Forcepoint's Approach to Zero Trust (ZTX)

A data-centric security architecture, protected by behavior-based controls

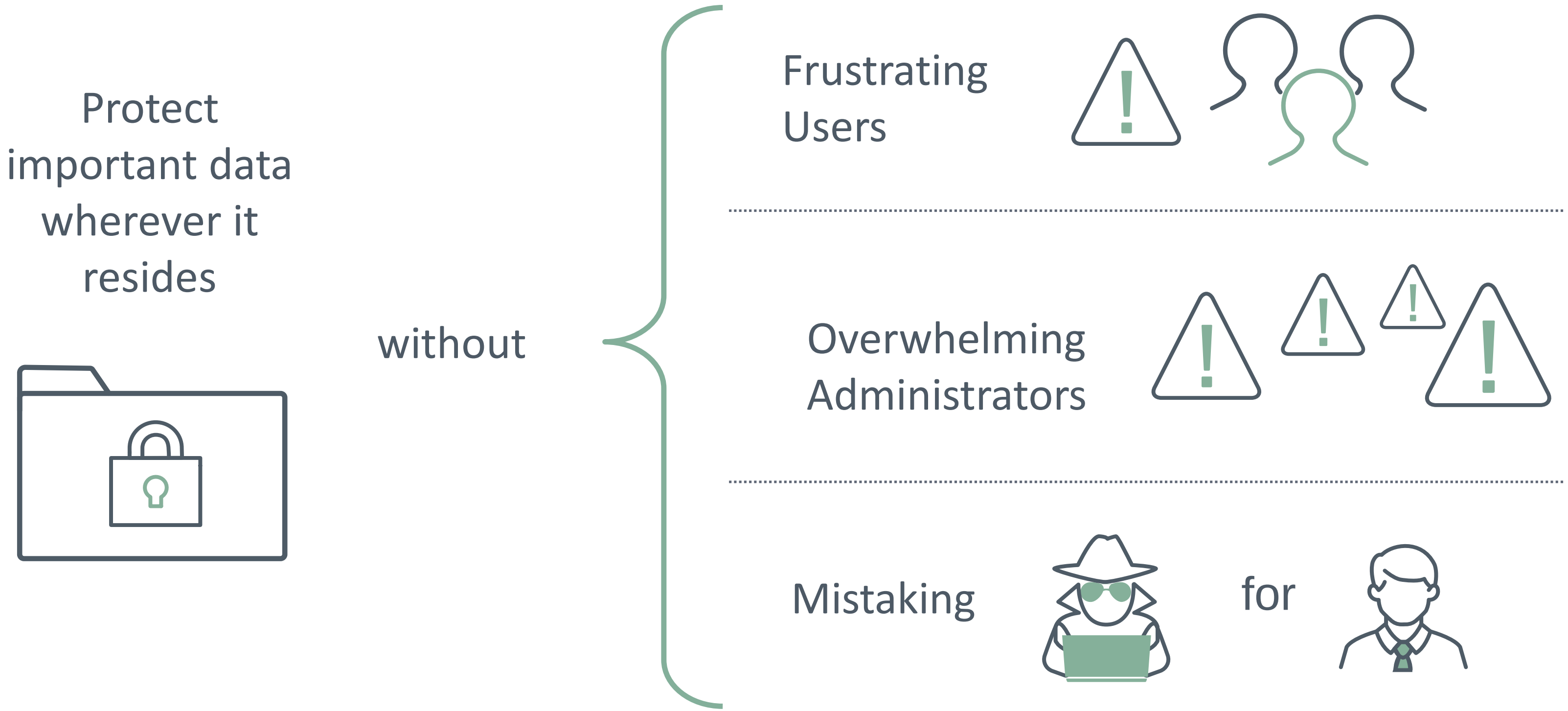
Victor Martinez

Sales Engineering Manager, Forcepoint Global Governments

FORCEPOINT

Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain

The Current Mission for Data Security



Protect important data wherever it resides

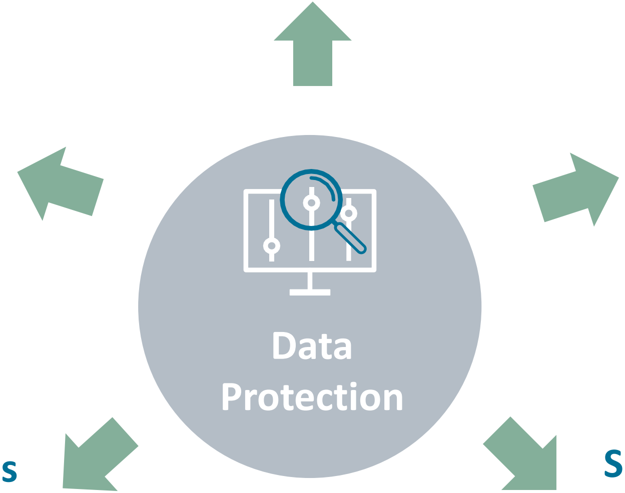
without

Frustrating Users

Overwhelming Administrators

Mistaking for

Data Protection Point of View



Data Discovery & Classification

Discovery across network, endpoint & cloud apps
Partnerships: Microsoft, Boldon James, Titus, Seclore

Data Detection

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

Analytics

Behavioral Analytics Module
Risk Adaptive Protection

Deep Forensics

Unified Endpoint
Insider Threat
Cloud Apps

SaaS App Protection

API Integration
Inline Cloud Proxy Infrastructure
Data in motion, in use, at rest

FORCEPOINT Next Generation Data Protection

Legacy DLP

- **Strong policy enforcement** prevents data exfiltration **but can reduce workplace productivity**
