The X-Factor in Data-Centric Security

Webinar, Tuesday July 14th 2015

63%
Data Leaks

57%
Inadvertent
Data Breach
(careless user)

53%
Malicious
Data Breach

36% Fraud

29% IP Theft

23% Espionage

20% Sabotage

4% Not Sure/Other

*The Insider Threat Spotlight Report

Q: What type of insider threats are you most concerned about?

Agenda

- Introductions & "House Rules"

- A Data-Centric Approach Is Required For Security Today

- Are You Controlling Information Disclosure?

- RightsWATCH Live Demo

- Questions & Answers

Introductions

Heidi Shey

Heidi serves Security & Risk Professionals in solutions for data security and privacy and for security architecture and operations. Her research focus is on data discovery and classification, secure file sharing and collaboration, cybersecurity and privacy topics such as policy and regulatory concerns, biometrics, and consumer security.

Rui Melo Biscaia

Rui serves as the Director of Product Management for Watchful Software, and is responsible for the company's product direction and go-to-market

Some "House Rules"

- You are muted centrally. You don't need to mute/unmute yourself

- This webinar is being recorded. The recording will be available tomorrow at www.watchfulsoftware.com

- The Q&A session will be at the end

- You are welcomed to enter questions anytime, using the Chat feature in the GoToWebinar Control Panel

Agenda

- Introductions & "House Rules"

- A Data-Centric Approach Is Required For Security Today

- Are You Controlling Information Disclosure?
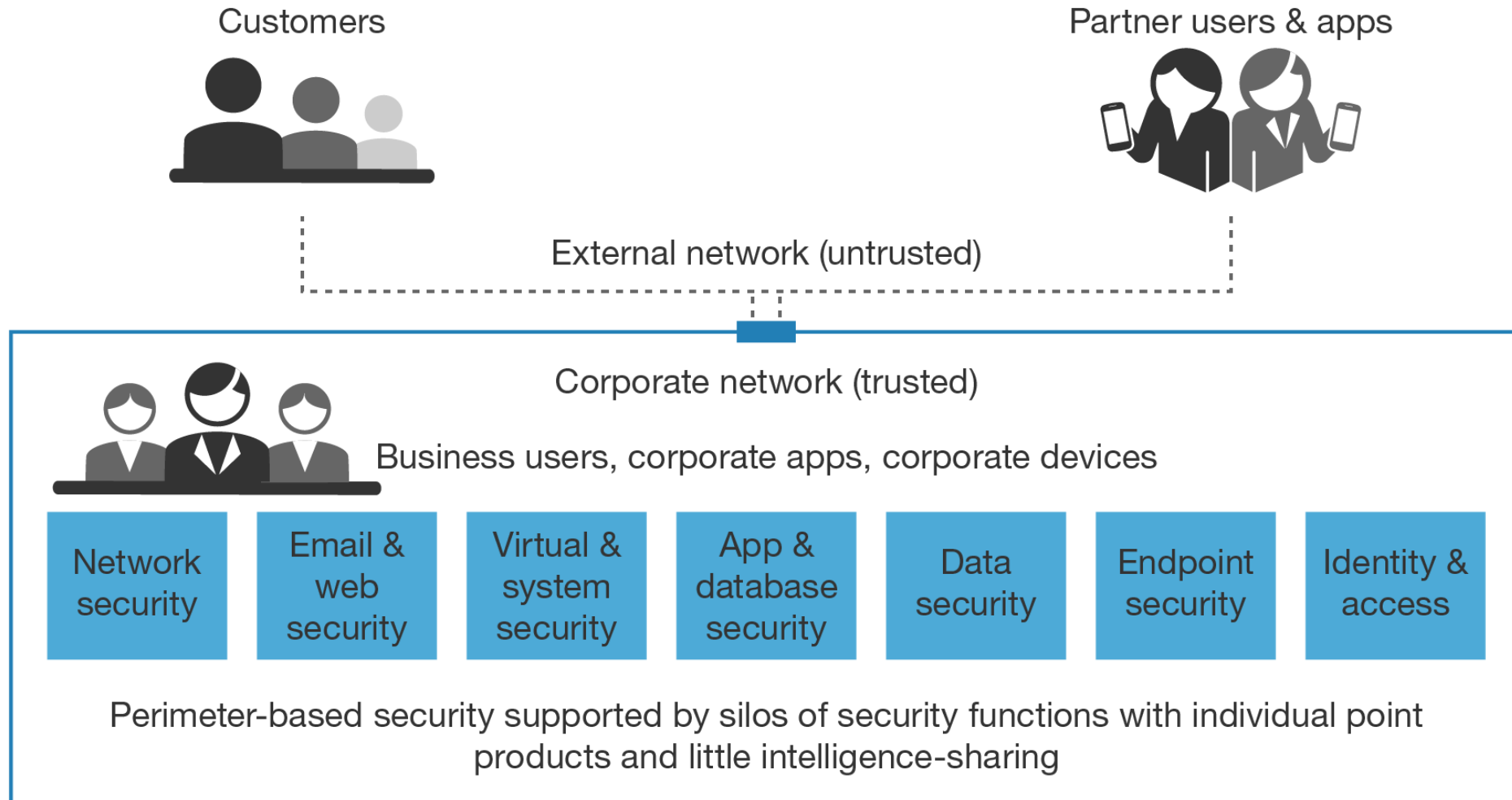
- RightsWATCH Live Demo

- Questions & Answers

FORRESTER®

A Data-Centric Approach Is Required For Security Today
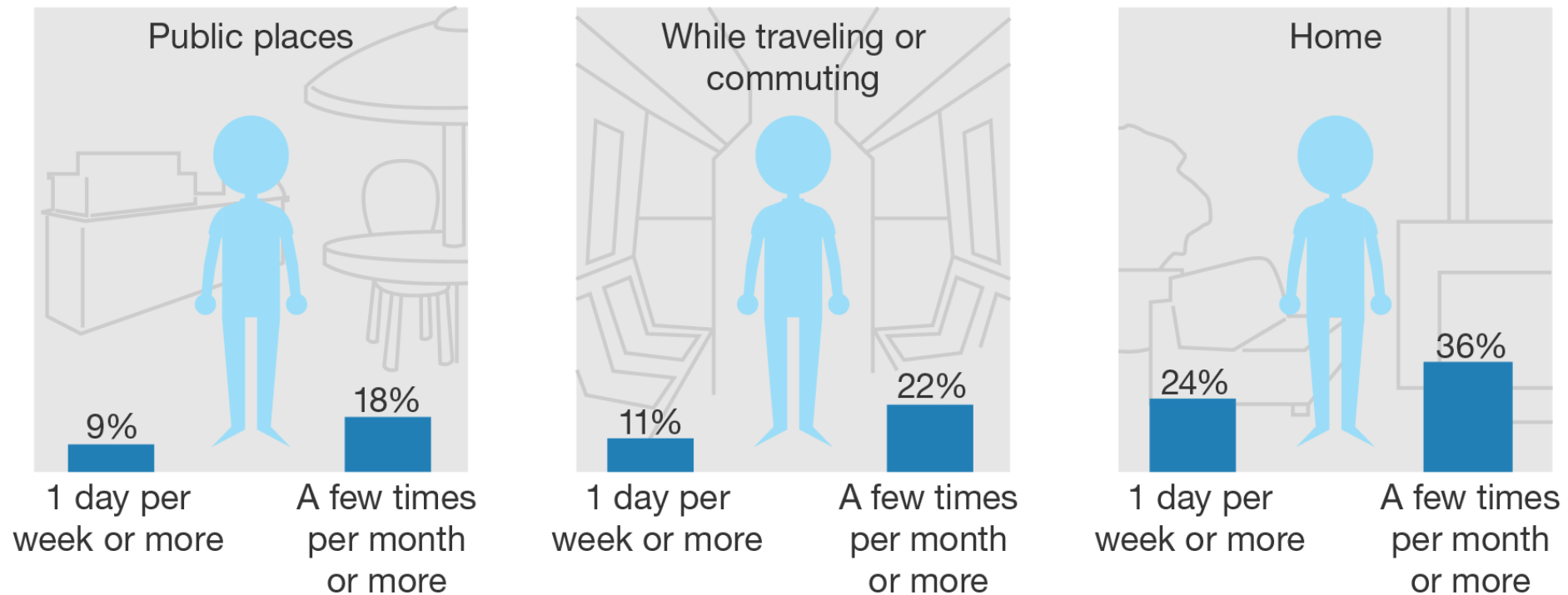
Heidi Shey, Senior Analyst

