March 2018

RETHINK CYBERSECURITY Risk Adaptive Security

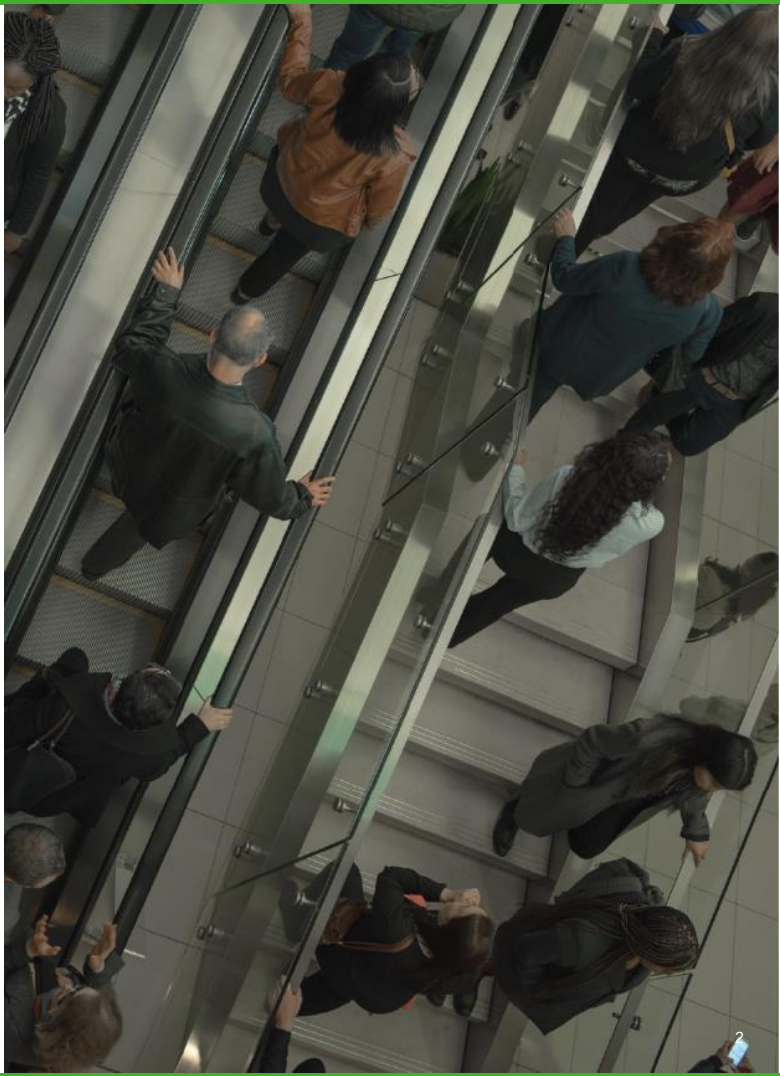
Nick Nicolescu – SEE Territory Manager

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

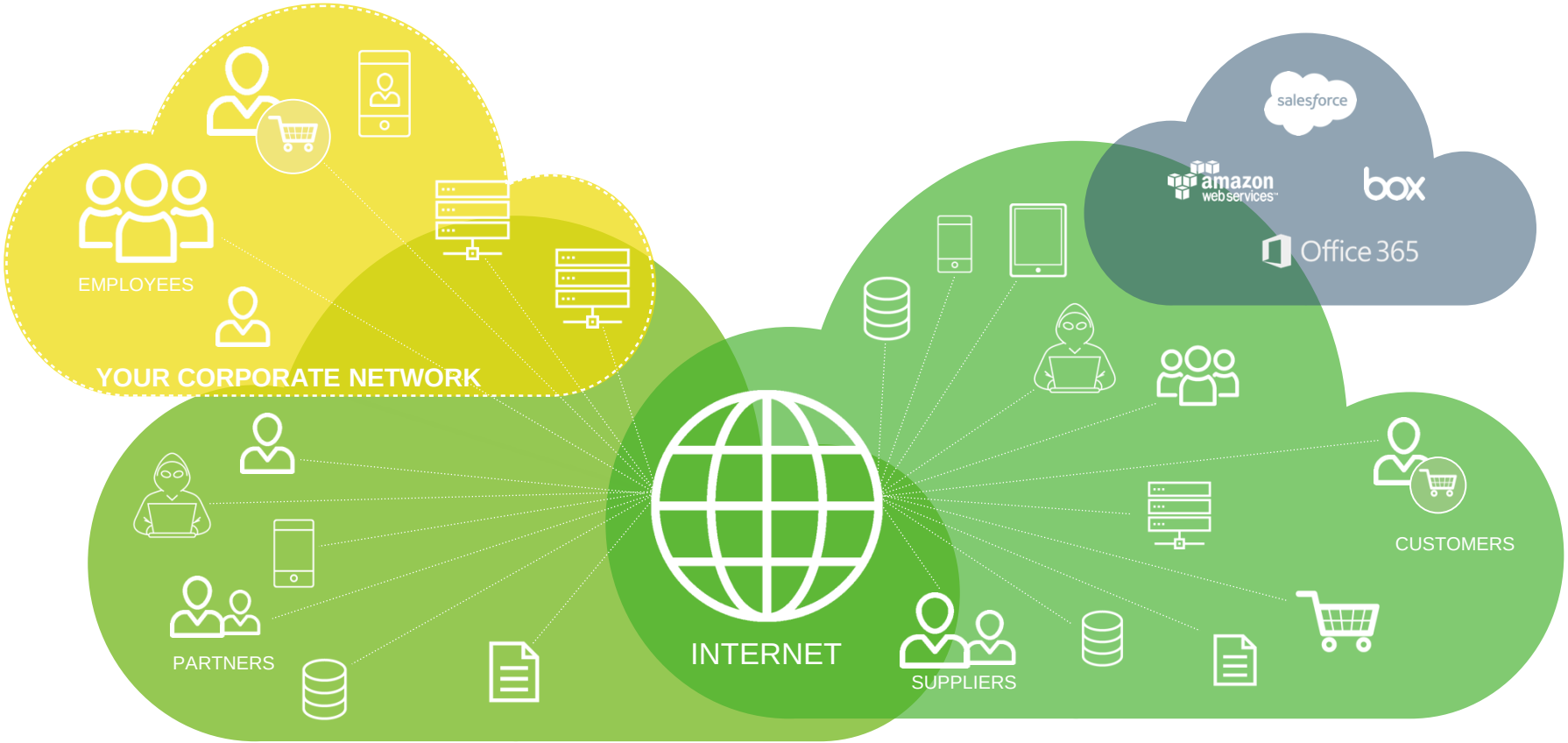
PURPOSE-BUILT TO PROVIDE A NEXT GENERATION CYBERSECURITY SOLUTION

- Created by Raytheon in 2016 to commercialize defense-grade technologies for the enterprise security market.
- One of the largest private cybersecurity companies in the world, with thousands of enterprise and government customers in more than 150 countries.
- Leading supplier to global Intelligence community and high assurance cyber missions.
- One of the most comprehensive security product portfolios in the industry.



