Hello ….

One Identity

Tanya Moreno

CEE Channel Manager

ONE IDENTITY™

The Company

Balabit

ONE IDENTITY™

Who we are …

- Started in 2000 in Identity Management Market
- More than 200 developers focused on IAM
- Worldwide presence with 7,500+ customers
- 17% YoY growth 2016 (3X market rate)
- 425+ partners WW
- Re-launched 1 year ago and named “LEADER” in Gartner Quadrant (Feb ’18)
- Acquired Balabit (Leading company in PAM)

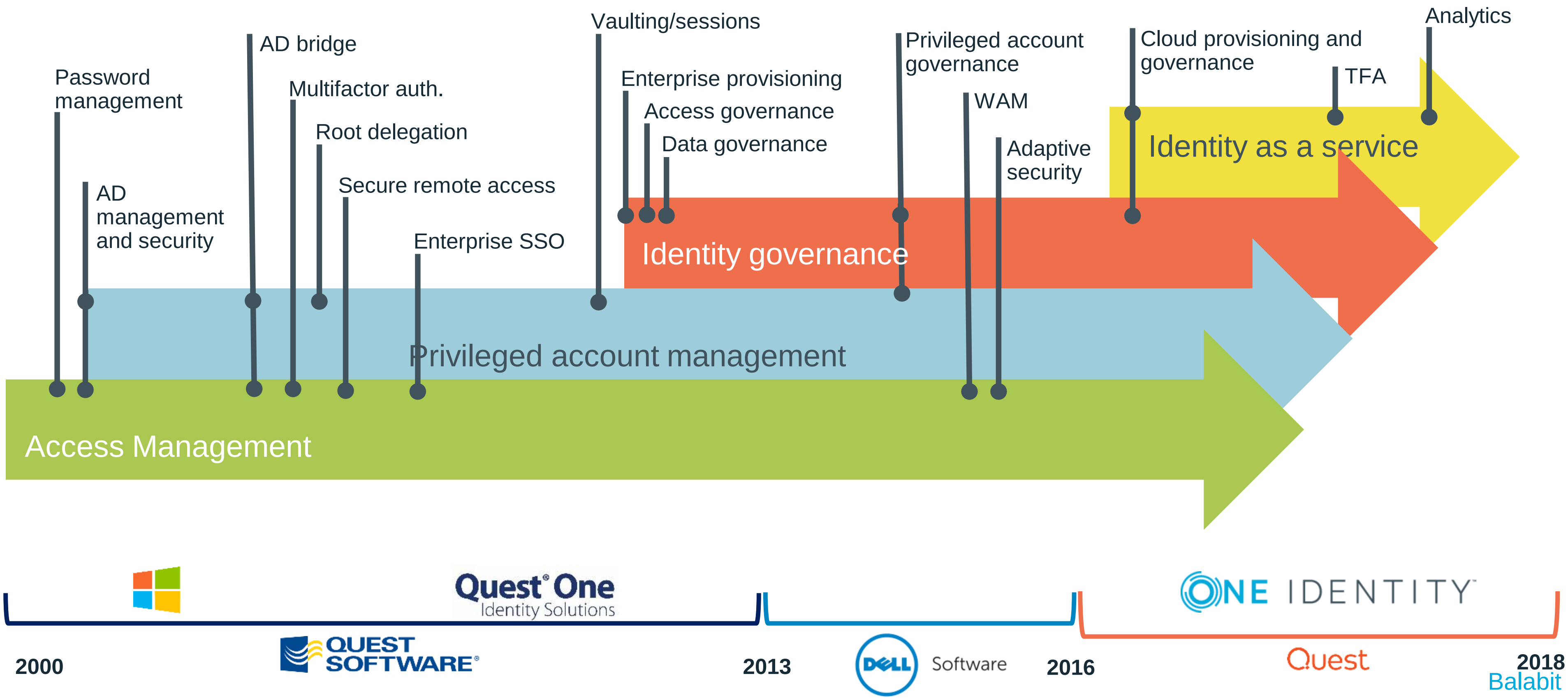
Balabit …In Summary …

- Founded in 2000
- 230+ Employees
- 1,500 Customers
- Offices: New York, Munich, Paris, London
- 100+ Partners in 50+ Countries
- 1 Million + Open source users

And some of the customers…

Rabobank
SNS REAAL
sky
Walmart
COSTCO WHOLESALE
dun & bradstreet
Hilton HOTELS & RESORTS
BankABC
ING BANK
The Walt Disney Company
Pratt & Whitney
A United Technologies Company
Liberty Mutual INSURANCE
PNC BANK
Telefónica
Adobe
Deutsche Bank
Williams
BOSCH
HSBC
Munich RE
Deutsche Bank

History


Vaulting/sessions
AD bridge
Privileged account governance
Analytics
Cloud provisioning and governance
Password management
Enterprise provisioning
TFA
Multifactor auth.
Access governance
WAM
Root delegation
Data governance
Identity as a service
Adaptive security
AD management and security
Secure remote access
Enterprise SSO
Identity governance
Privileged account management
Access Management
Quest® One Identity Solutions
ONE IDENTITY
QUEST SOFTWARE®
DELL Software
Quest
2000
2013
2016
2018
Balabit

