Identity & Access Governance:

Key to Security or

Completely Useless?

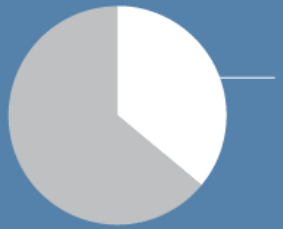
Jason Remillard
Product Manager
Dell Software Group

Cloud

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

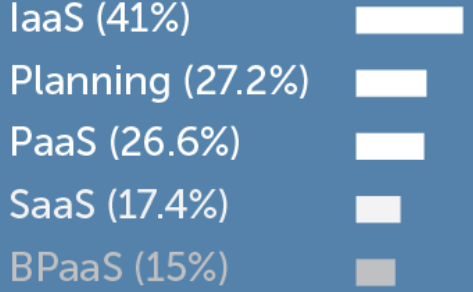
68% of spend in private cloud solutions.

- Bain and Dell

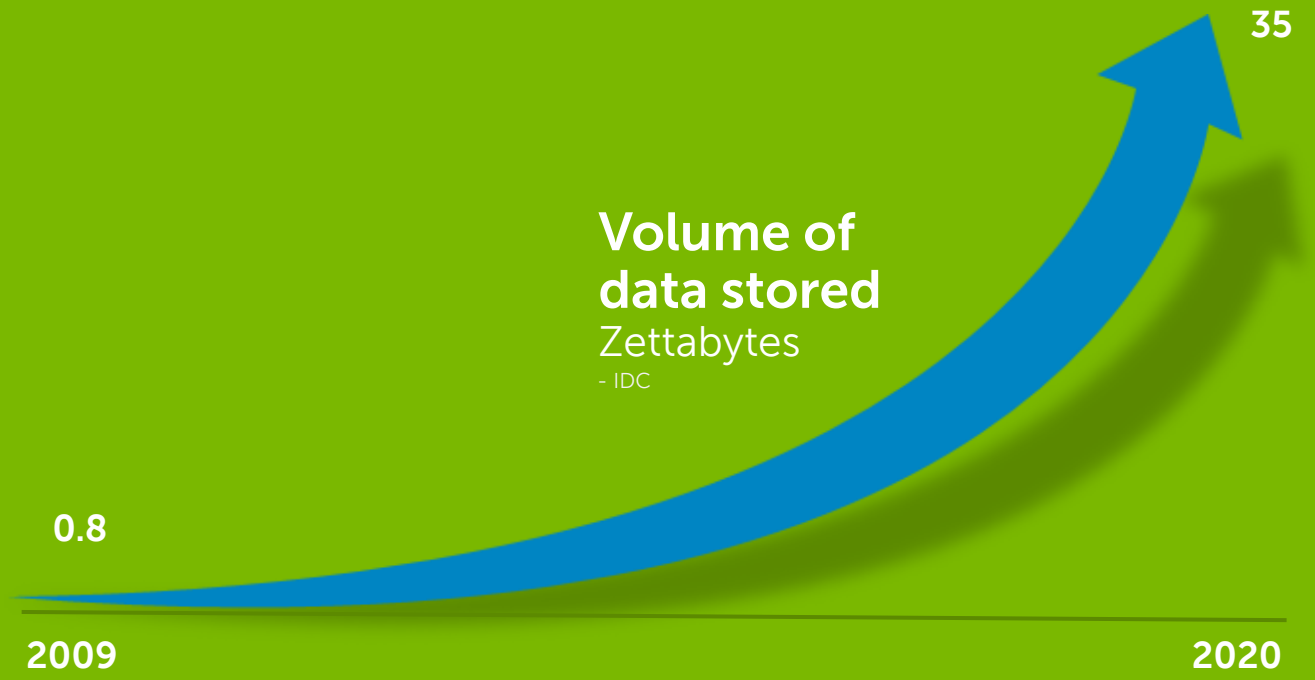


Consumers will store **36 %** of their digital content in the cloud by 2016.
—Gartner

