GDPR – How we can help

Solvit Networks

01.11.2017

ca technologies

GDPR – The facts

- The General Data Protection Regulation (GDPR) applies to all companies trading in the EU and processing personal data of EU Residents
- GDPR comes to effect on 25th May 2018
- Sanctions of up to €20,000,000 or 4% of annual worldwide turnover
- GDPR is not a best practice it is a privacy regulation

GDPR – Who is affected

- Public sector
- Financial sector
- Healthcare
- Industry sector
- Retailers
- Telco sector
- Cloud providers
- Transport sector
- Marketing sector

GDPR - Changes

NEW REQUIREMENTS

Data protection by design/default

Data protection impact assessments

Data protection officers - DPO

NEW USER RIGHTS

Data breach notification

Right to be forgotten/erasure

TECHNOLOGY STRATEGY

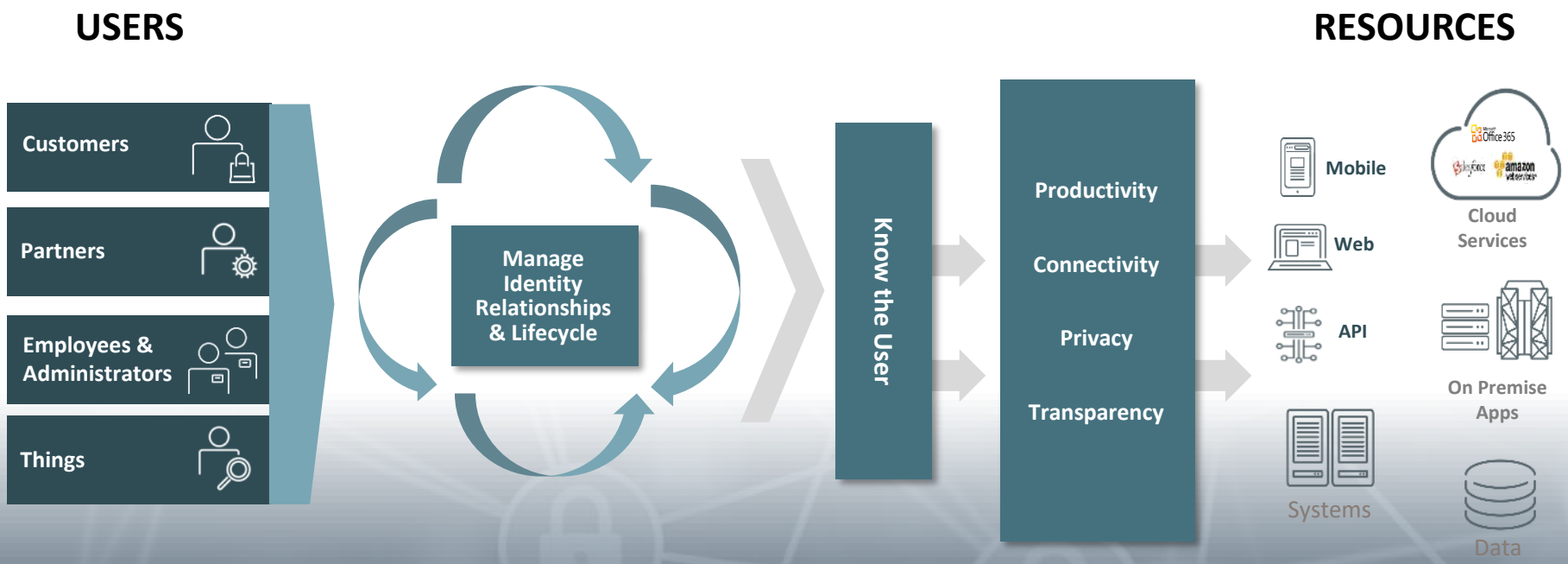
Where your data is, how you collect it, and who can touch it

STRONG IDENTITY

Strong, identity policies and tools for authorization and authentication to ensure ccompliance

ca technologies

GDPR – CONTROL ACCESS – CONTROL DATA



HOW CAN WE HELP YOU WITH GDPR

- Perform detailed analysis
- Create a good and achievable plan
- Redesign your processes
- Implement technology

