MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

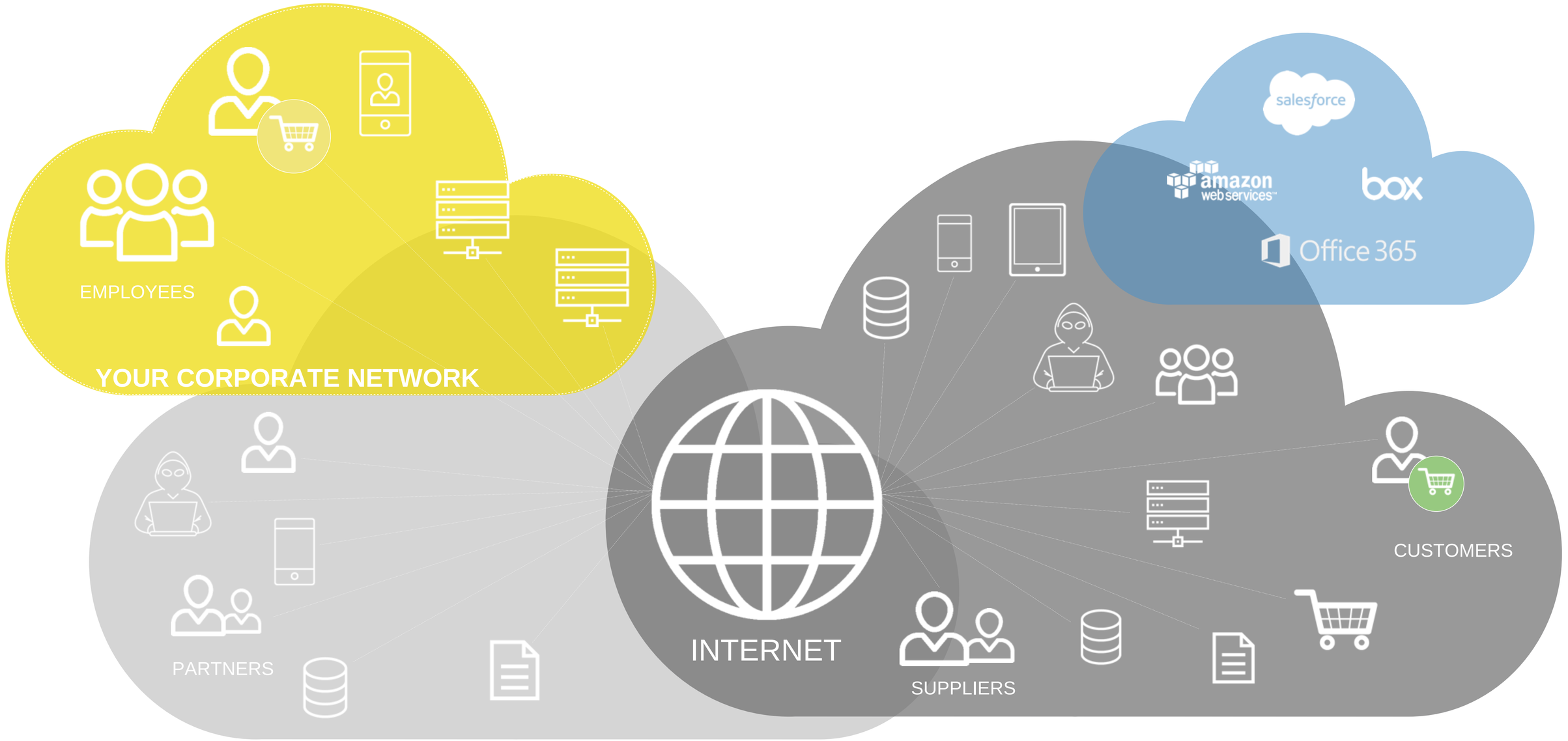
A RISK ADAPTIVE APPROACH TO DATA PROTECTION

Rakesh Shah

Senior Director of Product Management

rakesh.shah@forcepoint.com

HOW DO YOU SECURE A GLOBAL NETWORK YOU DON'T FULLY OWN OR MANAGE?