Yesterday's approach to data security

Customers

Partner users & apps

External network (untrusted)

Corporate network (trusted)

Business users, corporate apps, corporate devices

Network security	Email & web security	Virtual & system security	App & database security	Data security	Endpoint security	Identity & access

Perimeter-based security supported by silos of security functions with individual point products and little intelligence-sharing

…is insufficient for today's reality

...is insufficient for today's reality

❯ Your employees get work done in different ways

Public places

9%
1 day per week or more

18%
A few times per month or more

While traveling or commuting

11%
1 day per week or more

22%
A few times per month or more

Home

24%
1 day per week or more

36%
A few times per month or more

Base: 7,032 global information workers

Source: Forrester's Business Technographics Global Telecom And Mobility Workforce Survey, 2014

...is insufficient for today's reality

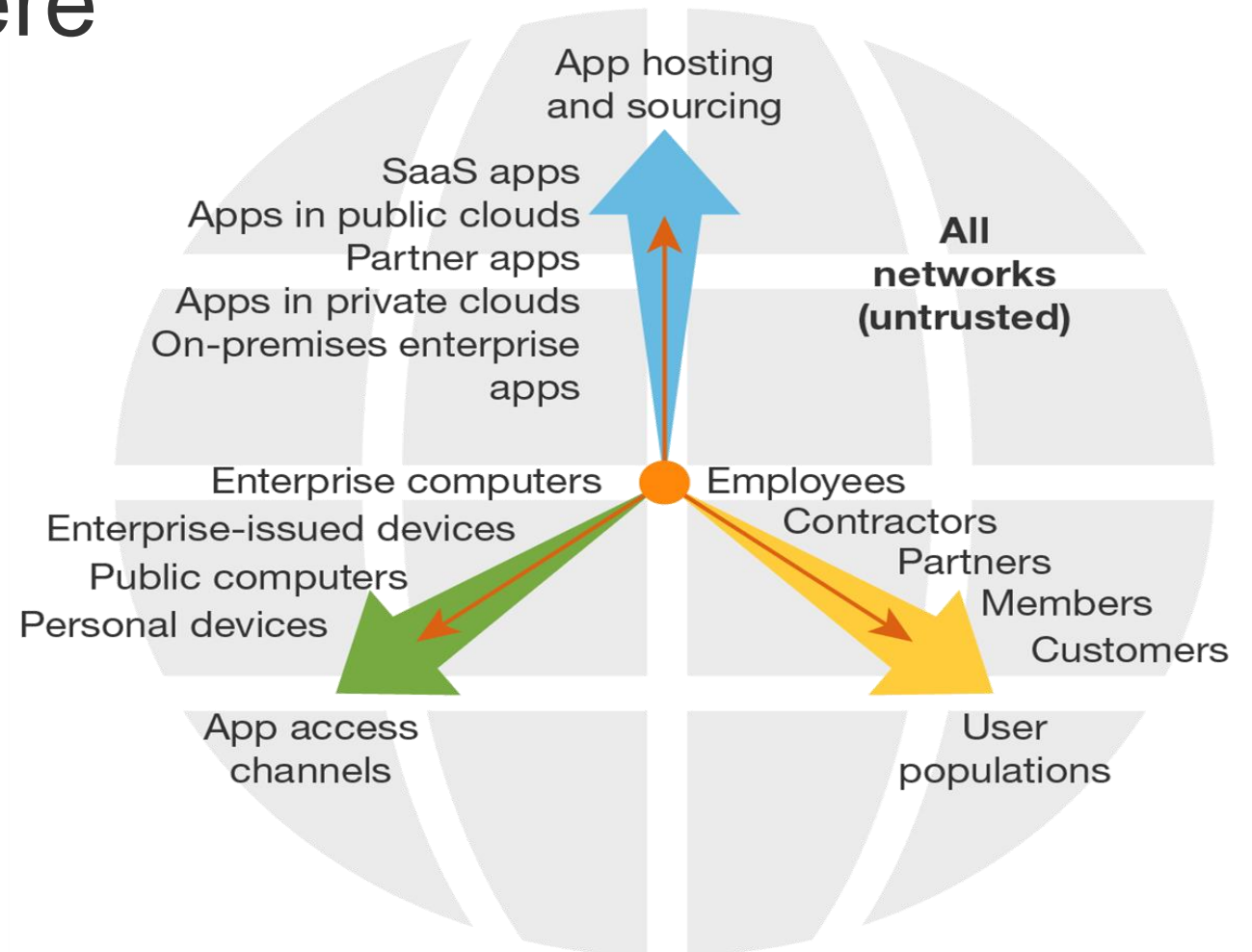› Your employees get work done in different ways

