Making Security a Business Enabler
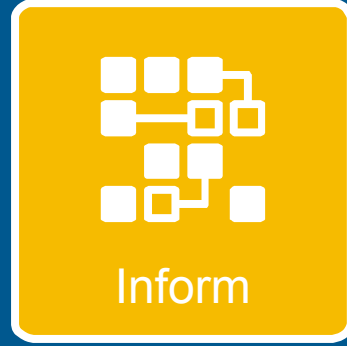
Ronny Stavem, Sales Specialist IAM, CISSP
Dell Software

Twitter: @RonnyStavem
LinkedIn: no.linkedin.com/in/ronnystavem

Technology **trends** forcing change

Transform

Connect

Inform

Protect

Cloud challenge: managing an increasing number of workloads in and across clouds
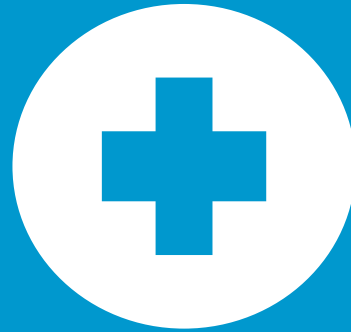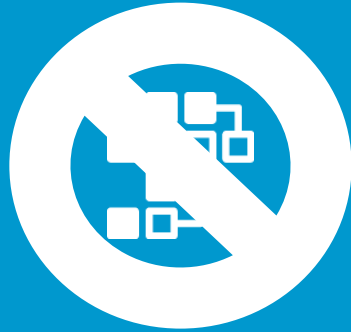**Mobility challenge:** delivering secure and robust connectivity to any device on demand
Big Data challenge: turning large volumes of diverse data into actionable insights
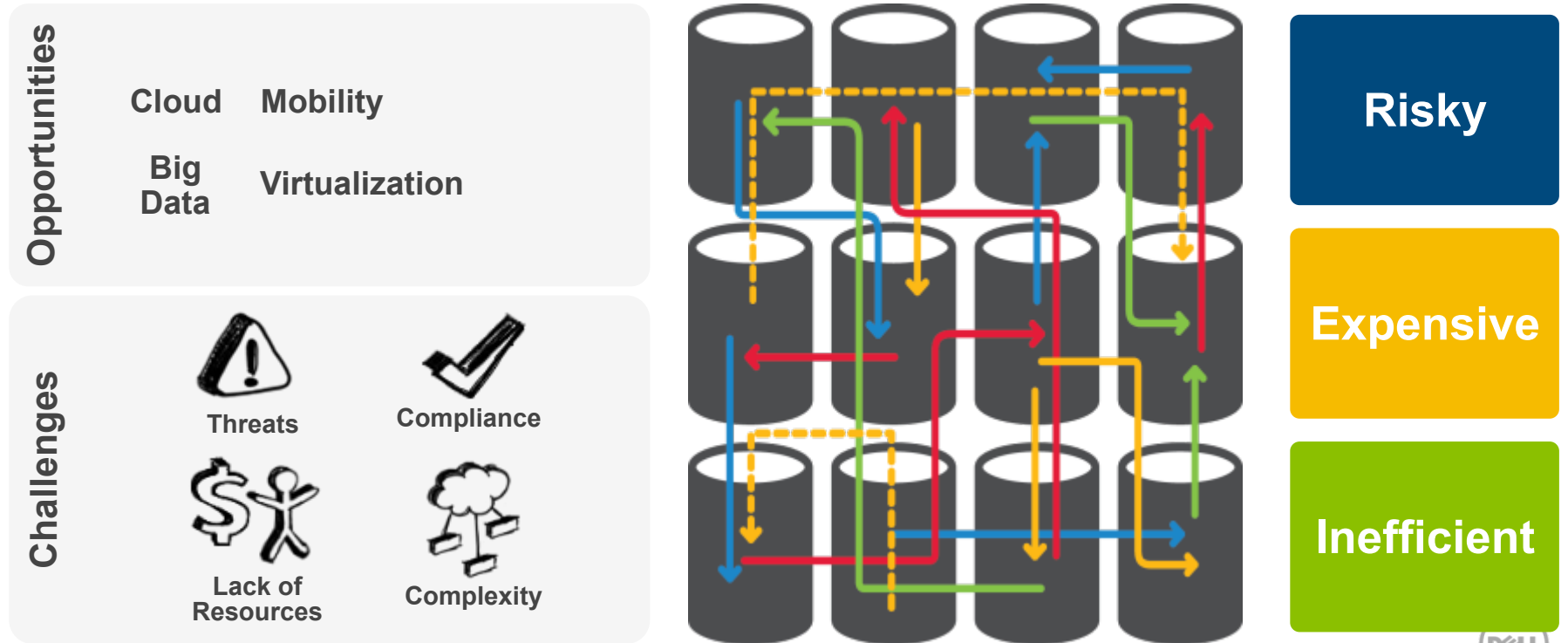**Security challenge:** protecting against ever evolving threats and vulnerabilities

DELL

In a connected world there is opportunity…

… and it's ITs job to enable the business.

Security silos create risk that impedes agility

Opportunities

Cloud   Mobility

Big
Data   Virtualization

Challenges

Threats   Compliance

Lack of
Resources   Complexity

Risky

Expensive

Inefficient

Typical barriers to agility

- Manual processes to request access

- Heavy IT involvement

- Delays due to lack of communication

- Over-provisioning to ensure access

- Ad-hoc access control

- Limit scope due to technical inconsistencies of apps

- Redefining of roles just for the new app

- Scramble to adequately train IT to support new app and users

- Restrict access to ensure security

- Divert internal resources to "watch"

AGILITY

5

There's chaos out there, and chaos means opportunity.

