A Human-Centric Approach to Risk Adaptive Cybersecurity

Brijesh Miglani – Lead Consultant

Forcepoint

6TH CYBER SECURITY INDIA SUMMIT 2020

Four Elements Of Digital Transformation That Create Advantage And Risk

DATA

"Data is the new oil and artificial intelligence the new engine of the digital economy."

- More critical data is being created than properly protected.
- Data should flow freely across the business.

NETWORK

"Workforce, devices, and business processes are globally hyperconnected."

- Network transformation to support cloud-centric IT breaks existing security architectures.
- Personnel and IoT devices are security vulnerabilities.

WORKFORCE

"Employees and partners collaborate using all of a company's assets."

- A critical need is created to ensure trusted interactions across the extended enterprise.

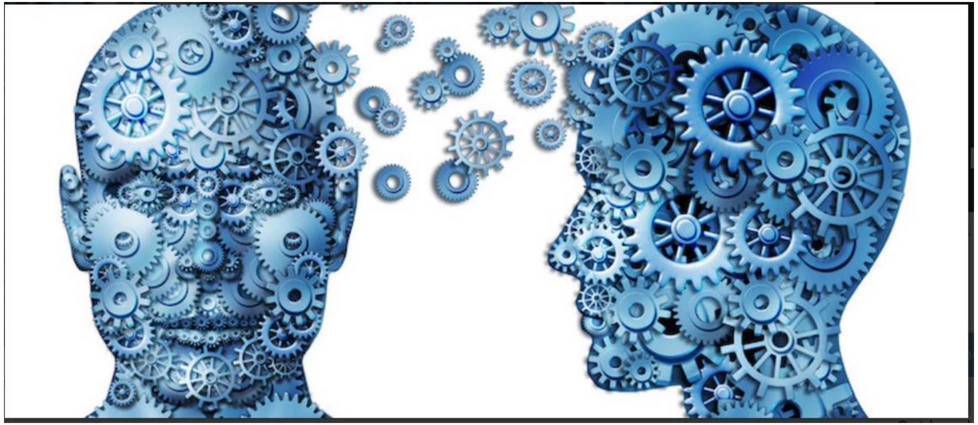
CLOUD

box workday. salesforce Office 365

"Your IT infrastructure is going to the cloud, driven by business need and speed."

- Cloud IT creates security blind spots and fragmented security management and accountability.

HUMANT ELEMENT IS ALIVE AND WELL



- RSA Theme – Human Element
- Automation in security without Human
- Perimeter Dissolved
- CARTA
- Risk Adaptive Protection

