RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PART1-W11

Modern Strategies for Protecting Users and Data in a Borderless World

Homayun Yaqub

Senior Security Strategist
Forcepoint

Homayun Yaqub

- Partners with executives across various industries to architect and deliver strategies addressing core business issues to reduce risk exposure
- 25 years of security experience in the U.S. military, government, and private sector
- Led multiple security initiatives at JPMorgan Chase & Company
- Advised Global 1000 companies on improving risk management strategies
- Leadership and executive roles in the Department of Defense and U.S. Intelligence Community
- Former U.S. Army Officer


Office 365
Azure
Workday
Google Cloud
Branch Office
Remote Users
Salesforce
Github
SAP
Cloud Services
Slack
BOX
Branch Office
Remote Users
Business Partners
Enterprise HQ
Remote Users
Branch Office
Customers
Customers

The Universe

Create – Interact – Share

The Reality

Personal Data

Organizational Data/IP

BYOD

SaaS

On Prem

Remote

Hybrid

The Challenges

Continuously Expanding Attack Surface

Lack of Visibility

Disjointed Security Policy

Siloed Security Solutions

Signals Become Noise

Disparate Compliance Regulations

The World Changes… But There Are Two Constants

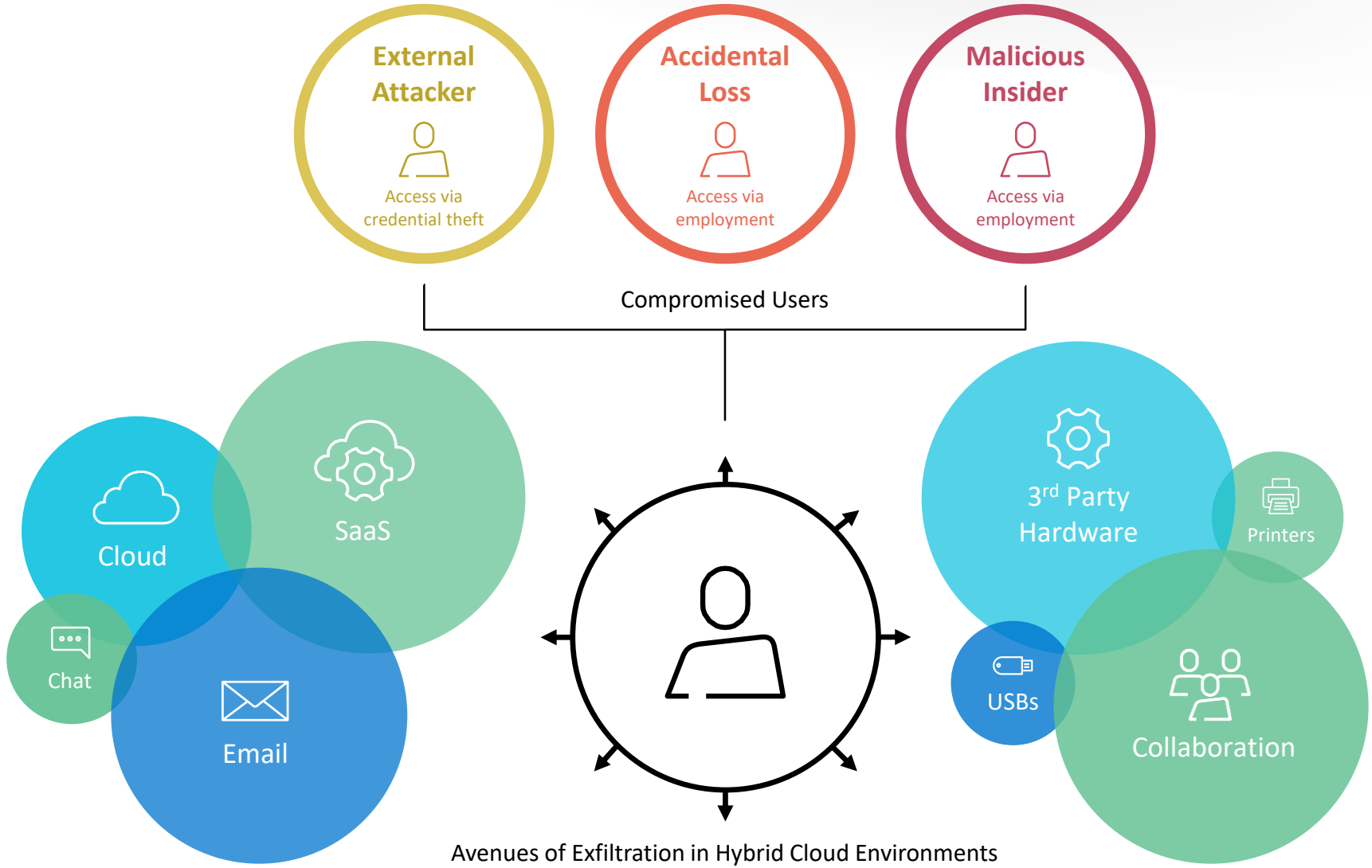
People

Data (IP)