Marc Ostrofsky

Even in the
dark clouds of chaos
and complexity, there's a
sliver lining….even…an
Opportunity!

Business agility with Identity and Access– the future

The big question:

"How can I ensure that all users can get to all the systems and data they need to do their jobs, without compromising security, compliance, or efficiency?"

The real world gets in the way

Users — The organization no longer has tight control over how people access resources

Systems — The perimeter must be secured without impeding user access needs

Business — It is not practical to address mobility, cloud and big data security, compliance, and governance separately from other security concerns

…but…

We still need to know that however users access our systems and data they are doing it **securely**, in a **compliant** manner, and with full organizational **visibility** and **control**

Enable the business and increase security

- Enable IT to offload decisions of who needs access to what and put them in the hands of business owners who can better address them

- Empower auditors to get what they need without interrupting the business

- Enable individual workers to get swift and controlled access to the things they need to be productive

So how can IAM enable business agility??

–Self-service access request and fulfilment available to LOB

–Federation

–Contextual authentication

–Single sign-on

–Enterprise provisioning

–Role engineering

–Web access management

–Privileged account management and governance

Your IAM project can solve today's (and tomorrow's) security threats, and also add business value by increasing operational agility

Hitting close to home

Sometimes just keeping your head above water is challenging enough

27

A typical enterprise end user must access 27 different applications*

A typical enterprise user has a minimum of 6 enterprise-issued passwords.*

6

A day & a half

On average it takes a day and a half to fully provision a new user*
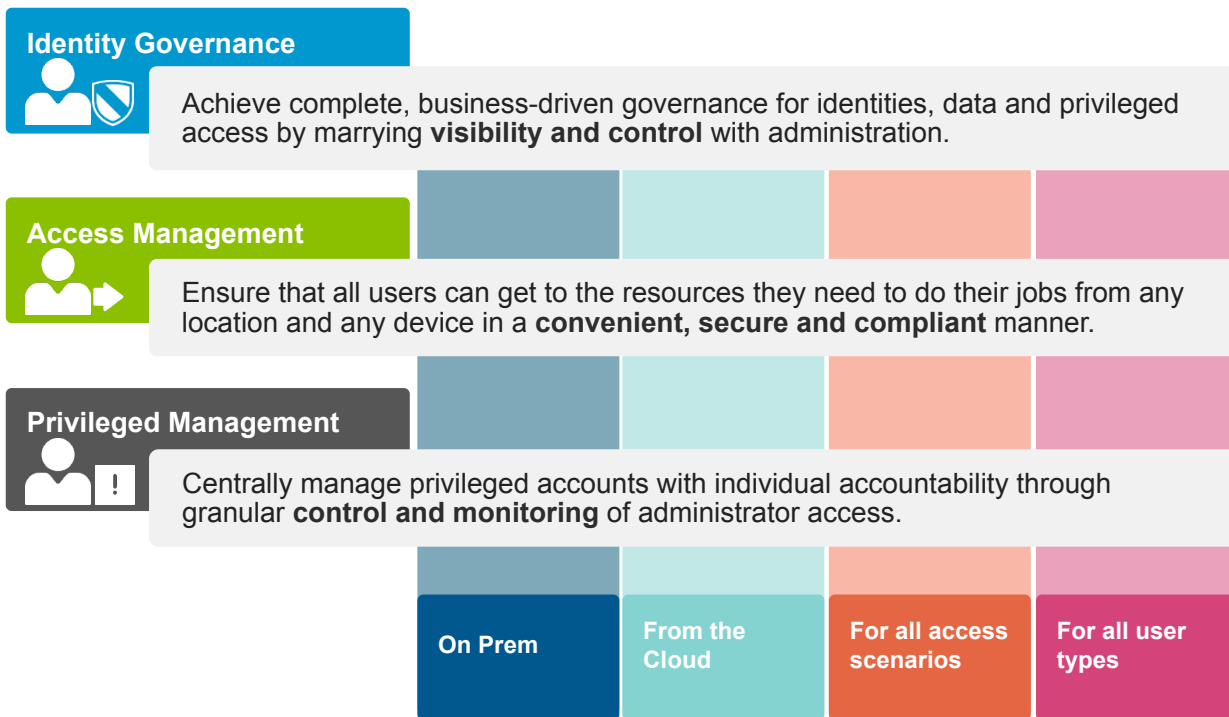
More than half a day

On average it takes more than half a day to de-provision a user*

- How long until a new user is FULLY provisioned in your organization?

- How many former employees still have access to your stuff?

- How many different IT people/teams must get involved in provisioning/de-provisioning?

*Source: Aberdeen Group Research
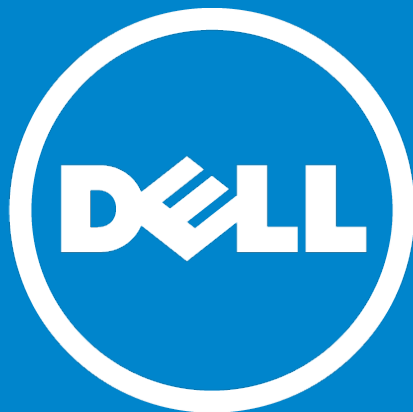
What Identity areas must be delivered?

Identity Governance

Achieve complete, business-driven governance for identities, data and privileged access by marrying **visibility and control** with administration.

Access Management

Ensure that all users can get to the resources they need to do their jobs from any location and any device in a **convenient, secure and compliant** manner.

Privileged Management

Centrally manage privileged accounts with individual accountability through granular **control and monitoring** of administrator access.

On Prem	From the Cloud	For all access scenarios	For all user types

Call to action:

Følg:

- Blogg: delldirekte.no

- Twitter: @RonnyStavem

- LinkedIn: no.linkedin.com/in/ronnystavem