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

1,600 + software engineers
2,500 + software sales

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

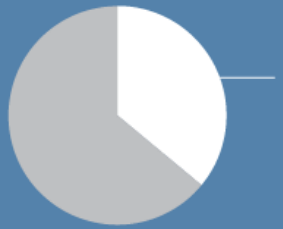
Gartner
9 Magic Quadrants

Cloud

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

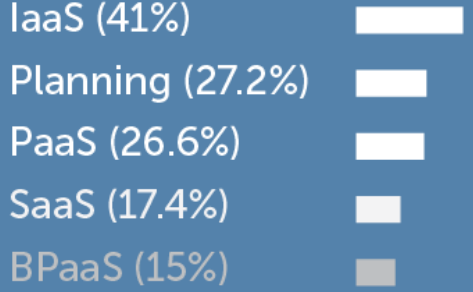
68% of spend in private cloud solutions.

- Bain and Dell

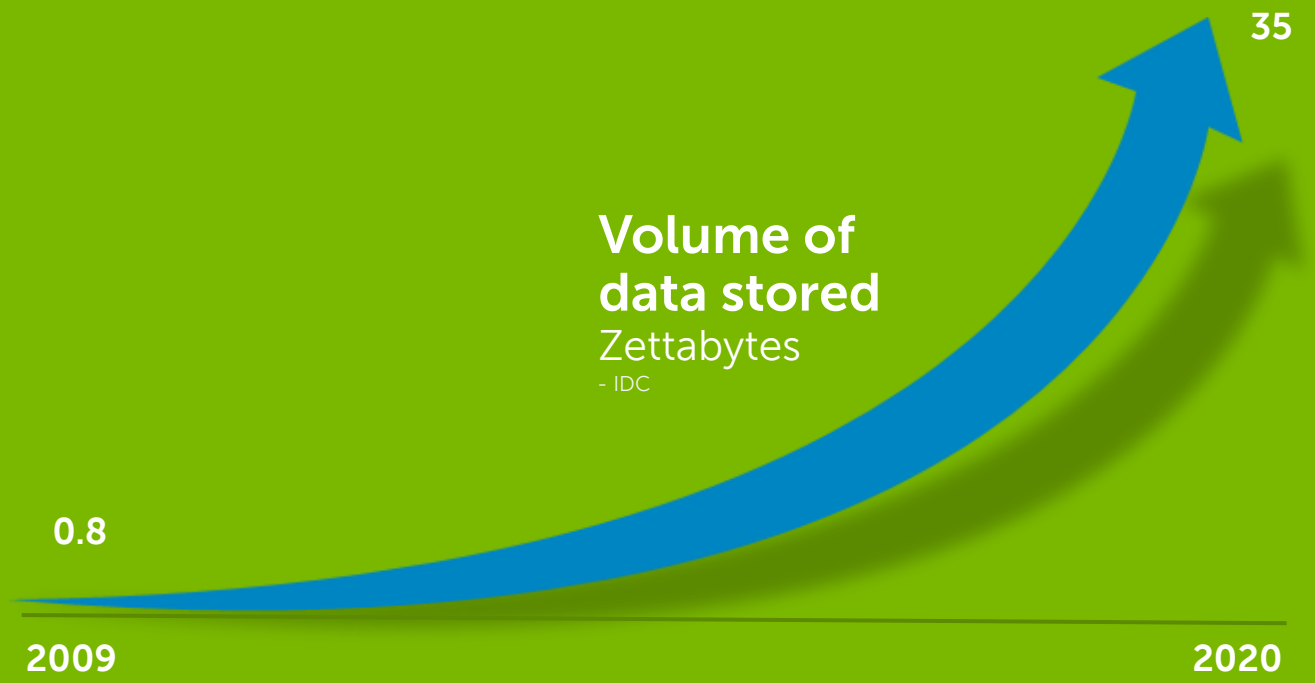


Consumers will store **36 %** of their digital content in the cloud by 2016.
—Gartner

