Przejmij kontrolę nad użytkownikiem, czyli unifikacja dostępu do aplikacji w zróżnicowanym środowisku

Łukasz Knysak – Senior System Inżynier w Veracomp SA
The generals – fearing delays in launching a retaliation attack – set the passcode to 00 00 00 00 (and in fact also wrote the number in the deployment instructions).

Back in 1963 JFK ordered that all nuclear warheads were fitted with a passcode to allow them being armed.
User Credentials

- £514M Personal Profiles Stolen
- 1.2B Credentials Amassed by CyberVor
- 19 Average # Passwords Per Person
SaaS market drivers

Any device
Bring your own device

Any location
Mobility

Any time
24x7 workforce
Who’s Requesting Access?

Manage access based on identity

IT is challenged to:
• Control access based on user type and roles
• Unify access to all applications (mobile, VDI, web, client-server, SaaS)
• Provide fast authentication and single sign-on (SSO)
• Audit and report access and application metrics
The New Perimeter Is An App Perimeter

TRADITIONAL NETWORK PERIMETER

PER-APP / PER-USER PERIMETER
The problem with SaaS – not if, but when?

IDENTITY AND ACCESS MANAGEMENT SILOS

“For an average of 26 different online accounts, users had only five different passwords.”
—Experian, 2012

“A quarter of the people surveyed admitted to using less secure passwords on mobile devices to save time.”
—Deloitte, 2013
Single Sign-On (SSO) Challenges

- Not all tokens work across all domains
- Some SSO tools must check in with an authorizing decision point
- Difficult to visualise SSO topology and deployment
Identities in Many Places, One Source of Truth

Enterprise Directory Services

SaaS Apps

Private Cloud Apps

Public Cloud Apps

Corporate Applications
Not this kind of Federation...
A federated identity in information technology is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.

- Wikipedia
Identities in Many Places, One Source of Truth
F5 BIG-IP Access Policy Manager Drives Identity Federation, Single Sign On, and Adaptive Authentication

Virtual Apps

Web-based Apps

Mobile Apps

Web Access Management

Remote Access and Application Access

Secure Web Gateway

Identity Federation/SSO

Virtual Edition

Appliance

Chassis

VDI

Enterprise Mobility Gateway

Enterprise Apps

Cloud, SaaS, and Partner Apps

Websites/Web Applications
Consistent security across all services
Flexible, Extensible Identity Federation and SSO Support

- Transforms one type of authentication into another
- Supports various standards-based protocols (SAML, Kerberos, NTLM)
- Enables flexible selection of SSO techniques appropriate to the application
- Allows for centralized session control of all applications, even SaaS apps
### APM Supported Authentication Methods

<table>
<thead>
<tr>
<th>Client-side Authentication Methods</th>
<th>Server-side Authentication Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HTTP Form</td>
</tr>
<tr>
<td>HTTP Form</td>
<td>YES</td>
</tr>
<tr>
<td>HTTP Basic</td>
<td>YES</td>
</tr>
<tr>
<td>NTLM</td>
<td>NO</td>
</tr>
<tr>
<td>Kerberos</td>
<td>NO</td>
</tr>
<tr>
<td>Certificate</td>
<td>NO</td>
</tr>
<tr>
<td>SAML*</td>
<td>YES*</td>
</tr>
<tr>
<td>RSA SecurID</td>
<td>NO*</td>
</tr>
<tr>
<td>One-time Passcode</td>
<td>NO*</td>
</tr>
</tbody>
</table>
APM and Adaptive Multi-Factor Authentication (MFA)

- Integrates with most multi-factor authentication offerings
- Provide native MFA, including one-time password (OTP) via email or SMS, cert checks
- Applies authentication mechanisms of varying severity, based increased risk factors
APM’s Webtop Unifies Access to All Apps, Including Those Using Identity Federation/SSO

APM’s webtop including app access via identity federation, SSO, and adaptive authentication
“I trust my SaaS providers implicitly to store a copy of my credentials.”