- DLP policy management is **static**, **set for an entire group**, must be **manually** changed if users is identified as high risk
- Organizations forced to adjudicate DLP alerts with **no context**, making **determination of false positives difficult**
- Most DLP deployments forced into **monitor only** mode

Dynamic Data Protection (DDP)

Leverage User Behavior Analytics to:

- Provide **full operational context** to more effectively adjudicate DLP alerts
- Automatically escalate more stringent policy deployment and enforcement for users **based on data exfiltration risk indicators**
- Dynamic mapping of policies with multiple enforcement options
- Maximize workforce productivity

Data Protection – Pathway to Blocking

Problem

- DLP implementers are concerned with being viewed as a strain on user productivity in the event their policies result in too many false positives.

The Security Requirements

- Having the ability to forensically audit their alerts if important data leaks.

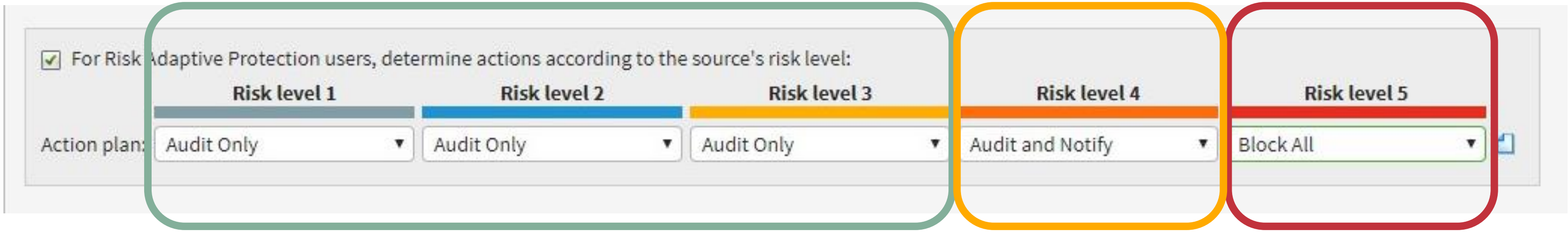
Result

- Many large enterprises have deployed DLP in audit only mode. The security team can mine alerts to identify data exfiltration, but they don’t actively block it.