GAP ANALYSIS

RISK ANALYSIS

PROJECT PLANNING

DATA PROTECTION

ca technologies

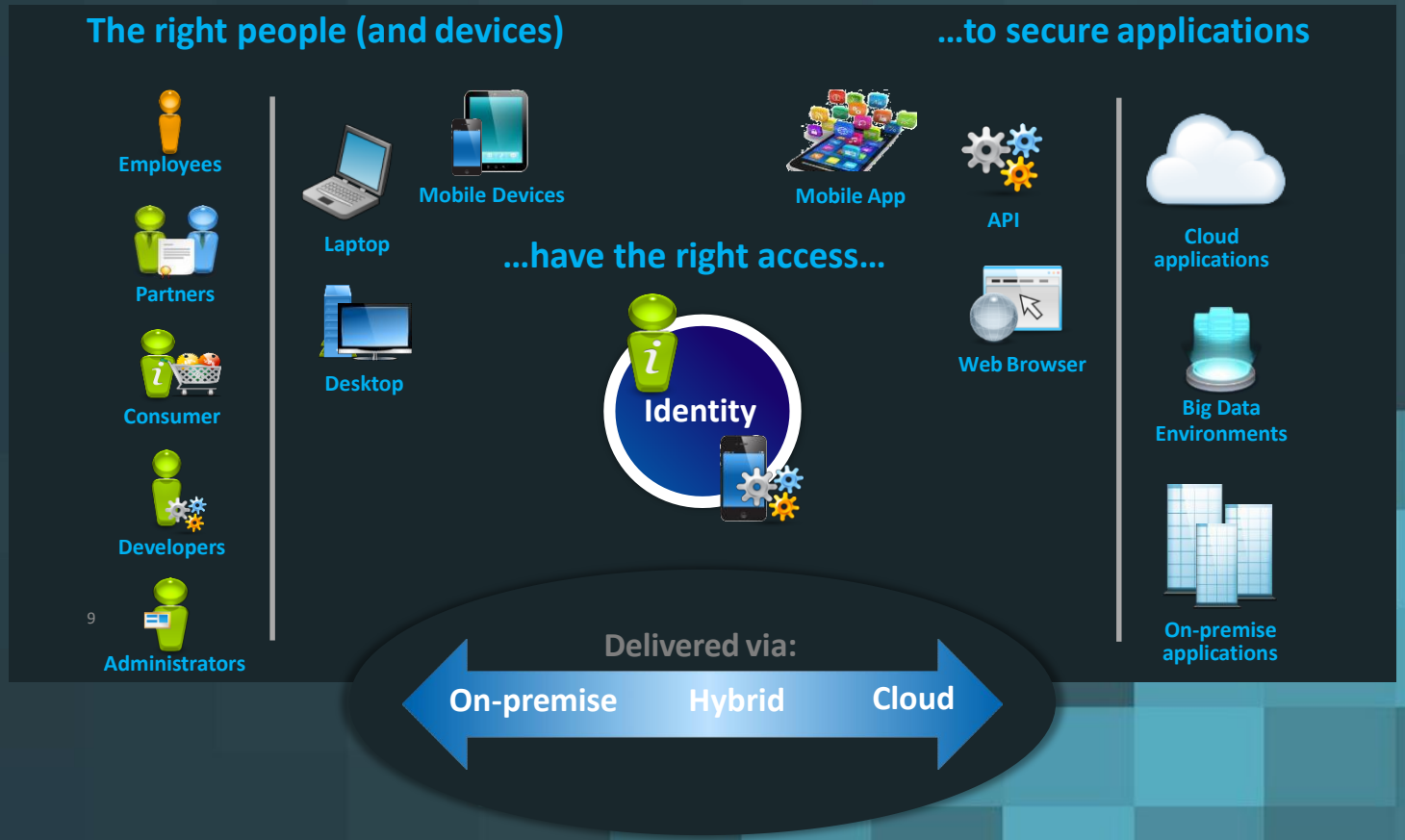
CA Solutions for GDPR

- Identity and governance management
- Privileged access management
- Advanced authentication
- Single Sign On
- API Management

ca technologies

CA Identity Management & Governance

Identity


The right people (and devices)
...to secure applications
Employees
Partners
Consumer
Developers
Administrators
Laptop
Mobile Devices
Desktop
...have the right access...
Identity
Mobile App
API
Web Browser
Cloud applications
Big Data Environments
On-premise applications
Delivered via:
On-premise
Hybrid
Cloud

Demands of the Business User

Unified interface

Support my device

Productivity

Business friendly

Decision support tools

Customized experience

But, the IT user has needs too!

Fast provisioning

Policy enforcement

Fast ROI

Low TCO

Application connectivity

Compliance reporting & auditing

CA Identity Suite

Designed with your IT & Business needs in mind

Capabilities

IT

Access Governance

Privilege Cleanup

Risk Analysis

Performance Analytics

Deployment Tools

Business

Deep Provisioning

Access Requests

Certifications

One-stop shop for Identity

Self-Service

SOLVIT works naturally

ca technologies

Convenient, intuitive, business-oriented user experience

A One-Stop Shop for business user access to all identity services

User experience that is specifically designed for business. Uses terms that business users understand.

- Business-oriented proactive analytical & advisory tools
- Personalized dashboards
- Business-oriented resource names

Automated Provisioning

Wizard-based on-boarding of new users (including self-registration), such as employees, business partners and contractors.

Manages identities, roles, and policies across on-premises & cloud applications

Customizable workflows support the unique way each organization approves, and schedules these activities.

Broad set of connectors to target systems

Access Requests

Easy-to-use access request process through an intuitive 'Shopping Cart‘ experience.

Conveniently request roles and entitlements from a Business Entitlements Catalogue

Advice Tools such as real-time context-based access recommendations

All requests can be checked for segregation of duties compliance.

Certification Campaigns

Simplifies and centralizes all necessary compliance activities in one place.

Business entitlements catalogue simplifies certifications

Risk analysis highlights risky access to:

- Enable real-time remediation
- Improve policy enforcement
- Simplify regulatory compliance.