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

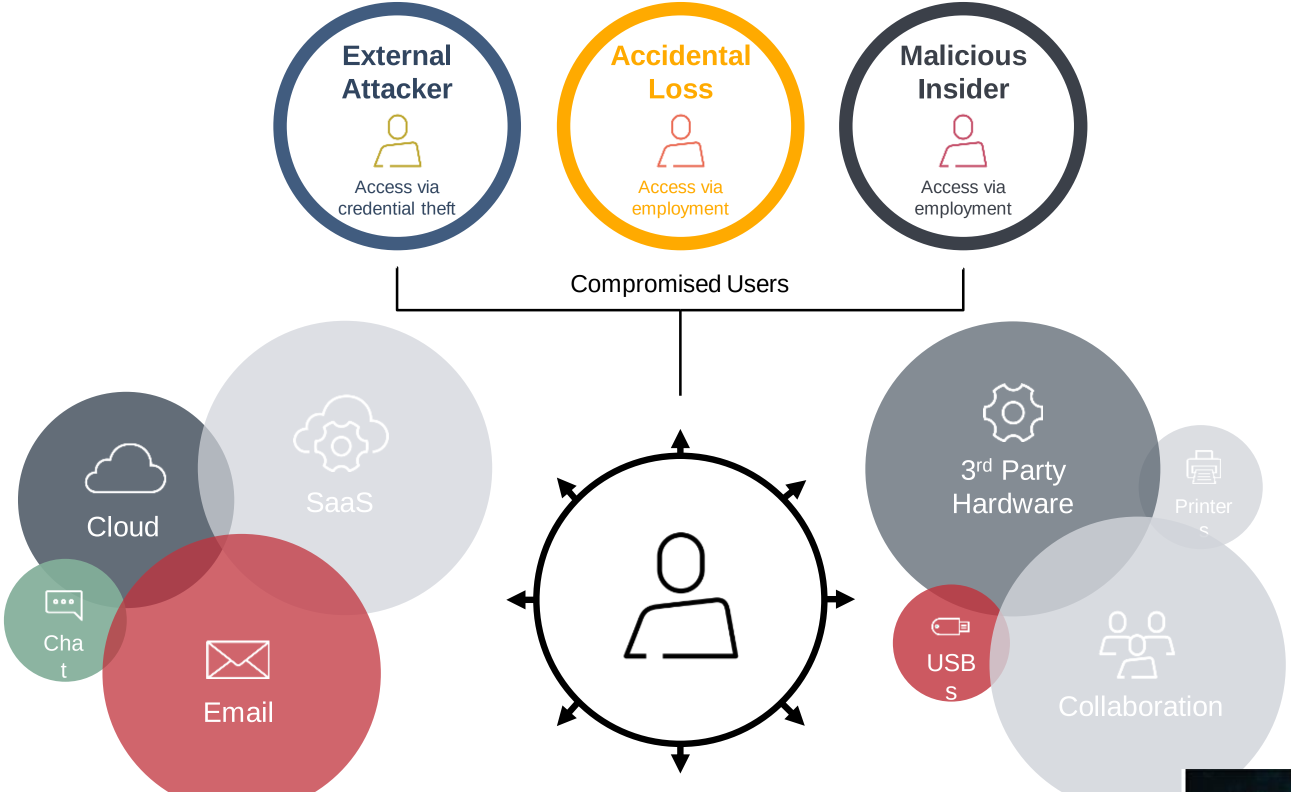
People

Data (IP)

Innovation
Growth
Productivity

Theft
Damage
Misuse

Greatest Risk – Compromised Access



External Attacker