52% of information workers use multiple devices for work

Source: Forrester's Business Technographics Global Telecom And Mobility Workforce Survey, 2014
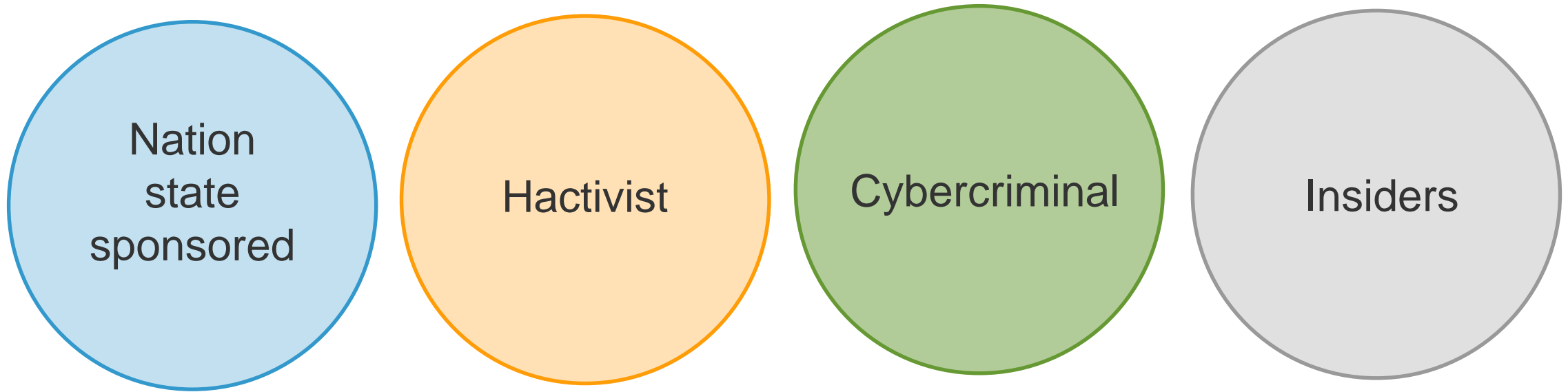
…is insufficient for today's reality
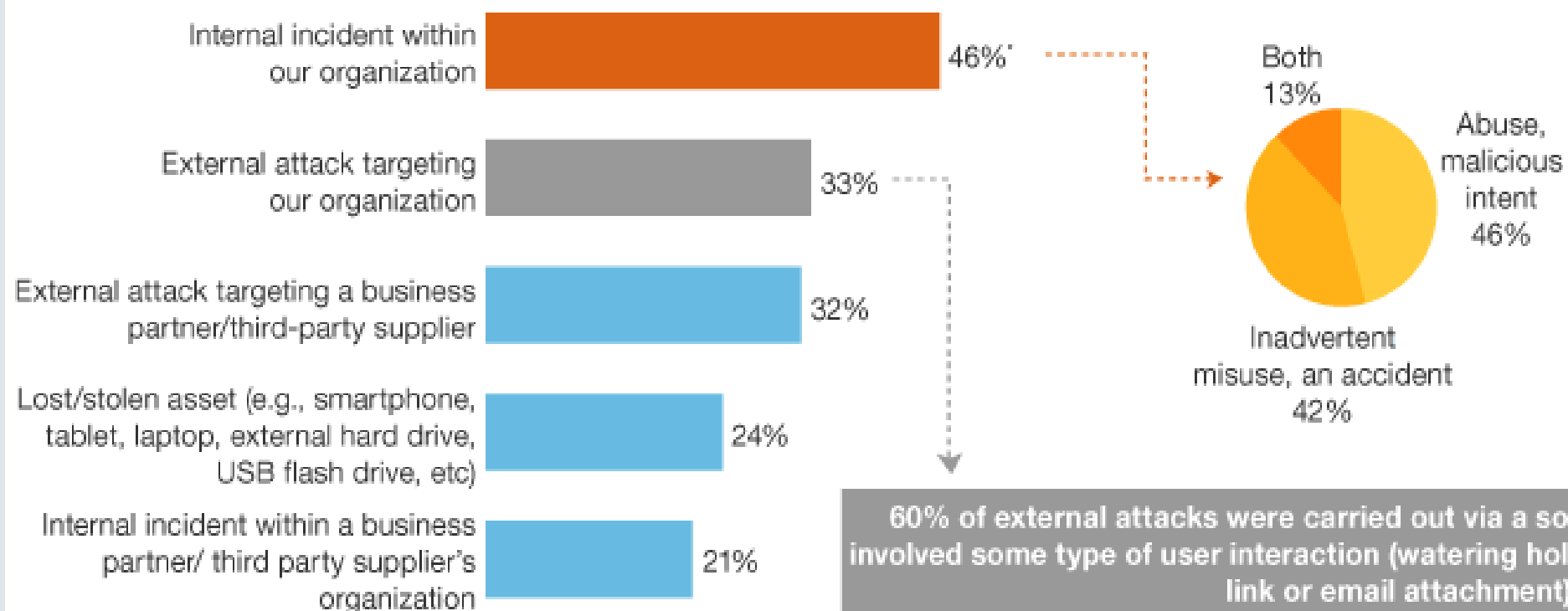
› Your data is everywhere

App hosting and sourcing

SaaS apps
Apps in public clouds
Partner apps
Apps in private clouds
On-premises enterprise apps

All networks (untrusted)

Enterprise computers   Employees
Enterprise-issued devices   Contractors
Public computers   Partners
Personal devices   Members
    Customers

App access channels

User populations

…is insufficient for today's reality

› The threat landscape has changed

Nation state sponsored

Hactivist

Cybercriminal

Insiders

…is insufficient for today's reality

"What were the most common ways in which the breach(es) occurred in the past 12 months?"

Category	Percentage
Internal incident within our organization	46%
External attack targeting our organization	33%
External attack targeting a business partner/third-party supplier	32%
Lost/stolen asset (e.g., smartphone, tablet, laptop, external hard drive, USB flash drive, etc)	24%
Internal incident within a business partner/ third party supplier's organization	21%

Pie chart:
- Both 13%
- Abuse, malicious intent 46%
- Inadvertent misuse, an accident 42%

60% of external attacks were carried out via a software exploit, while 42% involved some type of user interaction (watering hole attack, phishing, malicious link or email attachment).*

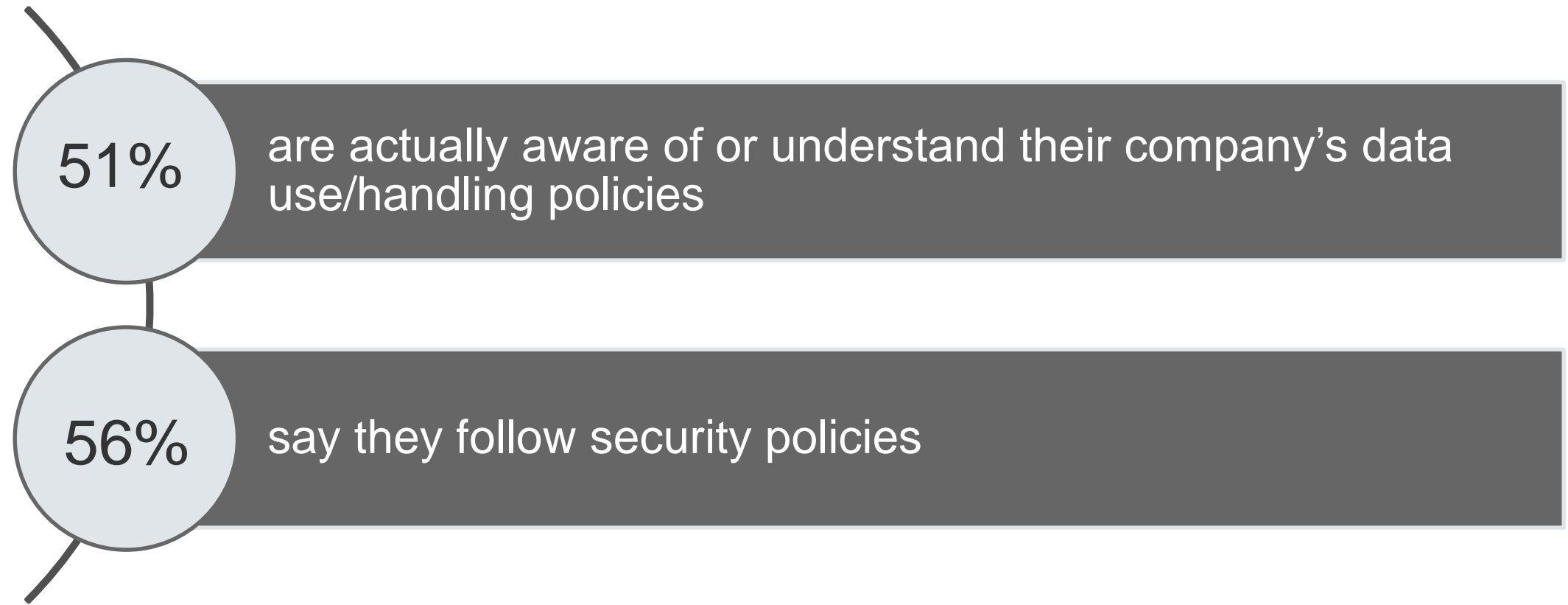Base: 318 North American and European technology decision-makers who have experienced data breaches in the past 12 months (20+ employees); *181 to 184 North American and European technology decision-makers who have experienced the specified breaches (20+ employees)

