RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SPO1-T10

EXTENDING BEHAVIORAL INSIGHTS INTO RISK-ADAPTIVE PROTECTION & ENFORCEMENT

Guy Filippelli

Vice President of User and Data Security Solutions
Forcepoint

Meerah Rajavel

Chief Information Officer
Forcepoint

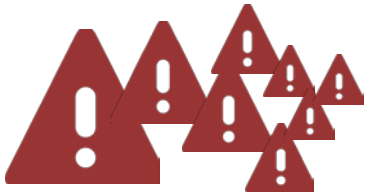
SO WHAT ARE WE TRYING TO SOLVE?

Protect the important data wherever it resides

without

Frustrating Users

Overwhelming Administrators

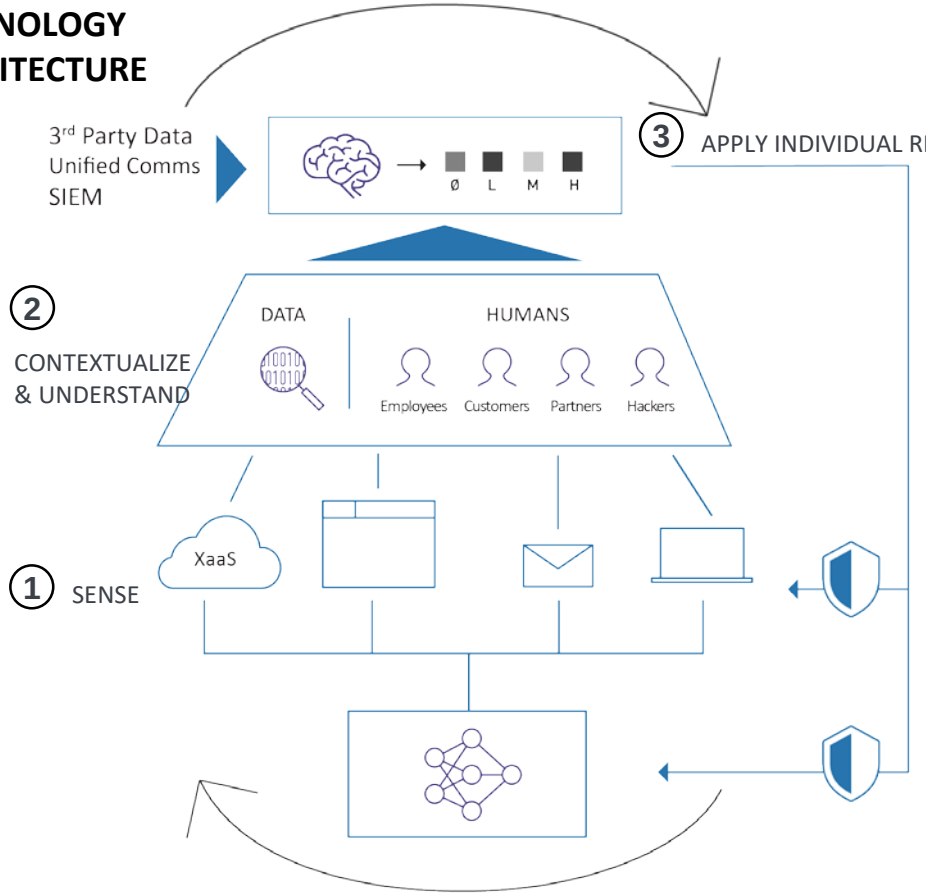


Mistaking

for

CLOSED LOOP, RISK ADAPTIVE APPROACH

TECHNOLOGY ARCHITECTURE



5 OPERATIONAL MODEL

- Set unified policy
- Orchestrate
- Case management
- Investigate

BUILDING A HOLISTIC VIEW OF THE USER

Communication Channels

What are they feeling?

With whom are they interacting?

Data: Email, chat, voice

System Logs

How are they behaving digitally?

What sites and systems are they accessing?

Data: SIEM, endpoint, web browsing, logins, file sharing

Traditional HR Data

What is their motivation?

Why might they have malicious intent?

Data: Performance reviews, Active Directory

Physical Sources of Data

How are they behaving physically?

Where are they going and when?

