Identity & Access Governance: Key to Security or Completely Useless?

Jackson Shaw
Sr. Dir. of Product Management
Dell Software Group
Dell leadership in software

+$1.5B software revenue (approx. based on run rate)

+6,000 team members

2M user community members

90% of Global 1000 are Dell Software customers

+1M customers

EMA Radar Report Value Leader for Boomi Cloud Integration

NSS Labs Highest overall protection Next-Gen Firewall

Gartner 9 Magic Quadrants

1,600 + software engineers

2,500 + software sales

+$1.5B software revenue

+6,000 team members

2M user community members

90% of Global 1000 are Dell Software customers

+1M customers

EMA Radar Report Value Leader for Boomi Cloud Integration

NSS Labs Highest overall protection Next-Gen Firewall

Gartner 9 Magic Quadrants

+$1.5B software revenue

+6,000 team members

2M user community members

90% of Global 1000 are Dell Software customers

+1M customers

EMA Radar Report Value Leader for Boomi Cloud Integration

NSS Labs Highest overall protection Next-Gen Firewall

Gartner 9 Magic Quadrants

+$1.5B software revenue

+6,000 team members

2M user community members

90% of Global 1000 are Dell Software customers

+1M customers

EMA Radar Report Value Leader for Boomi Cloud Integration

NSS Labs Highest overall protection Next-Gen Firewall

Gartner 9 Magic Quadrants
85% of businesses said their organizations will use cloud tools moderately to extensively in the next 3 years. 

68% of spend in private cloud solutions. 

- Bain and Dell

Consumers will store 36% of their digital content in the cloud by 2016. 

- Gartner

Cloud implementation growth —Gartner

IaaS (41%)
Planning (27.2%)
PaaS (26.6%)
SaaS (17.4%)
BPaaS (15%)
Volume of data stored
Zettabytes
- IDC

Big data

 Enterprises and big data projects
— Informatica, May 2012

- Considering (44%)
- Planning (22%)
- Testing (13%)
- Running (20%)
Mobility

5X growth in smartphones and tablets used at work...

2010

Smartphone and tablets used at work
% of total customer type

2015

Corporate
Personal

...and source shifts from 62% / 38% corporate / personal owned to 37% corporate owned and 63% personal owned

- IDC, Dell internal analysis
57% of companies have made policy adjustments to mitigate mobile computing risks. —Ernst & Young

1/2 of sensitive information is actually protected. —IDC

79% of the surveyed companies experienced some type of significant security incident within the past year that resulted in financial and/or reputational impact

$1.1M average data loss impact for reactive organizations —McAfee
“Most of today’s security infrastructure is static – enforcing policies defined in advance in environments where IT infrastructure and business relationships are relative static. This is no longer sufficient in an environment that is highly dynamic, multisourced and virtualized, and where consumer-oriented IT is increasingly used in lieu of enterprise-owned and provisioned systems.”

- Neil MacDonald, Gartner
Towards Risk-based Adaptive Authorization

Identity Manager → AuthZ Policy → Firewall → Devices and Networks
# Authorization Policy Attributes

<table>
<thead>
<tr>
<th><strong>Static Data</strong></th>
<th><strong>Dynamic Data</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>from IAM Defines</strong> Risk Values</td>
<td><strong>from Firewall Determines</strong> Transaction Risks</td>
</tr>
<tr>
<td>Resource identity and risk tolerance</td>
<td>Specific device in use</td>
</tr>
<tr>
<td>Application Role risk tolerance</td>
<td>Device location</td>
</tr>
<tr>
<td>Role membership</td>
<td>Account in use</td>
</tr>
<tr>
<td>User/Account identity</td>
<td>Authentication strength</td>
</tr>
<tr>
<td>Device risk and ownership</td>
<td>Time of day</td>
</tr>
<tr>
<td>Business hours and risk</td>
<td>Recent device activity</td>
</tr>
</tbody>
</table>