Access via credential theft

Accidental Loss

Access via employment

Malicious Insider

Access via employment

Compromised Users

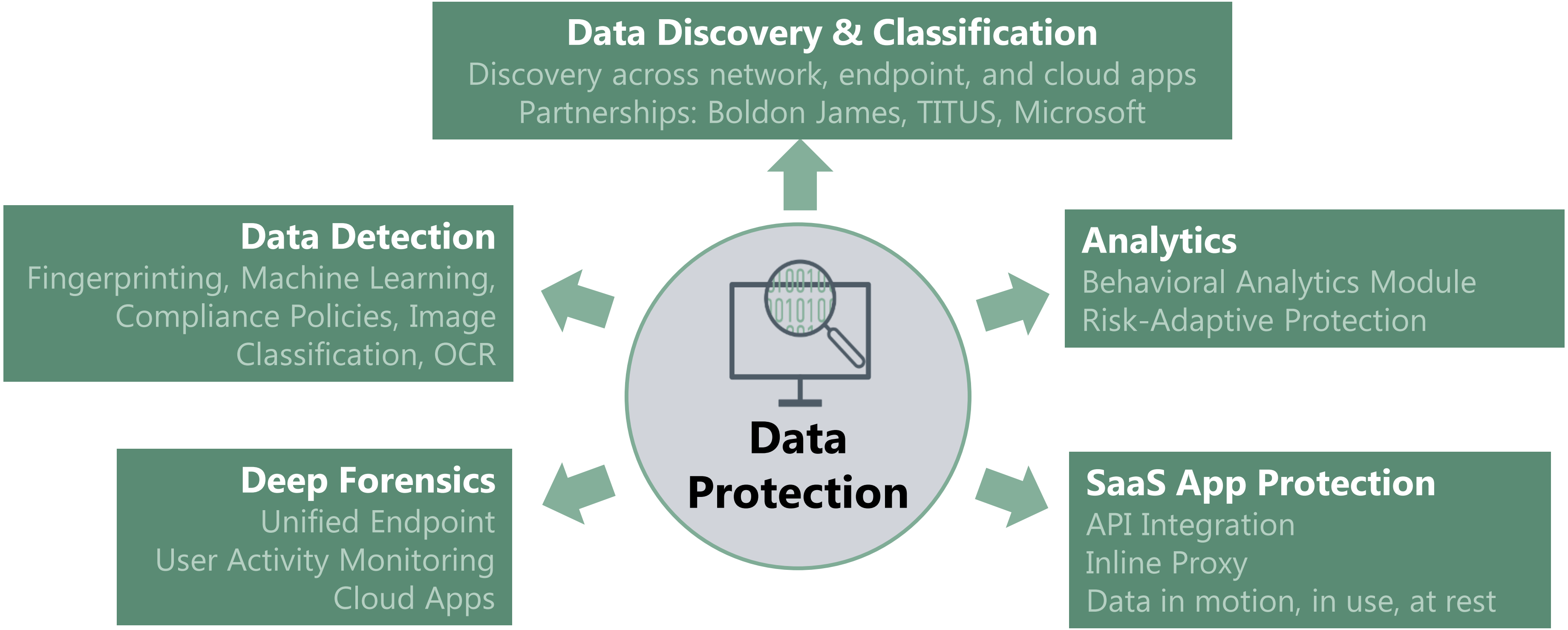
Avenues of Exfiltration in Hybrid Cloud Environments