Easily customizable for the needs of each role/user

CA Privileged Access Management

But the reality is … attacks using privileged accounts ever

CYBERCRIME

- Target—70 million credit cards stolen
- Home Depot—56 million credit cards stolen
- JP Morgan Chase—76 million account records stolen

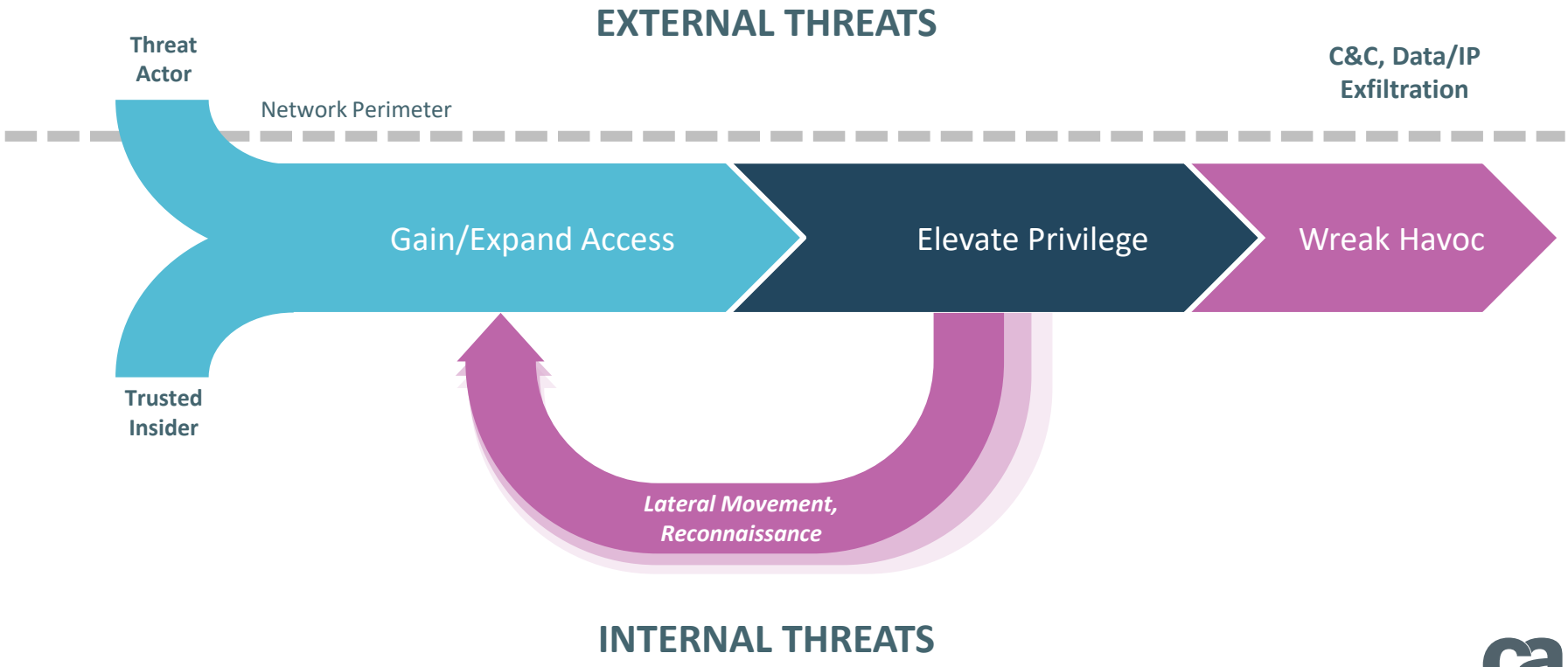
CYBERESPIONAGE

- Anthem—80 million personal records stolen
- Forbes.com and unidentified health insurer—targeted (defense contractors, government workers) information gathering of individual data

BUSINESS IMPACT

- CodeSpaces—forced out of business
- Sony Pictures—extensive disruption
- German Steel Mill—physical damage
- Saudi Aramco—physical systems damage and business disruption