Cloud implementation growth
—Gartner



Big data



Enterprises and big data projects

—Informatica, May 2012

Considering (44%)

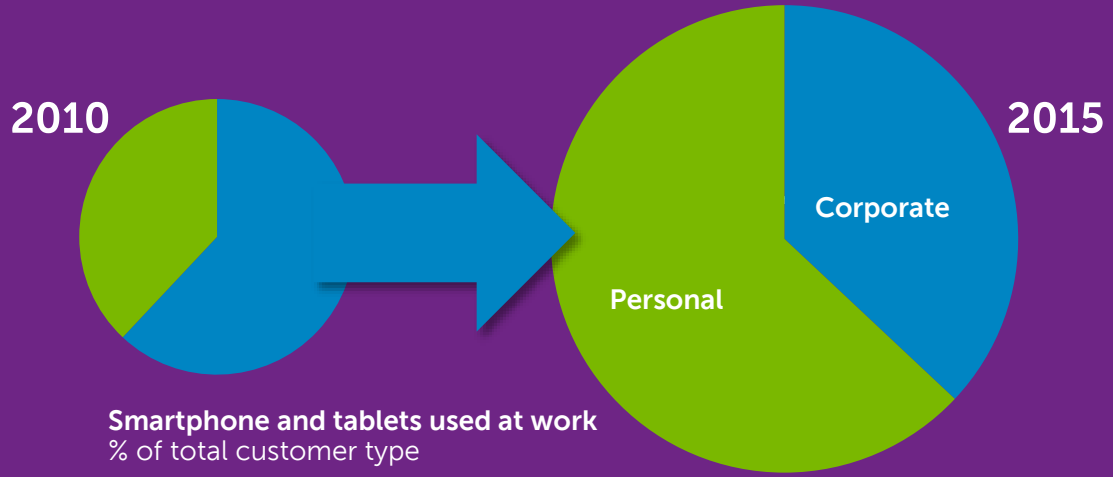
Planning (22%)

Testing (13%)

Running (20%)