A CASE FOR CHANGE

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 exfil

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

THE TRADITIONAL APPROACH TO CYBERSECURITY

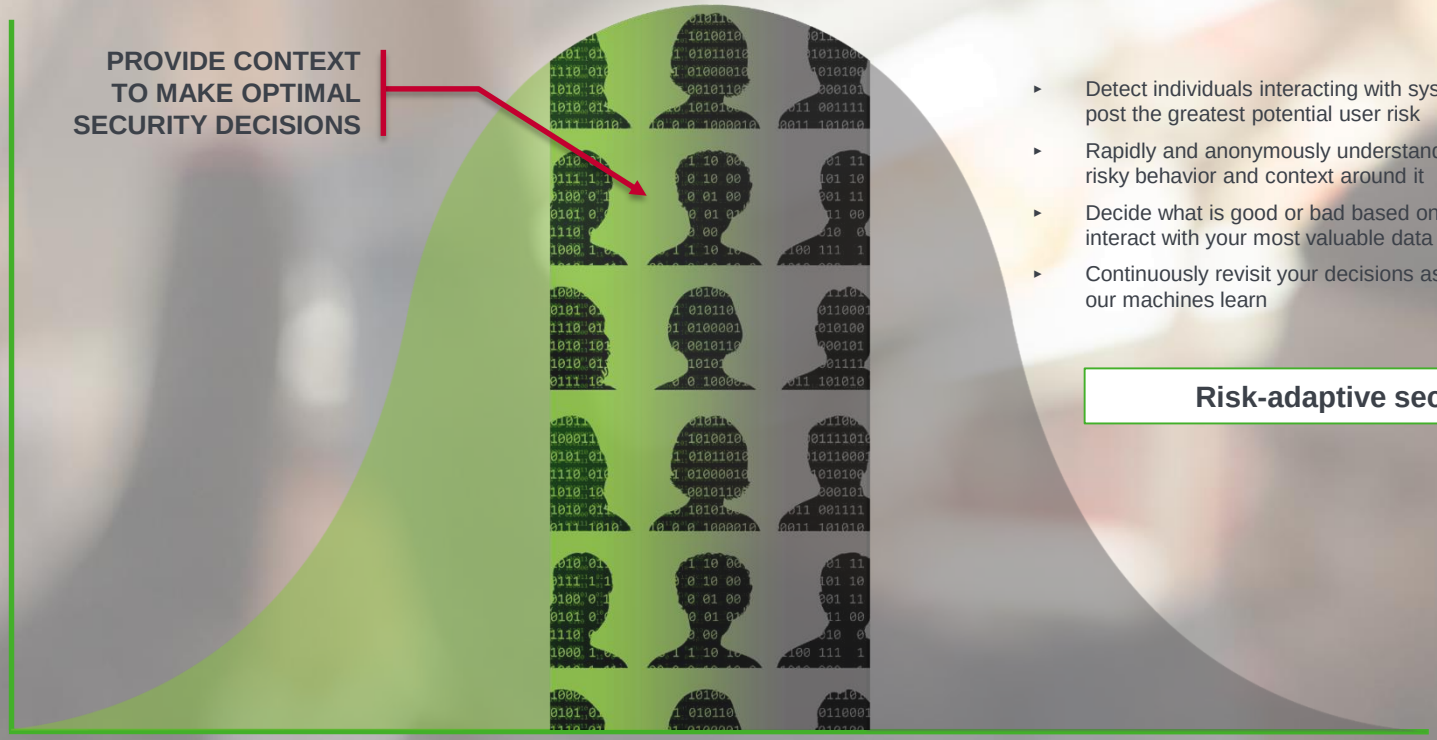
THREAT CENTRIC

- 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

SHIFTING THE APPROACH

A NEW PARADIGM: HUMAN-CENTRIC CYBERSECURITY



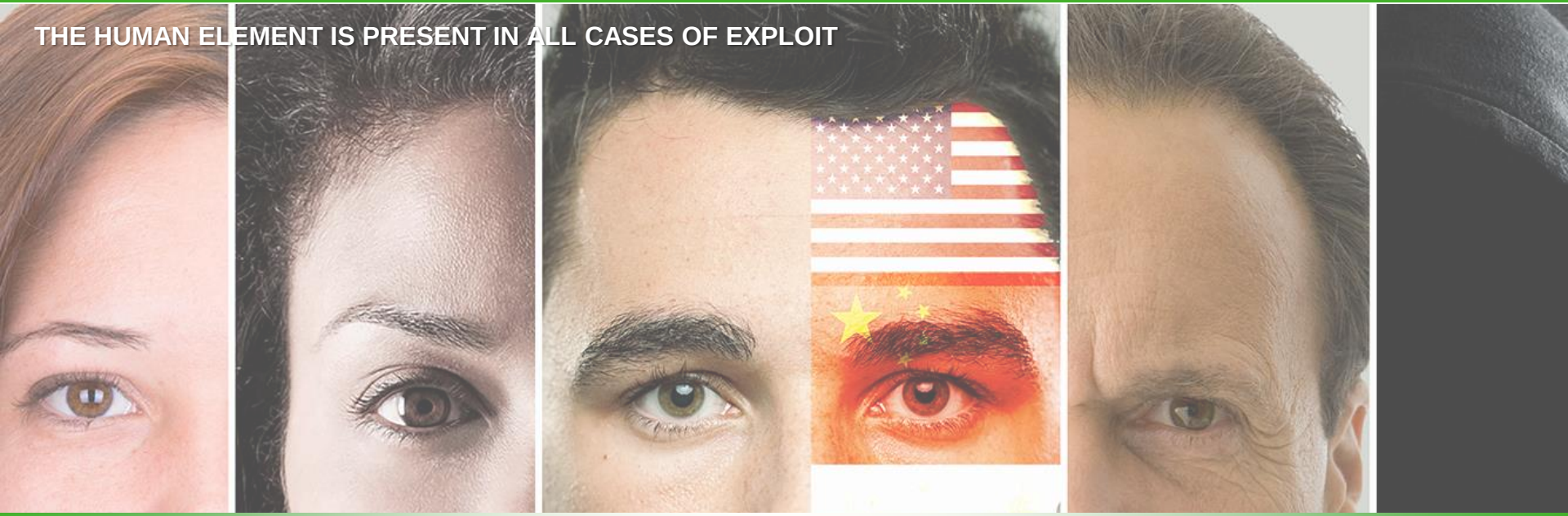
BEHAVIOR CENTRIC

- 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

PROTECT YOUR MOST VALUABLE ASSETS THROUGH **A HUMAN-CENTRIC APPROACH**