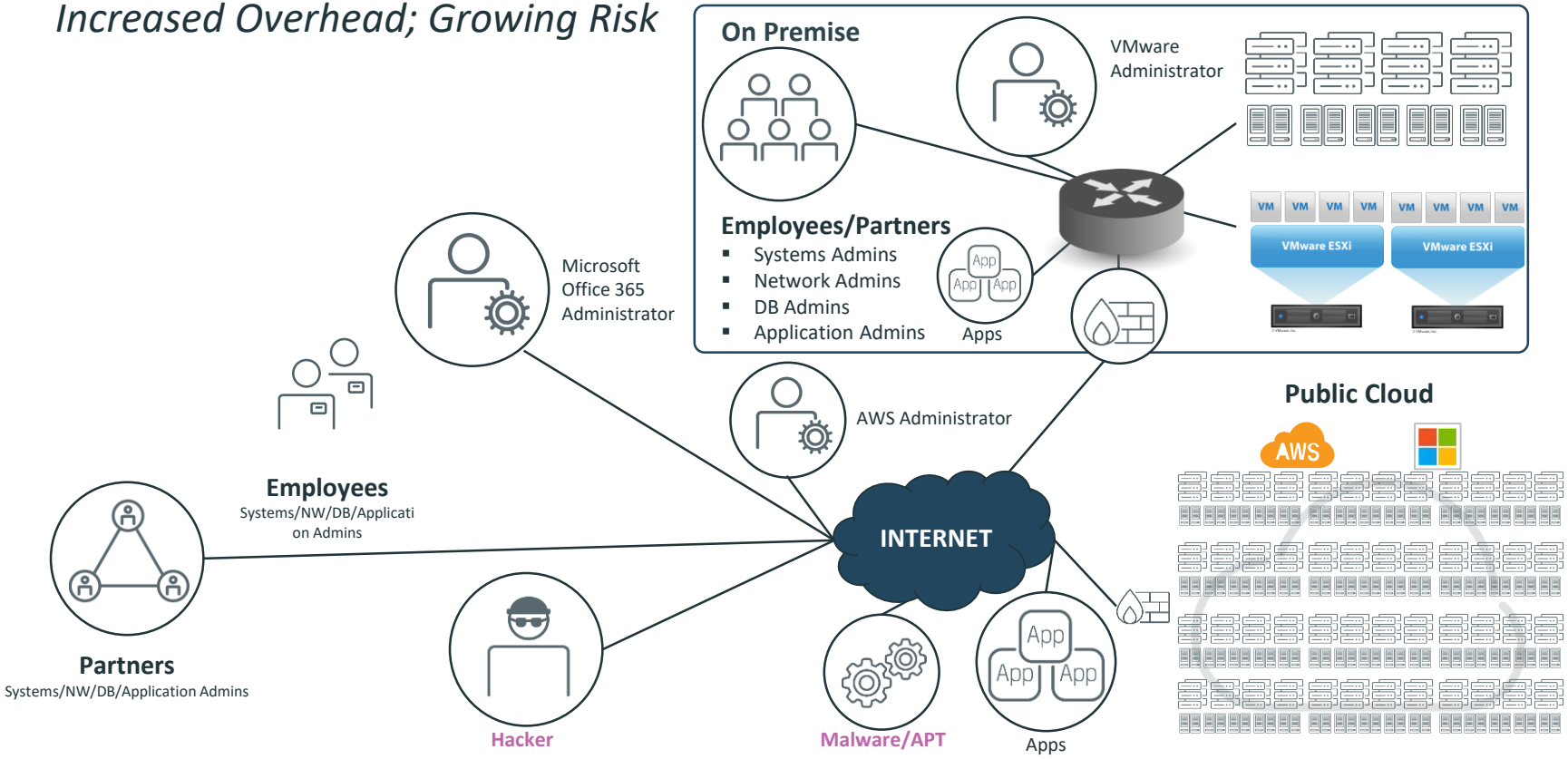
Privilege: Core of the Breach Kill Chain



ca technologies

The Problem is Getting Worse

Increased Overhead; Growing Risk



ca technologies

CA PAM Key Capabilities

Credential Safe

- Privileged credentials
- SSH Session Keys
- FIPS 140-2 Level 1 & 2 compliant encryption
- Optional HSM for FIPS 140-2 Level 3 support
- Application-to-Application Support
- Industry's broadest platform support

Authentication

- Active Directory & LDAP
- RADIUS integration
- PKI/X.509 & Smartcard (PIV/CAC) support
- Multi-factor authentication (CA Technologies, RSA, VASCO, SafeNet, Entrust, etc)

Access Control

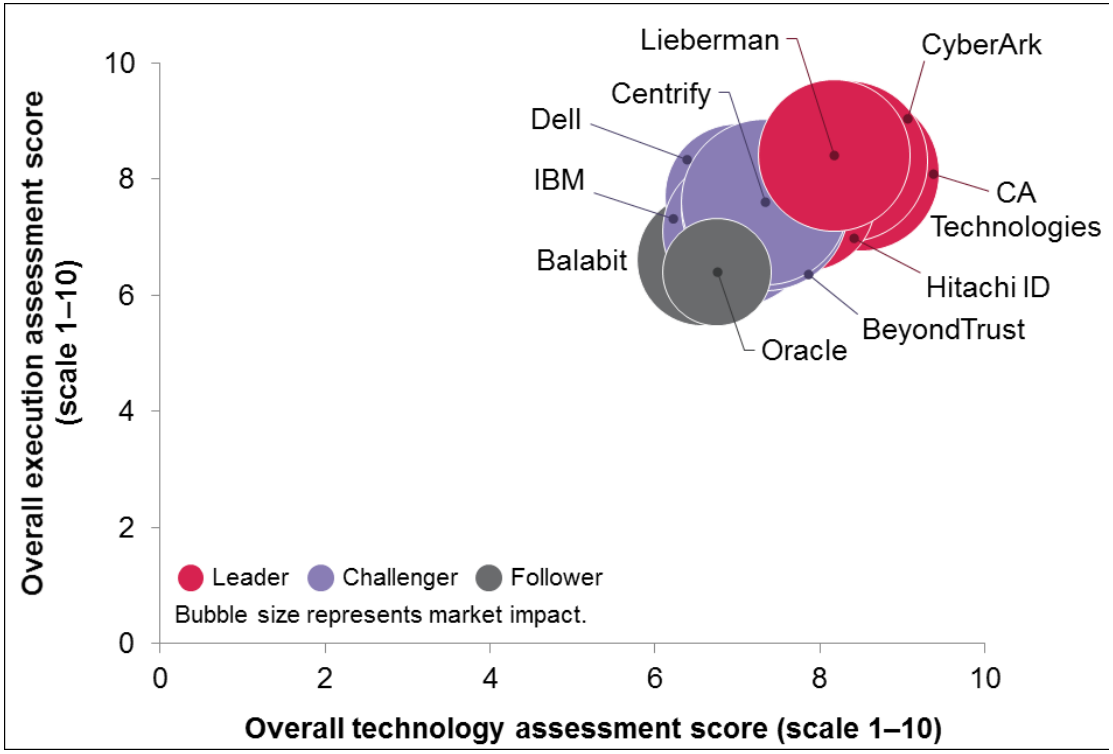
- Privileged user SSO
- Federated Identity & attribution
- Role-based privileged user access limits
- Zero Trust – deny all, permit by exception policy engine