TODAY’S CYBERSECURITY CHALLENGES

My data is now stored everywhere (including systems beyond my control) and accessed from anywhere

3rd party cloud apps
increased 11x
from 2014-16

I have too many point solutions with a disjointed security policy

Companies have
30-75
disparate security solutions

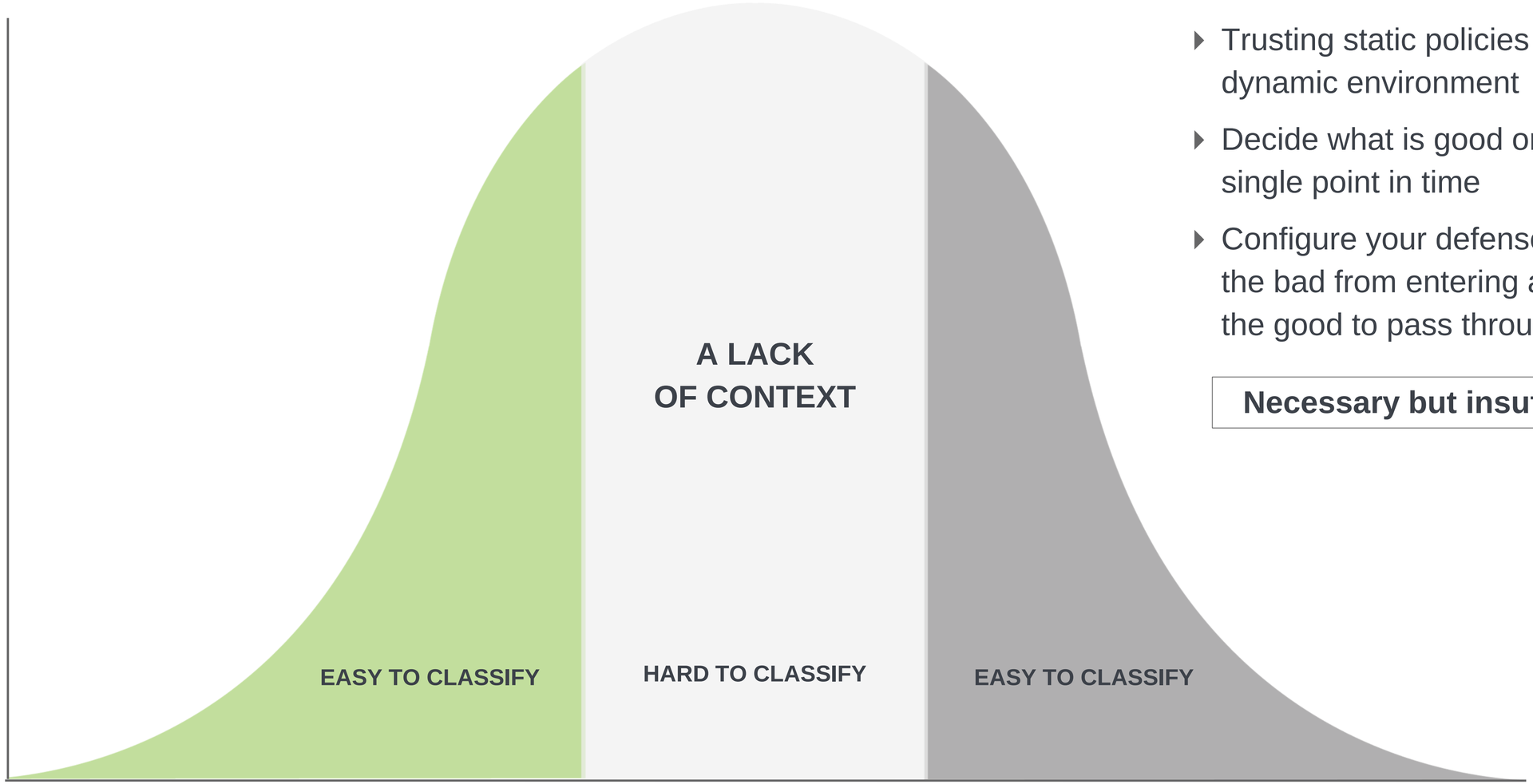
I am drowning in alerts and cannot determine critical signal