Cloud implementation growth
—Gartner



Big data



Enterprises and big data projects

—Informatica, May 2012

Considering (44%)

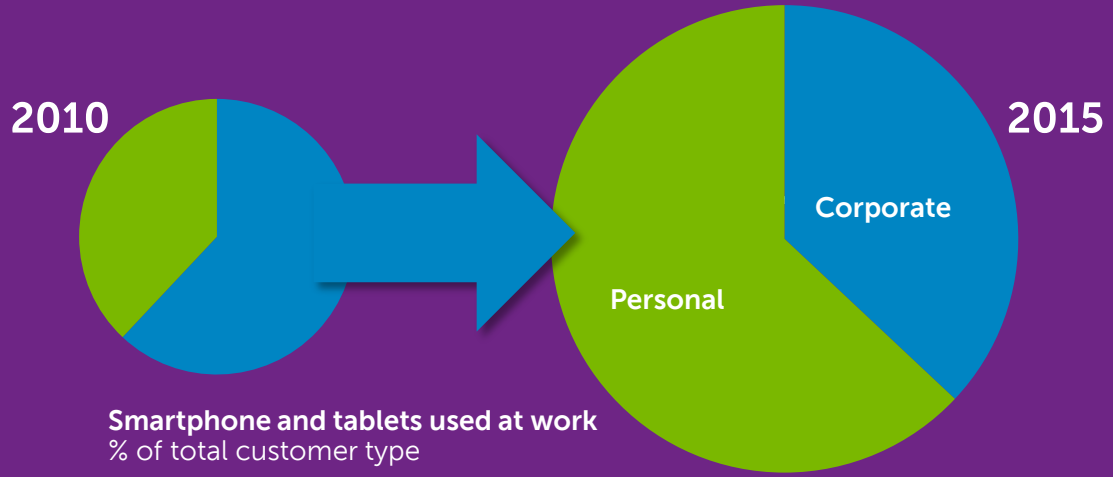
Planning (22%)

Testing (13%)

Running (20%)