Monitoring, Alerting & Intervention

- Continuous monitoring & logging
- DVR-like session recording
- Command filtering
- Leapfrog prevention
- Proactive policy violation prevention

ca technologies

Ovum Decision Matrix: Selecting a Privileged Identity Management Solution, November 2015



CA Advanced Authentication

Why Breaches Are Occurring

Passwords, identities and breaches

- Passwords are created by humans
- Authentication is needed for multiple applications
- Enormous number and type of users
- Passwords are valuable to fraudsters
- Getting ahold of a password, the digital world is open to them
- **Traditional credentials are not enough!**

Year after year, cyber threats continue to increase in both **sophistication** and **frequency**.
Many of the attacks involve **compromised user names and passwords**.

What Organizations Must Do to Protect Themselves

The average **total cost** of a data breach for the participating companies increased 23 percent over the past two years to **$3.79 million***

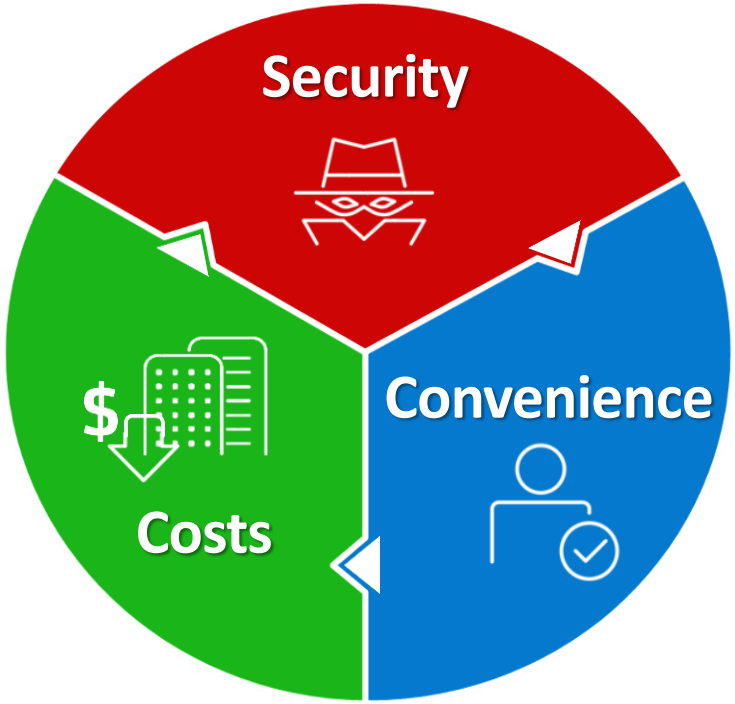
**IBM and Ponemon Institute, "2015 Cost of Data Breach Study: Global Analysis."*

How to get protected

- Protect user identity from online attacks
- Provide security for mobile devices
- Secure privileged identities
- **Use best practice Intelligent Authentication methods (MF and RISK based authentication)**

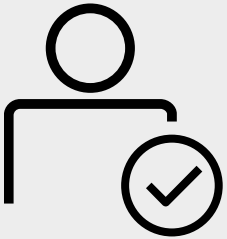
Business Decisions for More Effective Authentication

Enterprises will select their password replacement / password enhancing technology based on ***three criteria****.*

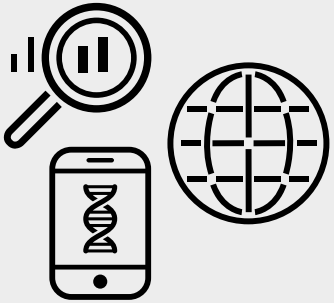


What if you could…

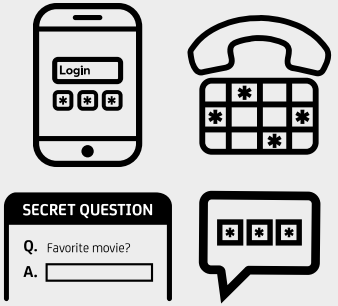
Authenticate User with Simple Password



Analyze Risk on Behavior, Device and Location



Initiate Step-Up Authentication when Risk is High



From a **Single** Authentication Solution?