Data: Badge data, traveling

USER BEHAVIOR ANALYTIC APPROACH

EVENTS OF INTEREST

PEOPLE OF INTEREST

SCENARIOS
"Connect the dots" across event/entity models for a composite measure of risk

EVENT ANALYTICS - "What They Do"

Enrich events with observed features of interest, scored for rarity and normalized by **individual** or **peer group**

EVENT INGEST AND ENRICHMENT
(Streaming or Batch Ingest via API)

ENTITY ANALYTICS - "Who They Are"

Score non-activity based indicators about an entity to influence scoring

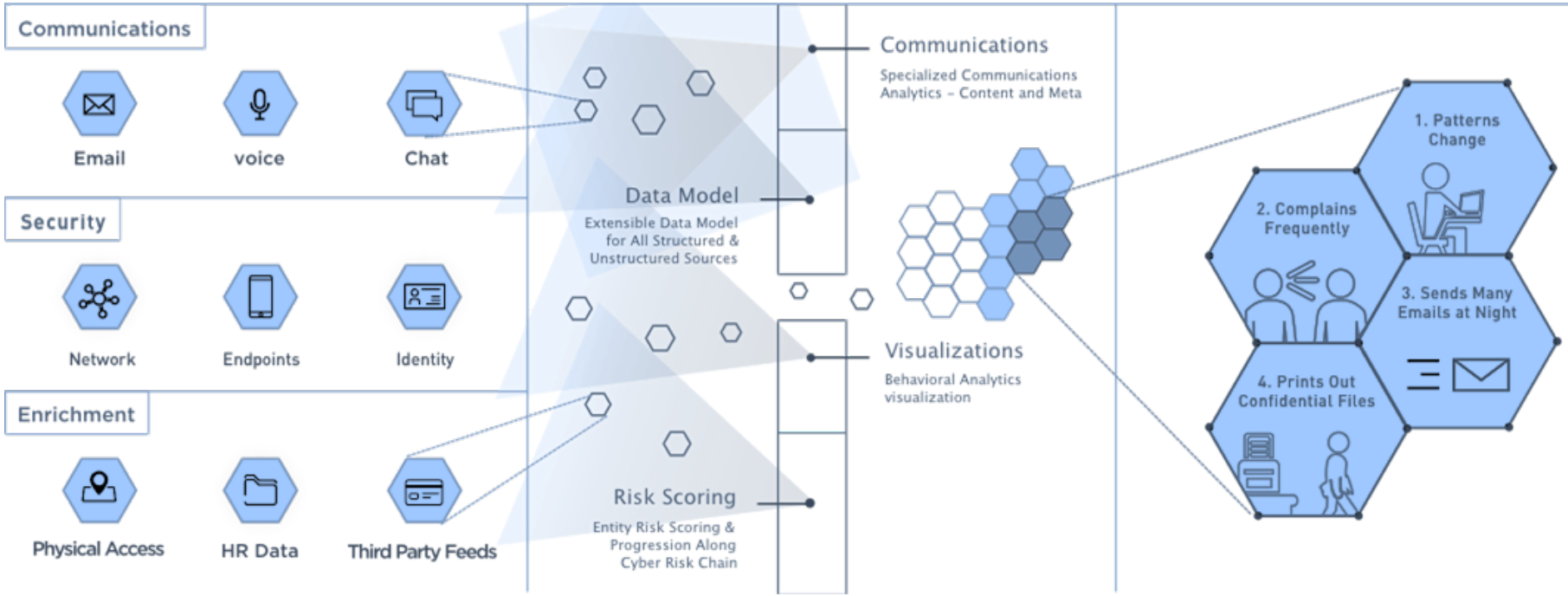
Entity Features | Entity Attribute

ENTITY ATTRIBUTE AND FEATURE COLLECTION
(gathered from HR, Active Directory, CMDB)

What They Do ← **INSIDER INSIGHTS BASED ON** → Who They Are

HOW A TYPICAL ANALYTICS PLATFORM WORKS

DATA SOURCES 〉 ANALYTIC ENGINE 〉 INFORMED NARRATIVE



ANALYTICS ALONE IS NOT ENOUGH

TRADITIONAL UEBA

Forensic Analysis

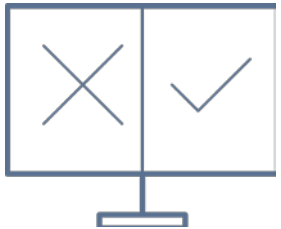
Learning why something happened yesterday does not stop the problem.

TRADITIONAL INSIDER THREAT

Constant Monitoring

Balancing workforce privacy and IP protection is critical.

TRADITIONAL DLP



Block it or Allow it

Current policies are far too rigid to be effective.

An effective solution should cut through the noise of alerts, highlight early warning signals to **prevent** the loss of important data.