Mobility

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



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

- IDC, Dell internal analysis

Security and risk mitigation

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

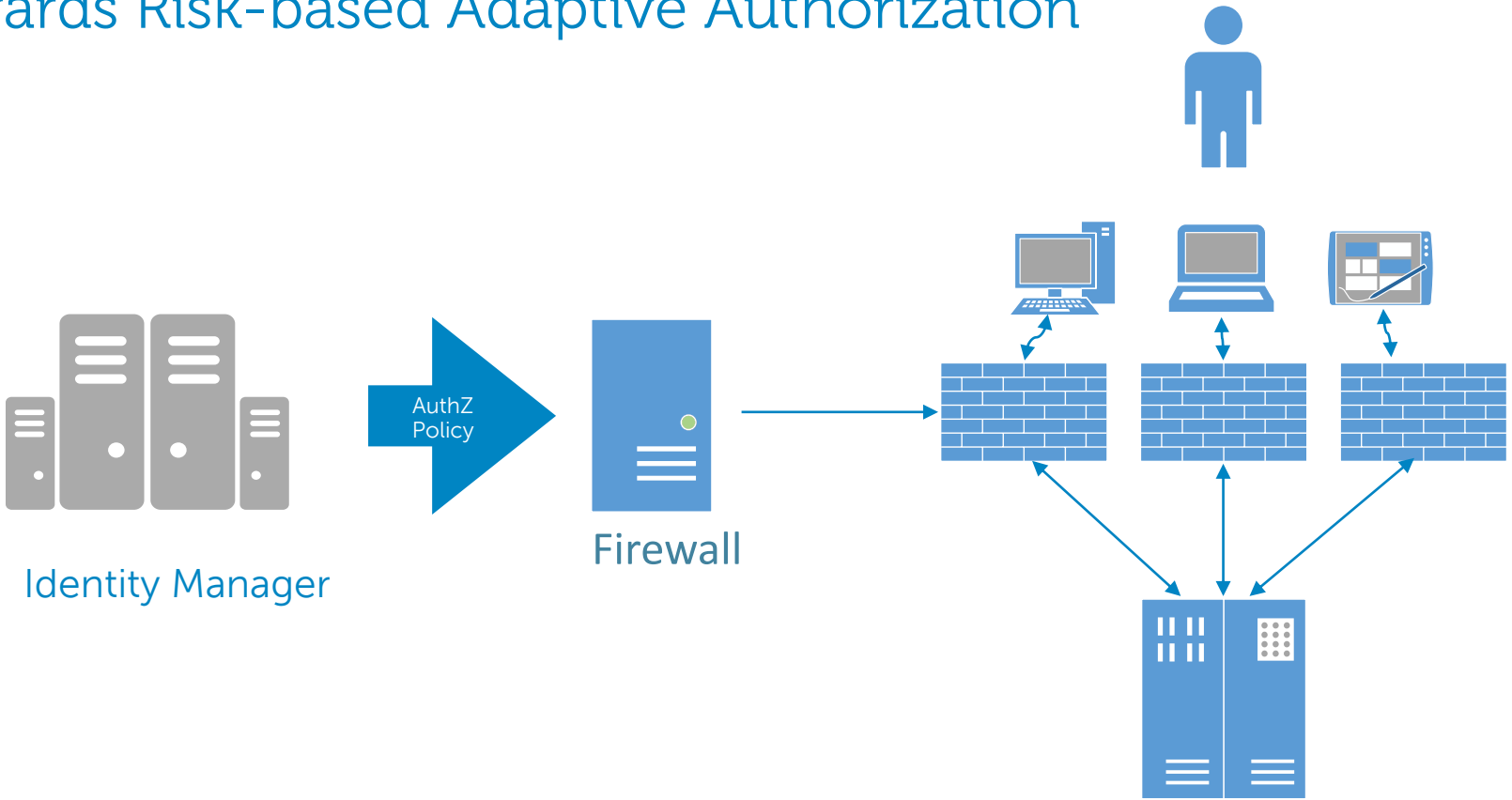
- McAfee

Adaptive Security is Required for the New Normal

"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



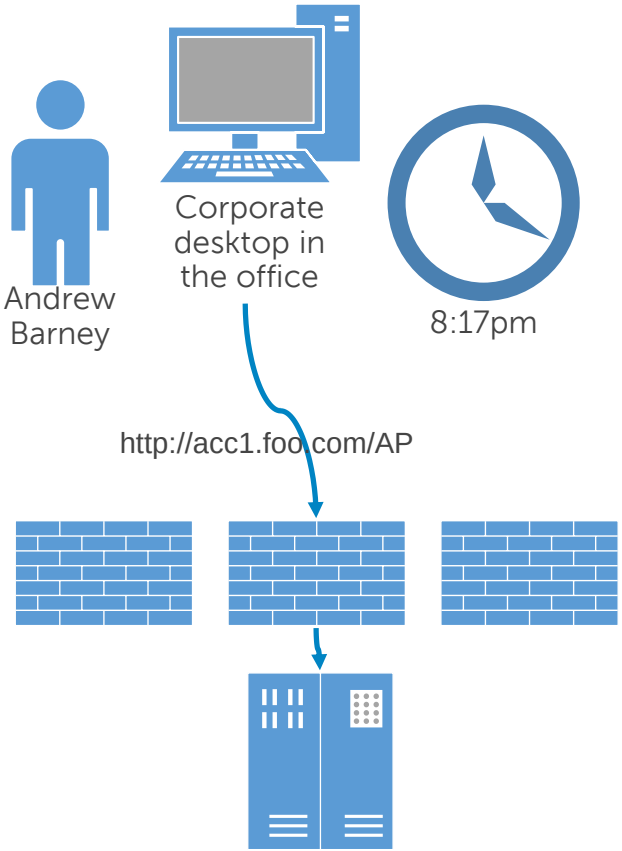
Authorization Policy Attributes

Static Data from IAM Defines **Risk Values**
Resource identity and risk tolerance
Application Role risk tolerance
Role membership
User/Account identity
Device risk and ownership
Business hours and risk
Location Risk
Device Health
Authentication Methods risk