Innovation
Growth
Productivity

Theft
Damage
Misuse

Greatest Risk – Compromised Access



Avenues of Exfiltration in Hybrid Cloud Environments

The Evolution

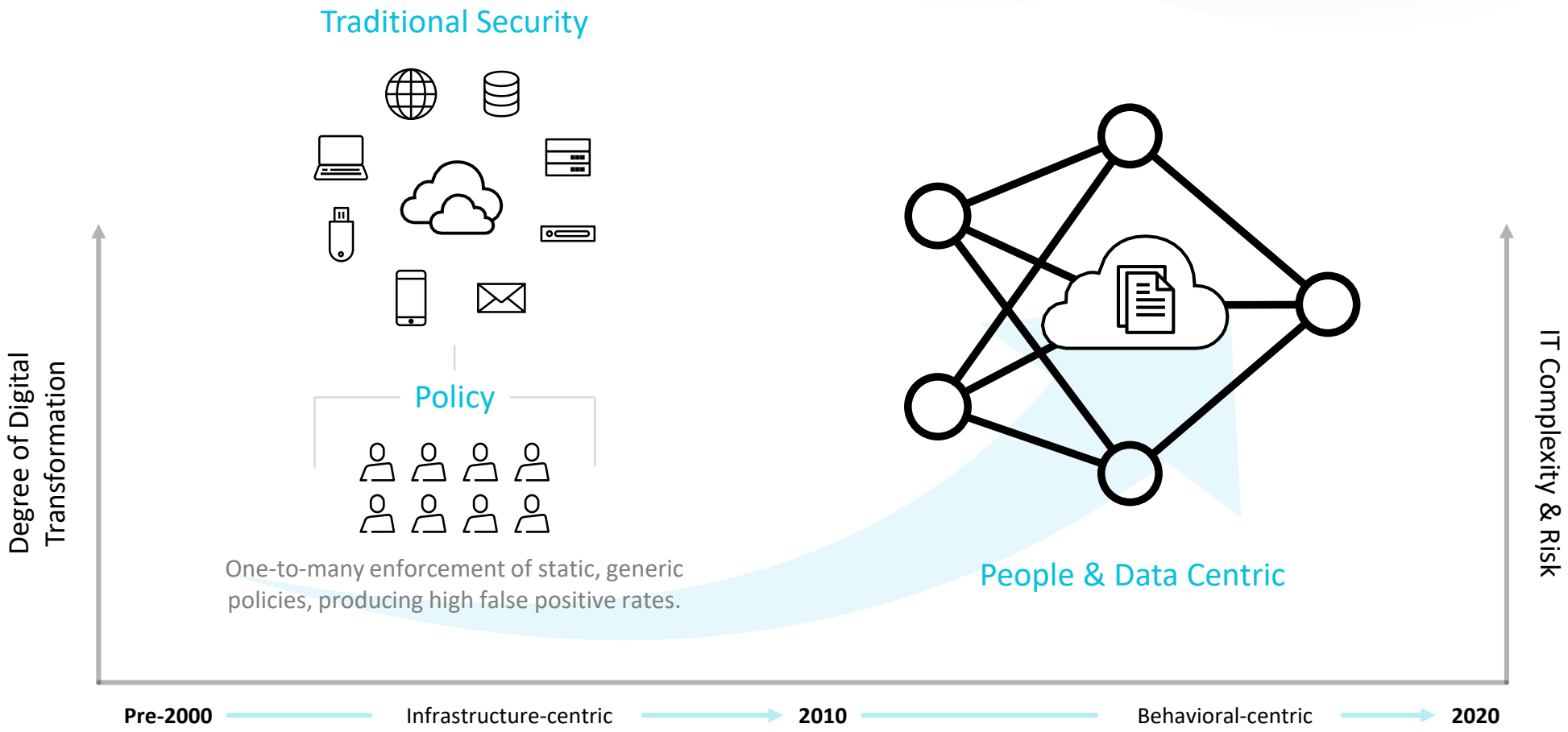
Paradigm Shift

- Centralized Data Lakes and Analytics
- Events
- **Threat Intelligence** (IOCs)
- Fixed rules
- External Attacker
- Infrastructure Security