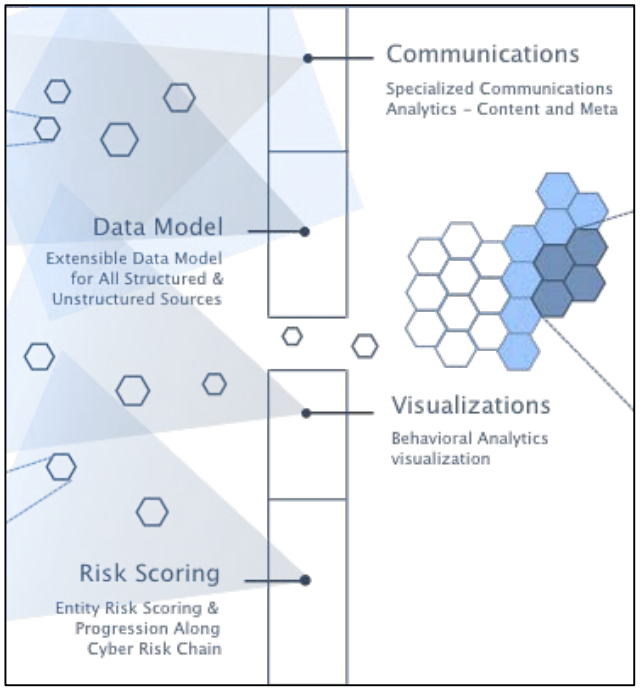
A MORE POWERFUL WAY TO LEVERAGE ANALYTICS

DATA SOURCES 〉 ANALYTIC ENGINE AND INSIGHTS 〉 POLICY ENFORCEMENT

Traditional Security Log Data

Non-Security Log Data

3rd Party Data Sources



Decision Making Channels

(DLP, CASB, NGFW, EMAIL, WEB)

RISK ADAPTIVE PROTECTION

Risk adaptive protection dynamically applies monitoring and enforcement controls to protect data based on calculated behavioral **risk level of users** and the **value of data** accessed.

This allows security organizations to better understand risky behavior and automate policies, dramatically reducing the quantity of alerts requiring investigation.

HOW RISK ADAPTIVE PROTECTION WORKS:

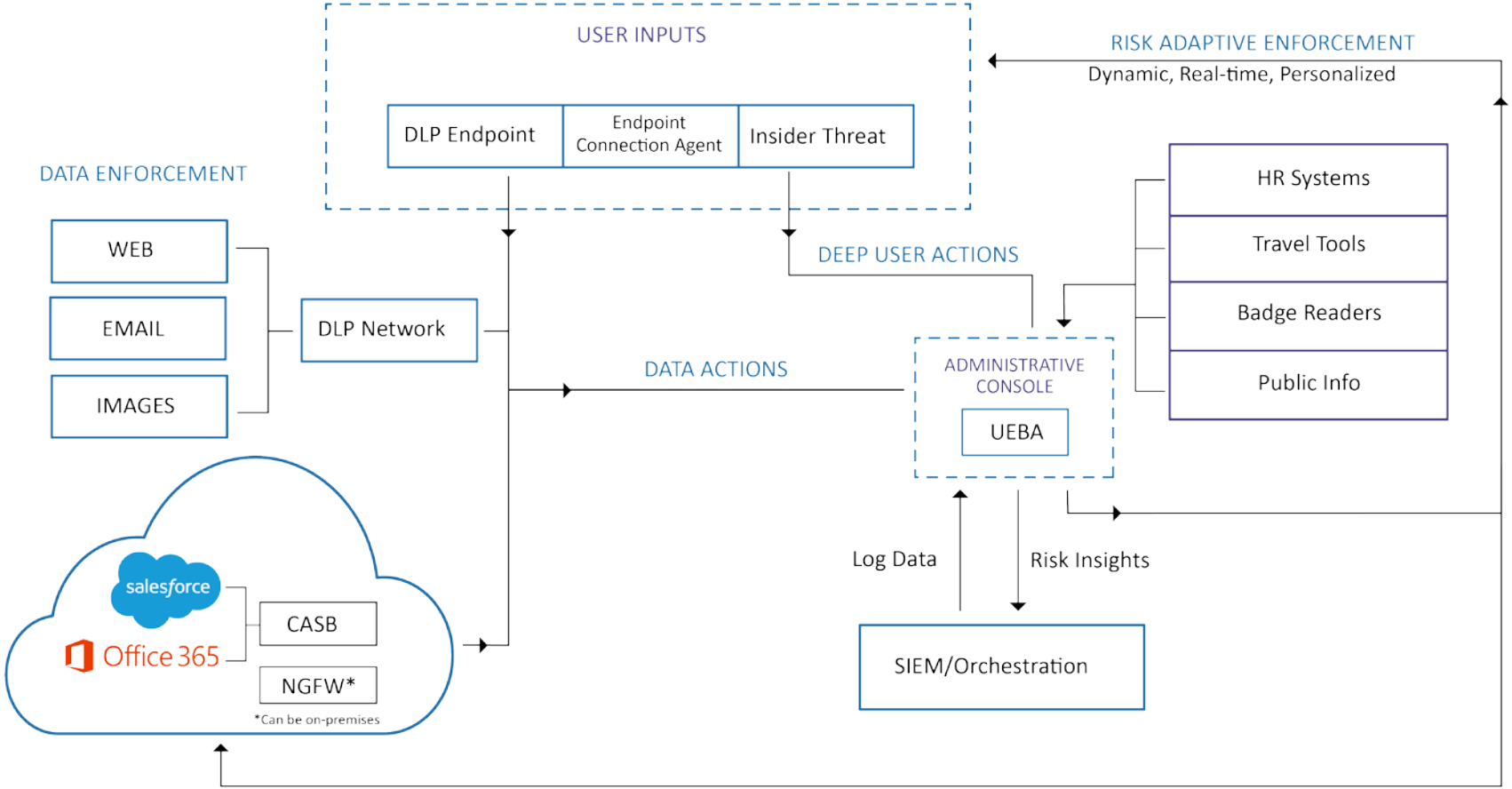
1) Risk levels are driven up and down by human behavior