Half of SecOps mgrs.
report seeing
>5000 alerts/day

By the time I figure out what is going on, it’s too late to stop the data exfiltration

Takes **46 days**
on average to contain an attack after detection

THE TRADITIONAL APPROACH TO CYBERSECURITY

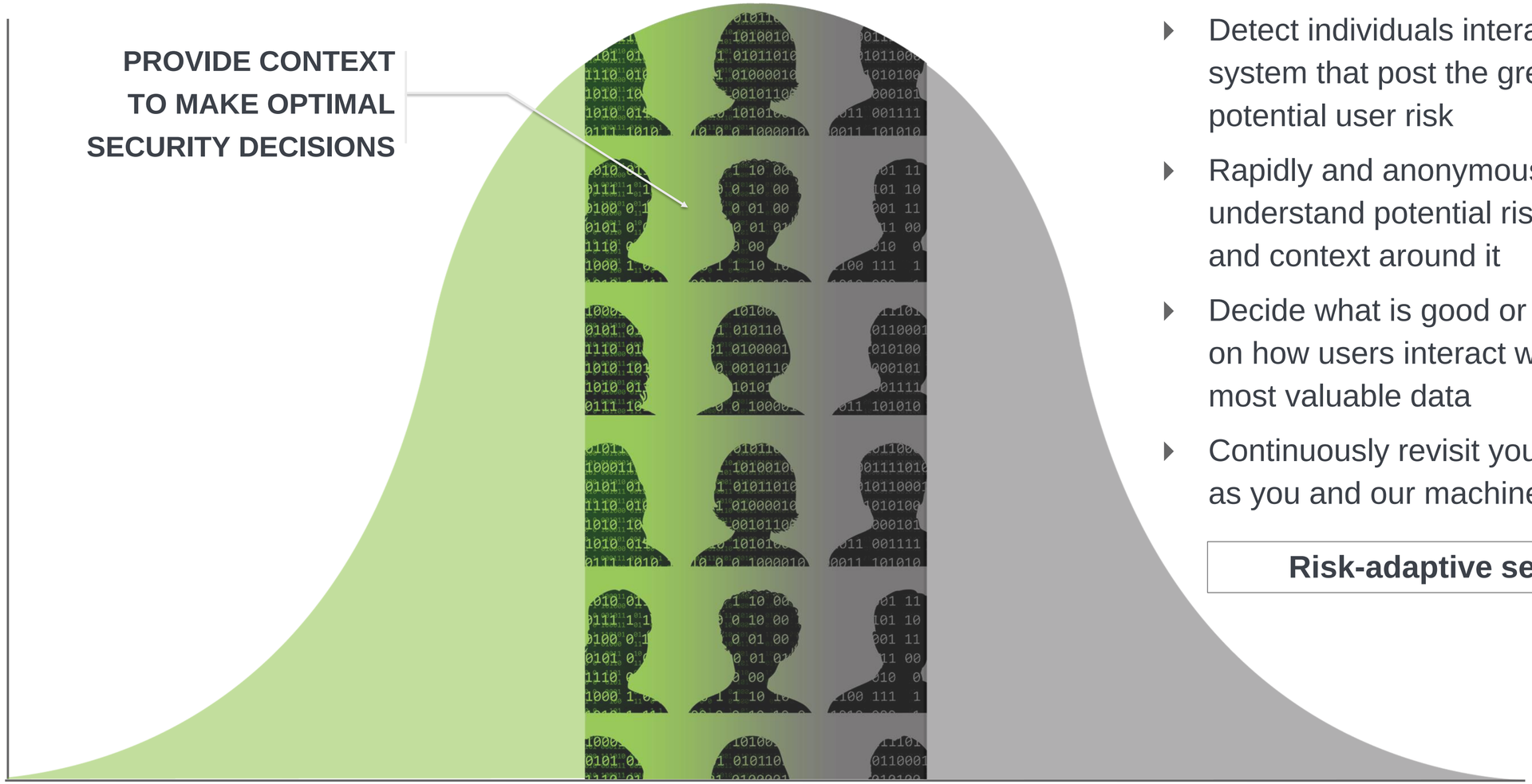


THREAT CENTRIC

- Trusting static policies in a dynamic environment
- Decide what is good or bad at a single point in time
- Configure your defenses to stop the bad from entering and allow the good to pass through