- Decentralized Data and Analytics
- Entity Based Activities
- **Behaviors and Context** (IOBs)
- Risk Adaptive
- Compromised Accounts and Devices
- User and Data Security

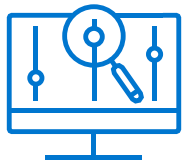
- Place People and Data at the center of your design thinking
- Ensure meaningful visibility
- Implement Privacy by Design
- Shift from Threats to a Risk and Behavior centric approach
- Enable Adaptive Responses
- Focus Uses Cases on User and Data Protection

1 Design


Traditional Security
Policy
One-to-many enforcement of static, generic policies, producing high false positive rates.
People & Data Centric
Degree of Digital Transformation
IT Complexity & Risk
Pre-2000
Infrastructure-centric
2010
Behavioral-centric
2020

2 Meaningful Visibility

User Activity Monitoring (UAM) is the monitoring of user behavior



Observation of user interaction with data

Use of analytics to understand user behavior

Visibility to potential risk and threats

Operationalizing more effective investigations and adaptive approaches to managing risk

Continuous evaluation for real time risk quantification at the user level

UAM stakeholders are from across the business

Stakeholders must be involved from design to implementation

Worker's Advocates will focus on protecting employee rights

HR teams hold very sensitive data and are also involved in investigation process.

Legal teams can help you navigate the various laws & regulations

Privacy regulations put employees at the center of your program

Conduct a Data Protection Impact Assessment:

- Ensures there is a balance between Personal data & IP protection & workforce privacy

Start with a Data Protection Impact Assessment:

- Ensures there is a balance between Personal data & IP protection & workforce privacy

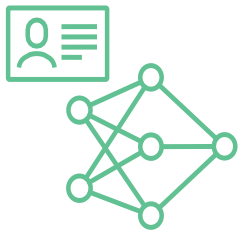
Limit scope of program to critical risks & necessary data collection first

- Reduce how long you keep data
- Don’t get involved in diagnosis!

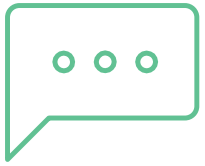
Impact is much lower when you apply privacy by design or by default.

3 Manage Appropriate Access to your Employee Data

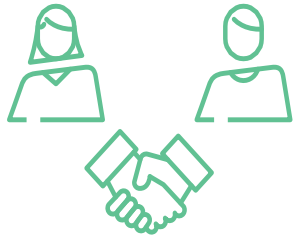
Limit access to the data collected



Anonymize user identity in risk evaluation and reporting



Use real-time notifications to indicate and educate users



Ensure worker advocates and related stakeholders are part of the re-identification

4 Behavior and Risk Centric

Monitor Entities

- Learn their normal behavior
- Learn how they behave relative to their peers
- Learn how they interact with critical data and IP
- Based on deviations, compute an entity risk