2) Each user has a unique and dynamic Risk Level which changes based upon behavior

3) Risk Levels drive different outcomes

4) The security adapts to the risk levels as behaviors change

THE ROLE OF ANALYTICS IN THE CLOSED LOOP SYSTEM

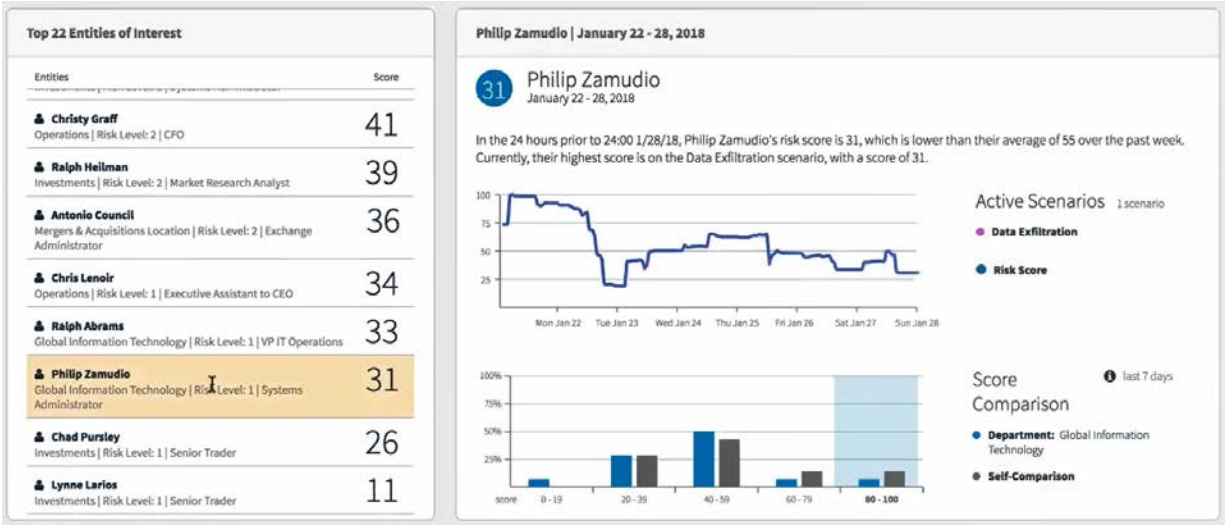


SETTING UP THE DEMO: WHAT'S THE SCENARIO

User: Philip Zamudio
System Administrator
Global IT Team

Current Risk Score: *31*
Risk Score is based on monitoring user activities through numerous channels:

- *Endpoint*
- *3rd Party Applications*
- *Web & Email*
- *Network*



Current Risk Level: *1 (of 5)*
Actions of enforcement, notification, monitoring or enforcement driven by Risk Level