Necessary but insufficient

A NEW PARADIGM: HUMAN-CENTRIC CYBERSECURITY



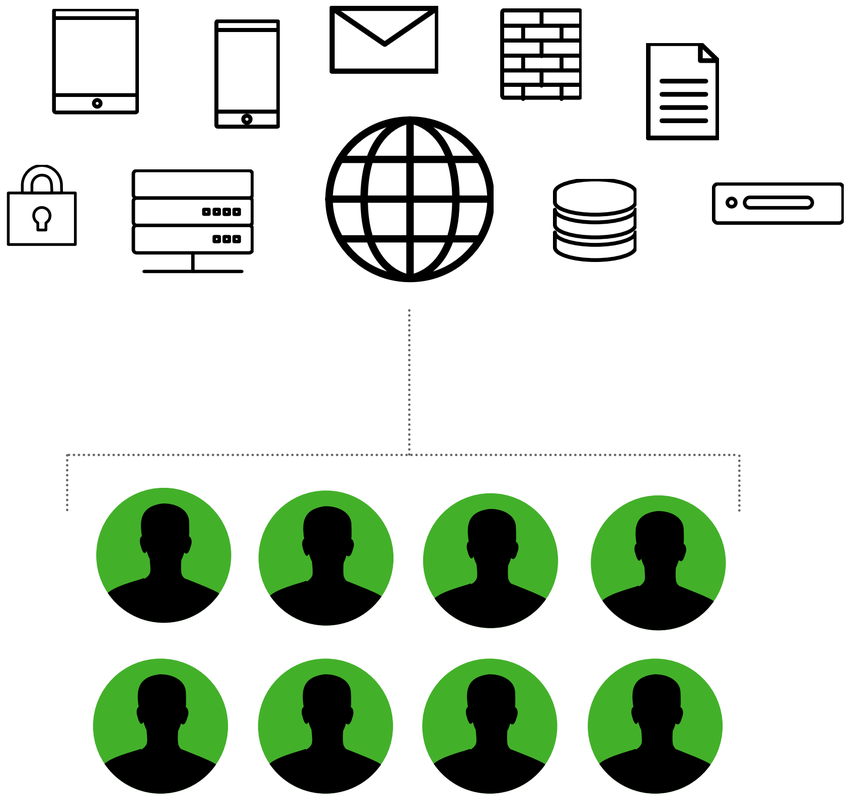
BEHAVIOR CENTRIC

- Detect individuals interacting with system that post the greatest potential user risk
- Rapidly and anonymously understand potential risky behavior and context around it
- Decide what is good or bad based on how users interact with your most valuable data
- Continuously revisit your decisions as you and our machines learn