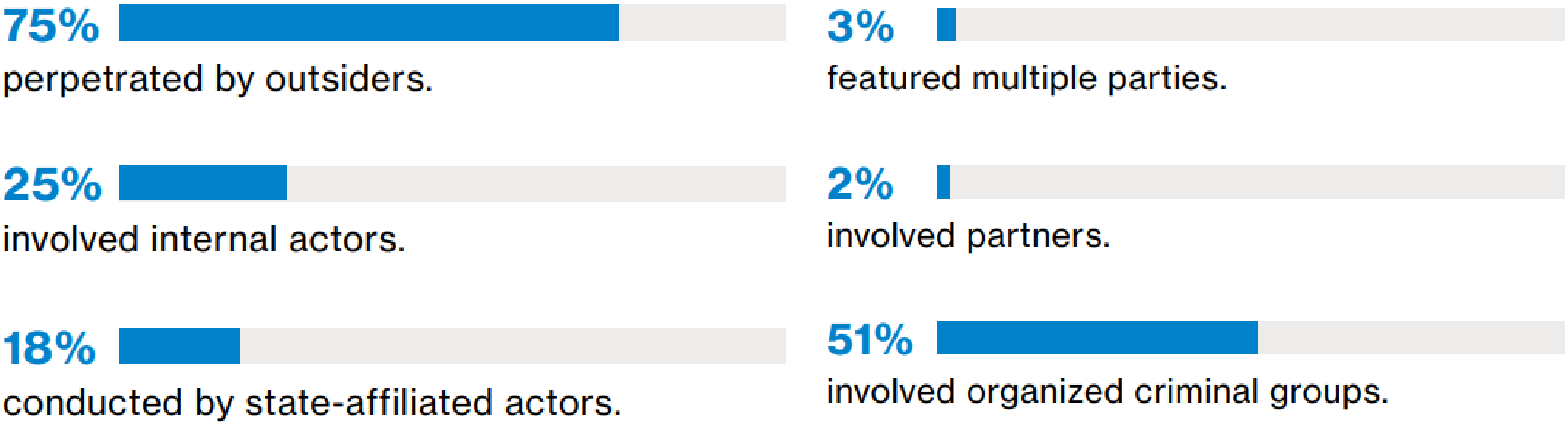
Cyber Threat Involves Compromised Privileged Credentials

- Data breaches are a huge problem
- Forrester estimates that 80% of all data breaches involve misuse of local endpoint administrative privileges
- Admin credentials are often stored on endpoints (PCs, mobile devices, etc.)
- Requires behavioral analysis Network forensics are inadequate and slow

Shift identity to the center of your threat detection ecosystem

- Perimeter is long gone. Can you give a laptop with VPN to every admin (contractor and employee)???
- Holistic approaches business and admin users are essential
- Password replacements are mandatory
- Unified treatment of Application, Data, Endpoint, and Network access controls
- Identity has emerged as the new perimeter

Who’s behind the breaches?



75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

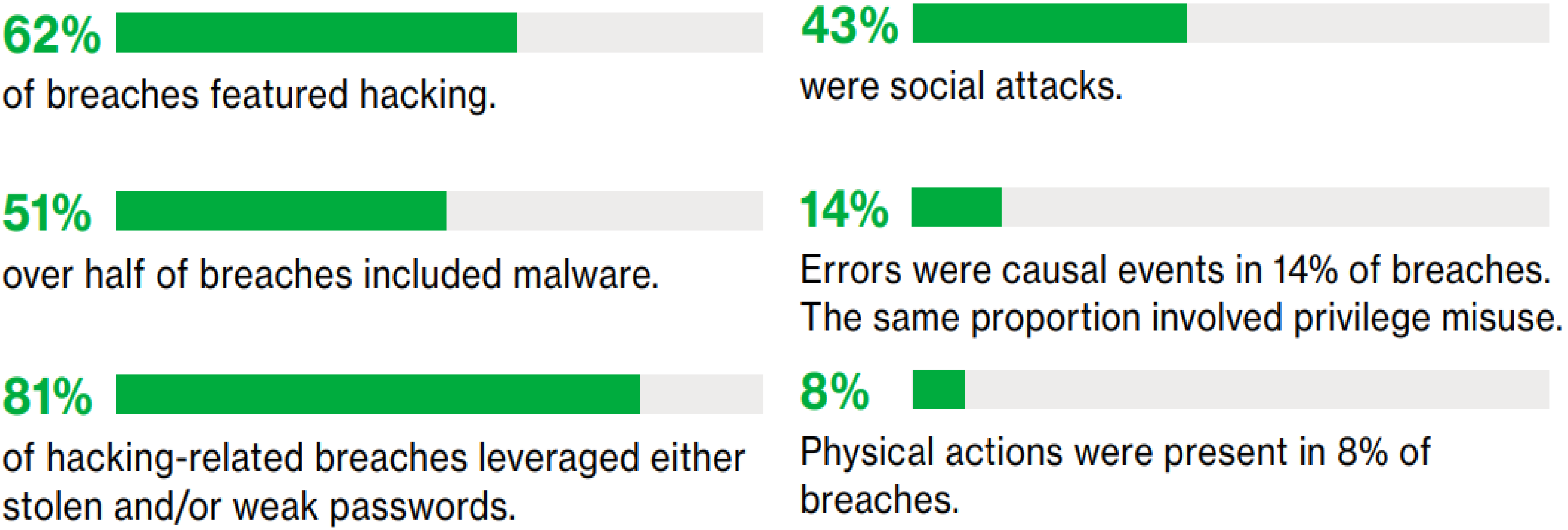
3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

Source: Verizon 2017 Data Breach Investigations Report http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

What tactics do attackers use?



62%

of breaches featured hacking.

51%

over half of breaches included malware.

81%

of hacking-related breaches leveraged either stolen and/or weak passwords.

43%

were social attacks.

14%

Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8%

Physical actions were present in 8% of breaches.

Source: Verizon 2017 Data Breach Investigations Report http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

What is GDPR?