Mobility

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



Smartphone and tablets used at work
% of total customer type

...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

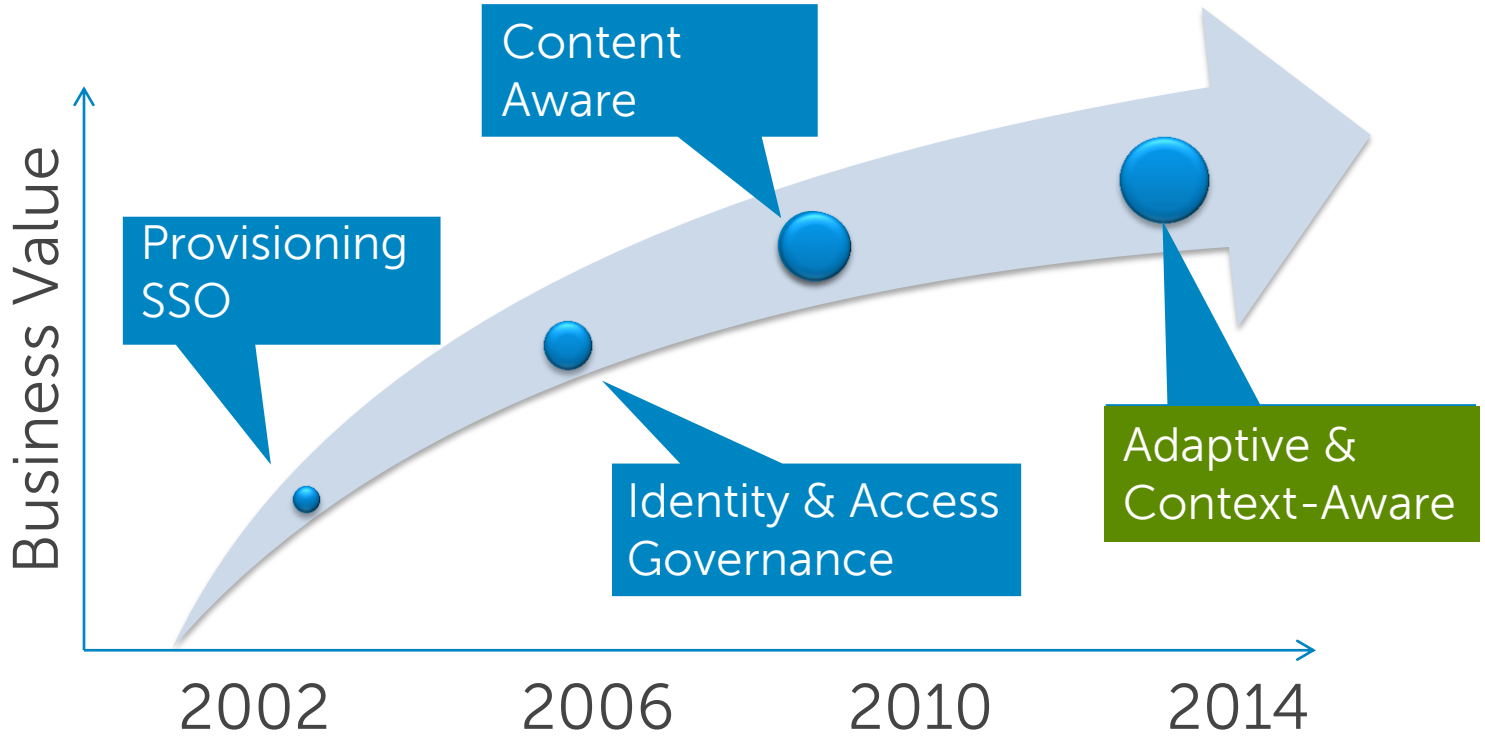
"Most of today's security infrastructure is static – enforcing policies defined in advance in environments where IT infrastructure and business relationships are relative static. This is no longer sufficient in an environment that is highly dynamic, multisourced and virtualized, and where consumer-oriented IT is increasingly used in lieu of enterprise-owned and provisioned systems."