THE HUMAN ELEMENT IS PRESENT IN ALL CASES OF EXPLOIT



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.

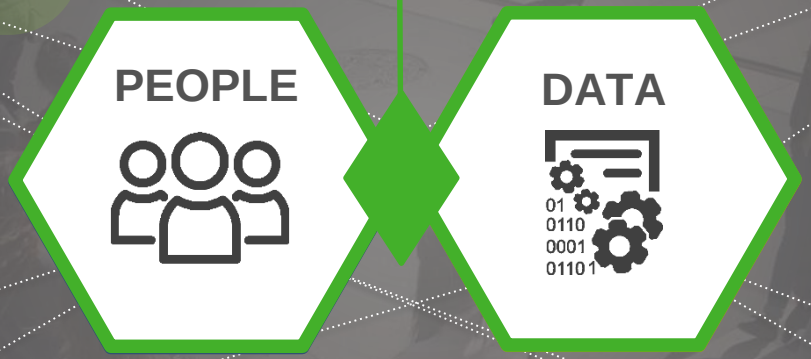
You need to understand them.

*Verizon, Data Breach Investigations Reports, 2017

FOCUS ON THE TRUE CONSTANTS

FOCUS ON THE TRUE CONSTANTS

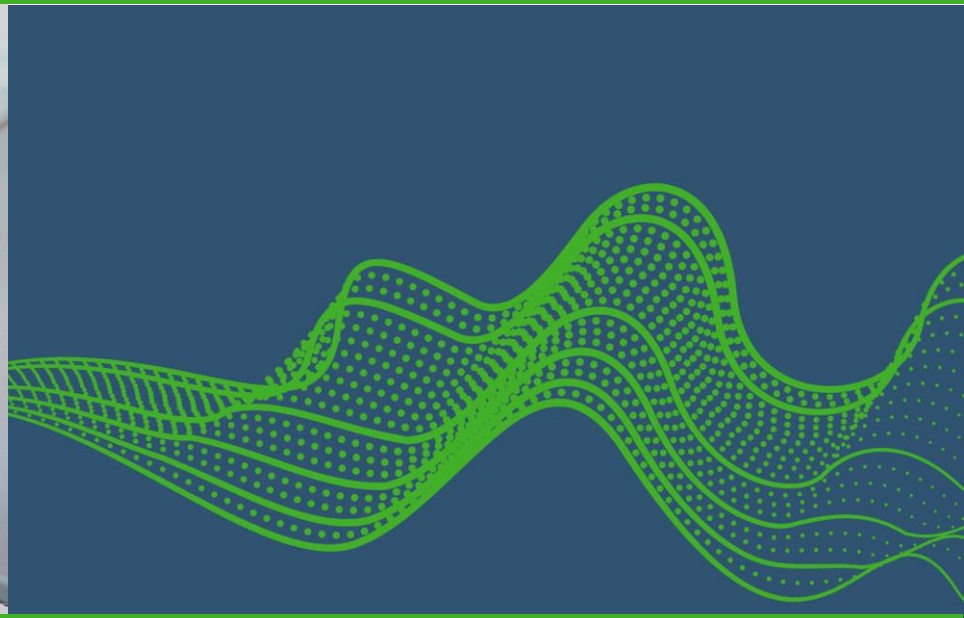
THE HUMAN POINT



salesforce
amazon web services
box
Office 365

Understanding the intersection of people, critical data and IP over networks of different trust levels.