It’s a European Regulation that affects the GLOBE

A quick summary

Who

Any organisation that stores personal data of European Union Citizens
(250 employees or more)

What

Must report data breaches, prove compliance in the case of an audit, pay fines of up to 4% of annual global revenue if found in violation

When

Effective from May 25th 2018 (yes, this year)

Where

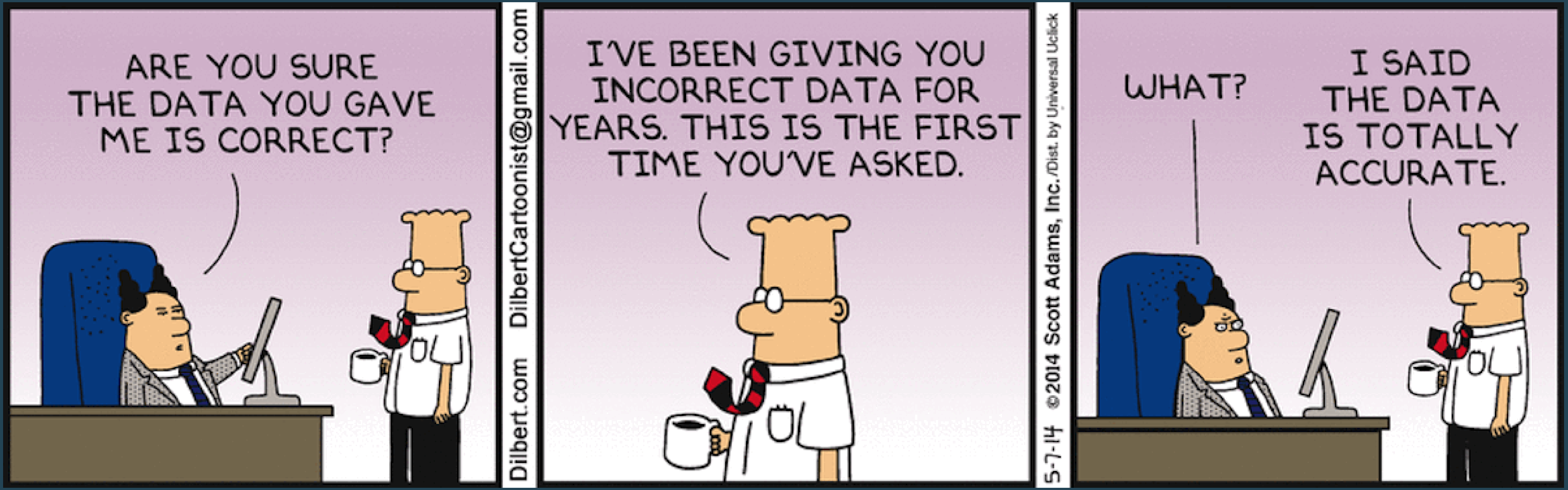
Applicable worldwide (as long as the organization stores personal data on EU citizens)

Only 8% feel they are compliant

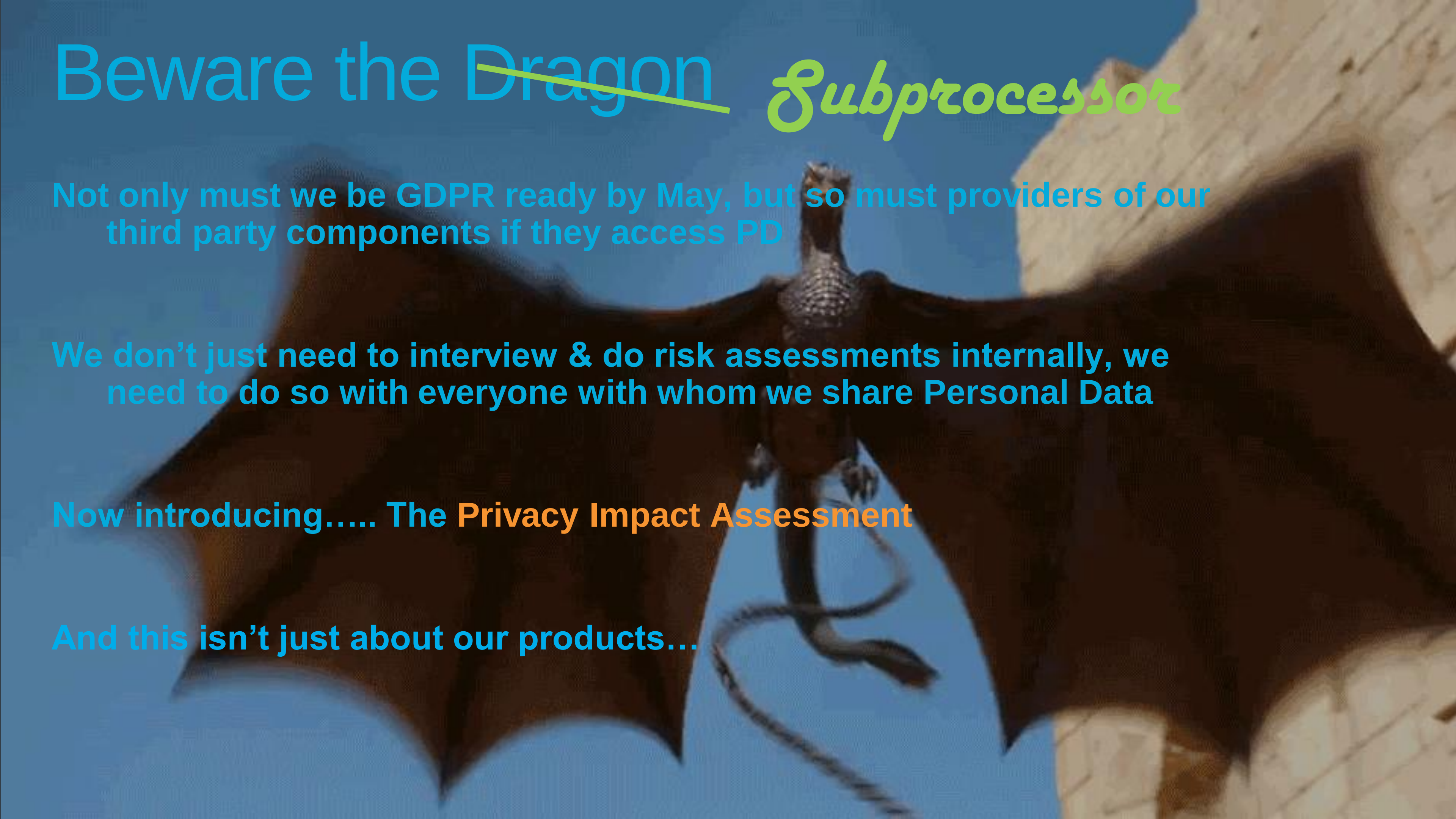
days after TODAY then on borrowed time !