ca technologies

CA Advanced Authentication - Product Overview

Business Problems Addressed

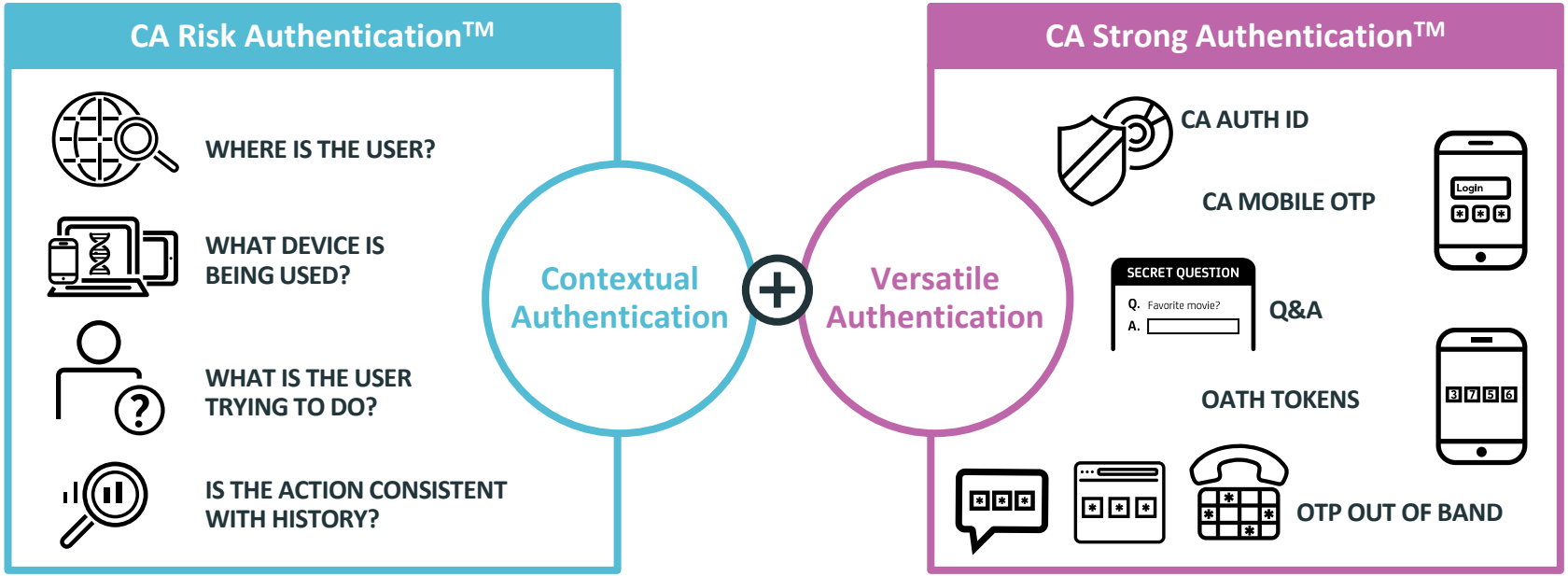
- Providing greater identity assurance
- Detecting anomalous user behavior
- Dynamic risk assessment
- Forcing additional proofing of identity when elevated risk is detected
- Reduces the need for additional proofing when the user is recognized

Key Capabilities

- Multi-factor and “step-up” authentication with Risk assessment
- Policy enforced using rules, contextual information, and behavioral analytics
- Integration with CA SSO, PAM and APIM solutions
- Open “white box” rules engine

CA Advanced Authentication - Product Overview

Two best-of-breed components that can be deployed *individually or together*:



Risk Assessment is a Strong Credential

AVAILABLE RISK DATA

Where is the user?

What device is being used?

What is the user trying to do?

Is the action consistent with history?

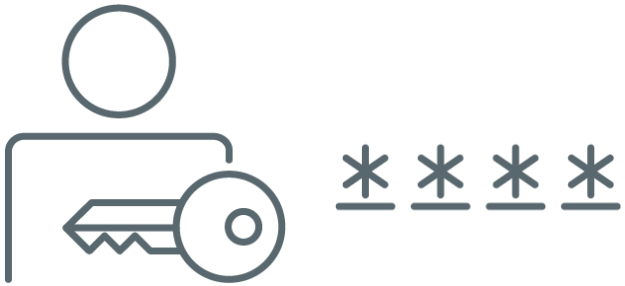
LOCATION	DEVICE DNA™	BEHAVIOR	HISTORY
• Is the **location** inherently suspect? • Have they been **there** before? • Where were they **recently**?	• What **kind** of device is it? • Have they **used** it before? • Has it **changed** since they last it?	• Is this a typical **action** for the user? • Is the action inherently **risky**? • Have they taken **similar** actions before?	• Is this a normal **time** of day for them? • Is their frequency of **login** abnormal? • Is this action **consistent** with prior actions?

ca technologies

CA Single Sign On (CA SSO)

When Users Have Multiple Identities, There Are User and Administrative Costs

End User



Users are continually asked to present their online identity again and again.

Administrator

Administrators have to create access policies in parallel for every user identity.