The Evolution

Paradigm Shift →

• Centralized Data Lakes and Analytics	• Decentralized Data and Analytics
• Events	• Entity Based Activities
• **Threat Intelligence** (IOCs)	• **Behaviors and Context** (IOBs)
• Fixed rules	• Risk Adaptive
• External Attacker	• Compromised Accounts and Devices
• Infrastructure Security	• User and Data Security

Data Protection Evolved



Data Discovery & Classification
Discovery across network, endpoint, and cloud apps
Partnerships: Boldon James, TITUS, Microsoft

Data Detection
Fingerprinting, Machine Learning, Compliance Policies, Image Classification, OCR

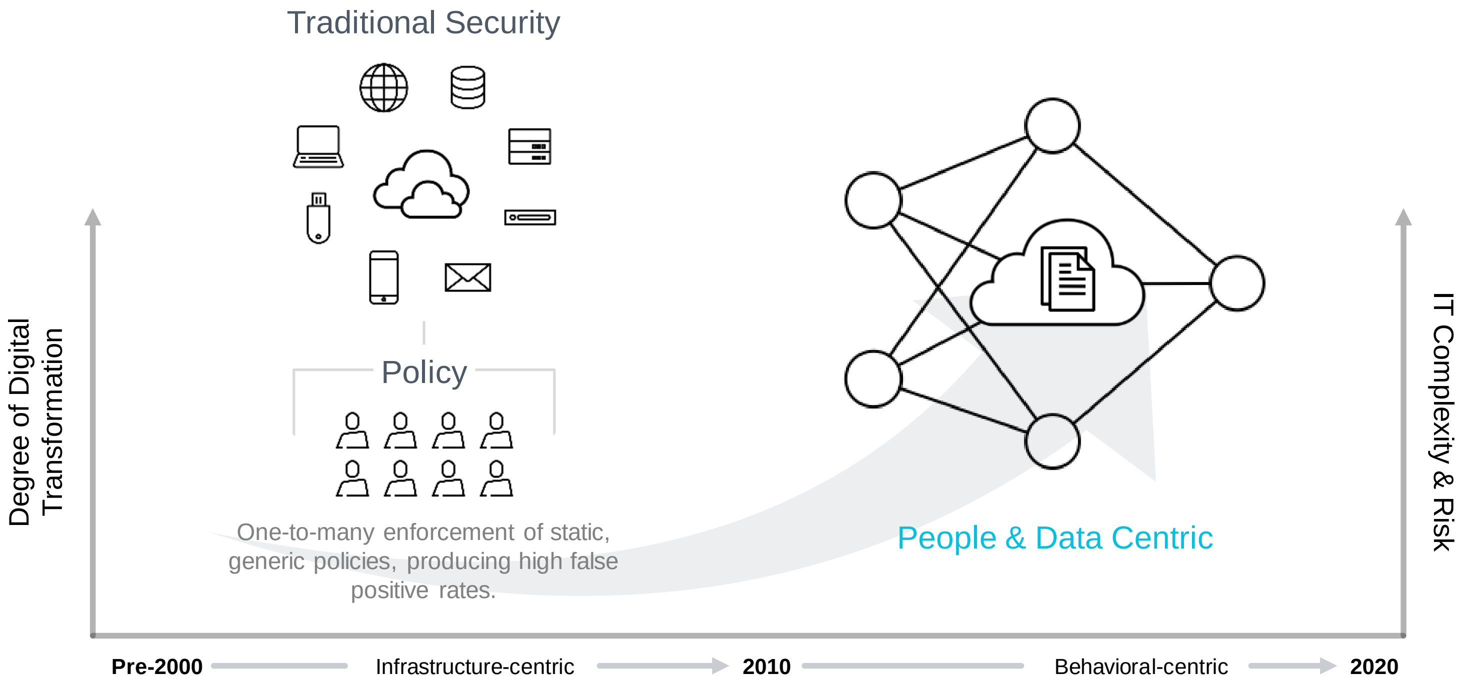
Data Protection

Analytics
Behavioral Analytics Module
Risk-Adaptive Protection

Deep Forensics
Unified Endpoint
User Activity Monitoring
Cloud Apps

SaaS App Protection
API Integration
Inline Proxy
Data in motion, in use, at rest

Design



Traditional Security

Policy

One-to-many enforcement of static, generic policies, producing high false positive rates.