64

This is not good enough anymore…


ARE YOU SURE THE DATA YOU GAVE ME IS CORRECT?
I'VE BEEN GIVING YOU INCORRECT DATA FOR YEARS. THIS IS THE FIRST TIME YOU'VE ASKED.
WHAT?
I SAID THE DATA IS TOTALLY ACCURATE.
Dilbert.com DilbertCartoonist@gmail.com
5-7-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick

Beware the ~~Dragon~~ *Subprocessor*



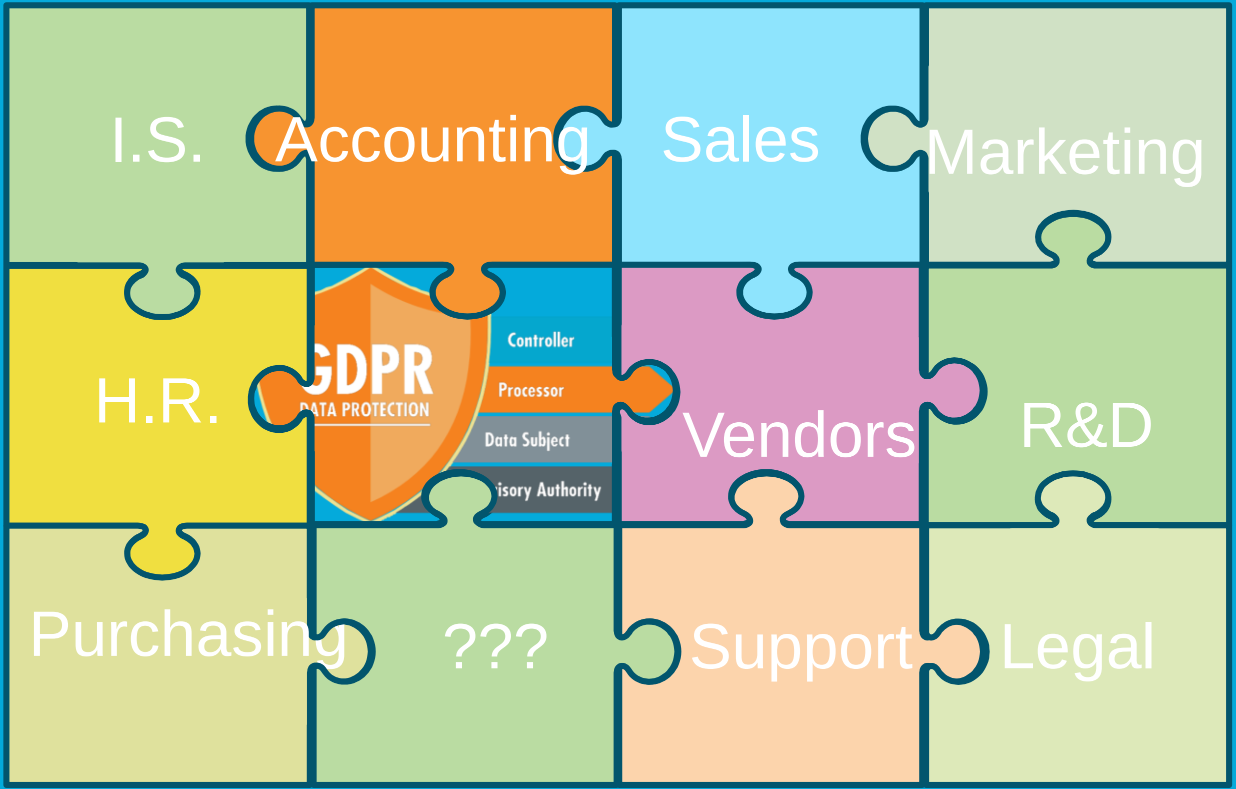
Not only must we be GDPR ready by May, but so must providers of our third party components if they access PD

We don’t just need to interview & do risk assessments internally, we need to do so with everyone with whom we share Personal Data