- Neil MacDonald, Gartner

Prevent Unwanted Access

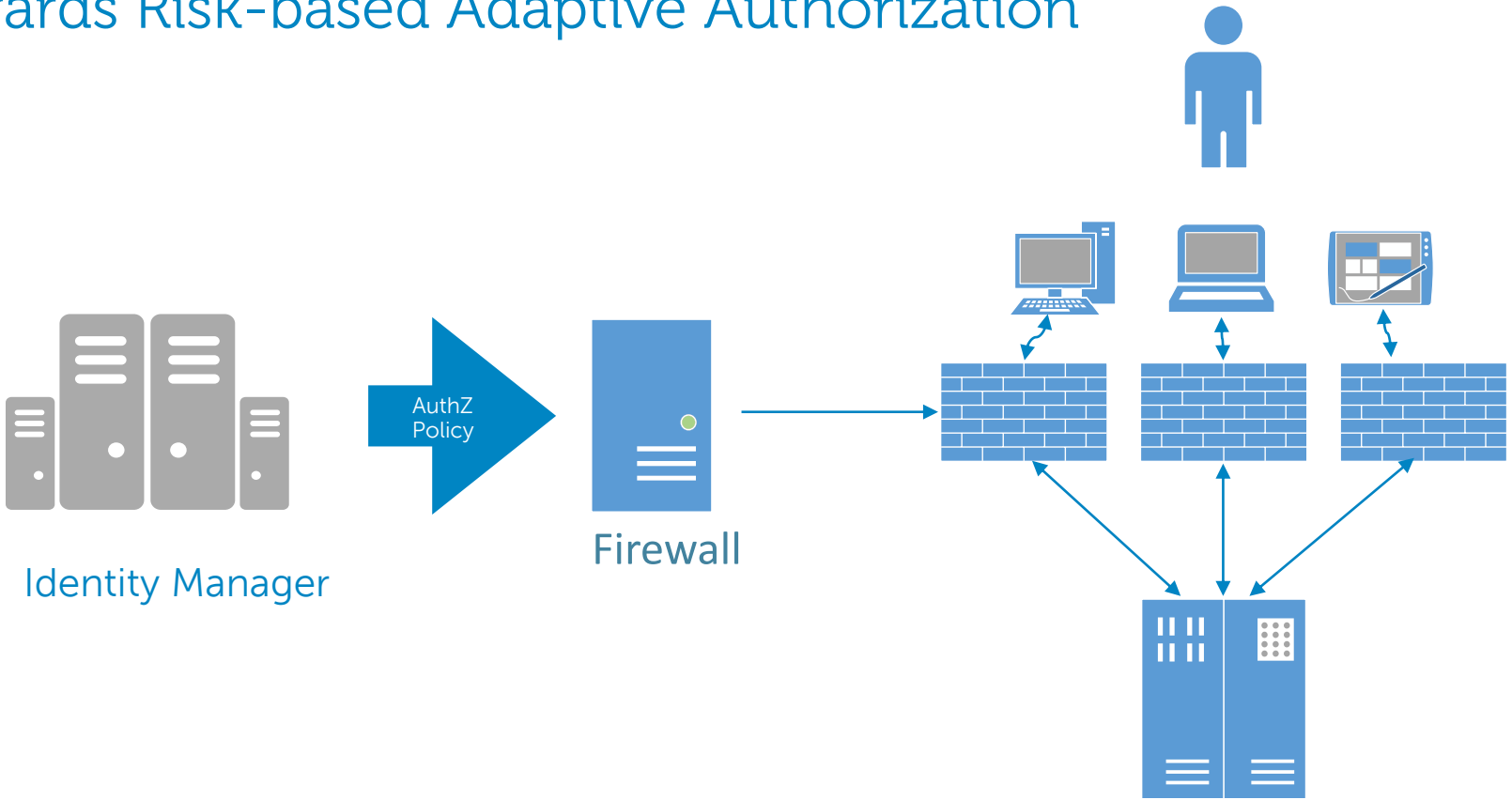
Enable Wanted Access

Identity & Access Management Market Shift



Adaptive and context-aware authorization

Towards Risk-based Adaptive Authorization



IAM

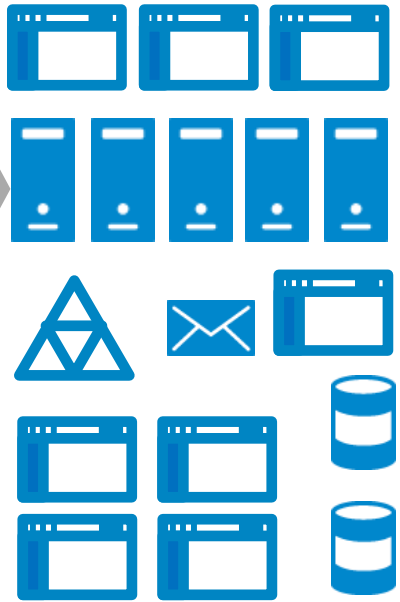
Access based on:

- Identity
- Role
- Permissions
- Attributes

Authentication

Administration

Governance

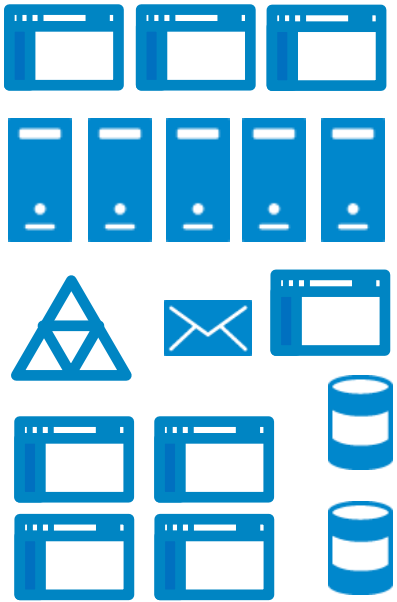


Does not consider:

- Location
- Time
- Device
- History
- Target system
- Volume
- Situational risk

Does not consider:

- Identity
- Role
- Attributes
- Permissions
- Approvals/exceptions
- Granular policy



NGFW

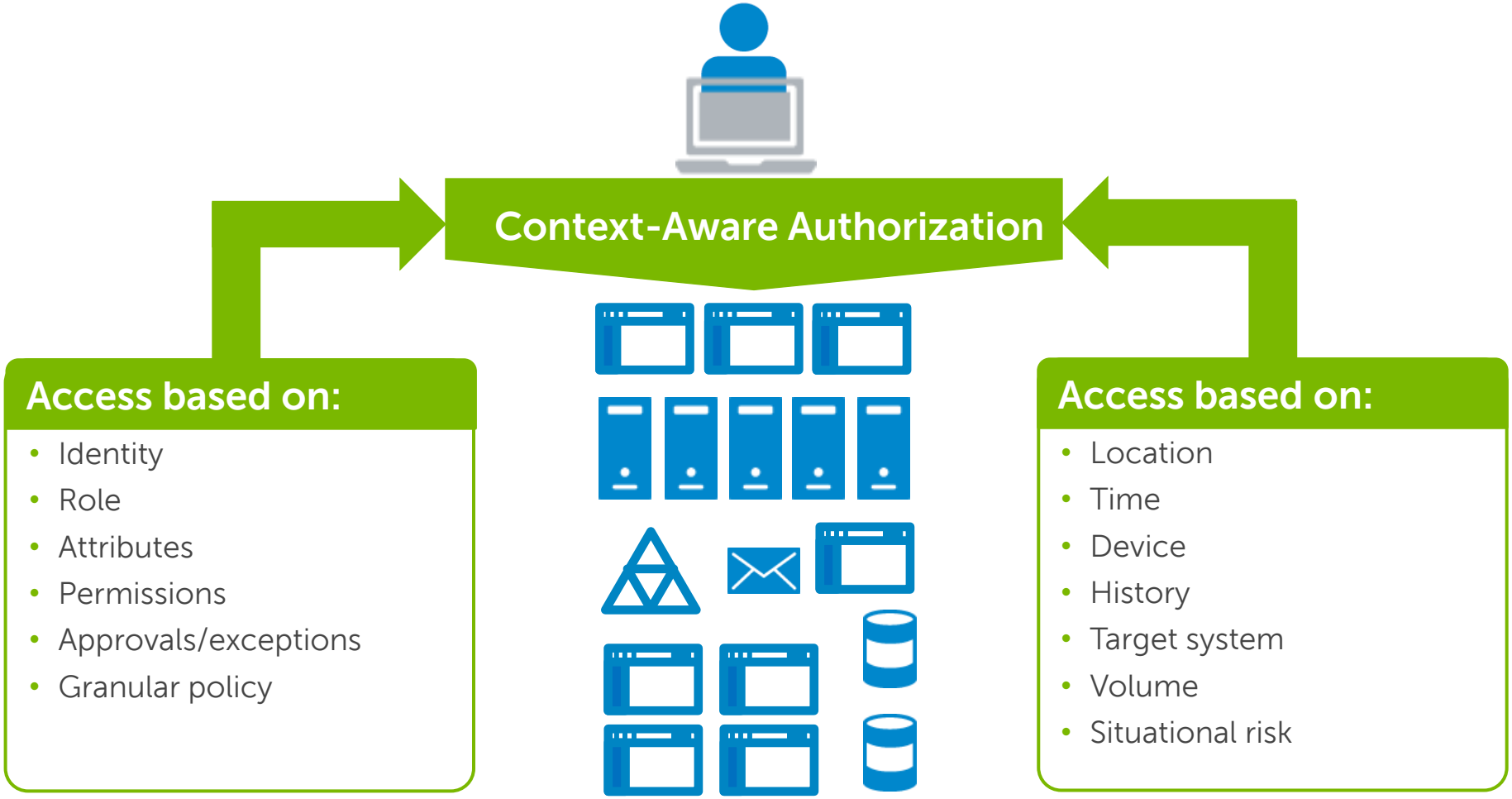
Access based on:

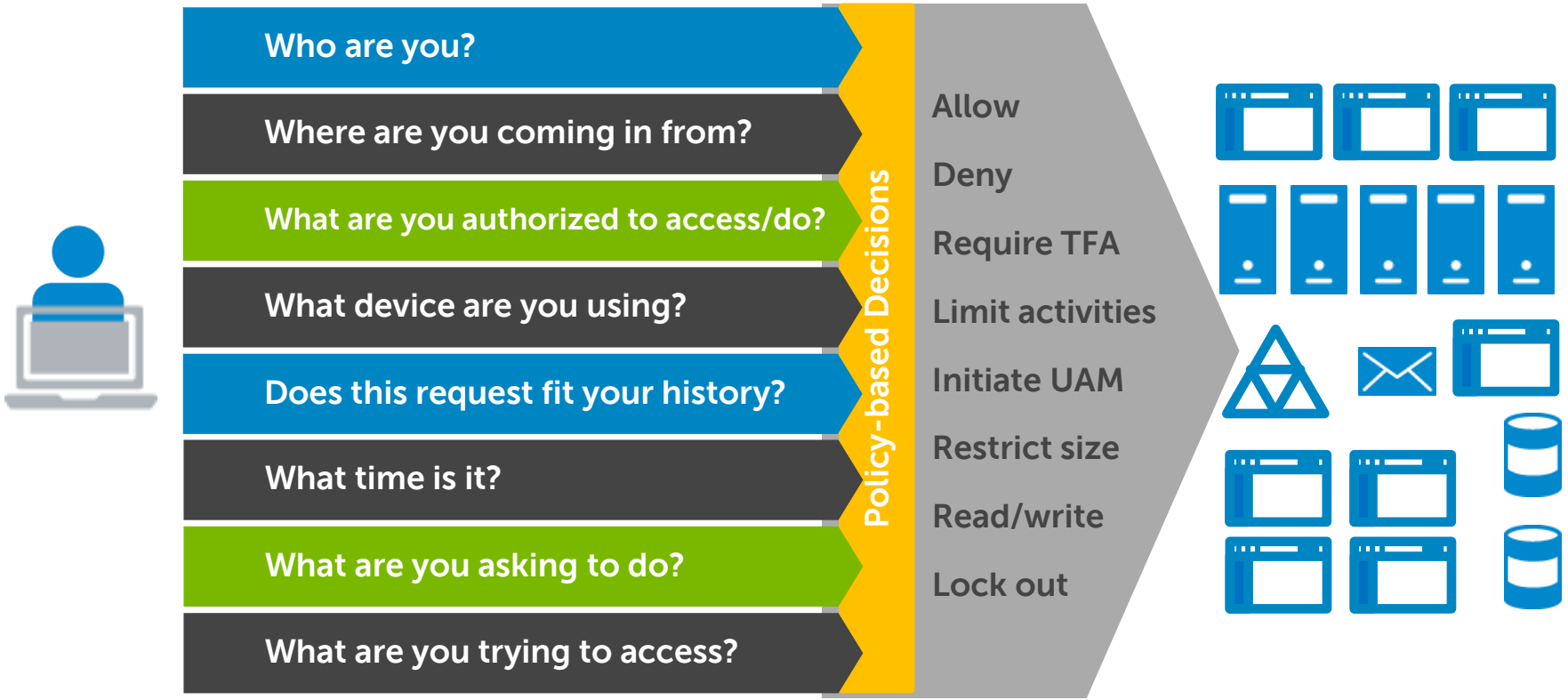
- Route
- Request
- Location
- Threat level

