Multi-Factor Authentication for Cloud Applications

PRESENTED BY:
Oscar Sanchez, Sr Sales Engineer
Ariel Santa Cruz, Channel Enablement Manager
Session: Multi-Factor Authentication for Cloud Applications

Related Labs: Introduction to Universal Access and F5 SAML IDP (Self-paced)

One of the main problems that customers face with the adoption of SaaS and cloud-based apps is how to deliver the same level of security as they do for on-premises apps. The rapid growth of SaaS apps has resulted in a challenge to manage, share, and secure identity between these cloud-based apps. Another important thing is the necessity to achieve PCI compliance, where multi-factor authentication (MFA) is a must.

Outline:
• Market Overview
• Mobility and Cloud Adoption Challenges
• Identity Management Challenges
• Multifactor Authentication Overview
  • MFA with F5
• F5 Adaptive Auth (MFA)
• DEMO
• Q and A
Market Driven by Mobile and Cloud Adoption

Worldwide workforce by end of 2015

- Non-mobile: 63%
- Mobile: 37%

~1.3 Billion mobile workers by end of 2015

X 100M
Market Driven by Mobile and Cloud Adoption

- 72.3% of the total U.S. workforce will be mobile in 2 years (2020)
- 15.4% cloud services supporting multi-factor authentication
- 715 average number of cloud apps per enterprise
Market Driven by Mobile and Cloud Adoption

25+% of organizations have 1,000 or more cloud-based applications

- 25% >1,000 Cloud-based Apps
- 75% <1,000 Cloud-based Apps

1,083
the number of cloud services used by an average organization

1,586
number of business partners an average organization connects with via the cloud
## Weak Passwords and Credentials Hurt Customers

### Rising (monetary) costs of data breaches

<table>
<thead>
<tr>
<th>Cost</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$3.8M</td>
<td>Average total cost of a data breach(^1)</td>
</tr>
<tr>
<td>23%</td>
<td>Increase in data breach cost, ‘14 to ‘15(^1)</td>
</tr>
<tr>
<td>$154</td>
<td>Average cost per lost or stolen record(^1)</td>
</tr>
</tbody>
</table>

### Rising (business) costs of data breaches

- Damage to brand reputation
- Compromises sensitive enterprise, employee and customer data
- Can result in significant downtime and lost revenue
- Breaches regulatory and/or government compliance required to conduct business
Mobility and Cloud Create the Challenge of Sharing Identification Across Any Application, Anywhere, Anytime

- **Silos of identity**
- Identity may still be on premises, but apps and data are moving to the cloud
- Users experiencing “password fatigue” (too many passwords to remember)
- **Weaker passwords** make it easy for credentials to be hacked
What can I do to alleviate “password fatigue” for my employees and users?

Who can help me employ dynamic, adaptive access control?

How can I ensure only authorized users access my apps and data?

Who can help me integrate and deploy multi-factor, layered, differentiated authentication?

What can I do to ensure my users are using strong passwords and credentials?

How can I ensure my users’ credentials aren’t compromised?
The Challenges of Managing Access Today

Rapidly expanding, changing mobile workforce

Explosion in number of users, use cases, in-use devices

Increased virtualization

Fast rising number of security threats and attacks

Need to manage access based on identity and context
User Identity ≠ Just User ID
Controlling Access Through Identity

User Identity and Device Information + Network / Connection + Application Health and Risk
User Identity in Secure Access

- Device type and integrity
- Operating system
- Browser
- Location
- Intelligence and visibility
MULTI-FACTOR AUTHENTICATION
Why Do Organizations Need Multi-Factor Authentication?

• **Passwords Aren’t Enough**
  - Passwords are often compromised through phishing and malware, a second auth factor protects the organization

• **Compliance**
  - MFA is required for many environments due to compliance requirements

• **We know it works**
  - The 2015 Verizon Data Breach Investigations Report says **MFA was the appropriate control** to stop 24% of incidents
MFA Authentication and SSO

- Dramatically reduce infrastructure costs; increase productivity
- Provide seamless access to all web resources
- Integrated with common SaaS applications

Corporate managed device
Latest AV software
AAA server
User = Finance

Office365.com
Salesforce.com
Finance
Expense report app
F5 Identity Federation, SSO, and MFA

- Federates user identity across apps located anywhere—networked, cloud, SaaS, etc.

- Integrates with existing MFA and IAM solutions to deliver seamless SSO and adaptive MFA

- MFA capabilities with F5 Adaptive Auth or as one-time password (OTP) via email and certificate check

- Delivers integrated IdF with remote/mobile access, native VDI, and enterprise mobility
MFA with F5

• Fast
• Change in one place and apply the policy to many applications, can easily try new solutions with a test group and roll changes out to users selectively

• Easy
• Change using a single method

• Complete
• Doesn't rely on application compatibility with MFA solution
MFA Changes Without F5

Mobile User

Remote User

Contractor

Multifactor Auth Provider

Salesforce

Office 365

Concur

Google

SaaS
F5 Has a Rich and Powerful Ecosystem of MFA Partners

[Image of various logos including Salesforce, Toopher, Symantec, LoginPeople, RSA SecurID, SafeNet, ActivIdentity, Duo, Swivel, Microsoft, Yubico, SMS Passcode, Intel Security, SecureAuth, SecurEnvoy, and Vasco]
Customization
Unified Access to All Apps, Using Identity Federation/SSO with MFA

How portal will look to a user whose company is deploying AM for identity federation, SSO, and MFA authentication
F5 ADAPTIVE AUTH (MFA)
F5 Adaptive Authentication & MFA

- **Phase 1: Modern MFA For Access Control**

- **Phase 2: Advanced Adaptive Auth (device fingerprinting, geo-velocity checks, auth failure tracking)**

- **Phase 3: Analytics Based Adaptive Auth With Extended Protocols (risk engine)**

A platform & service for advanced adaptive auth, access control, and visibility with modern multi-factor authentication with F5 Access Manager (formerly APM)
F5 Adaptive Authentication in Action

F5 Secure Logon

Username
paolod

Password
******

Logon
F5 Adaptive Authentication in Action

Receive a link through SMS
1. Download F5 Verify from the app store.
2. Enter mobile number.

*Example: +1 123 456 7890*

Use QR Code with F5 Verify app
1. Download F5 Verify from the app store.
2. Open F5 Verify app and scan QR code.

OR

Submit
F5 Adaptive Authentication in Action

Accept Push Notification from F5
Verify

or

Enter Token Code:

Submit

ITC Demo: paolod

567891

25
### F5 Adaptive Authentication in Action

![Screen Shot](image)

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Sent</th>
<th>Compression</th>
<th>Received</th>
<th>Compression</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Access</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Network Tunnel</td>
<td>2.22 KB</td>
<td>0%</td>
<td>801 B</td>
<td>0%</td>
</tr>
<tr>
<td>- Optimized Applications</td>
<td>0 B</td>
<td>0%</td>
<td>0 B</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>2.22 KB</td>
<td>0%</td>
<td>801 B</td>
<td>0%</td>
</tr>
</tbody>
</table>

+ Show details
F5 Adaptive Authentication: Reporting
Demo Topology

User
Password

Google Auth

DUO

Salesforce
Amazon
Google Mail
Google Drive
Thank You