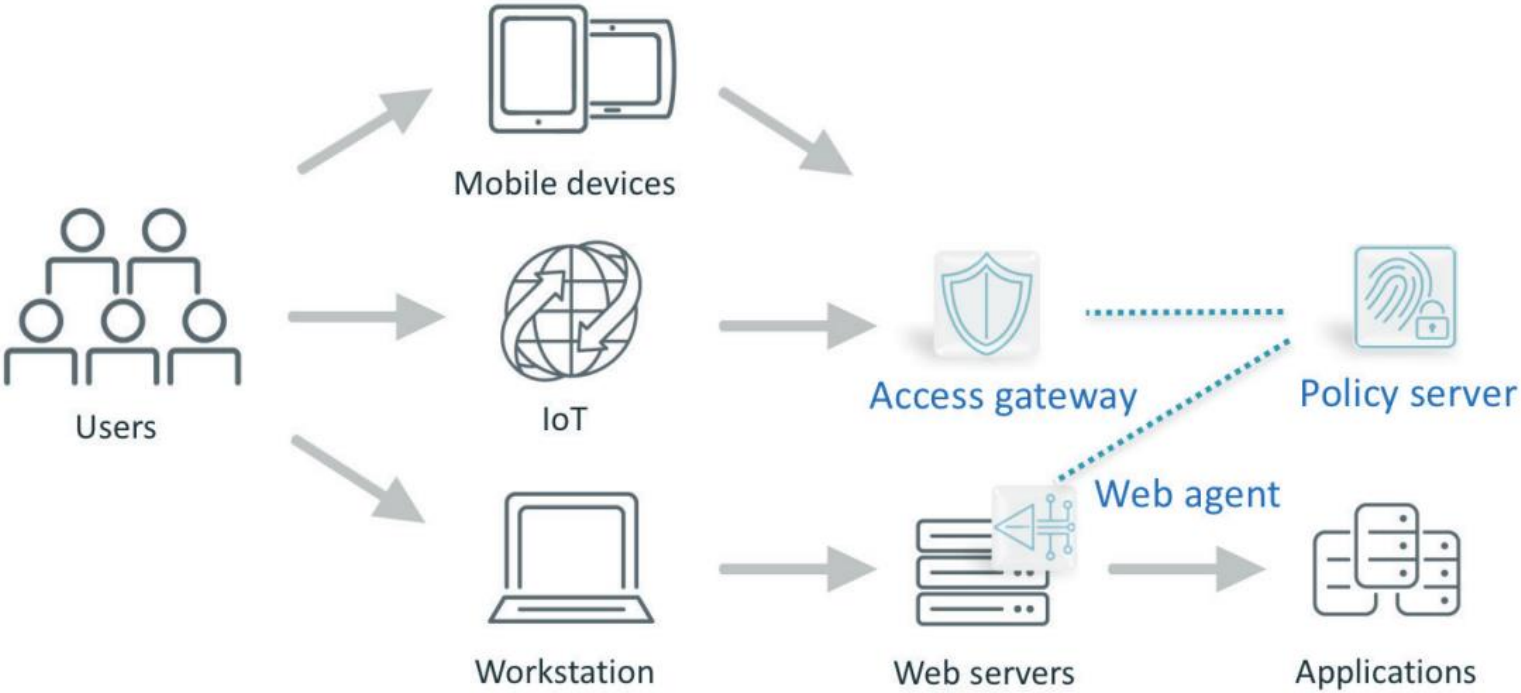
ca technologies

...SSO & Flexible Access Management is Business Critical to the Open Enterprise

Centralized solution value = | Fewer logins | Lower TCO | Less time to deployment | Lower risk of security policy gaps

ca technologies

Typical CA SSO environment



ca technologies

CA Single Sign-On - Product Overview

Business Problems Addressed

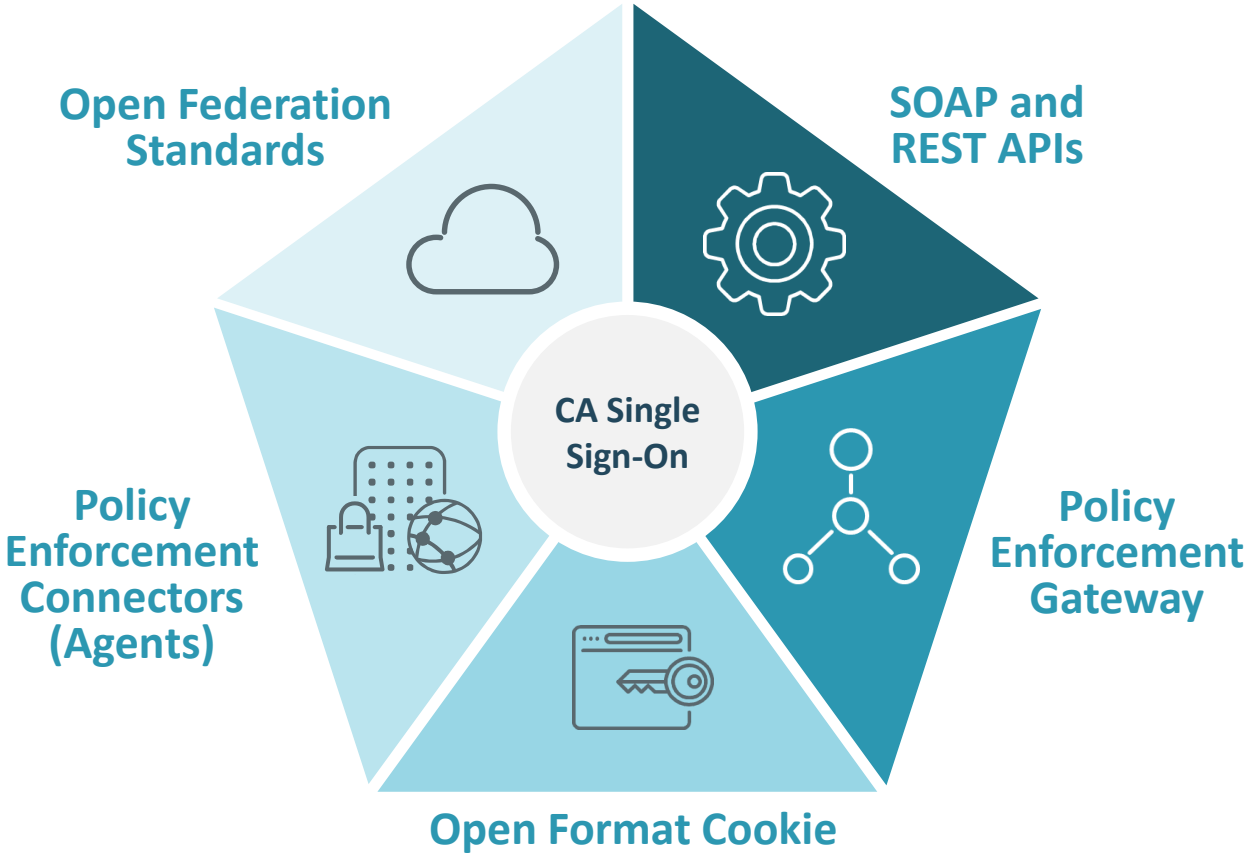
- Controlling access to various information resources
- Reducing costs of managing access
- Better user experience
- Raising end user productivity