Application Awareness

Intrusion Protection

Allow/Deny


Context-Aware Authorization
Access based on:
• Identity
• Role
• Attributes
• Permissions
• Approvals/exceptions
• Granular policy
Access based on:
• Location
• Time
• Device
• History
• Target system
• Volume
• Situational risk


Who are you?
Where are you coming in from?
What are you authorized to access/do?
What device are you using?
Does this request fit your history?
What time is it?
What are you asking to do?
What are you trying to access?
Policy-based Decisions
Allow
Deny
Require TFA
Limit activities
Initiate UAM
Restrict size
Read/write
Lock out

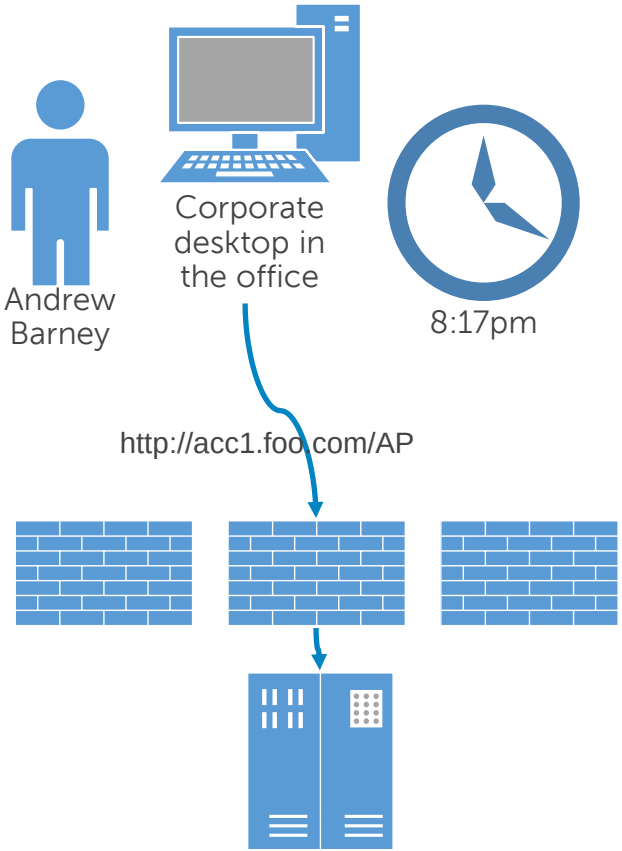
Authorization Policy Attributes

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

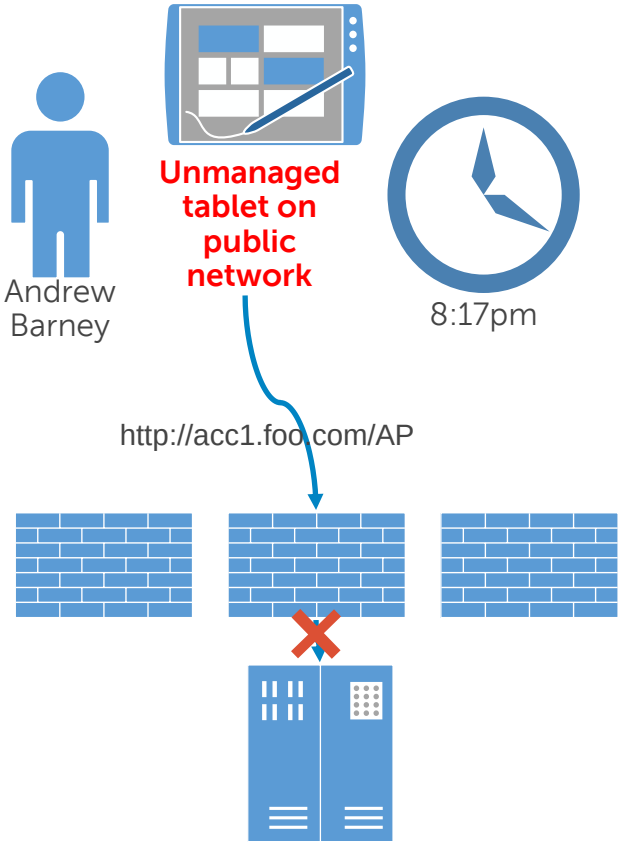


Context item	Risk value
Current time	10
Location	0
Device status	0
Account name	abarney

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**

Privileged accounts. . New Requirements

Need

1. Eliminate password sharing
2. Enforce as least-privileged model
3. Audit administrator activity
4. Assign individual accountability
5. Prove compliance

Management

1. Privilege safe
2. Delegation (sudo, root, AD etc.)
3. Session audit and keystroke logging
4. Granular policy
