IBM Security

High-Def Data Security:
Collaboration, Integration, Innovation

GUARDIUM – DYNAMIC DATA PROTECTION

Calvin Bench
Offering Manager – IBM Security Guardium

Steve Cumings
Vice President, Product Management

February 2019

FORCEPOINT IBM

Today’s Situation in Security Operations

- Despite heavy investing in IT solutions, security threats are taking too long to discover and mitigate
- On average it takes 197 days to identify a data breach and 69 days to contain it (Ponemon Institute's 2018 Cost of Data Breach Study)
- Constantly changing IT environments, tools and staffing make it difficult to achieve and maintain high readiness
- New potential threats to your data are continuous, and they are difficult to confirm

The current state of data protection

- The problem is growing, and so are the obstacles.

2.5 quintillion bytes of data are created daily

Data Uncertainty

2 billion records exposed by misconfigurations last year

Compliance Requirements

Privacy Risk

3.5 million predicted shortfall of cybersecurity jobs by 2021 (10x of what it is today)

Operational Complexity

27% of organizations globally will experience a recurring material breach in the next two years

Compliance Requirements

Privacy Risk

Challenges with data security

Where to start?

What data assets are high value?

Which cloud services are used?

Which repositories and databases are used?

How to address Compliance?

What compliance issues are there?

What controls exist?

What are the remediation action items?

Where is the critical data?

Are the crown jewels classified and protected?

Do they reside in the cloud? Unstructured?

How to maintain the right level of Data security?

How to keep up with the pace of change?

Who can access the data?

There is now a fluid perimeter

What to lock down?

What data should be encrypted?

What SaaS apps are used?

Who is responsible for data security?

With Cloud Service Providers – clients still have security obligations. What are they?

How to talk risk with the CRO?

Who are your riskiest users?

How can I focus investigations?

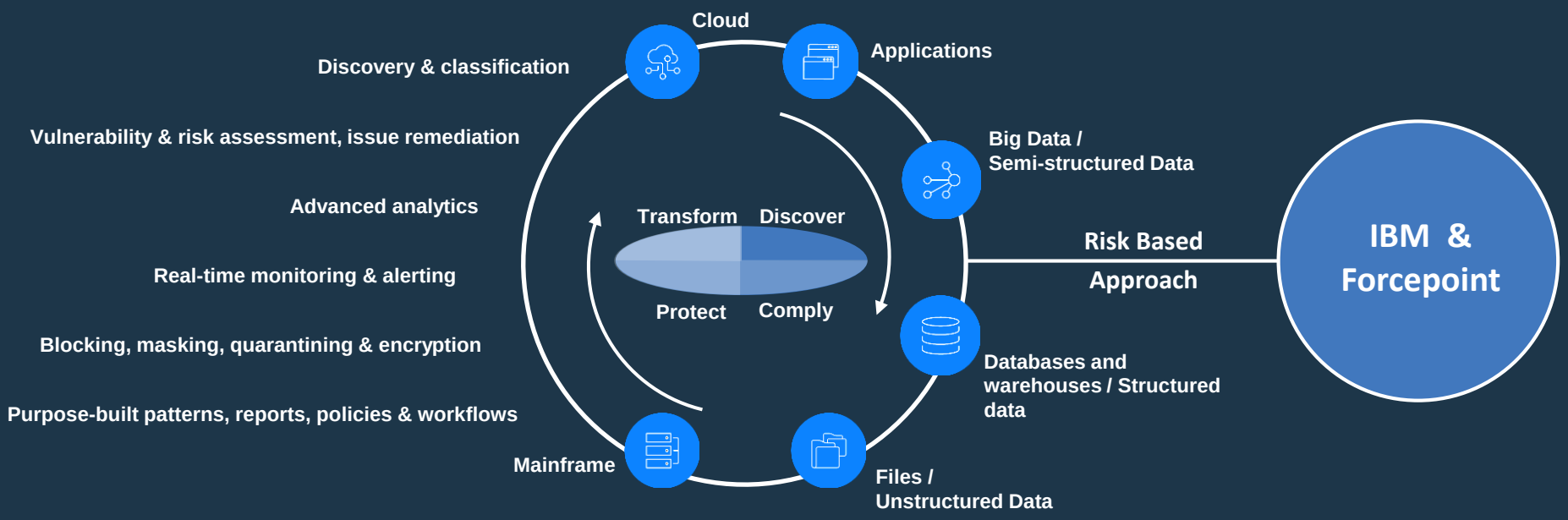
How can I graduate enforcement based on user risk?