Dynamic Data from Firewall Determines **Transaction Risks**
Specific device in use
Device location
Account in use
Authentication strength
Time of day
Recent device activity

Risk Evaluation and Access Allowed

Risk policy	Value
During work hours	0
Outside work hours	10
On-premises	0
Remote	10
Corporate device	0
BYOD managed device	5
Unmanaged device	10
"Sales Manager" role membership	abarney dsmith
"Sales Manager" risk tolerance	25

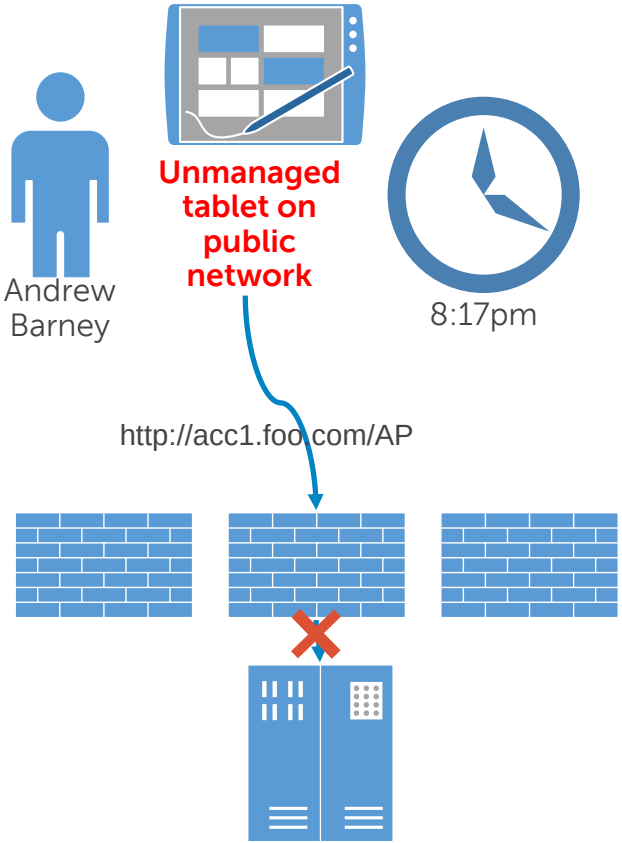


Context item	Risk value
Current time	10
Location	0
Device status	0
Account name	abarney