Risk-adaptive security

NEXT GENERATION CYBERSECURITY

TRADITIONAL SECURITY

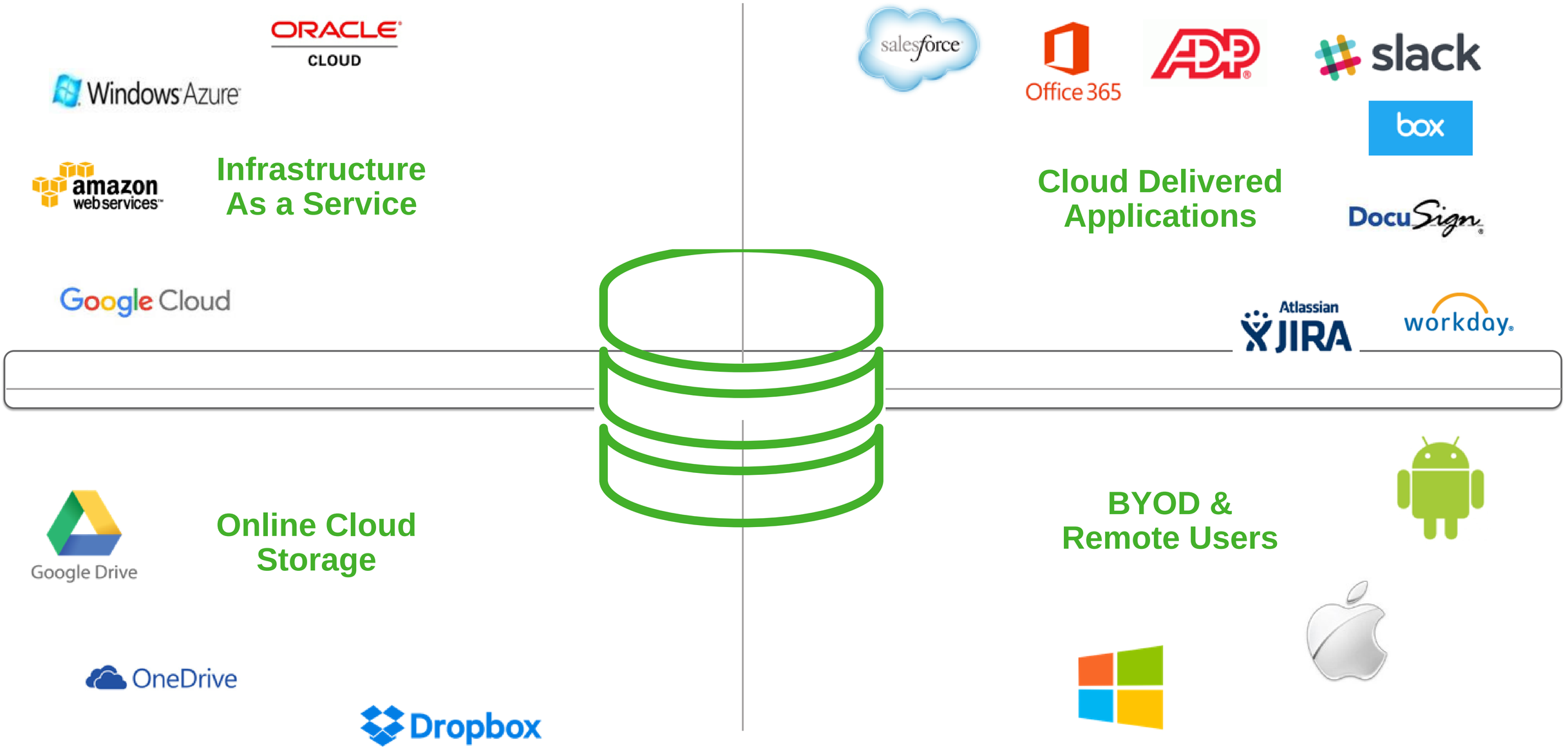


One-to-many

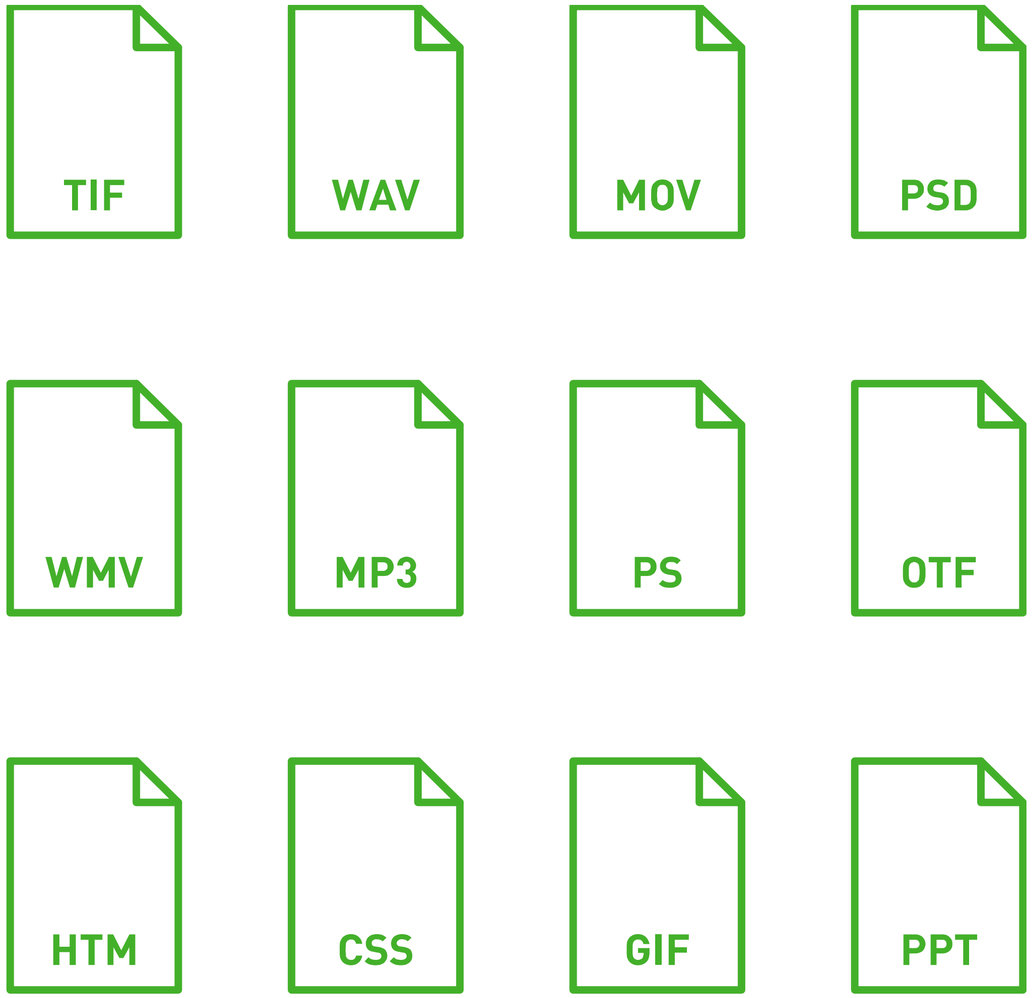
RISK ADAPTIVE SECURITY

One-to-one

WHERE CAN AN ORGANIZATION'S DATA RESIDE?



DETERMINING WHAT IS REALLY IMPORTANT



Is the criticality of data related to

WHERE IT RESIDES

or

WHAT IT CONTAINS

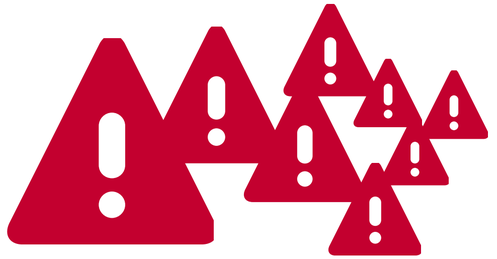
WHAT ARE WE TRYING TO SOLVE?

Protect the important data wherever it resides

without

Frustrating Users

Overwhelming Administrators



Mistaking

for

TODAY'S DATA PROTECTION OPTIONS ARE LIMITED

Traditional UEBA

Forensic Analysis

Learning why something happened yesterday does not stop the problem.

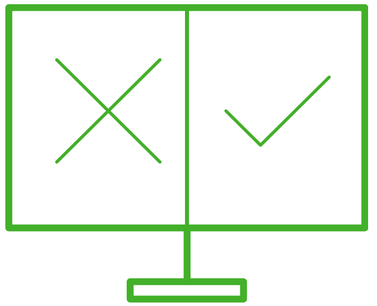
Traditional Insider Threat

Constant Monitoring

Balancing workforce privacy and IP protection is critical.