PROTECT THE HUMAN POINT BY UNDERSTANDING



the rhythm of your people **AND** the flow of your data

VISIBILITY

Know where your critical IP is & who is interacting with it everywhere

POLICY

One policy to manage data movement & access across ALL distributed systems

ENFORCEMENT

Risk adaptive protection to act on change in human risk to critical IP in real time

COMPLIANCE

Effectively adhere to compliance regulations no matter where your data resides

THE HUMAN POINT SYSTEM

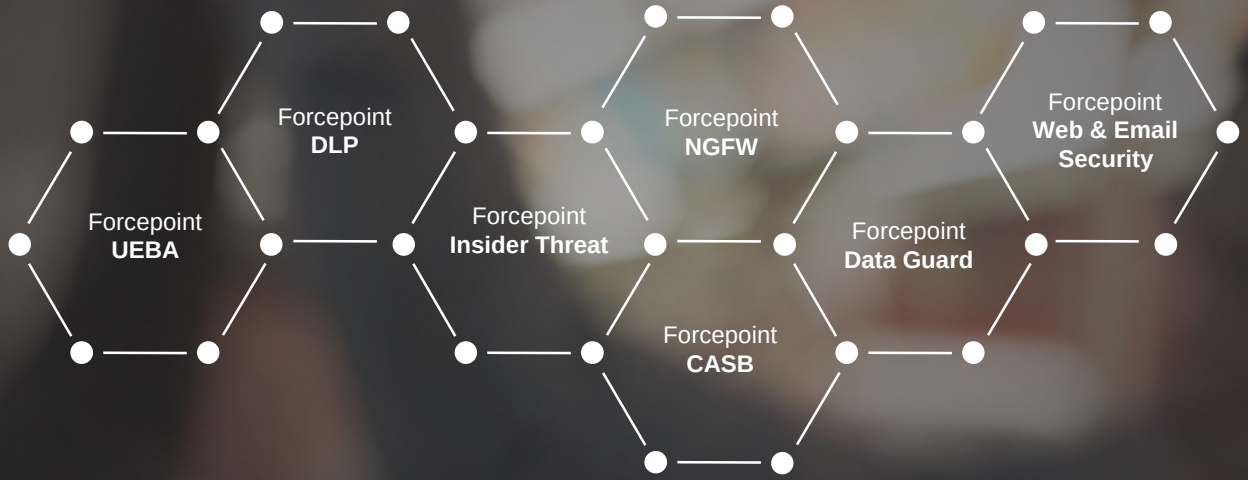
THE HUMAN POINT SYSTEM

DESIGN TENETS OF THE HUMAN POINT SYSTEM

EACH PRODUCT ELEMENT:

- Has best in class capabilities
- Can be your starting point
- Integrates together as a system with unified management and policy
- Works with an existing environment

BEST IN CLASS CAPABILITIES



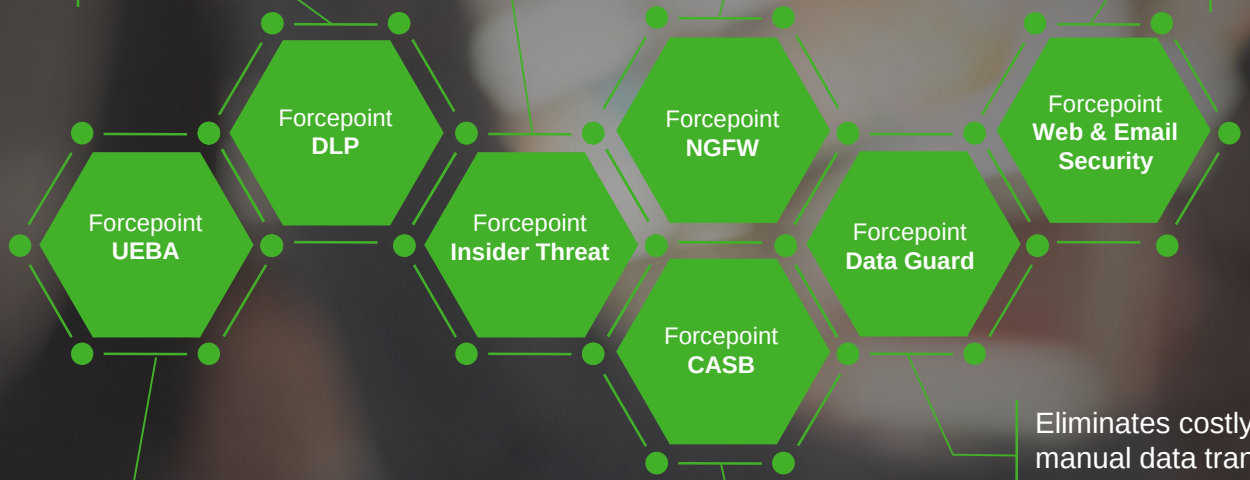
BEST IN CLASS CAPABILITIES

The most comprehensive understanding of user intent, trusted on over 1M endpoints.