Account risk threshold	**25**
Total risk	**10**
ACCESS	**ALLOWED**

Risk Evaluation and Access Denied

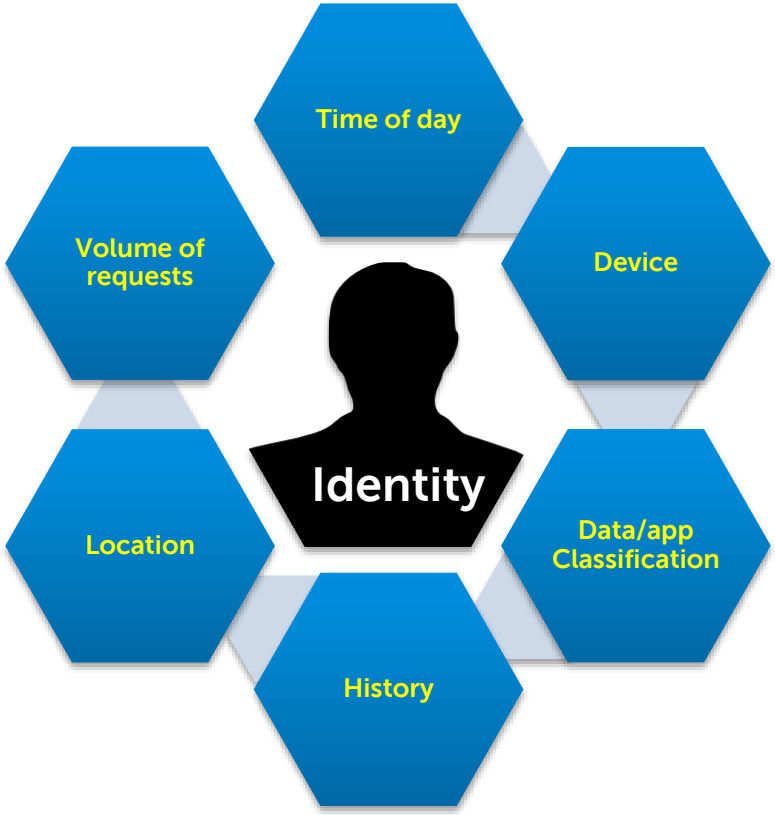
Risk policy	Value
During work hours	0
Outside work hours	10
On-premises	0
Remote	10
Corporate device	0
BYOD managed device	5
Unmanaged device	10
"Sales Manager" role membership	abarney dsmith
"Sales Manager" risk tolerance	25



Context item	Risk value
Current time	10
Location	10
Device status	10
Account name	abarney