Now introducing….. The Privacy Impact Assessment

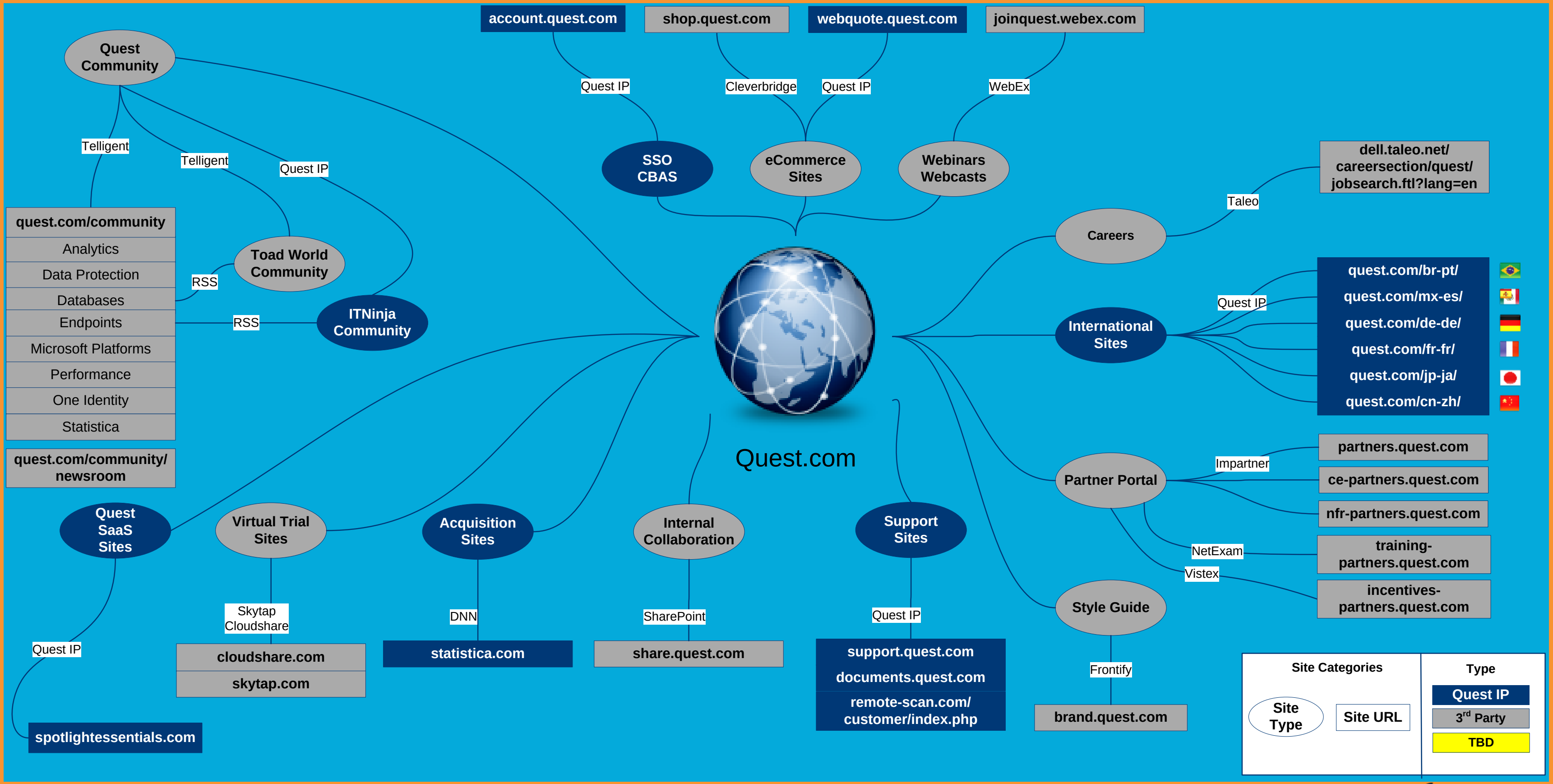
And this isn’t just about our products…

GDPR keeps involving more departments



ONE IDENTITY

Marketing!



Quest.com

Quest Community

Telligent

Telligent

Quest IP

quest.com/community

Analytics

Data Protection

Databases

Endpoints

Microsoft Platforms

Performance

One Identity

Statistica

quest.com/community/newsroom

RSS

Toad World Community

RSS

ITNinja Community

account.quest.com

Quest IP

SSO CBAS

shop.quest.com

Cleverbridge

webquote.quest.com

Quest IP

eCommerce Sites

joinquest.webex.com

WebEx

Webinars Webcasts

Careers

Taleo

dell.taleo.net/careersection/quest/jobsearch.ftl?lang=en

International Sites

Quest IP

quest.com/br-pt/

quest.com/mx-es/

quest.com/de-de/

quest.com/fr-fr/

quest.com/jp-ja/

quest.com/cn-zh/

Partner Portal

Impartner

partners.quest.com

ce-partners.quest.com

nfr-partners.quest.com

NetExam

training-partners.quest.com

Vistex

incentives-partners.quest.com

Style Guide

Frontify

brand.quest.com

Quest SaaS Sites

Quest IP

spotlightessentials.com

Virtual Trial Sites

Skytap Cloudshare

cloudshare.com

skytap.com

Acquisition Sites

DNN

statistica.com

Internal Collaboration

SharePoint

share.quest.com

Support Sites

Quest IP

support.quest.com

documents.quest.com

remote-scan.com/customer/index.php

Site Categories		Type
Site Type	Site URL	Quest IP 3rd Party TBD

The challenges are real

But the need to be secure and compliant does not go away, requirements and regulations keep evolving, and no one gets the benefit of the doubt.

Compliance is hard

3/4 & 1/3

While nearly3/4 of organizations have adopted access management solutions only 60% of those have confidence in the compliance of those solutions and practices and less than 1/3 have adopted the corresponding governance capabilities [3]

Relentless regulations

5%

Organizations that feel they are “definitely in compliance” [2]

Spending is growing

Expensive

73% of organizations have increased or maintained budget for compliance activities, and 84% have increased or maintained compliance staffing. [1]

The challenges are real

And, everything is getting more **complex**: number of users, types of users, methods of access needed and types of resources that must be accessed.