Moving Beyond Auditing Alerts

Blocking the riskiest users

Business as usual



☑ For Risk Adaptive Protection users, determine actions according to the source's risk level:

	Risk level 1	Risk level 2	Risk level 3	Risk level 4	Risk level 5
Action plan:	Audit Only ▾	Audit Only ▾	Audit Only ▾	Audit and Notify ▾	Block All ▾

Still non-blocking,
but notify the admin

Result

- Bad users are blocked, good users are unaffected
- Confidence in the system allows admins to deploy blocking posture
- Policies are now user specific based on individual behavior

Frustrating Users

Overwhelming Administrators

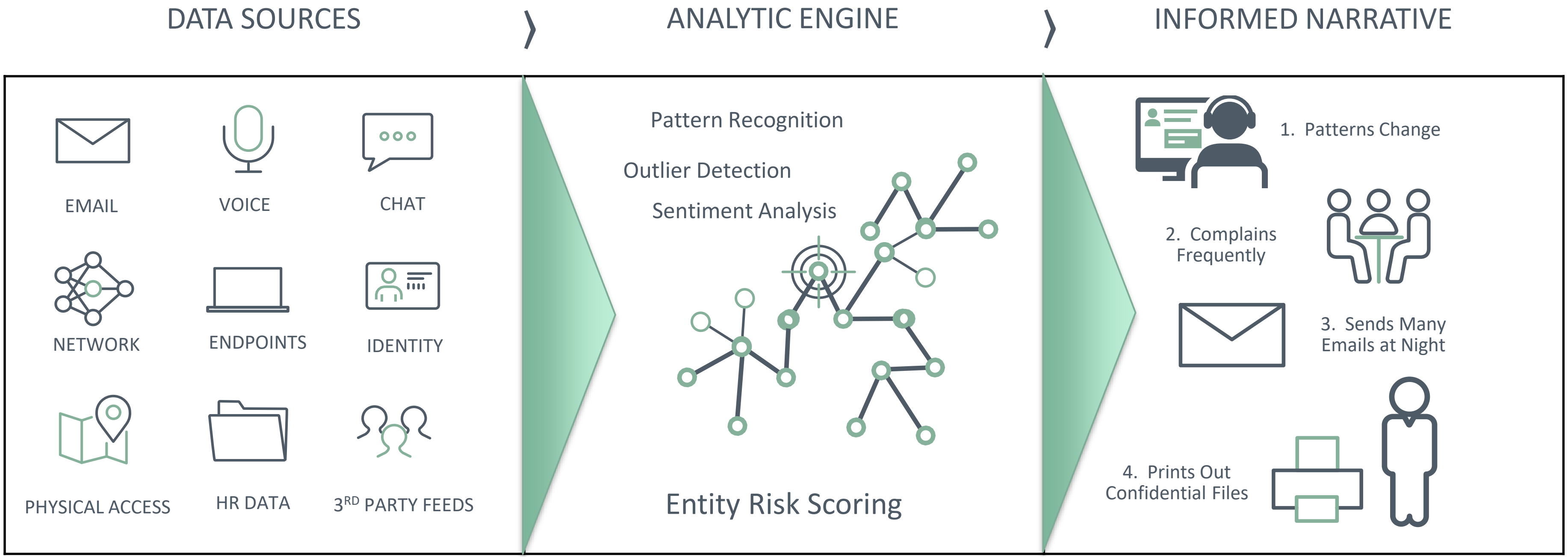
Mistaking for

Better Understanding of Intent

An employee tries to print an FOUO document and the DLP solution blocks it.

Is this employee a risk?