Cuts network expenses by 50%, reduces cyberattacks by up to 86%, slashes incident response time as much as 73%.

Gartner Magic Quadrant Leader in Enterprise DLP 9 consecutive times.

100x reduction in malware incidents when deploying Forcepoint.[1]



Eliminates costly and time-consuming manual data transfers of highly-regulated, sensitive data.

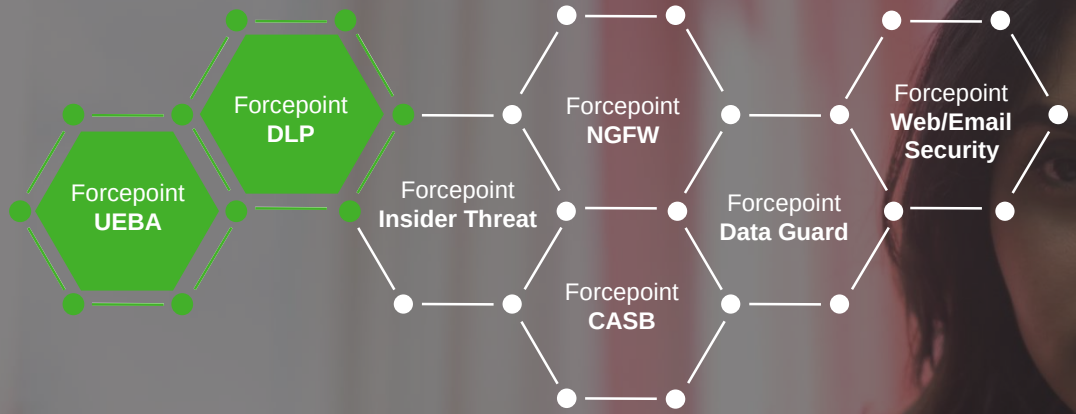
The leader in actionable insights based on risk-adaptive scoring.

Broadest cloud application support with unique customized risk assessment based on user behavior and data access classification.