Key Capabilities

- Centralized session management
- Flexible architecture models
- Identity federation
- Policy-based authorization
- Social login support
- Comprehensive access audit

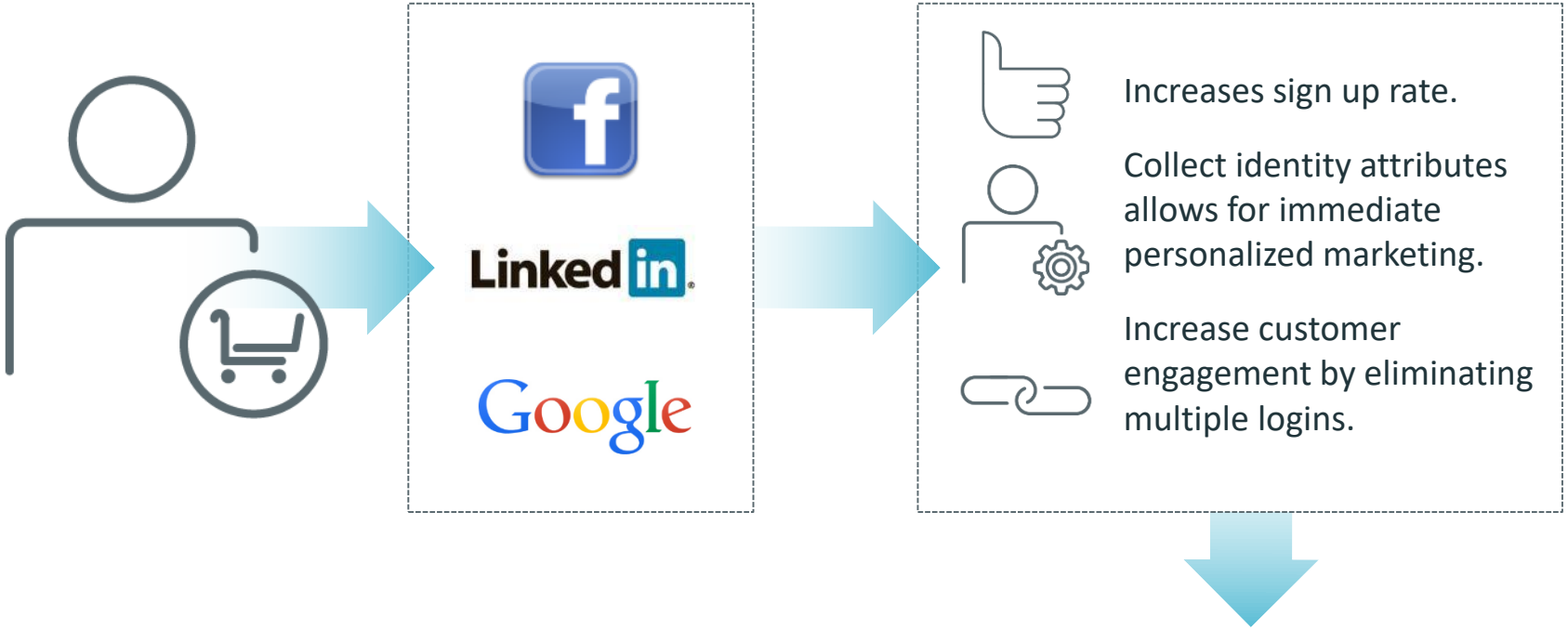
ca technologies

Flexible Architectures for Different Needs in a Single Deployment



ca technologies

Social Media Drives New Requirements



Sign in with ***stronger credentials*** when needed for high value transactions

ca technologies

Requirements Beyond Basic SSO

- ✓ Separate SSO zones
- ✓ Password policies
- ✓ Session replay prevention
- ✓ Session timeouts
- ✓ Single log out
- ✓ Centralized audit
- ✓ Scoped/delegated administration

- ✓ Directory mapping
- ✓ Attribute-based authorization
- ✓ Step up authentication
- ✓ Integrated multi-factor authentication
- ✓ Integrated risk-based authentication
- ✓ Risk-based authorization

ca technologies

Thank you!

Solvit Networks