Device Health |
Risk Evaluation and Access Allowed

<table>
<thead>
<tr>
<th>Risk policy</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>During work hours</td>
<td>0</td>
</tr>
<tr>
<td>Outside work hours</td>
<td>10</td>
</tr>
<tr>
<td>On-premises</td>
<td>0</td>
</tr>
<tr>
<td>Remote</td>
<td>10</td>
</tr>
<tr>
<td>Corporate device</td>
<td>0</td>
</tr>
<tr>
<td>BYOD managed device</td>
<td>5</td>
</tr>
<tr>
<td>Unmanaged device</td>
<td>10</td>
</tr>
<tr>
<td>“Sales Manager” role membership</td>
<td>abarney</td>
</tr>
<tr>
<td>“Sales Manager” risk tolerance</td>
<td>dsmith</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Context item</th>
<th>Risk value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current time</td>
<td>10</td>
</tr>
<tr>
<td>Location</td>
<td>0</td>
</tr>
<tr>
<td>Device status</td>
<td>0</td>
</tr>
<tr>
<td>Account name</td>
<td>abarney</td>
</tr>
</tbody>
</table>

Account risk threshold: 25
Total risk: 10
ACCESS ALLOWED
Risk Evaluation and Access Denied

<table>
<thead>
<tr>
<th>Risk policy</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>During work hours</td>
<td>0</td>
</tr>
<tr>
<td>Outside work hours</td>
<td>10</td>
</tr>
<tr>
<td>On-premises</td>
<td>0</td>
</tr>
<tr>
<td>Remote</td>
<td>10</td>
</tr>
<tr>
<td>Corporate device</td>
<td>0</td>
</tr>
<tr>
<td>BYOD managed device</td>
<td>5</td>
</tr>
<tr>
<td>Unmanaged device</td>
<td>10</td>
</tr>
<tr>
<td>“Sales Manager” role membership</td>
<td>abarney</td>
</tr>
<tr>
<td>“Sales Manager” risk tolerance</td>
<td>dsmith</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Context item</th>
<th>Risk value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current time</td>
<td>10</td>
</tr>
<tr>
<td>Location</td>
<td>10</td>
</tr>
<tr>
<td>Device status</td>
<td>10</td>
</tr>
<tr>
<td>Account name</td>
<td>abarney</td>
</tr>
</tbody>
</table>

Account risk threshold 25
Total risk 30
ACCESS DENIED

Andrew Barney
8:17pm

http://acc1.foo.com/AP

Unmanaged tablet on public network

http://acc1.foo.com/AP

Unmanaged tablet on public network
Adaptive & Context-Aware Authorization

Risk

Identity

Time of day

Volume of requests

Location

Device

Data/app Classification

History

Compliance

Cloud/SaaS
Prevent Unwanted Access

Enable Wanted Access
Identity & Access Management Market Shift

- **2002**: Provisioning SSO
- **2006**: Content Aware
- **2010**: Identity & Access Governance
- **2014**: Adaptive & Context-Aware

Business Value
Tying Governance to Enforcement

Identity and Access Governance
- Policy, entitlements, role management and self-service access request

Multi-faceted SSO, Federation & Authorization
- Web, Federated & Legacy SSO, Coarse & Fine Grained Authorization with Just-in-Time provisioning, audit and access management

Quest One Identity Manager

Quest One Cloud Access Manager

SonicWALL NGFW

Zero Touch Context-aware Adaptive Authorization
- Controlling application access at the network layer
What One Identity delivers

Improve visibility into **who has access to business-critical information**, automate provisioning and enforce access controls.

Centrally manage privileged accounts and provide **granular control and monitoring of administrator access**.

**Simplify the environment and user experience** with centralized account management.

Audit **what the users are doing** with the access they have been granted.
The One Identity advantage

- Solution simplicity
- Rapid time-to-value
- Business-driven
- Granular access controls
- Broad portfolio that is modular & integrated

Areas:
- Access Governance
- Privileged Account Management
- Identity Administration
- User Activity Monitoring
Complete identity & access management

Access Governance
Manage access to business-critical information
- Access request and certification
- Fine-grained application security
- Data access management
- Role engineering
- Automated provisioning

Privileged Account Management
Understand and control administrator activity
- Granular delegation
- Enforce Separation of Duty (SoD)
- Enterprise privilege safe
- Session management
- Keystroke logging

Identity Administration
Simplify account management
- Directory Consolidation
- AD Administration
- Virtual Directory Services
- Single Sign-on
- Strong Authentication

User Activity Monitoring
Audit user activity
- Granular AD auditing
- Permissions reporting
- Log management
- Event alerting
- Crisis resolution

One Identity
Simplify IT
Mitigate risk
Accelerate results