For this demonstration we're using DLP policy

RECORDED DEMO

MEERAH RAJAVEL

Chief Information Officer, Forcepoint

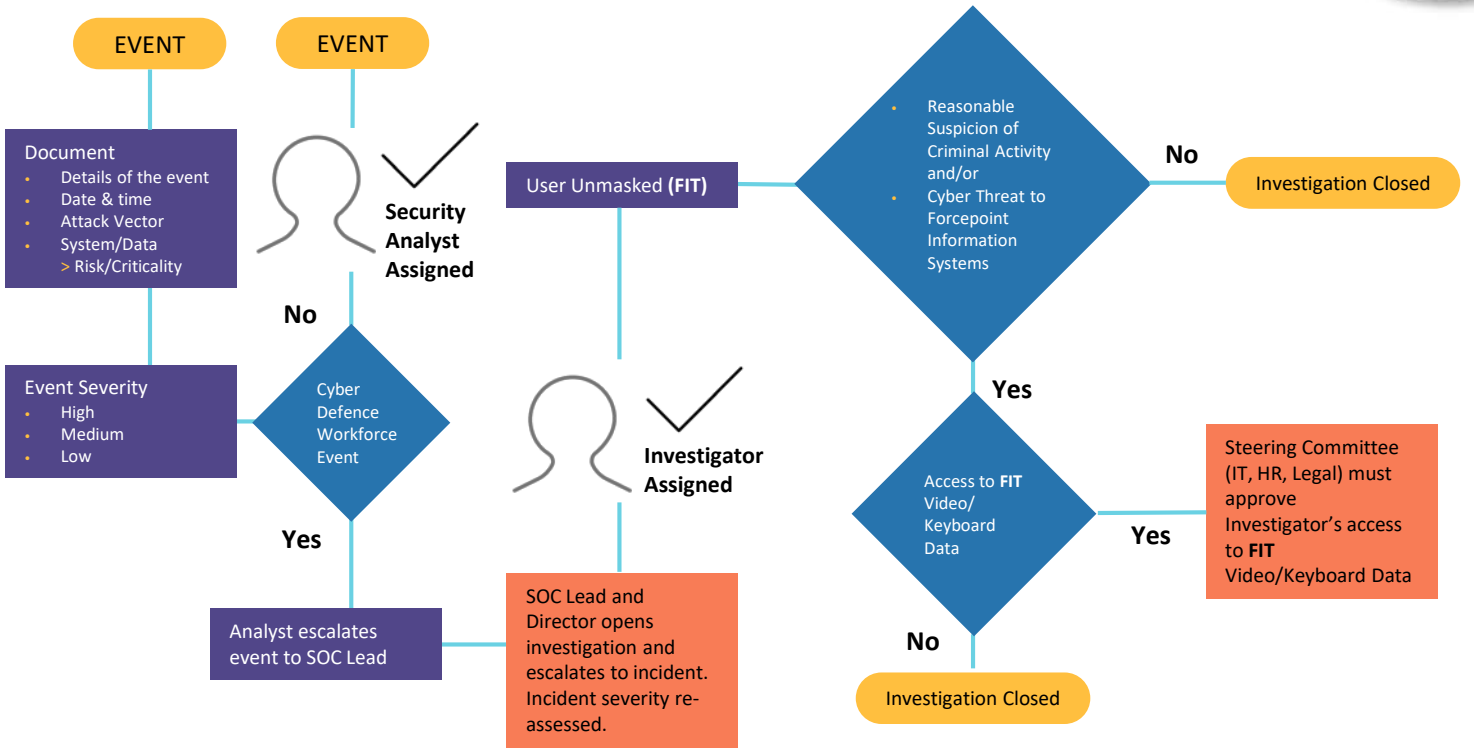
FOUR STEPS TO ROLLING OUT RISK-ADAPTIVE PROTECTION

1. Establish Privacy Policy
2. Establish Risk Policy
3. Establish Enforcement Baselines
4. Launch Risk Adaptive Protection