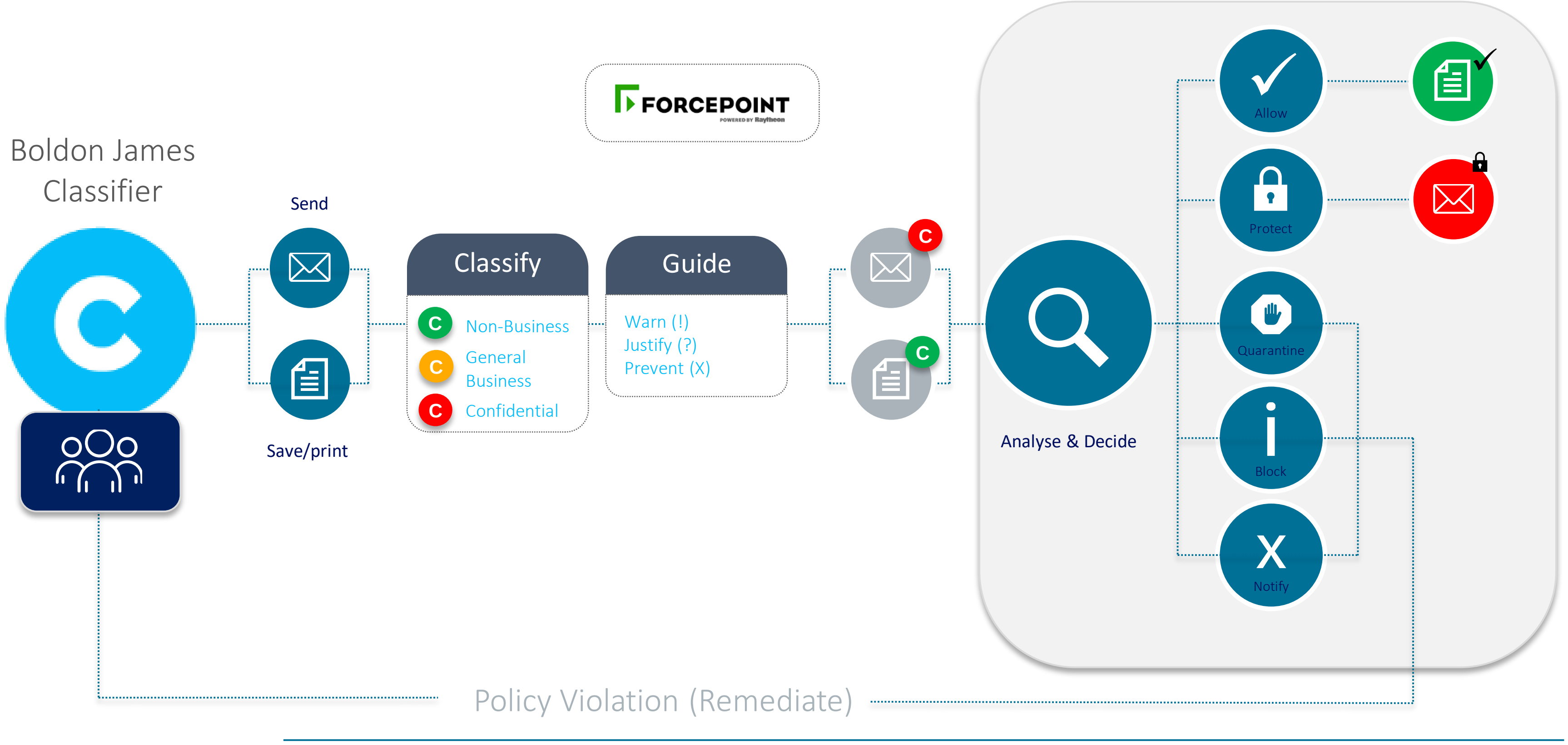
People & Data Centric

Degree of Digital Transformation

IT Complexity & Risk

Pre-2000 → Infrastructure-centric → 2010 → Behavioral-centric → 2020

Classifier & DLP



Meaningful Visibility

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

Observation of user interaction with data

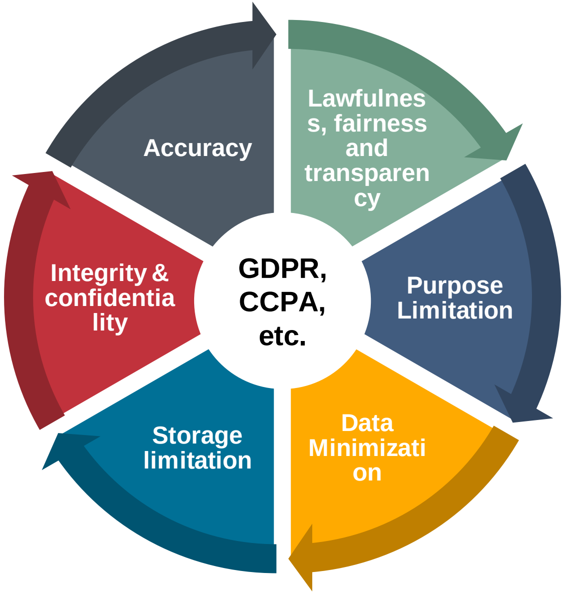
Use of analytics to understand user behavior

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

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:

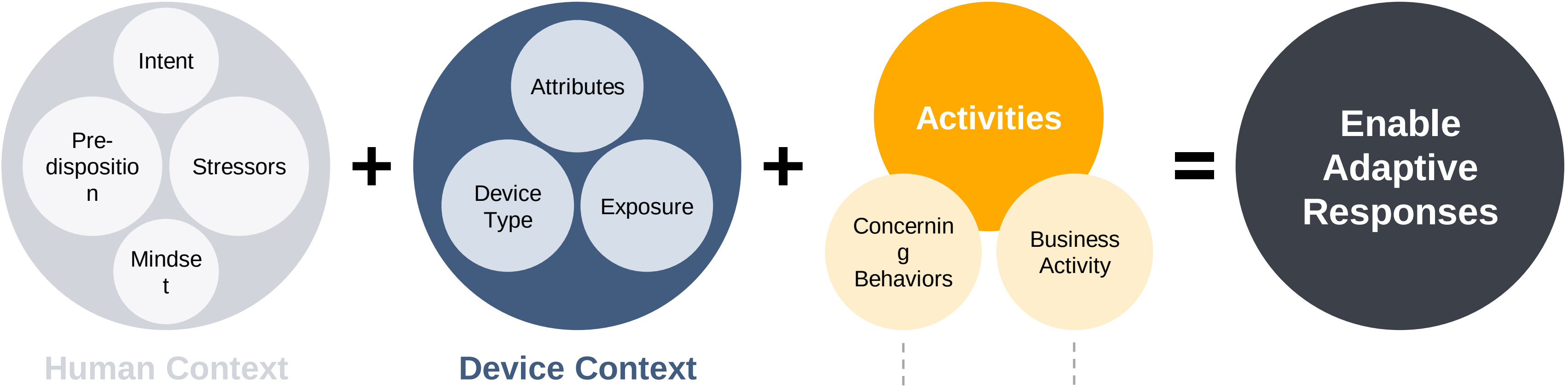
- Ensures there is a balance between Personal data & IP protection & workforce privacy

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.

The Inclusion of Human Factors



Intent

Pre-dispositio n

Stressors

Mindse t

Human Context

+

Attributes

Device Type

Exposure

Device Context

+

Activities

Concernin g Behaviors

Business Activity

=

Enable Adaptive Responses

- Critical Path to Insider Threat

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.

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:

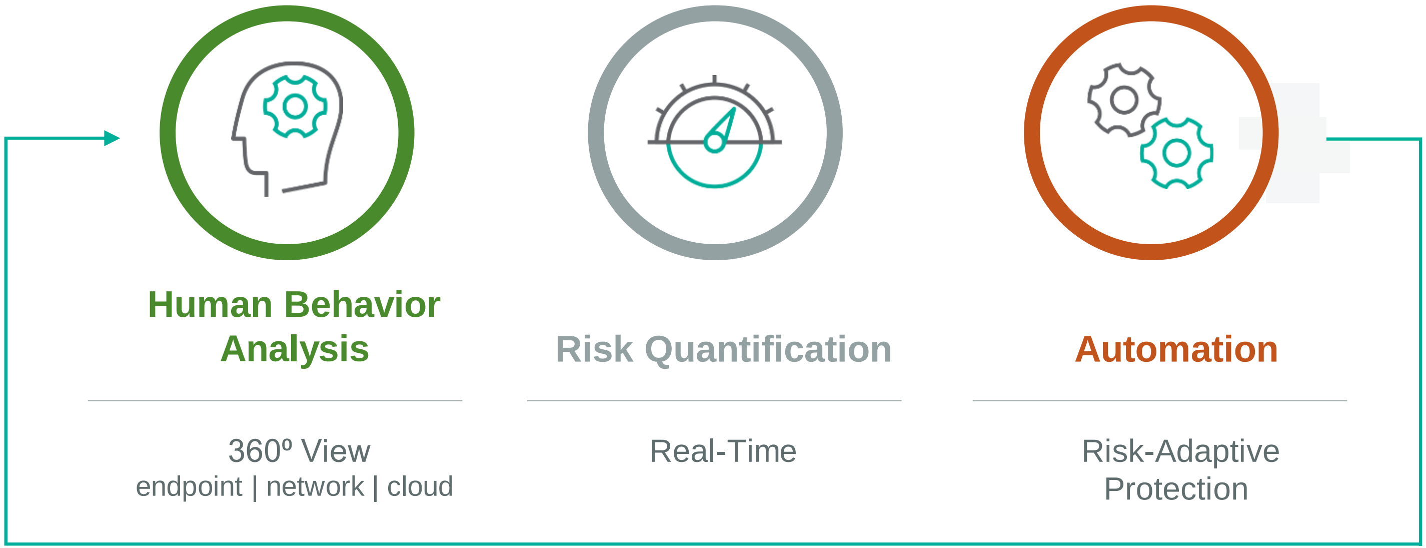
- Better understand risky behavior and automate policies
- Dramatically reduces the quantity of alerts requiring investigation.