Account risk threshold	**25**
Total risk	**30**
ACCESS	**DENIED**

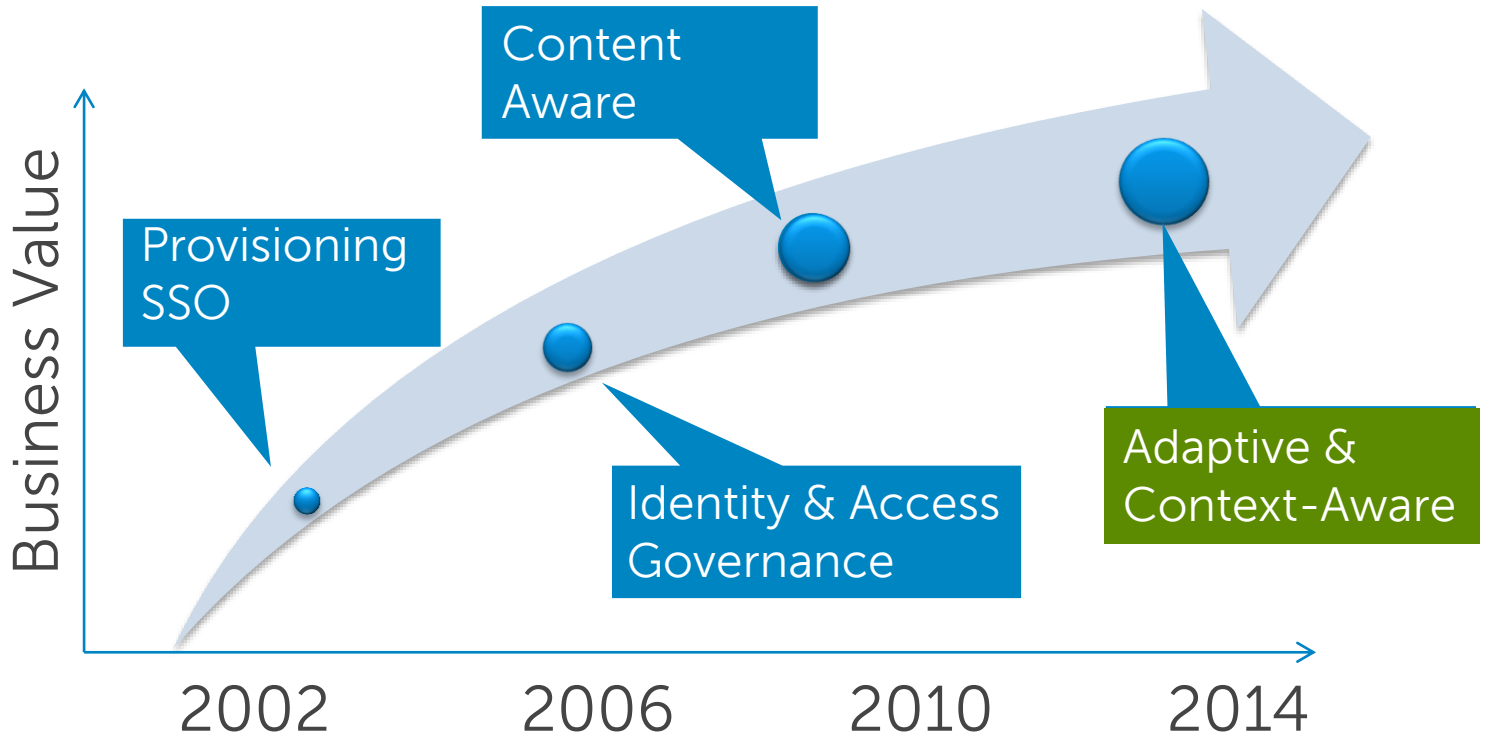
Adaptive & Context-Aware Authorization



Prevent Unwanted Access

Enable Wanted Access

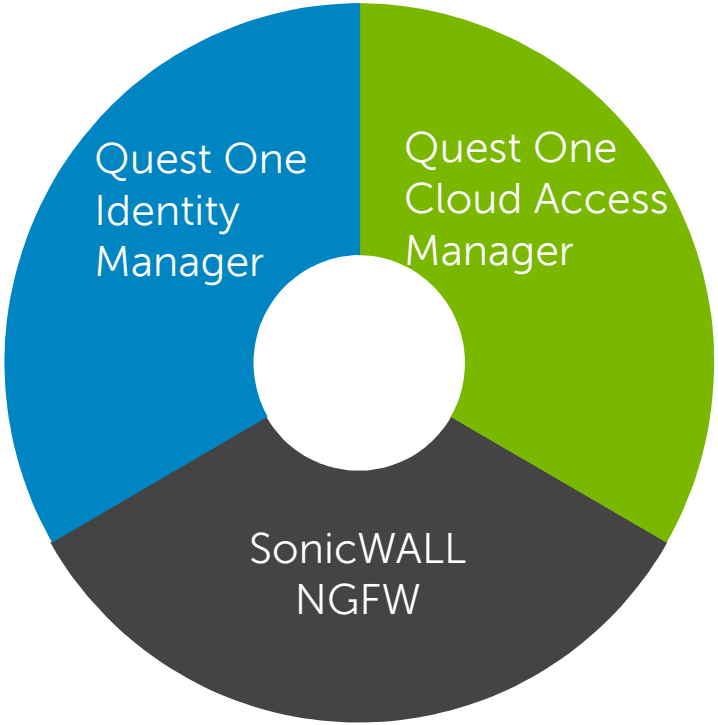
Identity & Access Management Market Shift



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

Zero Touch Context-aware Adaptive Authorization

Controlling application access at the network

What One Identity delivers

Improve visibility into **who has access to business-critical information,** automate provisioning and enforce access controls.	**Access Governance**
Centrally manage privileged accounts and provide **granular control and monitoring of administrator access**.	**Privileged Account Management**
Simplify the environment and user experience with centralized account management.	**Identity Administration**
Audit **what the users are doing** with the access they have been granted.	**User Activity Monitoring**

The One Identity advantage

Solution simplicity

Rapid time-to-value

Business-driven

Broad portfolio that is modular & integrated

Granular access controls

- 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

One Identity

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

Simplify IT

Mitigate risk

Accelerate results

The power to do more