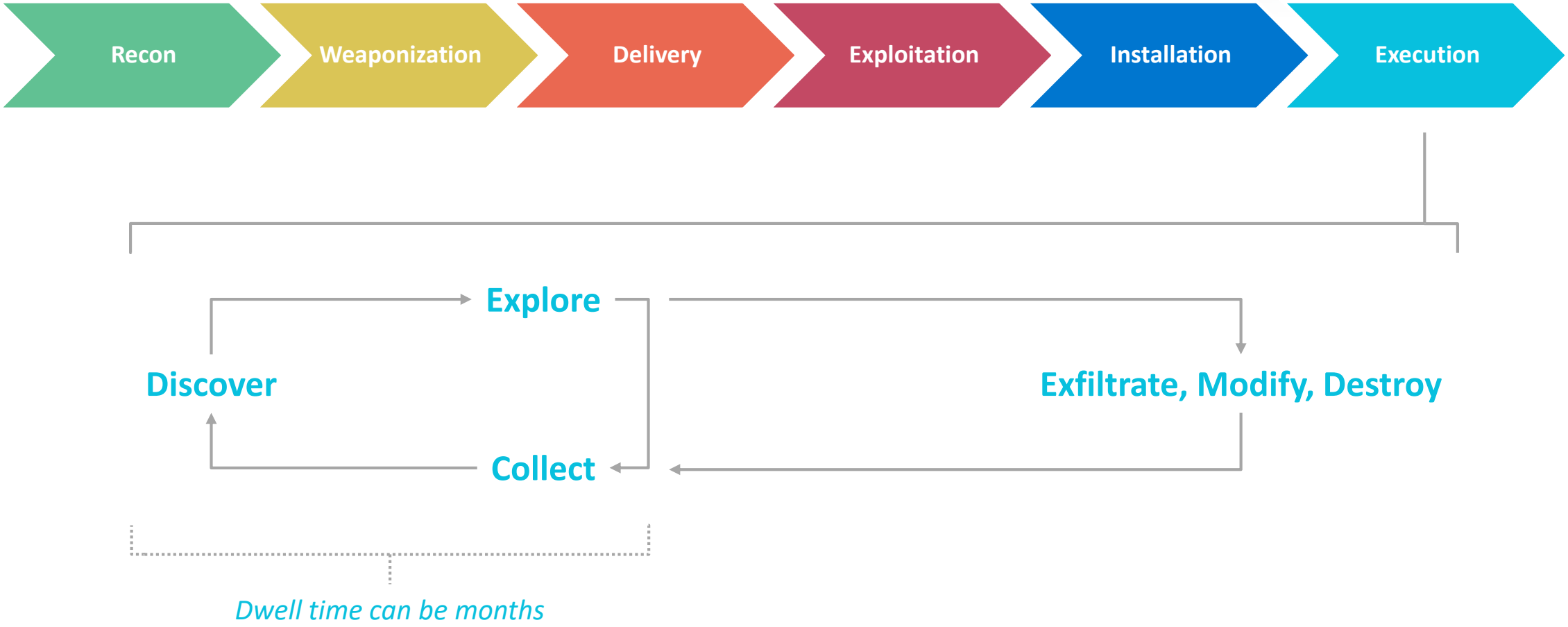
Understand Humans

- Track and assess human factors

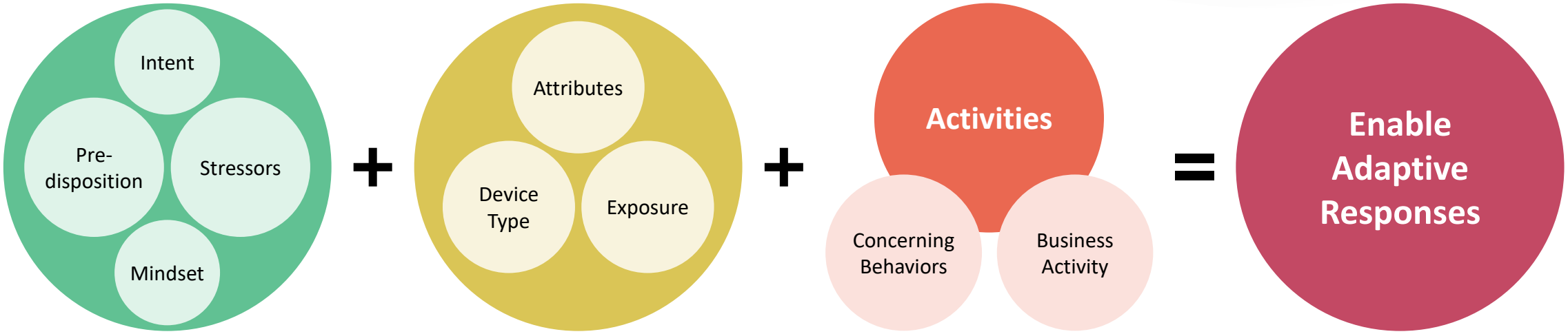
Shift to a risk-based approach

- An ‘event’ can both be good or bad, depending on the context of the entity

Expanding/Improving the Kill Chain



The Inclusion of Human Factors



- Critical Path to Insider Threat
- SOFIT

Activities that, out of **context** would be benign, now flag an attack

”Detection Rules” that normally generate a lot of **false positives** are now weighed by the risk of the entities.

5 Enable Adaptive Responses

Risk Adaptive Protection:

- Dynamically apply monitoring and enforcement controls
- Based on the calculated behavioral risk level of users and value of data accessed.

Benefit:

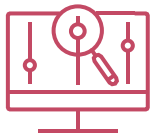
- Better understand risky behavior and automate policies
- Dramatically reduces the quantity of alerts requiring investigation.

How?

