Cybersecurity Summit 2018
Access Management: The Glue between Business Value and Security

Kent Purdy
Product Marketing Manager

Chan Yoon
Director of Product Management
Technology disruptors coupled with the continued increase in Cyber crime sophistication, is driving change *in Access and Authentication capabilities*.

- **68%** security leaders regard “achieving and maintaining regulatory compliance” as a critical priority. (Forrester 2017)
- **59%** technology decision makers adopting a hybrid cloud model. (Forrester 2017)
- **56%** of CEOs say that DTS has increased profits. (Gartner 2017)

“Although consumer technologies create new risks for the enterprise, eliminating their use is increasingly difficult, and impractical,” said Rich Mogull, research vice president for Gartner.
Digital Transformation Priorities

- Mobile development #1
- Mobile to back-end system integration
- “Platformization” of IT
- Hybrid integrations
- Maturing digital user interactions
Access Complications

Issues with current approach:

- View business as a place not an activity
- Can’t efficiently scale to meet the demands of a modern architecture
- Identities not centrally managed
- Siloed & disparate access and authentication implementations resulting in point based, duct tape solution architecture
The Growing API Economy

1960 - 1980
Limited Exchange

1980 - 1990
Interfaces

1990 - 2000
Middleware

2000 - today
API Layers

Source: ProgrammableWeb
Access and authentication should be monitored throughout the session.

Multiple forms of authentication should be leveraged dependent on perceived risk.

Access Should Never Be a One Time Thing
A New Phase of Access

“We are in the very early phases of this new stage in the evolution of IAM, where the leading edge of innovation has moved beyond linear workflow process automation to closed-loop, fully digital processes.”

Gartner Research, The Emerging Architecture of Modern Identity, 04 August 2015, Mary Ruddy
New Ways to Deliver Frictionless Access
It’s Determining the Matter of …

- **Who or What** is attempting access?
- **Where** are they *(or it)* located right now?
- **Where** are they *(or it)* normally located?
- **What** are they *(or it)* trying to access?
- **What** is the associated risk?
- **When** should access be granted?
- **What else** have they *(or it)* accessed lately?
- Does this reflect *past behavior(s)*?
How Identity Powers Access
The Micro Focus Platform – **Identity Powers Access**

- **Identity**
  - Governance
  - Provisioning
  - Privileged Identity
  - Self Service
  - Social Registration
  - Unified Identity
  - Roles
  - Analytics
  - Data Security

- **Access**
  - Risk Based Access
  - SSO
  - Privileged Access
  - Federation
  - Multi-Factor
  - Mobile
  - Social Access
  - Analytics
  - Data Security

- **Insight**
  - SIEM
  - File Integrity
  - Privileged Monitoring
  - Configuration Monitoring
  - Change Monitoring
  - Analytics
  - Data Security

**Cloud**

**Hybrid**

**On-Premise**

<table>
<thead>
<tr>
<th>Users</th>
<th>Devices</th>
<th>Things</th>
<th>Services</th>
</tr>
</thead>
</table>

**Integrations**

- Salesforce
- SAP
- Azure
- Amazon Web Services

**Technology Stack**

- Cloud
- Hybrid
- On-Premise
Onboarding Identities

Frictionless onboarding

- Users self register
- Social attributes imported

Identity matching

- Social to internal
- Use verified identity for controlled interaction

Sign up

Please create an account
Self-service User/Device Administration

Self-service authentication management

- Register
- Password Reset
- Account lockout
- Unregister
Relationships Drive Adaptive Access and Authentication

**DEVICES**
- Mobiles
- Browsers
- Computers

**IDENTITY SOURCES**
- Social
- Internal Directories
- Federations
- Cloud

**APPLICATIONS**
- Internal system
- SaaS
- Old heritages
- In-house development
- API's

**LEGAL AND REGULATORY REQUIREMENTS**
- Secure Access
- Strong Authentications
Risk-Based Adaptive Access Control

Risk Engine

- External Parameters
- Geolocation
- IP Address
- Profile
- History
- HTTP Headers
- User Cookies
- Device ID

Calculated Level of Risk
- Low risk
- Medium Risk
- High Risk

Allow Access
- Confirm Step-up
- Deny Access

Self-Service Account Management

Users

Devices

Things

Services
# Adaptive Access

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Username, Password</th>
<th>HTTP Header</th>
<th>IP Address &amp; History</th>
<th>Geo Location</th>
<th>Known Cookie</th>
<th>Device Fingerprint</th>
<th>Last Login Cookie</th>
<th>User Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Pattern</td>
<td>Entered</td>
<td>Inline with Configuration</td>
<td>Within Valid Range</td>
<td>Suspect location</td>
<td>Valid Cookie</td>
<td>Valid Device Fingerprint</td>
<td>Login from last used device present</td>
<td>Valid user attributes</td>
</tr>
</tbody>
</table>
### Adaptive Access

**Risk Score**

![Image](image_url)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Username, Password</th>
<th>HTTP Header</th>
<th>IP Address &amp; History</th>
<th>Geo Location</th>
<th>Known Cookie</th>
<th>Device Fingerprint</th>
<th>Last Login Cookie</th>
<th>User Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entered</td>
<td>Entered</td>
<td>Within Valid Range</td>
<td>Suspect location</td>
<td>Valid Cookie</td>
<td>Valid Device Fingerprint</td>
<td>Login from last used device present</td>
<td>Valid user attributes</td>
<td></td>
</tr>
</tbody>
</table>

132
## Adaptive Access

### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Username, Password</th>
<th>HTTP Header</th>
<th>IP Address &amp; History</th>
<th>Geo Location</th>
<th>Known Cookie</th>
<th>Device Fingerprint</th>
<th>Last Login Cookie</th>
<th>User Attributes</th>
</tr>
</thead>
</table>