72%

Organizations that report adopting business-enabling technologies such as mobile, cloud, and self-service but only **18%** address the security implications of these technologies from the start [1]

Digital Transformation

Provisioning

On average, it takes more than a **day and a half** to provision a new user and more than **half a day** to deprovision a user. [2]

Cumbersome, time-consuming, incomplete

Privileged Accounts

63% of organizations feel they could do a better job of securing privileged accounts and administrator access [3]

NEGLECTED

What happens if you don’t get it right?

- It becomes difficult to achieve objectives
- You lose your competitive edge
- Your organization may suffer irreparable harm
- People lose their jobs, reputations, suffer possible fines and legal penalties

Every high-profile breach is due, at least in part, to the misuse or abuse of legitimate user credentials.
In other words, these breaches could have been avoided with better identity and access management.

Translation: “ To hold the line on security and compliance, you must Get IAM Right

TESCO
UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
THE HOME DEPOT
T · · Mobile
Anthem
ASHLEY MADISON.COM
TARGET

What does right looks like?

The **right** people are in control

You achieve the outcomes that drove the program in the first place

Security is considered an ally, not an enemy, to organizational success

Your IAM program covers all of your needs today, and paves the way for future **success**

IAM has transitioned from a barrier or obstruction into an enabler

Your IAM program is a top-line revenue generator

Your vendors, service providers, and partners focus on **your** success, not just theirs

What does right look like?

The right people

Employees, administrators, partners, customers, whomever

In all the ways they want

On-prem, remote, mobile, company-controlled devices, BYOX, and over any connection

With the right governance

The line-of-business decides what is right and is able to attest to it

The right access

Precisely what they need to do their jobs… no more, no less

To the right resources

Applications, on-prem, in the cloud, SaaS and privileged accounts

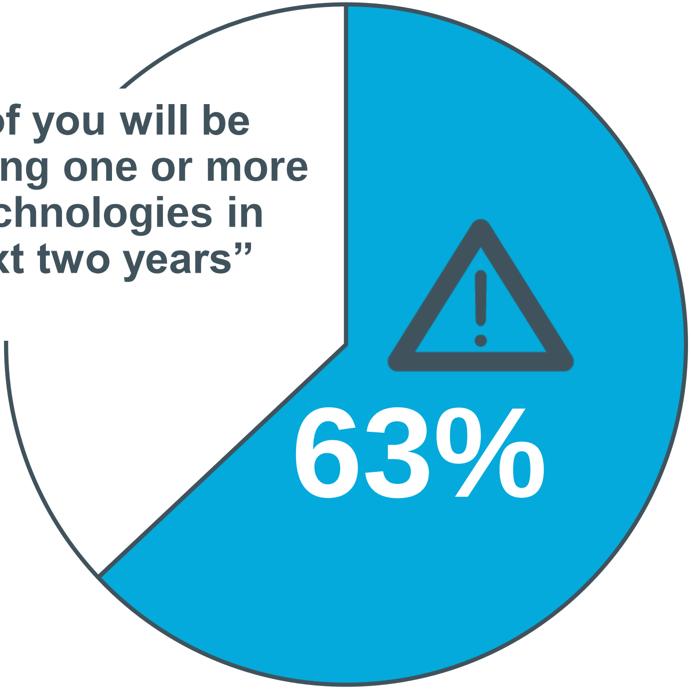
At the right time

During regular work hours, but also anytime anyone wants or needs access as well

And you can prove it

To whatever regulation or framework you need to adhere to whenever it is requested

Does IAM help you compete… and thrive?



“63% of you will be replacing one or more IAM technologies in the next two years”

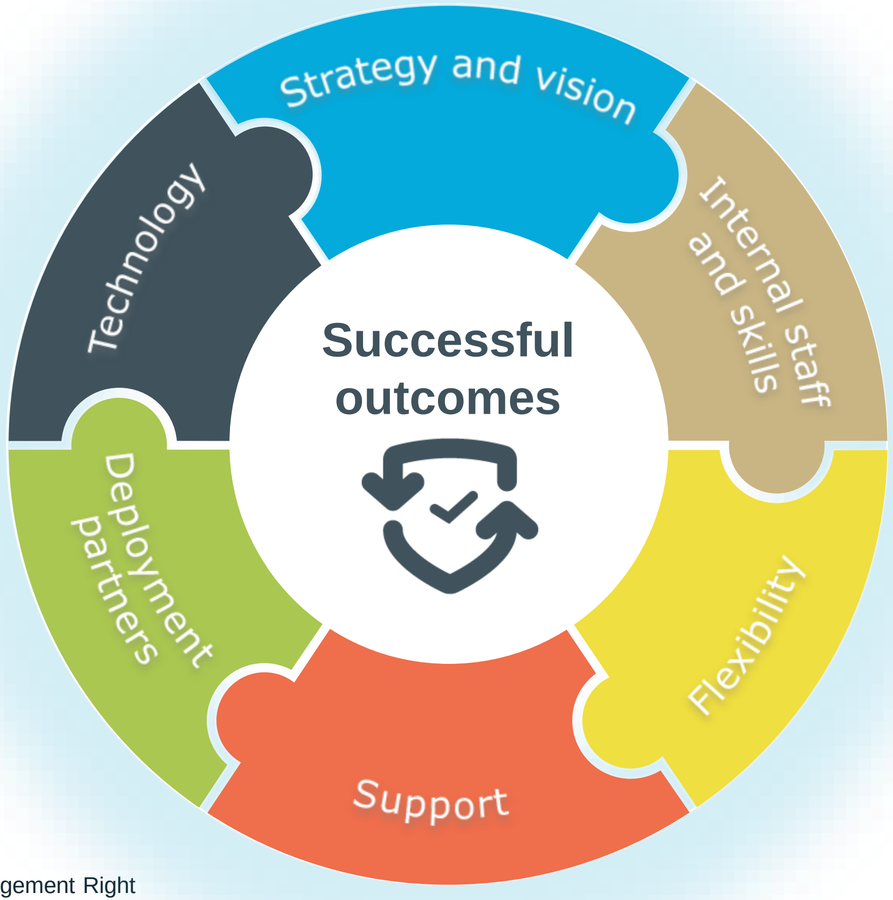
#1 REASON:

“The technology environment has **changed**, and the incumbent solution doesn’t address our requirements”

Gregg Kreizman, VP Research, Gartner
Gartner IAM Summit Nov. 2016

Get Identity and Access Management Right

Requirements to Get IAM Right



ONE IDENTITY

We provide

Managing enterprise identity on-prem or in the cloud

Identity Governance

Complete, business-driven governance

Access Management

Convenient, secure & compliant access

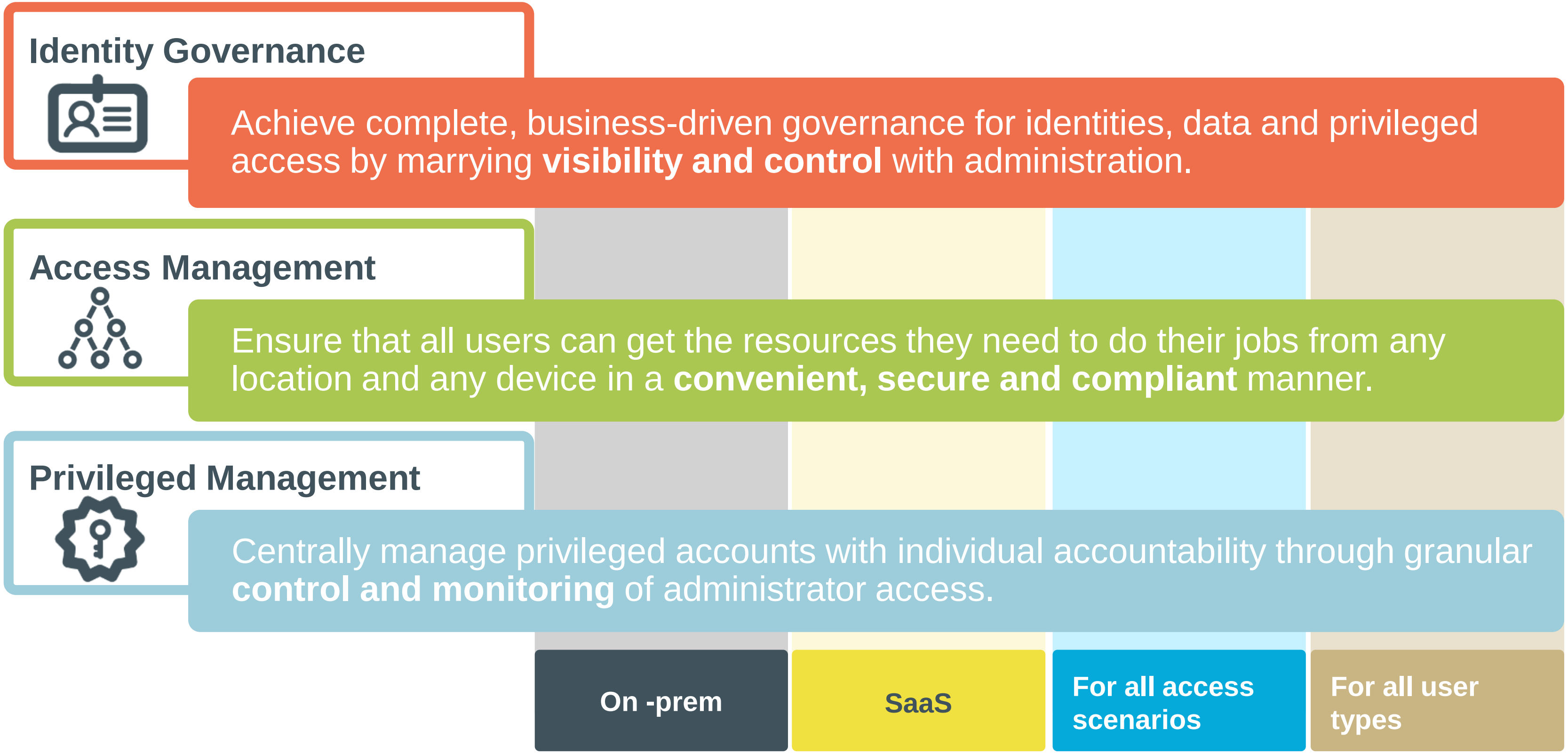
Privileged Management

Understand & control administrator activity

Log Management

Reliable, scalable, secure central log management

The scope



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 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

SaaS

For all access scenarios

For all user types

One Identity
Helps you Get IAM Right

ONE IDENTITY™

What it takes to Get IAM Right

The path to governance

- Ensure the right access
- Facilitate easy and accurate attestations
- Govern access, data, and privileged accounts

Business driven

- Empower the right people
- Focus on business objectives
- Streamline operations and reduce costs

Modular and integrated

- Start anywhere and build from there
- Cover every aspect of IAM
- Easily plug into existing tools and solutions
- Be cloud-ready

Future-ready

- Rapidly adapt to changing requirements
- Embrace digital transformation
- Superior deployment and technology support