- No one ever
SAML Participants

- **Principal (user)**: The party requesting access to a protected resource.
- **Identity Provider (IdP)**: Authenticates the user.
- **Service Provider (SP)**: Controls access to the protected resource.
1. User requests resource
2. Redirect to IdP SSO service
3. User requests SSO service from Idp
4. IdP Authenticates User
5. Idp Returns signed SAML assertion
6. User POSTs assertion to SP
7. Access granted based on assertion subject
F5 SAML SP Configuration Elements

- **IdP Connector**: Defines how to find and speak to an IdP Service.
- **Access Policy**: Defines criteria for allowing or denying access to a resource.
- **SP Service**: Sends AuthN requests, consumes assertions.
- **Virtual Server**: Listens for incoming connections, proxies the user to a resource.
Proof of Office 365’s Rapid Adoption

Top 20 Enterprise Cloud Services
GLOBAL

<table>
<thead>
<tr>
<th>Rank</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Microsoft Office 365</td>
</tr>
<tr>
<td>2</td>
<td>Salesforce</td>
</tr>
<tr>
<td>3</td>
<td>Cisco Webex</td>
</tr>
<tr>
<td>4</td>
<td>Concur</td>
</tr>
<tr>
<td>5</td>
<td>Yammer</td>
</tr>
<tr>
<td>6</td>
<td>Zendesk</td>
</tr>
<tr>
<td>7</td>
<td>ServiceNow</td>
</tr>
<tr>
<td>8</td>
<td>Oracle Taleo</td>
</tr>
<tr>
<td>9</td>
<td>Workday</td>
</tr>
<tr>
<td>10</td>
<td>Box</td>
</tr>
<tr>
<td>11</td>
<td>GoToMeeting</td>
</tr>
<tr>
<td>12</td>
<td>ADP</td>
</tr>
<tr>
<td>13</td>
<td>SuccessFactors</td>
</tr>
<tr>
<td>14</td>
<td>SharePoint Online</td>
</tr>
<tr>
<td>15</td>
<td>Hightail</td>
</tr>
</tbody>
</table>

Source: SkyHigh Cloud Adoption Report Q4 2015
“I love having to re-enter my credentials multiple times daily.”

- No one ever
APM Webtop

Cloud Apps

Local Apps

One Login.

Network Tunnels

VDI Apps
SAML Process (IdP Initiated)

1. User requests SSO service from IdP
2. IdP Authenticates User
3. IdP Returns signed SAML assertion
4. User POSTs assertion to SP
5. Access granted based on assertion subject
F5 SAML IdP Configuration Elements

- **SP Connector**
  - Defines how to find and speak to an SP Service

- **IdP Service**
  - Receives AuthN requests, issues assertions

- **Virtual Server**
  - Listens for incoming connections, delivers webtop, proxies the user to local resources

- **SAML Resource**
  - Creates Icon to Appear on Webtop

- **Webtop**
  - Displays a list of resources for the user to select from

- **Access Policy**
  - Defines criteria for allowing or denying access to a resource
Simplify federation with common SaaS apps

- Office 365
- Salesforce.com
- Workday
- Amazon Web Services
- Concur
- Service Now

- Jive
- Wombat
- Zendesk
- Webex
- Google Apps
F5 & SAML (Ingress & Egress)
APM: Your SSO/Federation Swiss Army Knife

So whether you are ...

Two-Factor Auth
APM: Your SSO/Federation Swiss Army Knife

So whether you are ...

Kerberos/NTLM

Two-Factor Auth

SAML

SaaS
APM: Your SSO/Federation Swiss Army Knife

So whether you are ...
APM: Your SSO/Federation Swiss Army Knife

Scalable Access Gateway
Consolidates into a single platform:
- Remote Access
- Web Access Management
- Mobile connectivity
- Identity Federation
- Secure Web Gateway

Single point of control for access policy enforcement
<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>09.00am</td>
<td>REGISTRATION AND WELCOME COFFEE – NETWORKING WITH SPONSORS</td>
</tr>
<tr>
<td>11.00am</td>
<td>COFFEE BREAK – NETWORKING WITH SPONSORS</td>
</tr>
<tr>
<td>11.30am</td>
<td>MORNING PLENARY SESSION – PART 1</td>
</tr>
<tr>
<td>01.00pm</td>
<td>LUNCH &amp; NETWORKING WITH SPONSORS</td>
</tr>
<tr>
<td>02.30pm</td>
<td>AFTERNOON TRACKS</td>
</tr>
<tr>
<td>02.30pm</td>
<td>AFTERNOON TRACKS</td>
</tr>
<tr>
<td>03.45pm</td>
<td>AFTERNOON TRACKS</td>
</tr>
<tr>
<td>03.45pm</td>
<td>AFTERNOON TRACKS</td>
</tr>
<tr>
<td>4.45pm</td>
<td>CLOSING COCKTAIL</td>
</tr>
</tbody>
</table>
Thank you!