Identity as the new Cloud Security Perimeter

Rodger Nichols, Director – Field Alliances
What Is Identity

People
- Employees
- Contractors
- Partners
- Customers
- Anyone

Technology
- Applications
- Devices
- Wearables
- IoT
- Anything
Transformation of IT Delivery

Traditional perimeter is disappearing – fast
Transformation of IT Delivery

Identity is the new perimeter
Transformation of IT Delivery

B2B

B2C

B2API
Breaches Happen

Security Incidents in 2016: 42,068
Confirmed Breaches in 2016: 1,935
Average Cost Per Breach: $3.8M

*Verizon 2017 Data Breach Investigations Report, Gemalto 2015 Breach Level Index
It's Not Getting Better

Figure 4.
Number of breaches per threat action category over time, (n=9,009)

*Verizon 2016 Data Breach Investigations Report
Phishing — Still #2 in 2016
Breach Metrics Don’t Lie

- 81% of breaches used stolen and/or weak credentials
- 73% of passwords are duplicates
- <10% of breaches leveraged new technical vulnerability

Credential harvesting is the most fruitful tactic for today’s threat actors.

Solution to Weak Credentials?
Killing the Password is Hard

<table>
<thead>
<tr>
<th>Category</th>
<th>Scheme</th>
<th>Usability</th>
<th>Deployability</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Incumbent)</td>
<td>Web_passwords</td>
<td>III [13]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware tokens</td>
<td>RSA SecurID</td>
<td>IV-G [34]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yubikey</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IronKey</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CAP reader</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pico</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone-based</td>
<td>Phoolproof</td>
<td>IV-H [36]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Crono</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MP-Auth</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OTP over SMS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Google 2-Step</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fingerprint</td>
<td>IV-I [38]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Iris</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Voice</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- • = offers the benefit; ○ = almost offers the benefit; no circle = does not offer the benefit.
- III = better than passwords; ≁ = worse than passwords; no background pattern = no change.
It All Starts and Ends with Authentication

Stolen and recycled passwords continue to pose an important security issue

Poor access control management leaves people with access to everything

Authentication strategies haven’t evolved in 15+ years
Solutions We’re Relying on Aren’t Working

Technology Realities

- Cost
- Complexity
- Management

Tools

- AV
- DLP
- Firewall/IDS/IPS
- WAF
- SIEM
- DAM
- DRM > Encryption

Targets

- Endpoints
- On-Premises Applications
- Application Servers
- Cloud Applications
- File Servers
- Data

Landscape Realities

- Devices
- Networks
- Services
Identity is the Missing Ingredient

Identity solutions represent a critical control point:
There’s no control over people, devices or services

Extend to cloud, mobile and on-premises

Safeguards from account compromise

Reduce identity silos and improved identity assurance

Improve security posture through cybersecurity ecosystem integration
With Identity, There’s a Better Approach

1. Centralize identity and access control via single sign-on

2. Enable visibility and response to credential compromise and account takeover attacks

3. Reduce your attack surface through automated provisioning and deprovisioning

4. Ensure strong authentication across all services, everywhere
1. Centralize Identity

- Unify identity infrastructure for IT to reduce account management complexity
- Unify access for users to eliminate passwords while simplifying access
- Mitigate risk and reduce identity sprawl by restricting access to services via intelligent SAML connections
2. Enable Rapid Response to Compromise

- Get centralized view into all authentication data across cloud, mobile and on-premises applications
- Identify unusual and suspicious behaviors
- Enrich and enhance your cybersecurity ecosystem investments by feeding SIEM, UEBA, alerting and workflow tools
3. Reduce Attack Surface

- Automated provisioning and deprovisioning accelerates consistent onboarding, while eliminating orphan accounts.
- Extend to custom applications via SCIM, SDKs and APIs.
- Complete lifecycle management ensures the right level of access to the right applications with access request workflows.
4. Enable Strong Authentication Everywhere

- Enable MFA on every cloud application
- Extend MFA to on-premises applications via RADIUS, RDP, ADFS and LDAP
- Make intelligent, contextual access decisions based on device and connection attributes
Multifactor Authentication

- Something you know
- Something you have
- Something you are
Traditional MFA Challenges

**Cost**
- Expensive on-prem infrastructure to deploy and maintain
- Burdensome hard token management

**Management**
- Difficult to integrate with cloud applications
- Each app integration independently managed

**Usability**
- Too many prompts add complexity to average login process
- Global and external users require different factors for verification
Recipe for an Effective MFA Solution

Central deployment and configuration

Flexibility to support for diverse user types

Consumer-grade user experience
200,000 Employees
20,000 Suppliers
15,000 Employees
65,000 Employees
Okta plays a role in all three of my initiatives: Cyber security, business productivity, and best of breed. It fits all three, so it’s a perfect match.

— Gus Shahin, CIO, Flex
Identity as the new Cloud Security Perimeter

Your Goal:

1. Secure authentication via SSO
2. Enable Rapid Response
3. Reduce Attack Surface
4. MFA Everything

Your Success Criteria:

1. Eliminate passwords where possible
   - Enable strong, unique passwords everywhere else
2. Centralized, real-time reporting for all auth events
   - Integrate with existing security tools
3. Automate provisioning with accurate entitlements
   - Deprovision at scale, and enable visibility and reporting
4. Harden critical applications with step-up authentication
   - Apply unified policy to on-premises, cloud and mobile

© Okta and/or its affiliates. All rights reserved.  Okta Confidential
Thank You