ESTABLISH THE PRIVACY POLICY

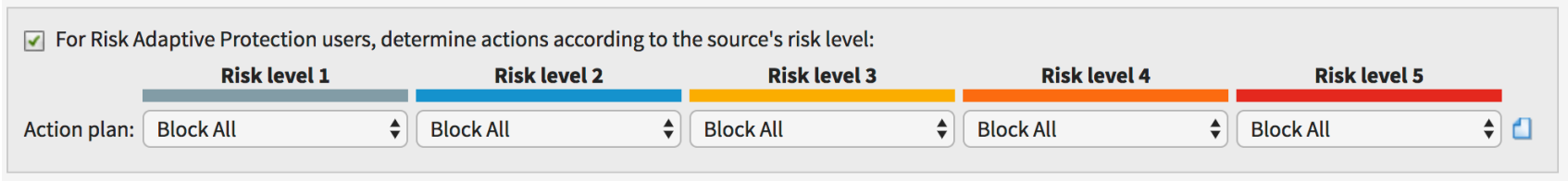
- Respect the privacy of employees.
- Conform with privacy laws in relevant nations.
- Privacy and Security are not mutually exclusive. Involve Legal and HR.
- Focus on transparent communications with employees.
- Establish clear Workforce Defense Policy & Procedure.

SAMPLE PSEUDONYMIZATION WORKFLOW

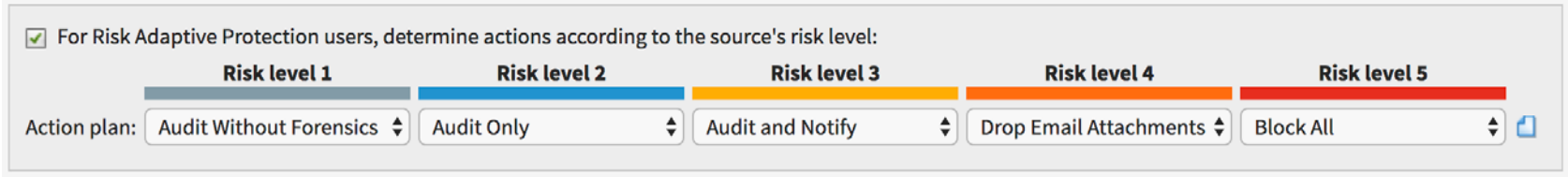


ESTABLISH RISK POLICY

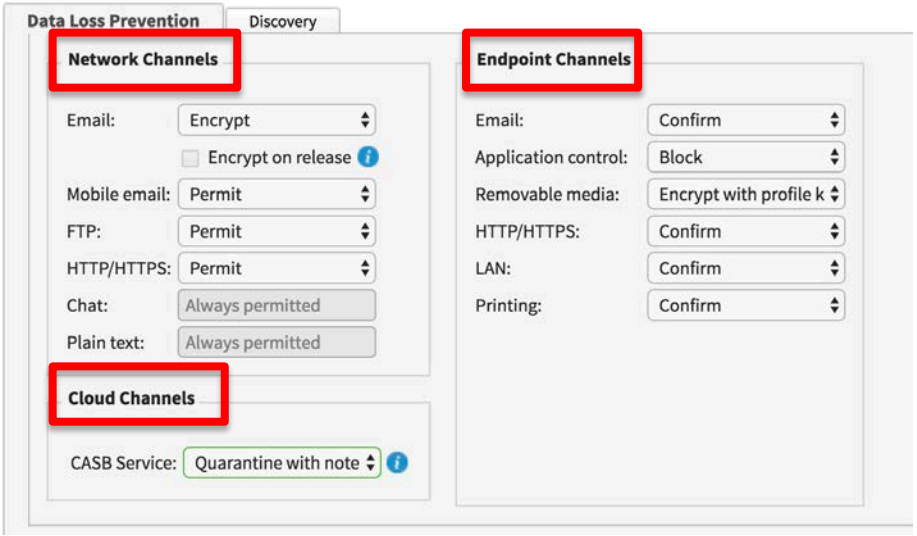
- For policies governing compliance use-cases or highly sensitive information, “Block All” was the action plan for all risk levels



- For policies where additional context can help inform decisions, additional granularity can get added



ESTABLISH RISK POLICY
MULTI-CHANNEL ENFORCEMENT



- ✓ Multiple Action Plans
- ✓ Protect data in motion and at rest
- ✓ Cloud and on-prem protection

ESTABLISH ENFORCEMENT BASELINE

Identify users to pilot

Enable Audit-only rules to fine-tune policies

Learn behavior baselines for 30-45 days

Calibrate risk policies and enforcement procedure

IN CLOSING

- Focus on user behaviour and data interactions
- Analytics is critical to solve this challenge, but it's only part of the solution
- Automating leads to speedy resolution of high risk events
- Risk Adaptive Protection will deliver better cyber-security