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

Forcepoint’s approach to human-centric cybersecurity



Human Behavior Analysis

360º View
endpoint | network | cloud

Risk Quantification

Real-Time

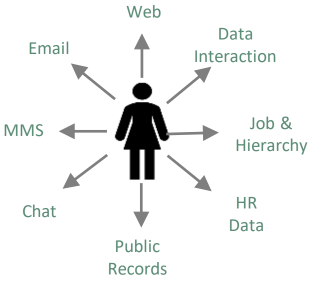
Automation

Risk-Adaptive Protection

Continuous Assessment of Compromised User Risk

Human-Centric Cybersecurity Changes Everything

1. RHYTHM OF PEOPLE



Web

Data Interaction

Job & Hierarchy

HR Data

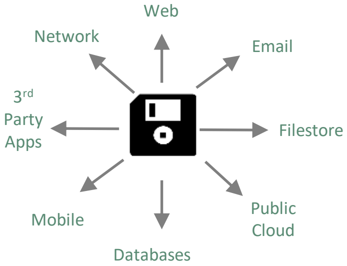
Public Records

Chat

MMS

Email

2. FLOW OF DATA



Web

Email

Filestore

Public Cloud

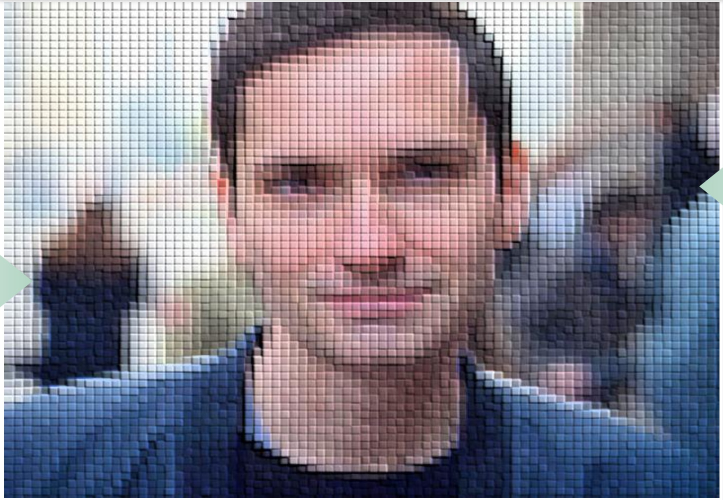
Databases

Mobile

3rd Party Apps

Network

ADAPTIVE TRUST PROFILE



Determine Mindset and Intent	Determine Riskiness of Behavior	Dynamically Score Risk **85**