IBM Security Guardium / Forcepoint Data Protection

Empowers you to meet your most important data protection needs

- Complete Visibility
- Actionable Insights
- Real Time Controls
- Automated Compliance

With smarter capabilities throughout your entire data protection ecosystem



IBM + FORCEPOINT ALLIANCE PARTNERSHIP

Enterprises demand deeper vendor integration and solutions that deliver security and business outcomes

Gives clients more value out of existing investments

Leverage market leadership portfolio synergies to address new challenges and frameworks

Forcepoint and IBM are working together to address enterprise customers' challenges in their digital transformation journey.

Focusing on the intersection of users interactions with critical data and IP, providing solutions in **data protection for your hybrid infrastructure (on-prem and cloud)**

Principles:

- Joint solutions that deliver:
  - Richer contextual awareness and dynamic response and enforcement
  - Continuous authorization
  - Extensibility to cloud and on-prem
  - Integration with Identity
- Effective security operations approach that improve detection, investigation, response and remediation time
- A streamlined GTM motion to help customers understand, buy and deploy our joint solutions
- An innovation platform alliance to add more use cases over time, including predictive, dynamic security protection in customers' journey to infrastructure transformation

Forcepoint Integration

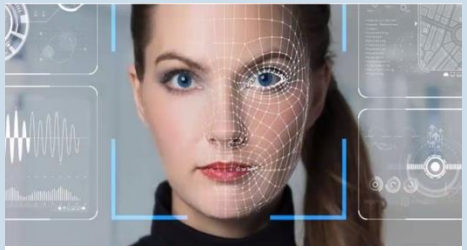
FORCEPOINT IS DRIVING AN INFLECTION POINT IN THE CYBERSECURITY INDUSTRY WITH A HUMAN-CENTRIC STRATEGY

- Created by Raytheon in 2016 to commercialize defense-grade technologies for large enterprises.
- One of the largest private cybersecurity companies in the world – more than 13,000 customers, operations in more than 150 countries, 2,700 employees across 50 offices, and 27 data centers worldwide.

Forcepoint's Commercial Portfolio

Email Security	CASB	Data Guard
Insider Threat		SD-WAN & NGFW
DLP	UEBA	Web Security

Understanding the rhythm of people…



OUR ROLE IN IDENTITY BEHAVIOR

Customers and partners need to learn about the behavior of the digital entities on networks and determine whether it is good or bad, thereby highlighting risk and urgency.

…and the flow of critical data

OUR ROLE IN DATA PROTECTION

Customers and partners need to protect their critical data from the accidental or malicious behavior of digital identities that lead to a data exfiltration event or a compliance and regulatory violation.

STATIC VS DYNAMIC POLICIES IN ACTION

STATIC POLICIES BASED ON PRE-DEFINED RULES

Kate, PhD
Research Chemist

Kate is giving a presentation to senior leadership and tries to copy her slides to a USB stick