### Current Pattern

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entered</td>
<td>Different values in header field</td>
</tr>
<tr>
<td>Request</td>
<td>Different IP address with no history</td>
</tr>
<tr>
<td>Location</td>
<td>Suspect location</td>
</tr>
<tr>
<td>Cookie</td>
<td>Not sure</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Not determined</td>
</tr>
<tr>
<td>Cookie</td>
<td>No cookie present</td>
</tr>
<tr>
<td>User Attributes</td>
<td>Valid user attributes</td>
</tr>
</tbody>
</table>
## Advanced Authentication

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Smartphone</td>
<td>Multi-Tenant</td>
<td>Windows CP</td>
</tr>
<tr>
<td>Geo-Fencing</td>
<td>- Support Multi Divisions or Clients - Tenant Dashboard</td>
<td>Citrix Devices</td>
</tr>
<tr>
<td>FIDO U2F</td>
<td>FIPS 140-2</td>
<td></td>
</tr>
<tr>
<td>Bluetooth</td>
<td>“FIPS Insider” Via OpenSIL FIPS Module</td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td>ADFS</td>
<td></td>
</tr>
<tr>
<td>Google Auth</td>
<td>SAML2</td>
<td>Mac OS X</td>
</tr>
<tr>
<td>Microsoft Live</td>
<td>RADIUS</td>
<td>Citrix SSO</td>
</tr>
<tr>
<td>Voice OTP</td>
<td>Internal RADIUS Server and RADIUS client</td>
<td></td>
</tr>
<tr>
<td>SMS OTP</td>
<td>REST</td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Light Weight Programming Interface</td>
<td></td>
</tr>
<tr>
<td>Soft Token</td>
<td>OAuth2</td>
<td>Linux PAM</td>
</tr>
<tr>
<td>Hard Token</td>
<td>Open Authorization Token / Open ID Support</td>
<td>Card Tool</td>
</tr>
<tr>
<td>PKI – PKCS7</td>
<td>AAaaS</td>
<td></td>
</tr>
<tr>
<td>PKI – PKCS11</td>
<td>MFA Available As-A-Service</td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Factor Caching</td>
<td></td>
</tr>
<tr>
<td>NFC</td>
<td>Impersonation</td>
<td>RDP/Term Svcs</td>
</tr>
<tr>
<td>RFID</td>
<td>Linked Account Authenticator</td>
<td>Off-Line</td>
</tr>
<tr>
<td>Emergency PW</td>
<td>HTTP Proxy</td>
<td></td>
</tr>
<tr>
<td>Email OTP</td>
<td>Secure AA Behind Network with Proxy</td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Dashboard</td>
<td></td>
</tr>
<tr>
<td>RADIUS Client</td>
<td>Customization</td>
<td>Tap-N-Go</td>
</tr>
<tr>
<td>Captcha</td>
<td>- Custom Mobile App - Brand logo - Set Security</td>
<td>BYOD</td>
</tr>
<tr>
<td>Voice Call</td>
<td>App Policy</td>
<td></td>
</tr>
<tr>
<td>Challenge</td>
<td>- Mobile App Policy Enforcement</td>
<td></td>
</tr>
<tr>
<td>PIN Code</td>
<td>Localization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- User facing interface strings all localized</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Kerberos</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSO with Kerberos Ticket Systems To Consoles</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ConnectWise</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Partner Dashboard Integration for RMM- to-MSPs</td>
<td></td>
</tr>
</tbody>
</table>

### Standards and Integrations

- FIDO U2F
- NFC ISO/IEC
- HSPD-3.2
- OAuth2
- Kerberos
- Windows
- Mac OS X
- Linux
- ADFS on Cloud
- Google Auth
- Microsoft Live
- OATH
- Swisscom
- MFP
- BYOD
Micro Focus Access Management

- Single Sign-On
- Application Federation
- Access Control
- Analytics
- Multi-Factor Authentication
- API and Services Access
- Consumer Access
- Social Identity
- Risk-Based Access
- Mobile Access
- Self Service
Identity Powers Access

- Takes a holistic approach to identity and access management
- Adapt to the right authentication experience
- Integrate the complex for the best access experience
- Maximize your existing investment and while innovating the new
- Complete foundation of standards with capacity to enhance
- Competitive TCO
## Customer Success

<table>
<thead>
<tr>
<th>Self-Service</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State Government</strong></td>
<td><strong>Worldwide Chemistry and Materials Powerhouse</strong></td>
</tr>
<tr>
<td><em>Servicing over 1,000,000 Citizens SSO and Self-Service</em></td>
<td>113,830 Global Employees</td>
</tr>
<tr>
<td>Centrally Managed Identities with self-service account management</td>
<td>Synchronized global identities with SSO to internal and external apps and services</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access &amp; Authentication</th>
<th>Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Healthcare Services Provider</strong></td>
<td><strong>Federal Tax and Services Organization</strong></td>
</tr>
<tr>
<td>2,800 employees and 500,000 <em>customers</em></td>
<td>21 Million Users</td>
</tr>
<tr>
<td>True Multi Factor Authentication</td>
<td>Secure access to a complex, hybrid IT environment</td>
</tr>
</tbody>
</table>
The Micro Focus Approach – **Identity Powers Security @ Scale**

- Governance
- Provisioning
- Privileged Identity
- Self Service
- Social Registration
- Unified Identity
- Roles
- Analytics

- Risk Based Access
- SSO
- Privileged Access
- Federation
- Multi-Factor
- Mobile
- Social Access
- Analytics

- SIEM
- File Integrity
- Privileged Monitoring
- Configuration Monitoring
- Change Monitoring
- Analytics
Thank You.