*Note: May not add up to 100% due to rounding
Source: Forrester's Business Technographics Global Security Survey 2014

…is insufficient for today's reality

❯ Your employees have varying attitudes about data

51% are actually aware of or understand their company's data use/handling policies

56% say they follow security policies

Source: Forrester's Business Technographics Global Devices And Security Workforce Survey, 2014

Defense in depth is a good concept

…but often turns into expense in depth

Causes of expense in depth

Lack of an overarching strategy

Causes of expense in depth

Lack of an overarching strategy

Insufficient due diligence; feature/capability overlap and redundancy

Causes of expense in depth

Lack of an overarching strategy

Insufficient due diligence; feature/capability overlap and redundancy

Difficulty integrating different solutions; too many silos

It's time for a data-centric strategy
Put your controls closer to the data

Forrester's data security and control framework

Define	
Data discovery	Data classification

Forrester's data security and control framework

Define	
Data discovery	Data classification

$$3P + IP = TD$$

The 3 P's
- PCI
- PHI
- PII

Intellectual property

Toxic data

Forrester's data security and control framework

Define

| Data discovery | Data classification |

Dissect

| Data intelligence | Data analytics |

Forrester's data security and control framework

Define	
Data discovery	Data classification

Dissect	
Data intelligence	Data analytics

Defend			
Access	Inspect	Dispose	Kill
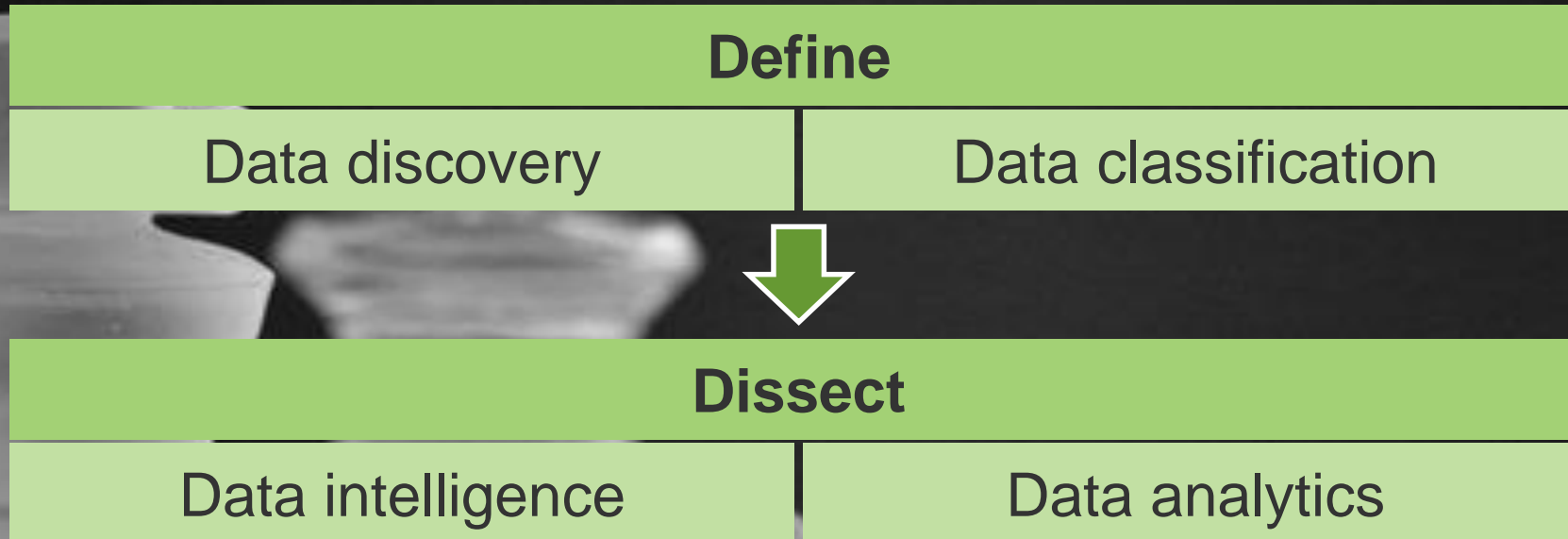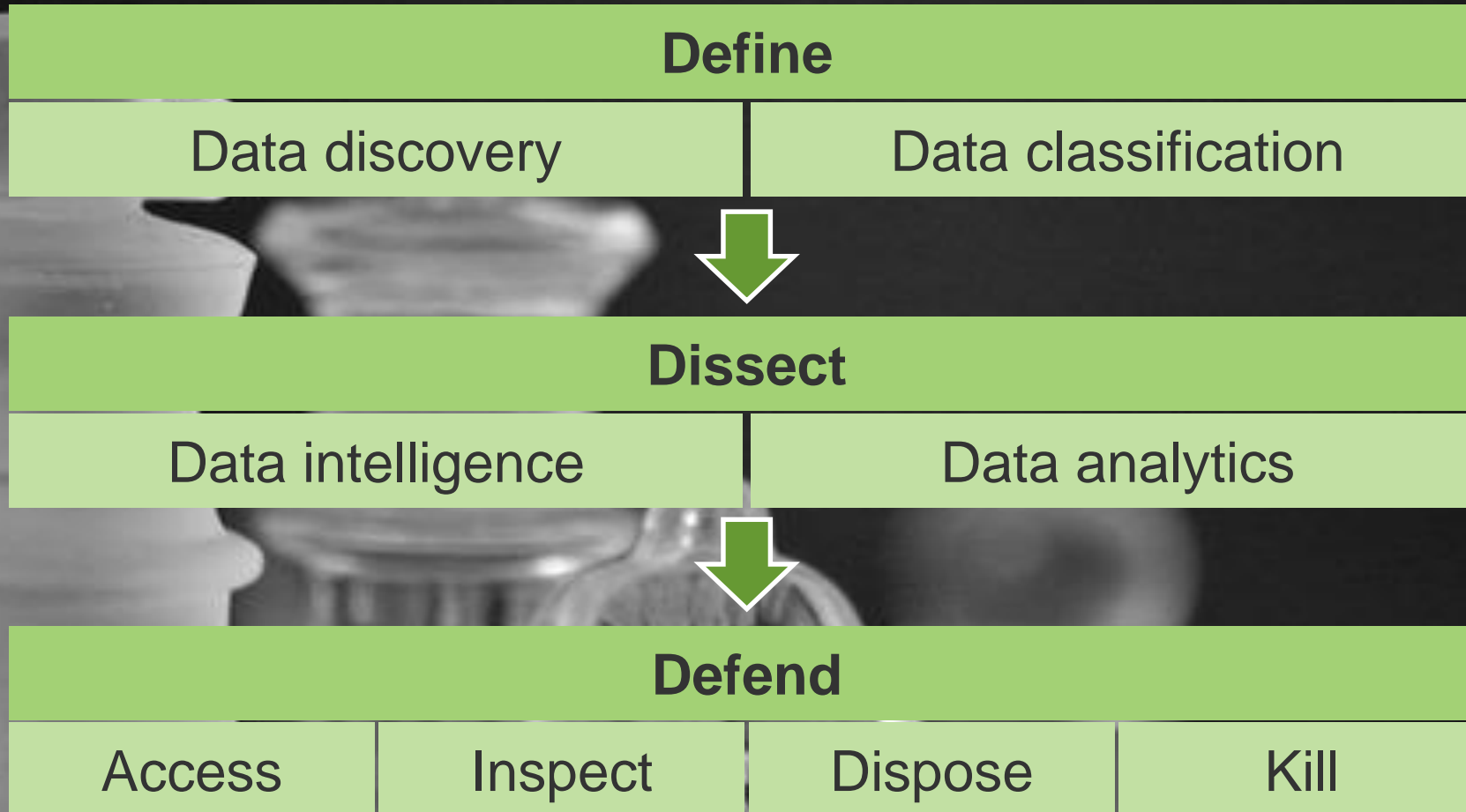
Key technologies and their outlook
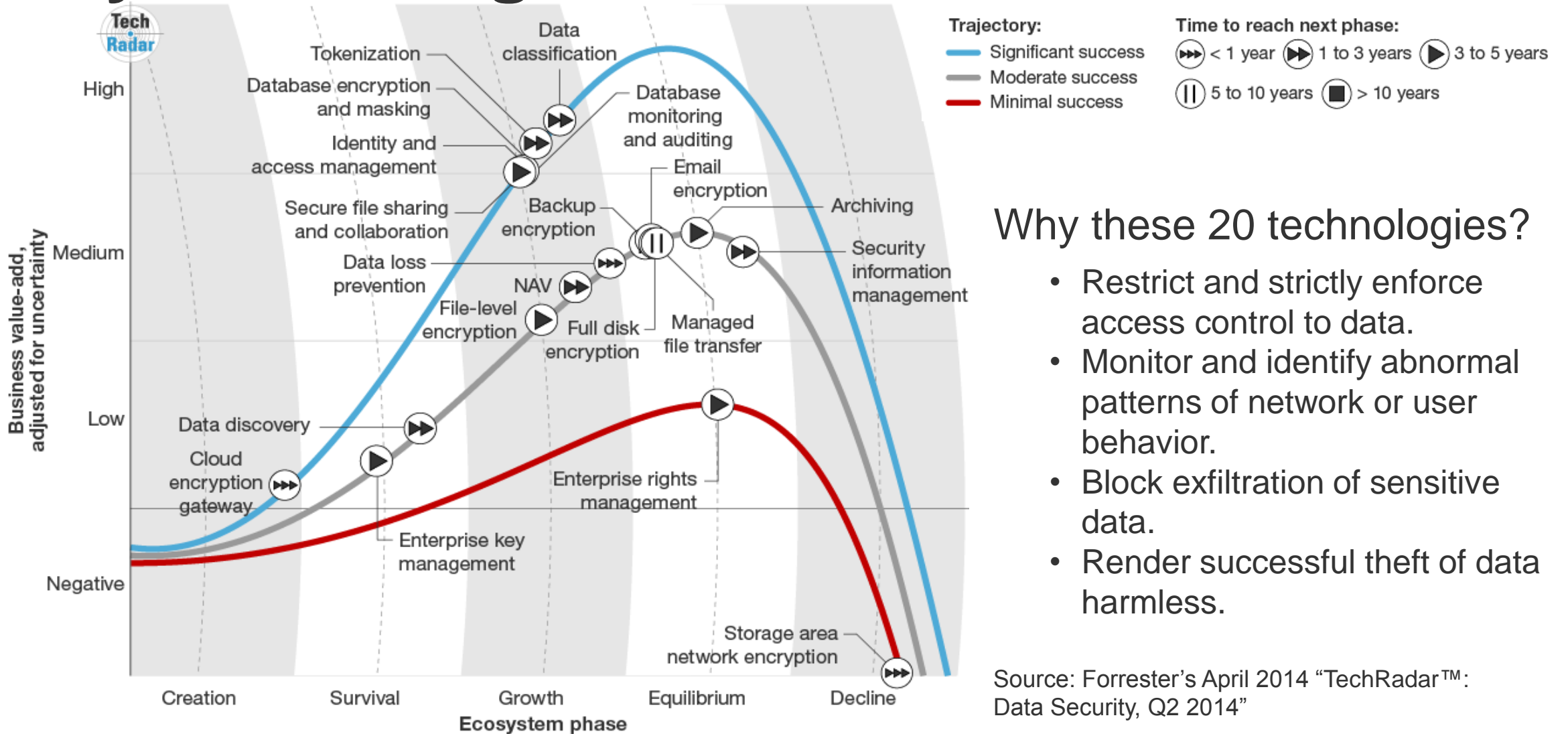
Why these 20 technologies?

- Restrict and strictly enforce access control to data.
- Monitor and identify abnormal patterns of network or user behavior.
- Block exfiltration of sensitive data.
- Render successful theft of data harmless.

Source: Forrester's April 2014 "TechRadar™: Data Security, Q2 2014"