Traditional DLP

Block it or Allow it

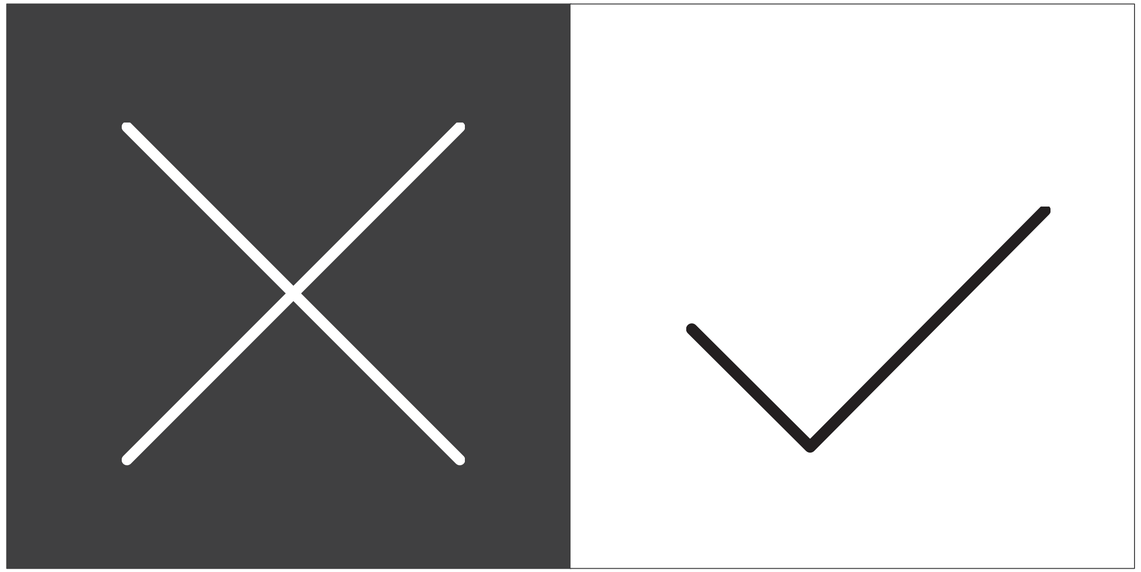


Current policies are far too rigid to be effective.

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

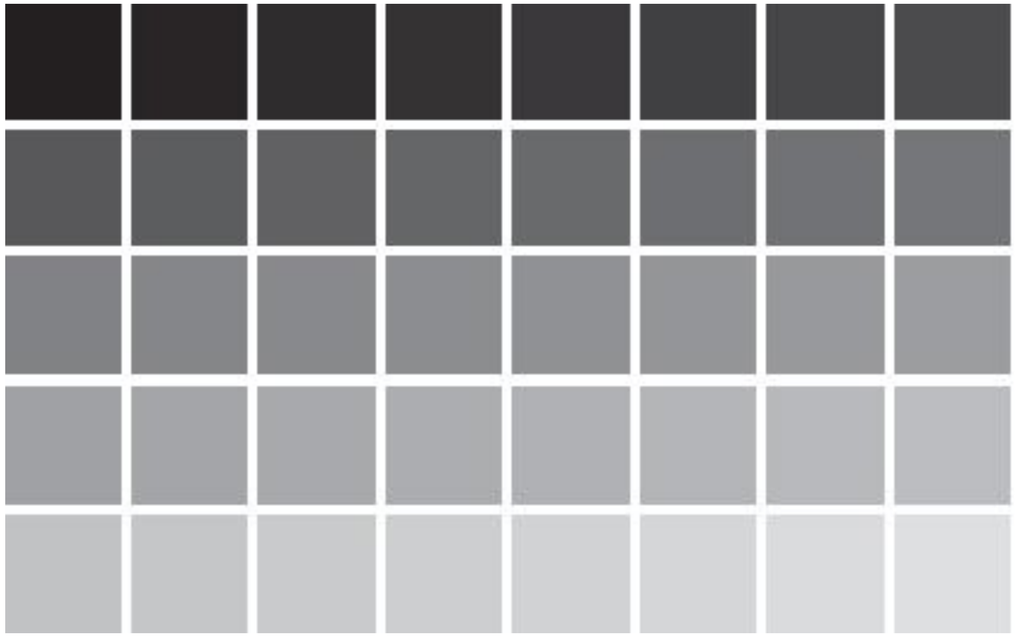
A NEW APPROACH IS NEEDED

Today's Data Protection Competitors



Machines are binary

FORCEPOINT
POWERED BY Raytheon



Human Behavior is not black and white

TODAY’S DATA PROTECTION APPROACHES

Fixed 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

RISK ADAPTIVE PROTECTION: A NEW APPROACH

Actions vary based on the risk level of people and the value of data

Kate, PhD
Research Chemist

Kate is giving a presentation to senior leadership and tries to copy her slides to a USB stick.
Kate begins to bulk copy files to her local machine at off hours.

She gets a supplier's query about an order she doesn't remember placing and then logs into the supplier's website to check on it.