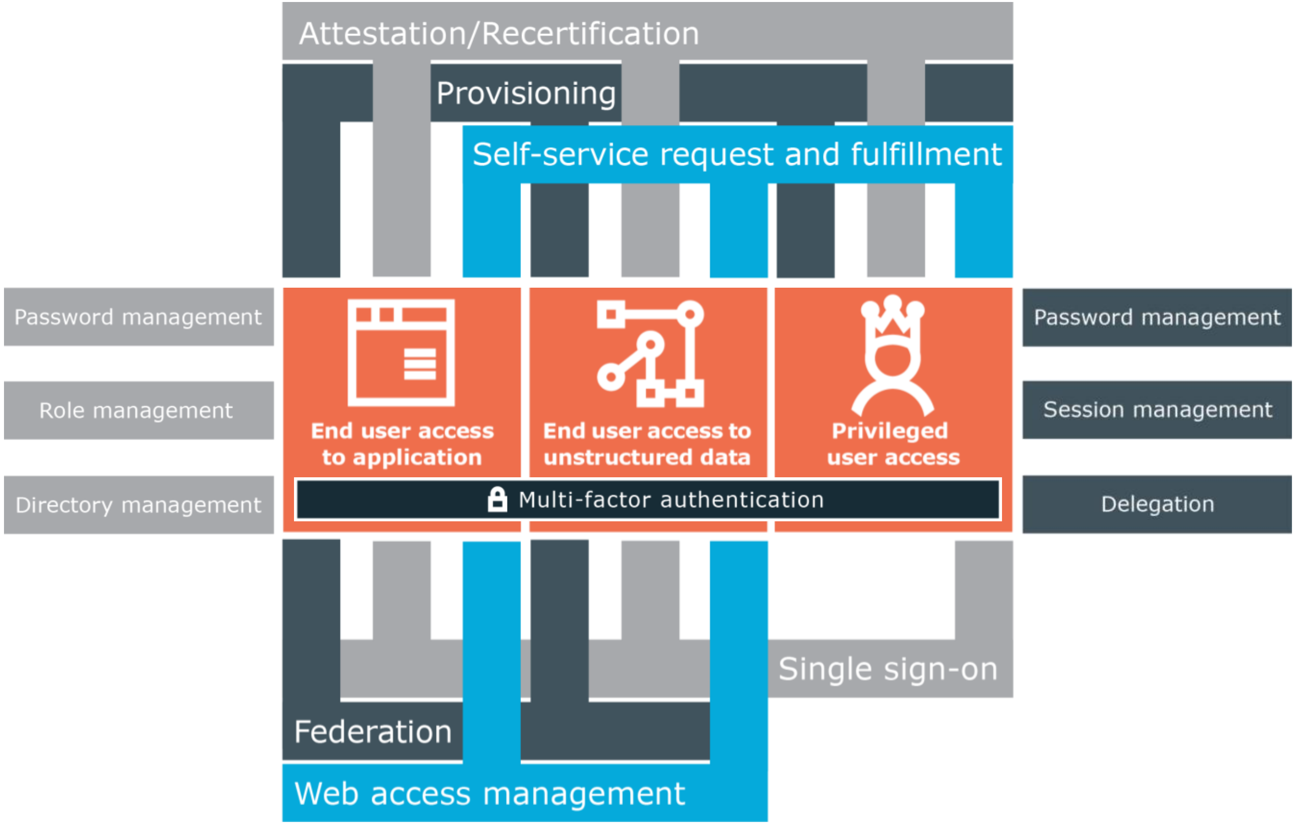
Rapid time to value

- Unify IAM components
- Streamline and automate tasks
- Relieve the burden on IT
- Rely on the right partners

Focused on successful outcomes

Get IAM Right

Identity governance



Access management

Privileged account management

Access management

ONE IDENTITY

Recognition

Success and leadership

Award-winning Support

The Association of Support Professionals
Award Winner 2016
The Year's Ten Best Web Support Sites

The Association of Support Professionals
Award Winner 2017
The Year's Ten Best Web Support Sites

130+ million

Identities managed through One Identity solutions

Leader

Position in the Forrester Wave for Identity Governance and Administration

Customer Satisfaction

94% of One Identity customers report "overall satisfaction on support experience" and a 75% Net Promoter Score

Reader's Choice

Awarded for Governance, Risk & Compliance by Information Security Magazine

Information Security Readers' Choice Awards
WINNER
2014

ONE IDENTITY™

Product Leader

Position in the Kuppinger Cole Leadership Compass on Access Management and Federation

Stable

13 consecutive years of profitability; $220M in revenue, $70M profit, and 29% YoY growth (FY17)

LEADER

Position in the Gartner Magic Quadrant for Identity Administration and Governance 2018

7,000+

Customers of One Identity solutions

Overall Leader

Position in the Kuppinger Cole Leadership Compass for Access Governance

LeadershipCompass KuppingerCole
Overall Leader
Access Governance
March 2013

What the industry is saying about One Identity

> “We expect One Identity to play a **strong role** in the growing IAM market, with both their established product portfolios and, the extensions they are likely to make to this portfolio. We rate One Identity amongst the major players in the IAM market segment.”

One Identity: Market Impact, Martin Kuppinger, KuppingerCole, October 2016

> “One Identity Manager provides **superior** policy and role management features, with a rich role framework … with sufficient flexibility to control the behavior of how users are added and removed from roles. It provides **deeper integration** with complex applications than other vendors. [An] increased focus on partnerships with resellers and system integrators is fueling rapid and continued improvement in execution.”

Magic Quadrant for Identity Governance and Administration
Gartner, February 2017

> “[One Identity] provides AD monitoring and group management as part of its IAM portfolio. Active Roles provides a proxy-based architecture that provides views of AD permissions and can **provision and delegate** access to AD.”

Vendor Landscape: Active Directory Security and Governance Solutions
Forrester, January 5, 2016

Hvala vam !