Key technologies and their outlook
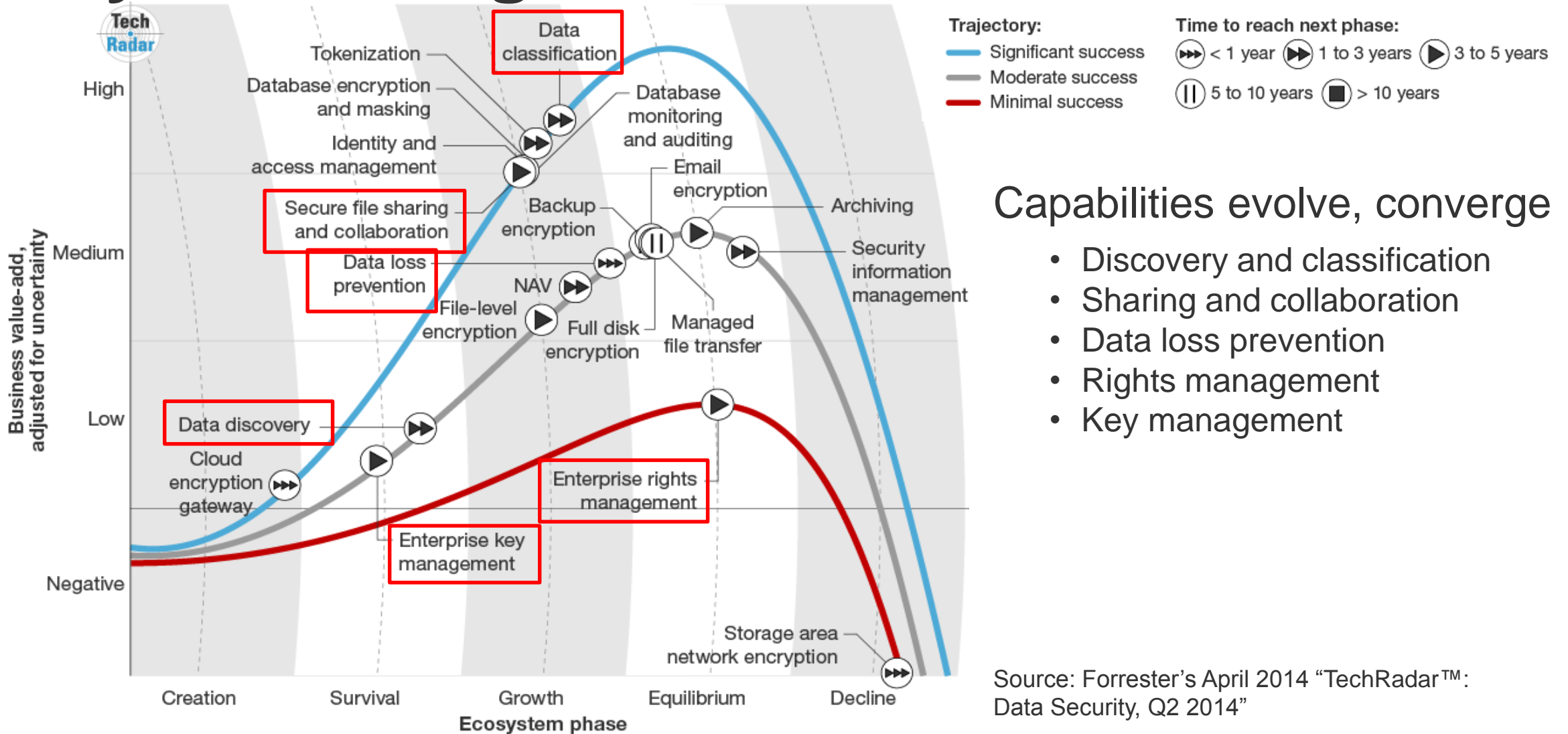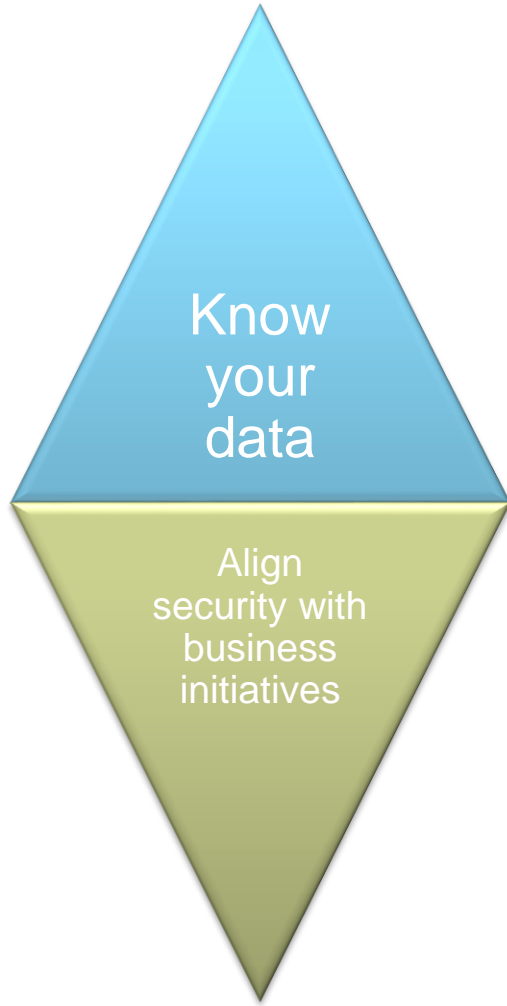

Capabilities evolve, converge

- Discovery and classification
- Sharing and collaboration
- Data loss prevention
- Rights management
- Key management

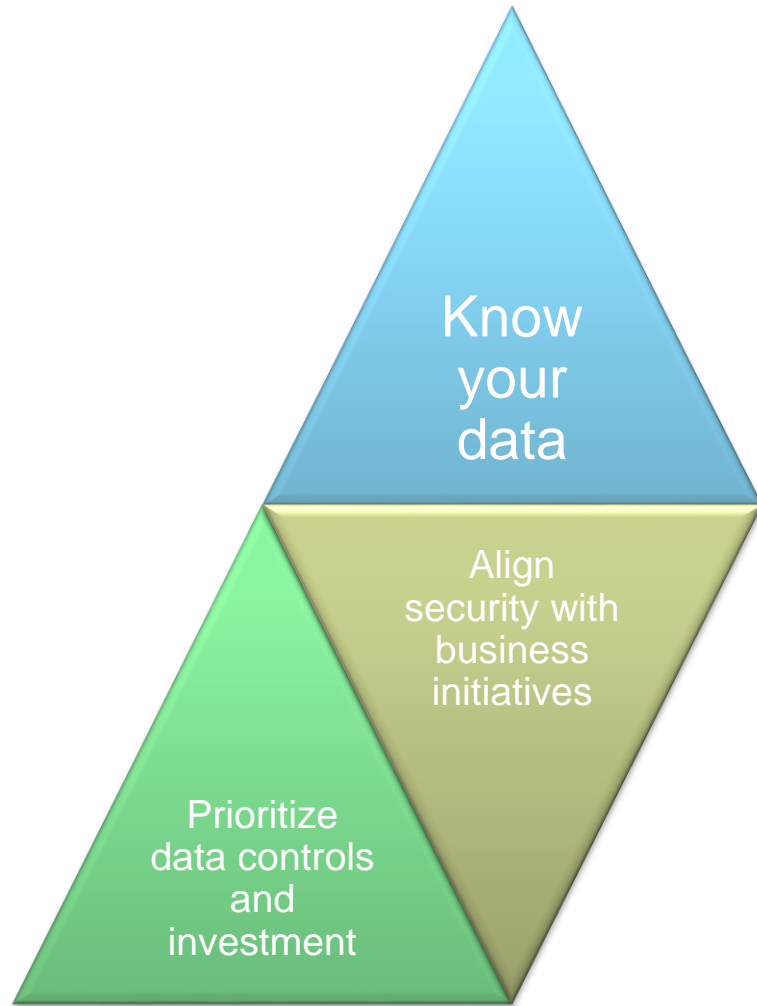Source: Forrester's April 2014 "TechRadar™: Data Security, Q2 2014"