Kate begins accessing highly sensitive drug formula data and attempts to copy it off the corporate network.

High Risk Group

Policy: **observe** Kate's every user & machine detail and **block** all data transfers or copies anywhere

Medium Risk Group

Policy: **observe** Kate much more closely with video from local cache.

Low Risk Group

Policy: **encrypt** fingerprinted files to USB drives but allow others to be copied.

THE HUMAN ELEMENT IS PRESENT IN ALL CASES

CYBER CONTINUUM OF INTENT

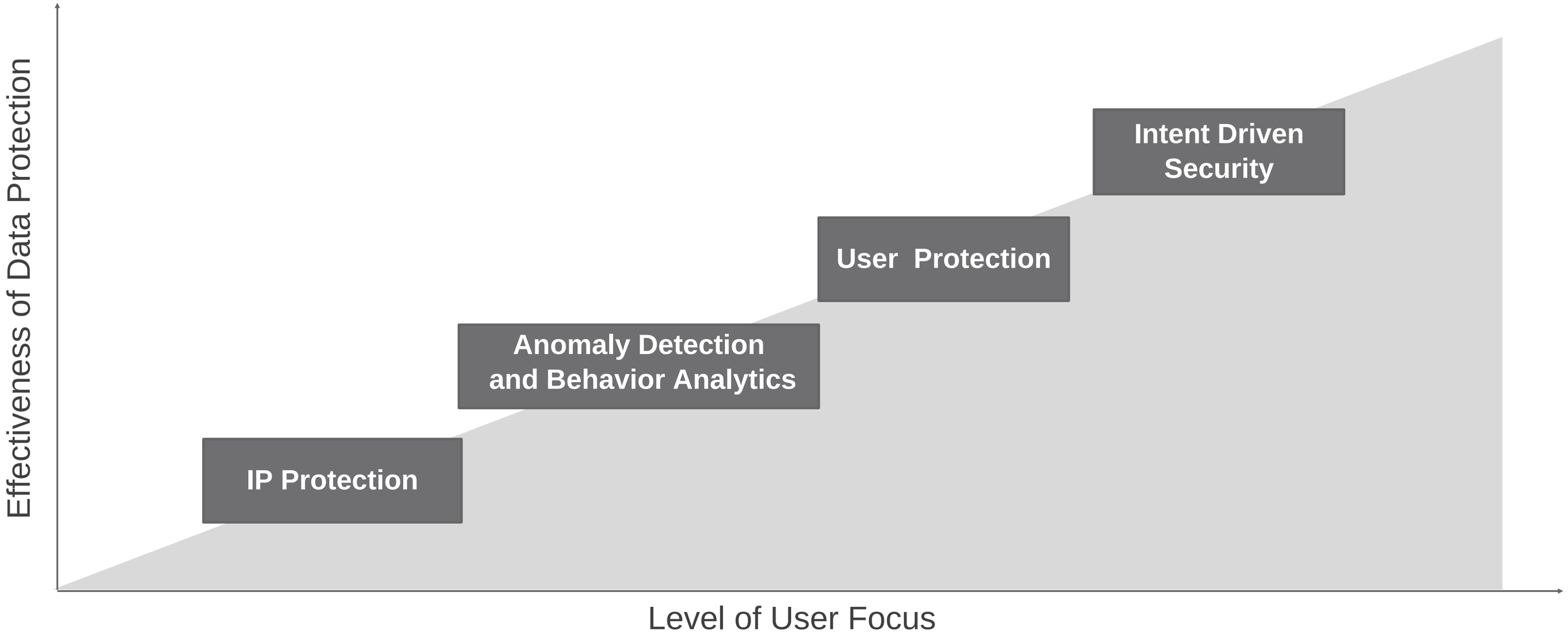
- 81% of hacking-related breaches exploited compromised credentials*
- People make mistakes
- Malware executes through impersonation
- People can be malicious

All of these behaviors are on your network at this very moment.

You need to understand them.

*Verizon, Data Breach Investigations Reports, 2017

THE JOURNEY TO BETTER DATA PROTECTION AND COMPLIANCE



MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Rakesh Shah

Senior Director of Product Management

rakesh.shah@forcepoint.com