REAL-TIME, RISK-ADAPTIVE SOLUTION PORTFOLIO

Web Security

Email Security

Advanced Malware Detection

CASB

DLP

Insider Threat

NGFW

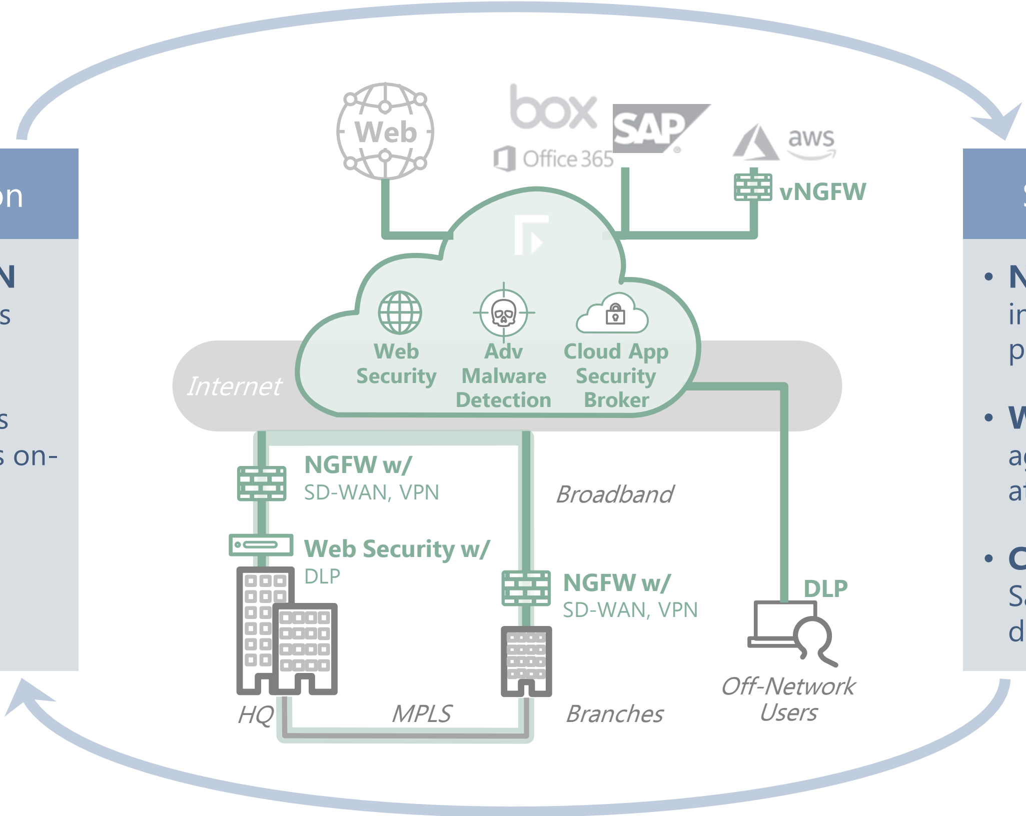
Cross Domain

Behavior Analytics

Transforming How to Connect & Protect the Edge

Network Transformation

- **Direct-to-cloud SD-WAN** connects sites to cloud/apps over local internet links
- **Site-to-site VPN** connects people to internal resources on-premises or in the cloud



Security Transformation

- **Network security** keeps intruders out and segments physical & virtual networks
- **Web security** protects users against zero-days, encrypted attacks, and risky apps
- **Cloud app security** enforces SaaS usage policies and guards data in the cloud

THE FORCEPOINT APPROACH

Threat Intelligence: Reputation, Signatures, Heuristics

Environmental: Device, Location, Time

Behavioural: Volumetric, Anomalous (User / Entity)

Entity Insight: Comms, HR Systems, Travel Systems

Data Insight: Value / Criticality

HUMAN POINT RISK ENGINE

Entity Analytics – "Who They Are"

Evaluate non-activity based indicators about an entity to influence risk judgements.

Event Analytics – "What They Do"

Enrich events with observed features of interest, measure the extent to which events are interesting.

Tone & Intent – "Why They Do It"

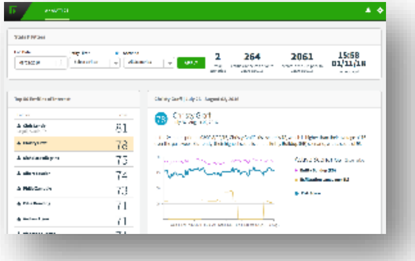
Mine communications content and correlate with entity information to discover signs of discontent, collusion, etc.

Continuous adaptive risk & trust assessment

O L M H

Operational Efficiencies

Insider Threat Detection



Risk-Adaptive

Allow	Allow and alert	Allow and record session	Allow but read-only	Allow but encrypt	Allow but throttle	Wait, ask for more context e.g. Step-Up	Block / Quarantine	Block / Prevent

The Forcepoint solution portfolio

Dynamic User Protection

Insider Threat

Behavioral Analytics

Emerging User Activity Monitoring market

Dynamic Data Protection

Data Loss Prevention

Cloud Access Security Broker

Email Security

Dynamic Edge Protection

Web Security

Enterprise Firewall & SD-WAN

Emerging SASE market

Q&A

6TH CYBER SECURITY INDIA SUMMIT 2020