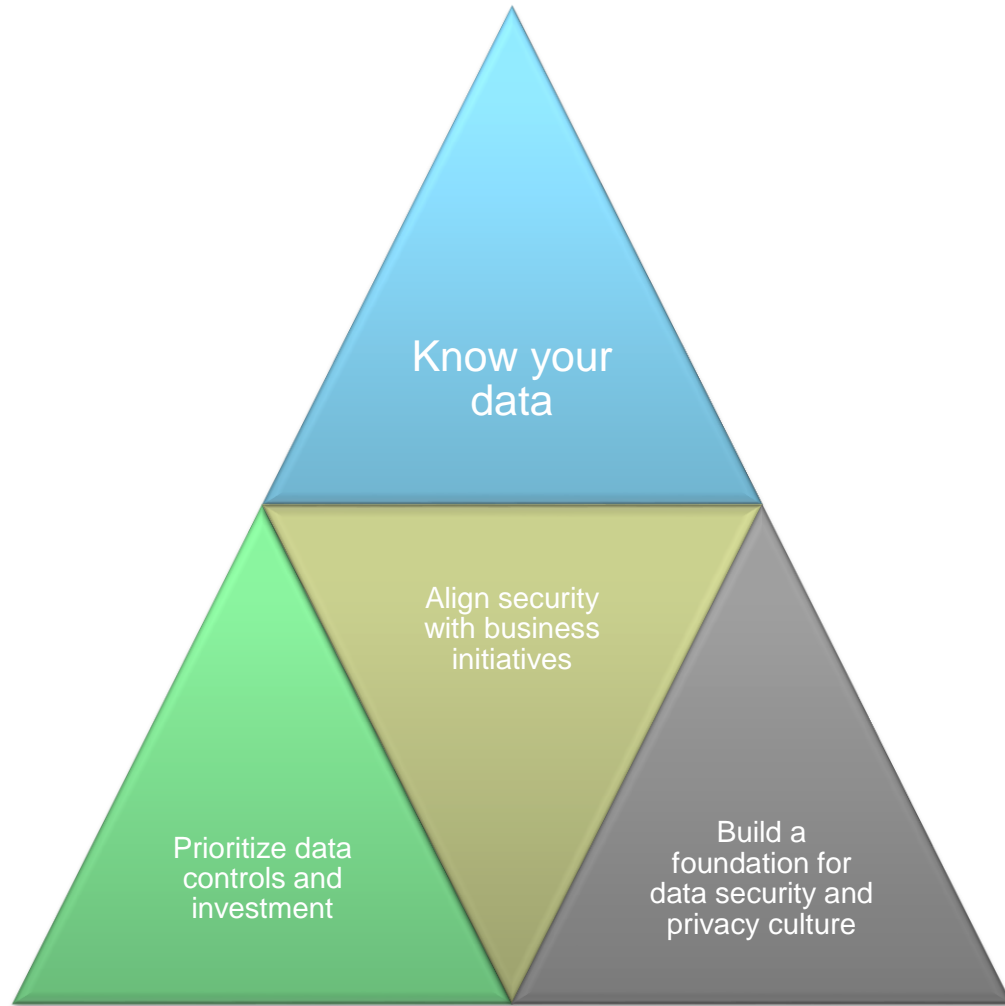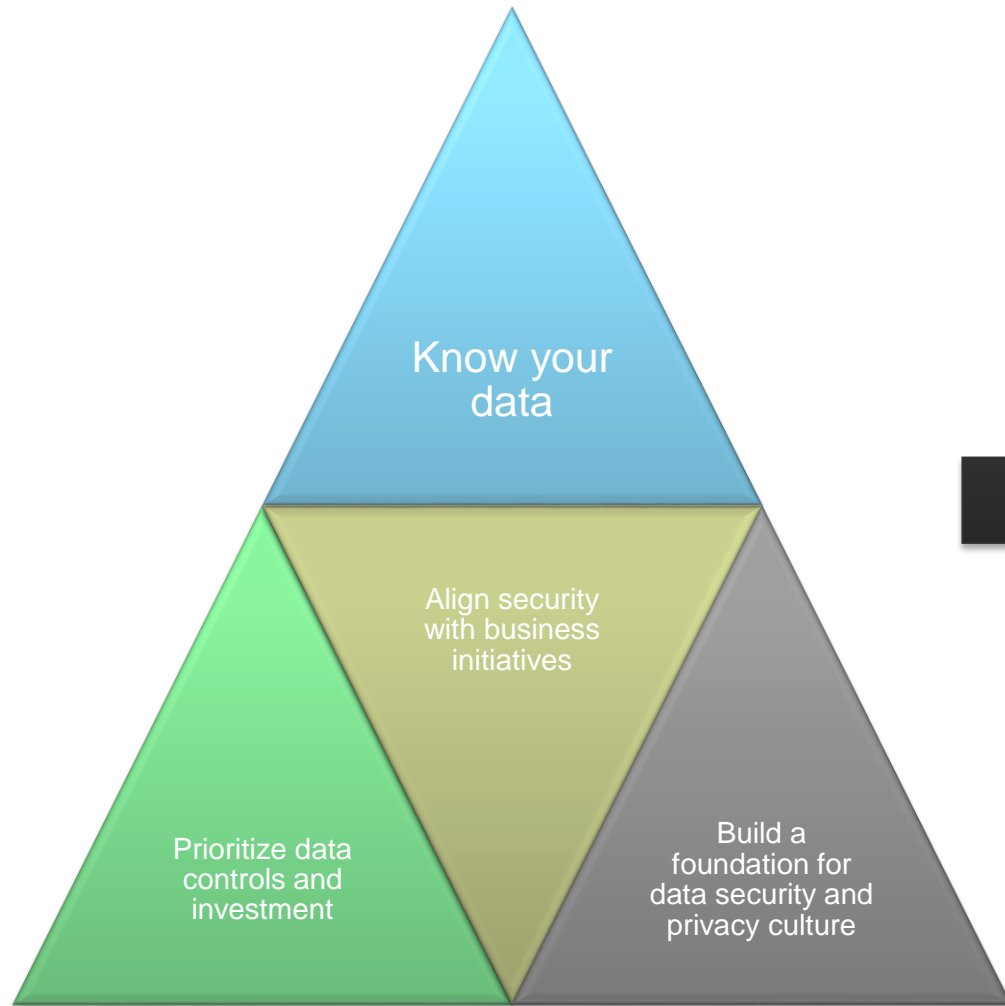# Benefits of a data centric strategy

Know your data

Benefits of a data centric strategy

Know
your
data

Align
security with
business
initiatives

Benefits of a data centric strategy

Benefits of a data centric strategy

Benefits of a data centric strategy

Know your data

Align security with business initiatives

Prioritize data controls and investment

Build a foundation for data security and privacy culture

Transform data security and privacy into a business differentiator

Poll

What do you anticipate as your biggest challenge for a data-centric approach to security?

1. Data classification
2. Budget; justification for investment
3. Staffing constraints
4. Prioritizing our investments
5. Addressing compliance requirements

Agenda

- ~~Introductions & "House Rules"~~

- ~~A Data-Centric Approach Is Required For Security Today~~

- **Are You Controlling Information Disclosure?**

- **RightsWATCH Live Demo**

- **Questions & Answers**
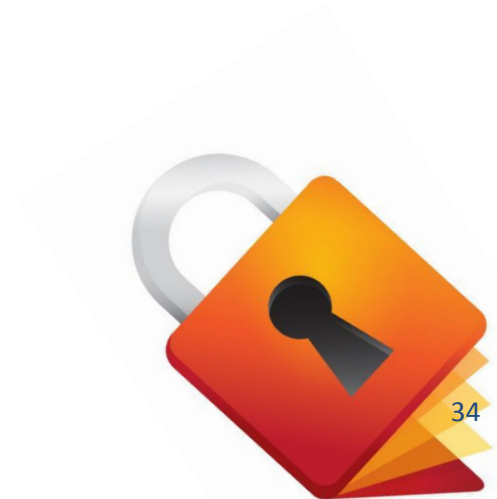
Watchful®

Keep IT secret.

Are you controlling information disclosure?

Rui Melo Biscaia, Director of Product Management

Are you controlling information disclosure?