START ANYWHERE USE CASES

USE CASE

DETECT ANOMALOUS BEHAVIOR THAT COULD LEAD TO DATA EXFILTRATION
ENFORCE POLICIES TO PREVENT DATA LOSS



start with

Forcepoint UEBA

+

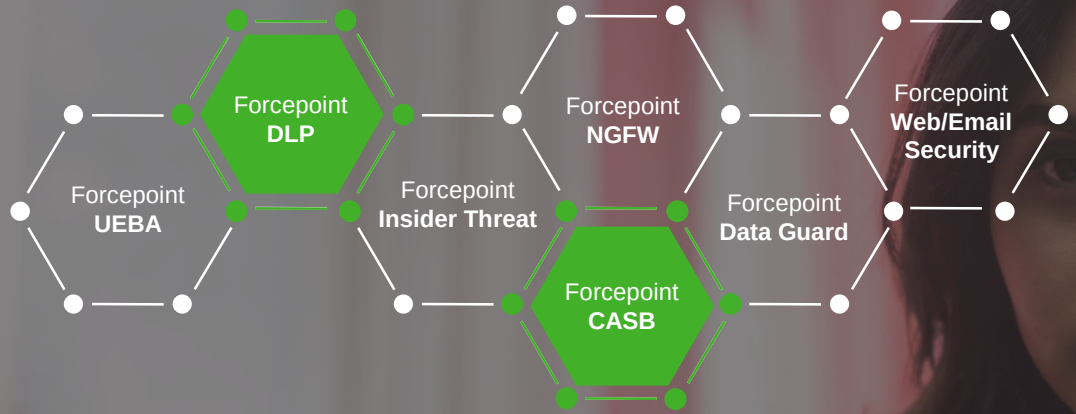
add

Forcepoint DLP

USE CASE

PROTECT CRITICAL DATA AND IP

DISCOVER AND PROTECT DATA IN THE CLOUD, AND CONTROL ACCESS TO CLOUD APPS



start with

Forcepoint DLP

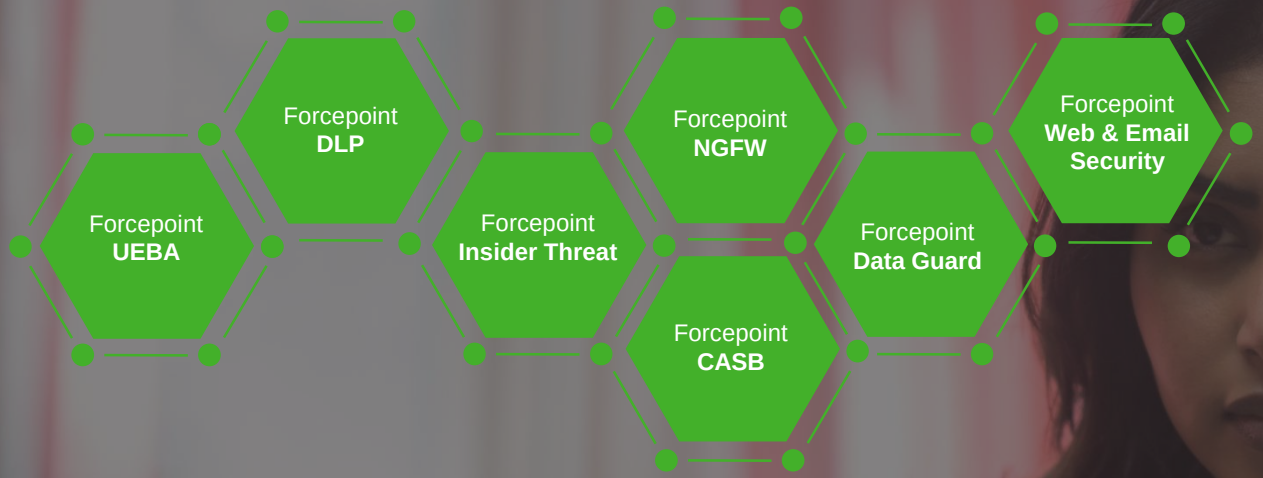
+

add

Forcepoint CASB

AN INTEGRATED SYSTEM

THE SYSTEM GETS SMARTER AND MORE EFFECTIVE AS YOU ADD MORE ELEMENTS



Increased visibility across the system

Unified policy protects against discontinuities

More options for enforcement

Increased analytic efficacy

A NEXT GENERATION CYBERSECURTY SOLUTION

Data is now stored everywhere and accessed from anywhere

Too many point solutions with no unified security policy

Too many alerts -- cannot determine critical signal

Enforcement is manual, reactive, and too late

Visibility

- Forcepoint DLP and Forcepoint Insider Threat combine to provide powerful investigation capabilities, including video
- Forcepoint NGFW offers central visibility into distributed locations

Integrated System

- Forcepoint's Human Point System provides an integrated view of clouds, 3rd party apps and users
- Forcepoint's system unifies multiple solutions in a single location

Alert Efficacy

- Forcepoint UEBA applies analytics to cut through the noise
- Forcepoint DLP's Incident Risk Ranking identifies and offers guidance to address the riskiest behavior

Dynamic Enforcement

- Forcepoint UEBA provides context into user actions across disparate data sources to identify out-of-compliance activity
- Forcepoint DLP remediates fraudulent activity before it happens

