-level Encryption
  Need-to-know access

- Hardened endpoints
  Monitoring and Detection

- Incident Response
  Industry Breach Reviews
Trust and Compliance

Highly available Architecture
Region-specific storage

Okta on Okta
Strong Access Controls

Multiple Industry Certifications
SOC2, ISO 27001, CSA STAR, HIPAA, FedRAMP
Don’t take my word for it

Audit Reports available to customers

3rd Party Pen test reports Public Bug Bounty Program

Customer Pen Testing
Your partner in security

Gain visibility into the cloud landscape

Make security mobile

Use automation to quickly react
SWAROOP SHAM
Sr. Product Marketing Manager, Security, Okta
Building for Security and Compliance
Building for security and compliance

Okta ThreatInsight

Okta Service Security & Compliance

*ThreatInsight is expected to be available in the second half of 2018
Okta ThreatInsight: Conditional Access Control

**Okta ThreatInsight**: Aggregated data powering security

- **National State Attackers**
  - Brute Force Attacks
  - Password Stuffing
  - Phishing

- **Financially Motivated Attackers**
  - Social Engineering
  - Password Spraying

- **Script Kiddies**
  - Ingest Intelligence and Identify Attackers

*ThreatInsight is expected to be available in the second half of 2018*
Okta ThreatInsight: Aggregated data powering security

- User Identifier
- IP Address
- Application

- Strong Authentication Policies
- Anomaly Detection
- Incident Enrichment
Building for security and compliance

Context

Okta Threat Insights
Network
App
User
Device
Location

Okta Service Security & Compliance

*ThreatInsight is expected to be available in the second half of 2018
Adaptive authentication: Context

- Group/Role
- Login velocity
- Work location
- Working hours
- Typing speed
- Concurrent login
- Auth. method
- User agent
- Device fingerprint
- Devices per user
- Managed
- Known device
- Secure device
- Lat/Lon
- Country
- State
- City
- Prohibited country
- In-Network IP
- Out-Network IP
- Proxy
- Anonymizer
- Known bad IPs
- Sensitive data
- User group
- Bad IPs
- Malicious user behavior
Building for security and compliance

Context

Okta Threat Insights  User  Rule Based  Policy Engine
Network  Device  Risk Based
App  Location

Okta Service Security & Compliance

*ThreatInsight is expected to be available in the second half of 2018
Match authentication to the risk observed from context

- **High Login Velocity**
- **New Device**
- **New Location**
- **New IP**
- **AWS S3**
- **Suspected IP**

**Low**
- Same location
- Same device

**High**
- Login within working hours, Same device, New location, New IP
- High login velocity, New device, New location, New IP, Suspected threat IP

**Okta Verify**
- Password
- Okta Verify with Push
- Okta Verify + U2F
Adaptive authentication: Customize response based on context

Context

- Okta Threat Insights
- Network
- App
- User
- Device
- Location

Response

- Rule Based
- Risk Based

Policy Engine

Response

Okta Service Security & Compliance

*ThreatInsight is expected to be available in the second half of 2018
Secure passwordless experience

- This is a user who is known to login only from 2 locations—office and home
- Using an Okta issued laptop or his personal iPhone for which we have identified the fingerprints
User experience

- This is a user who travels frequently and doesn’t have a known location other than office and home
- Using an Okta issued laptop/iPad or his personal iPhone for which we have identified the fingerprints
- New session interval changes to x hours once a public IP or an unknown IP is encountered
Response: Use authentication factors of choice

- 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 authentication
Building for security and compliance: Key takeaways

1. Security and compliance by design
2. Risk-based contextual access and response
3. Enforcement and visibility across all applications
Thank You