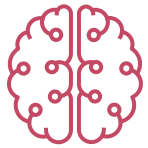
1. Stakeholders must be involved from design to implementation
2. Worker's Advocates will focus on protecting employee rights
3. HR teams hold very sensitive data and are also involved in investigation process.
4. Legal teams can help you navigate the various laws & regulations

+ Enable adaptive and continuous responses (Gartner)*

Operationalizing Risk Adaptive Protection

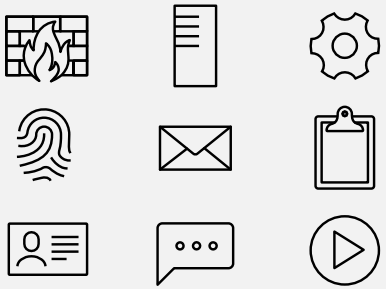


Collect Wide & Deep For Holistic Visibility

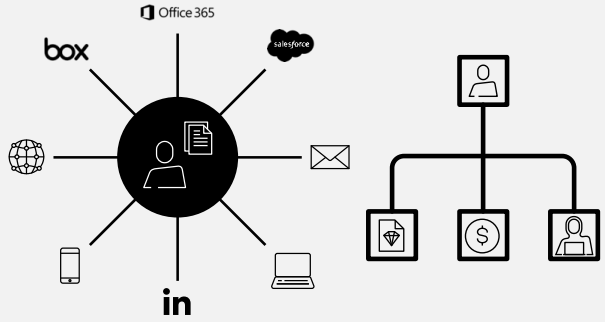


Analyze & Model To Understand Intent

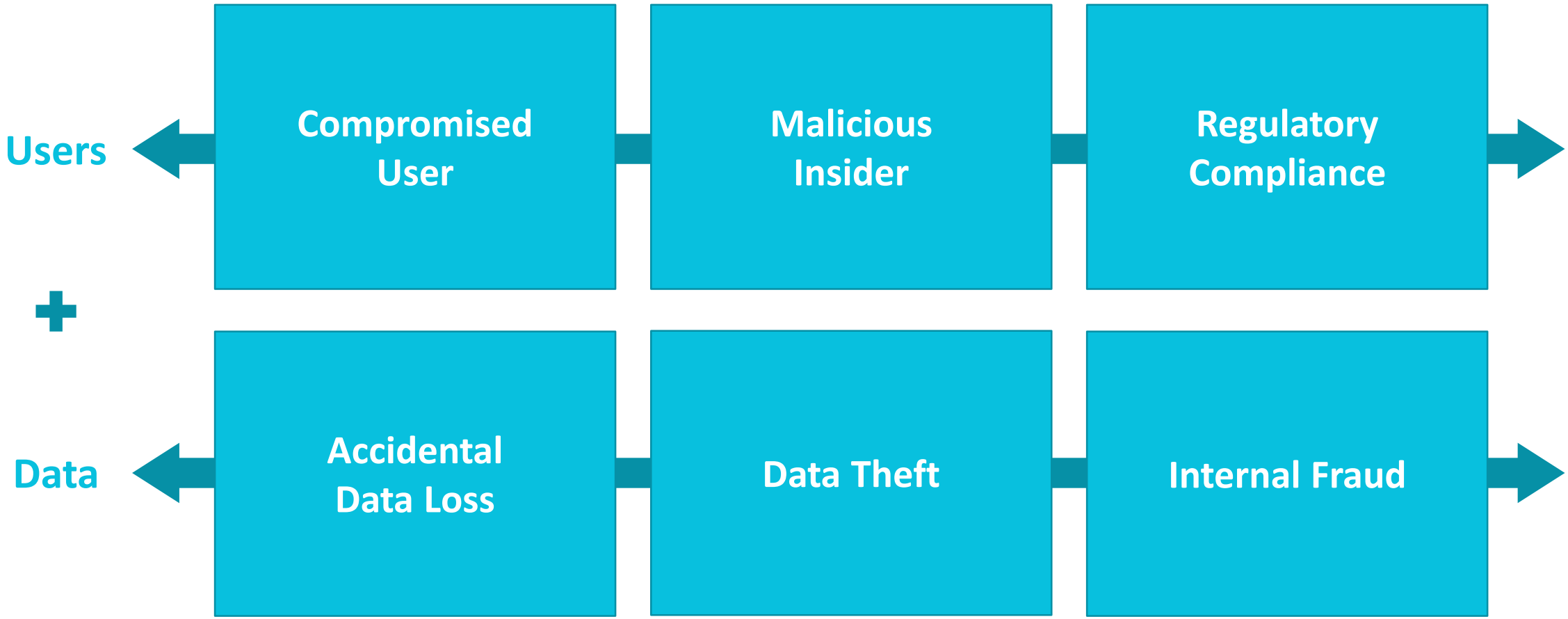
Take Action & Reduce Exposure



Data Sources ❯ Analytic Engine ❯ Informed Narrative



6 Focused Use Cases



6 Strategies for Protecting Users & Data

1. Place People and Data at the center of your design thinking
2. Ensure meaningful visibility
3. Implement Privacy by Design
4. Shift from Threats to a Risk and Behavior centric approach
5. Enable Adaptive Responses
6. Focus Uses Cases on User and Data Protection

RSAConference2020

Thank You!