5. Policy audit and session audit

New Requirements

1. One-action provisioning
2. Unified policy
3. Who should do it vs. who knows how to do it
4. Privileged identity not separated from regular identity
5. Easy attestation and reporting

Moving to Governance

1. Automated and unified request and fulfillment
2. Modeled approach to roles and rules
3. Power in the hands of LOB not IT
4. Unified namespace
5. Self-service, business-driven attestation and reporting

What's in it for you?

(Privileged) Account Governance

The Administrator

- Quicker and easier access
- Insulation from the dangers of uncontrolled, unlimited rights
- Increased efficiency in administration
- Audit trail of processes and activity (CYA)
- Moves the compliance burden to the business
- Accelerates time-to-productivity

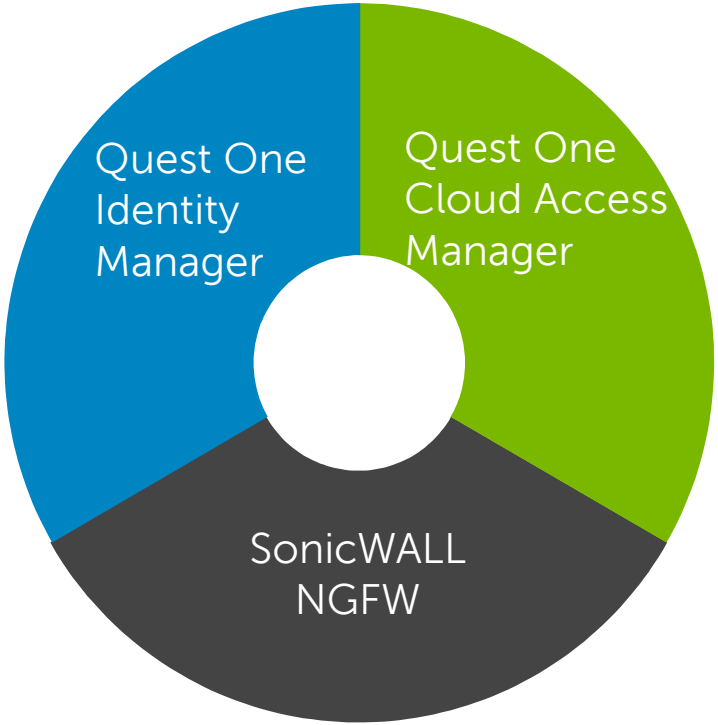
The Business

- Confidence in the appropriateness of access
- Ease of SoD
- User access and privileged access equals in the governance universe
- The right powers in the hands of the right people
- Unified everything…policy, identity, roles, rules, workflows, attestations, etc.
- Finally take control of your audits

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

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

The power to do more