- The sheer amount of data to protect is overwhelming

- Cloud, "BYO" and 3rd parties ultimately mean "Data has Left the Building"

- Data exists to be consumed, thus security MUST become Data-Centric

- Rendering your data useless is the strongest answer to the "not IF but WHEN" issue

Forrester's data security and control framework

Data discovery	Data classification

- Need to locate, index, and catalogue data for better control

- RightsWATCH:
  - Discovers data files in repositories and tags it according to the data toxicity
  - Always analyses content, context and file attributes to discover and classify every single data file, wherever the file resides

Forrester's data security and control framework (II)

Data intelligence	Data analytics

- **Need to provide business and other contextual insights about data, while identifying changing threats to data and guides decision-making**

- **RightsWATCH:**
    - Provides intelligent time access and content expiration controls over data
    - Delivers a comprehensive audit trail on who is doing, what, when and how with data that is valuable to the business and to security

Forrester's data security and control framework (III)

Access	Inspect	Dispose	Kill

- Need to ensure the right user gets access to the right data at the right time; understand patterns to identify risks; mitigate risk by discarding data; and ensure data can't be used or sold

- RightsWATCH:
  - Applies the principle of least privilege, by enforcing RBAC over data
  - Logs a comprehensive audit trail to mitigate the malicious internal user
  - Delivers a proper classification tags for data disposal purposes
  - Leverages encryption to devalue and/or remote "Kill" data

RightsWATCH is Data-centric Security

Identify

Dynamic Engine

Rules based on content, context, and metadata

Classify

Governs access, usage, and markings

Tied to company established compliance policy

Mark/Tag

Watermarks, headers, and footers

Disclaimers and metadata tags

Protect

Strong encryption, tied to use credentials

All rights managed

Track Report

All activity logged, tracked, reported
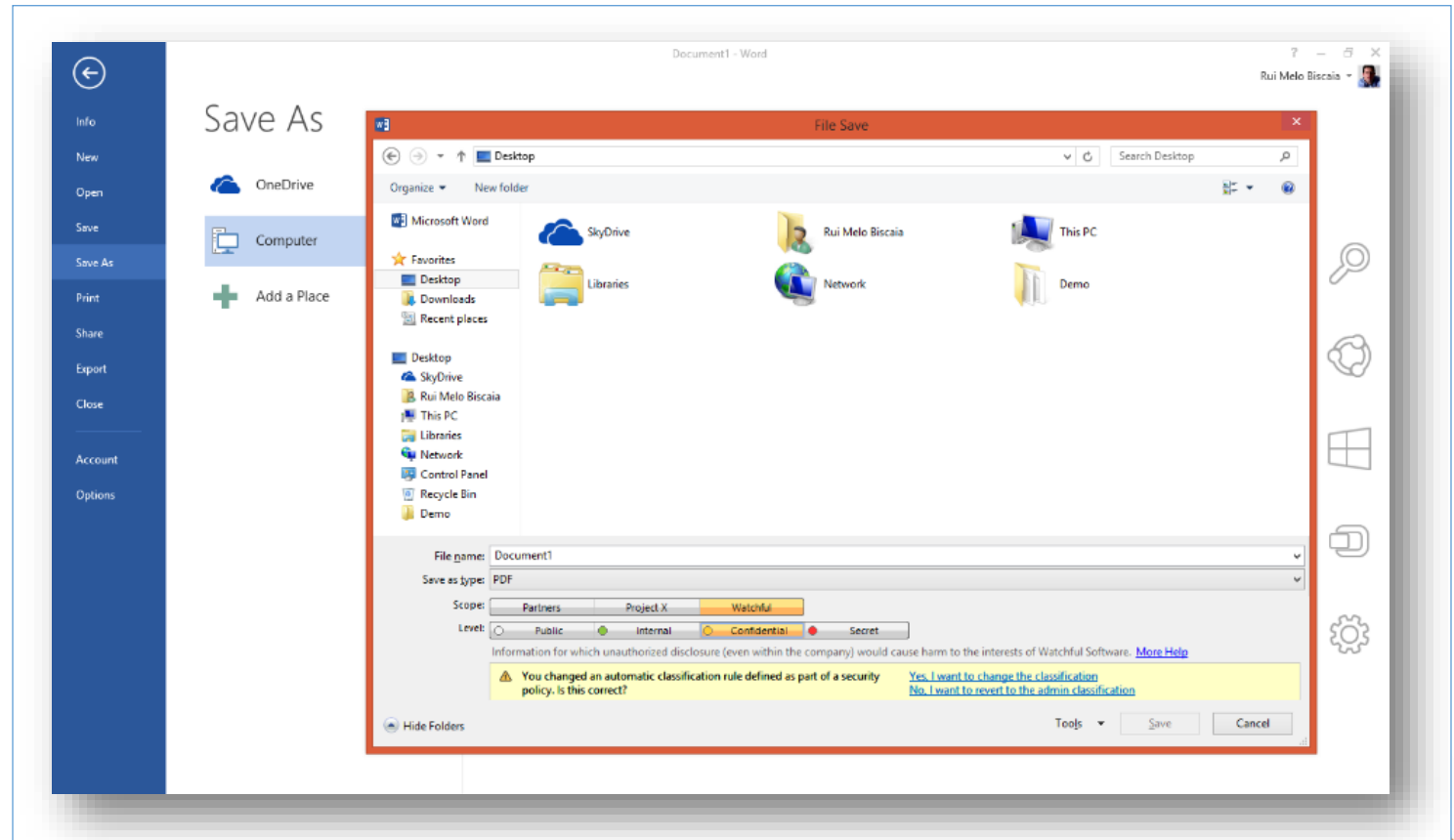
Centralized database

Agenda

- Introductions & "House Rules"

- A Data-Centric Approach Is Required For Security Today

- Are You Controlling Information Disclosure?

- **RightsWATCH Live Demo**
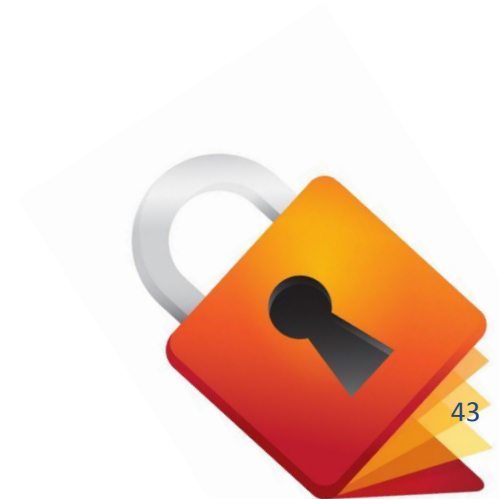
- **Questions & Answers**

RightsWATCH Live Demo

Agenda

- Introductions & "House Rules"

- A Data-Centric Approach Is Required For Security Today

- Are You Controlling Information Disclosure?

- RightsWATCH Live Demo

- **Questions & Answers**

The X-Factor in Data-Centric Security

Questions & Answers

Webinar, Tuesday July 14th 2015

Thank You!

Heidi Shey

+1 617.613.6076

hshey@forrester.com

Rui Melo Biscaia

+351 21 714 5430

rui.biscaia@watchfulsoftware.com

The X-Factor in Data-Centric Security

Webinar, Tuesday July 14th 2015