126% INCREASE IN BREACHES IN THE LAST 5 YEARS

Phishing attack on UC Davis health breaches data on 15,000 patients

Major health insurer Bupa hit by data breach

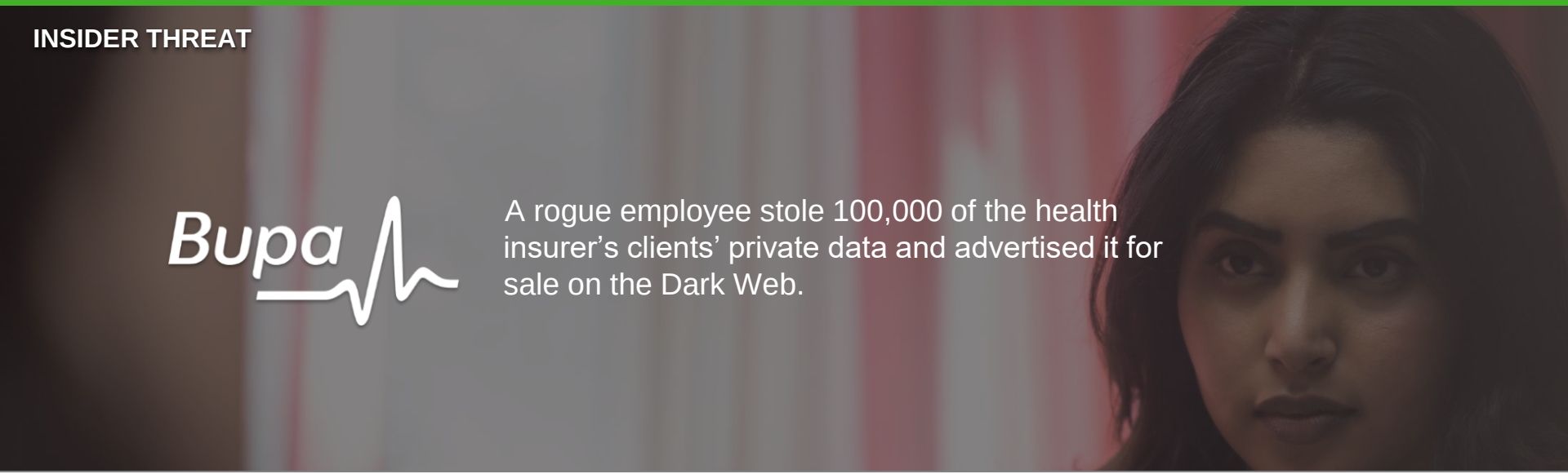
New Anthem data breach by contractor affects more than 18,000 enrollees

Equifax breach exposed data for 143 million consumers

GOP data firm accidentally leaks personal details of nearly 200 million American voters

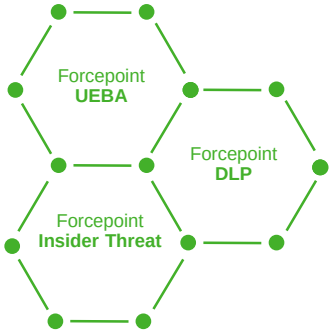
Dow Jones S3 cloud carelessness leaves door open on WSJ customer data

*Verizon, Data Breach Investigations Reports, 2012 & 2017



Bupa

A rogue employee stole 100,000 of the health insurer's clients' private data and advertised it for sale on the Dark Web.



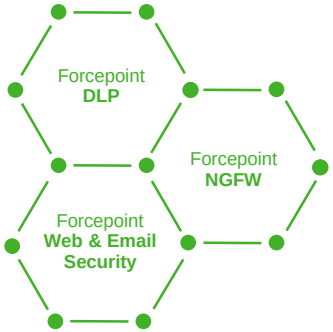
The Human Point System Solution:

- Forcepoint Insider Threat would have monitored the employee's activities in real-time and provided forensic evidence
- Forcepoint UEBA would have identified abnormal behavior and alerted the security team to behavioral changes
- Forcepoint DLP would have enforced policies to keep the fingerprinted data from being moved to a USB drive or uploaded

MALWARE ATTACK

Anthem®

What started with a phishing attack, led to malware moving within the internal network resulting in 37.5M personal records being lost.



The Human Point System Solution:

- Forcepoint NGFW deployed internally to segment the network would have captured and contained malware moving laterally
- Forcepoint Web/Email security would have stopped phishing as a vector to deploy malware
- Forcepoint DLP would have restricted access and movement of critical data

OUR JOURNEY TOGETHER

SECURITY EFFECTIVENESS

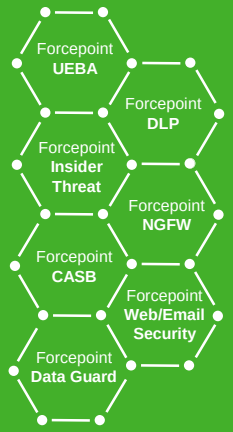
- Anti-Virus
- Firewall
- Secure Web Gateway

- NGFW
- Email Gateway

- DLP
- CASB

- UEBA

THE HUMAN POINT SYSTEM



Threat-centric

Data-centric

Risk adaptive

Source: Gartner, Cybersecurity Maturity Curve

OUR MISSION IS ALIGNED WITH YOURS

Protecting Livelihoods | Privacy | Profits