Traditional DLP Policy

Policy: **block** files from being copied to USB drives, alert gets sent to IT

USER IMPACTS

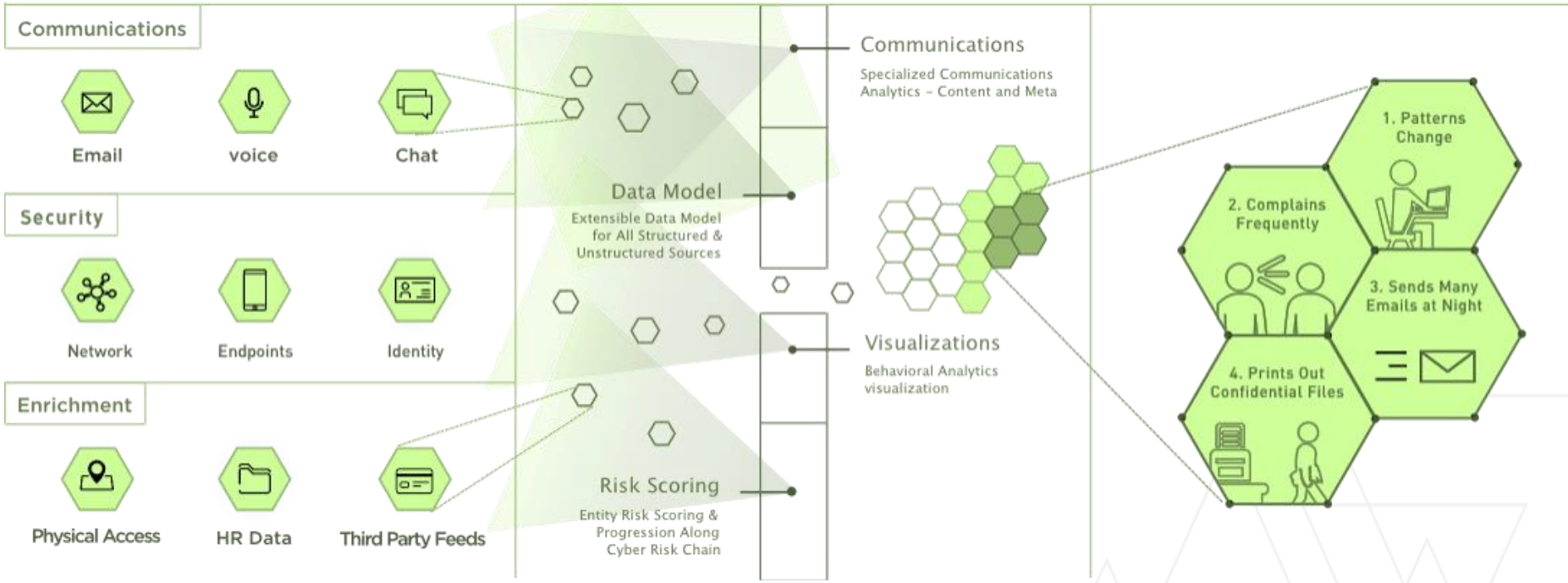
- Kate is frustrated because simple tasks are blocked
- Kate will find another way to solve her problem
- The data protection system becomes ineffective

ADMINISTRATOR IMPACTS

- The admin needs to track down the alert
- Thousands of alerts come in overwhelming the security admin team
- The security team turns off the DLP policy because there are too many false positives

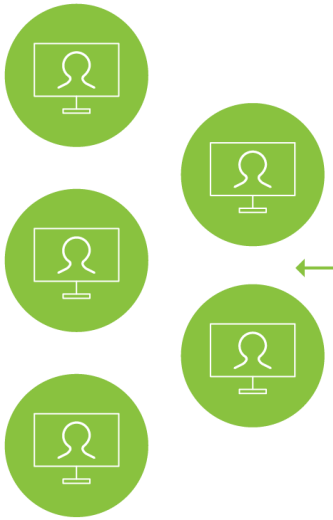
FORCEPOINT BEHAVIORAL ANALYTICS

DATA SOURCES 〉 ANALYTIC ENGINE 〉 INFORMED NARRATIVE



DYNAMIC DATA PROTECTION

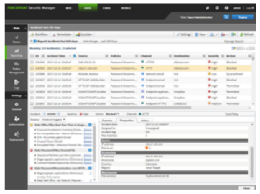
Enforcement



Endpoint monitoring, collection, and enforcement

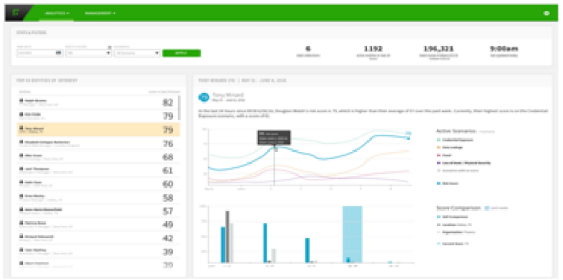
Set dynamic enforcement plan

Endpoint server



Proactively protect from data exfiltration

Analytics



Collect observed data, perform behavioral analytics, risk score individuals

Infer behaviors, contextualize

IBM GUARDIUM W/ FORCEPOINT DATA PROTECTION

Objectives

Extend data visibility across both structured and unstructured data stores

Address data protection including privacy and compliance

Use Cases

Data visibility / classification:

Guardium and FP Data Protection enable sensitive data detection across endpoint, network and cloud

Dynamic Data Protection:

Model user risk behavior, adapt dynamic customer policies

Managing Data Risk:

FP sends details on files and cloud system to IBM for risk scoring and management

Outcomes

Dynamic data protection from database to endpoint

Highlighting of critical risks

Faster, automated response

Reduced operational friction through risk-informed enforcement of data protection policies

EXAMPLE CUSTOMER SCENARIO

CURRENT

It's difficult for customers to gain visibility and make action around insight on risk across an organizational environment. For example if a privileged user engages in risky activity on an endpoint, currently they can still access sensitive data on the server. There's a lack in ability to mitigate and remediate risk regarding the gap between server and endpoint.

FUTURE

User risk score increases or decreases, Forcepoint informs Guardium to update policy update and remediate – block, mask, alert

- FP detects risky user behavior – combination of negative email sentiment, anomalous VPN usage, request for privilege escalation. FP sends list of potential IPs and user profiles to Guardium, Guardium blocks access. The same risky user behavior is sent to Guardium UBA to inform machine learning and influence policy and IBM Cloud Identity for suspension of user access – several remediation points

TECHNICAL STRAWMAN WITH GUARDIUM (CRITICAL DATA)

Phase 1

Add Forcepoint Data Protection Offerings to list of integrations for playbooks

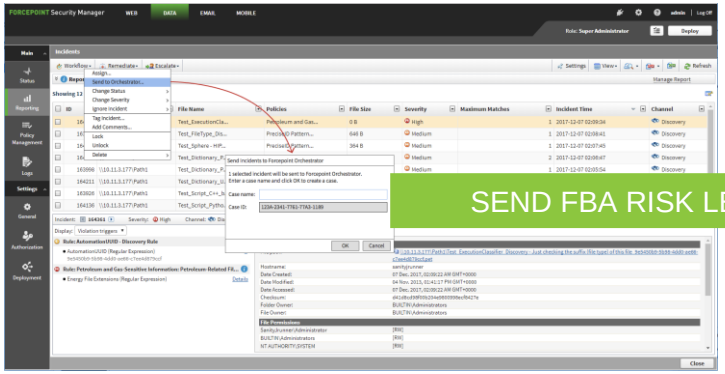
Phase 2

Build top-level integration from Forcepoint Behavior Analytics to Guardium

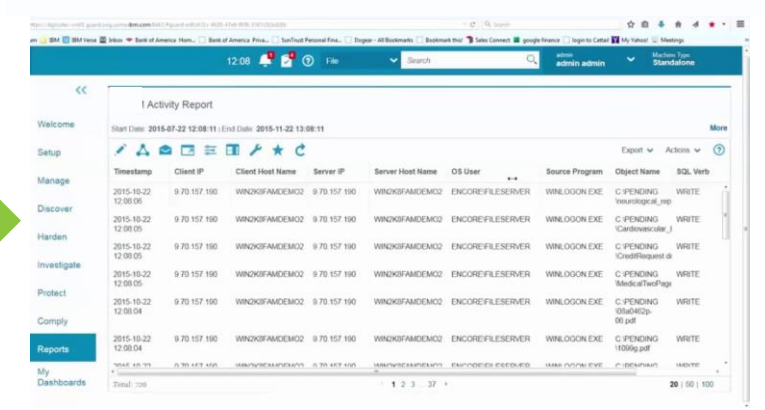
Phase 3

Joint solution in Market with customer-centric GTM / support motions

(OEM/resell)



SEND FBA RISK LEVEL CHANGE



Integration Highlights

Benefits

- Integration delivers conjoined functionality that effectively enables visibility and protection of sensitive data across our customers' environments
- Market leadership in multiple security segments and product synergy pave the way for future integrations and collaboration

Actions

- Determine who the riskiest users are and accelerate response to critical exposure
- Dynamically apply enforcement based on user risk

Be on the lookout for this integration in the IBM Security integration hub!

Visit Forcepoint in South Expo #126

IBM Security

THANK YOU

FOLLOW US ON:

ibm.com/security

securityintelligence.com

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

IBM®