Analyze & Model For Insights



DATA SOURCES

ANALYTIC ENGINE

INFORMED NARRATIVE

EMAIL

VOICE

CHAT

NETWORK

ENDPOINTS

IDENTITY

PHYSICAL ACCESS

HR DATA

3RD PARTY FEEDS

Pattern Recognition

Outlier Detection

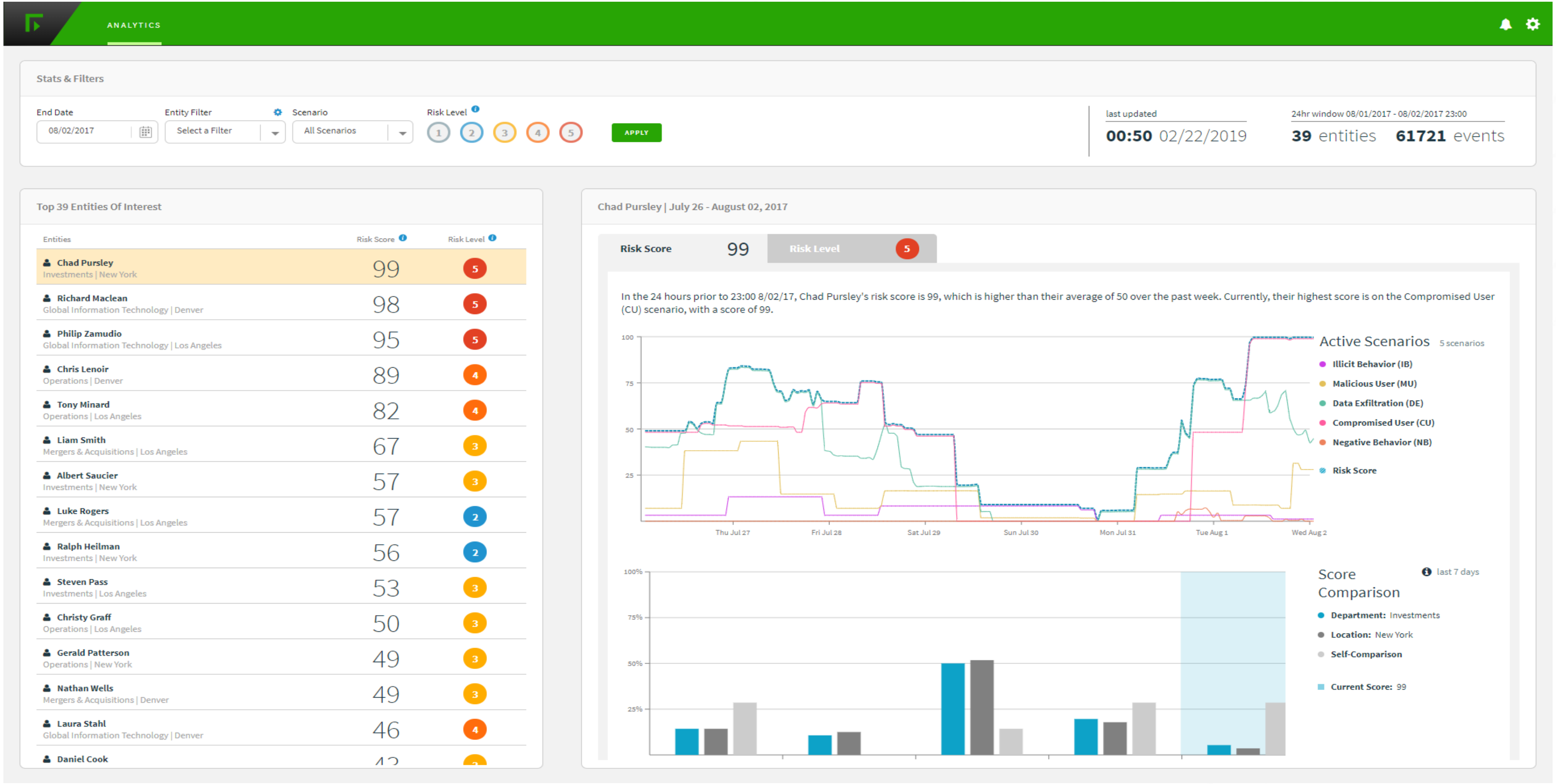
Sentiment Analysis

Entity Risk Scoring

1. Patterns Change
2. Complains Frequently
3. Sends Many Emails at Night
4. Prints Out Confidential Files

Understand Intent Through Deep Context

FORCEPOINT BEHAVIORAL ANALYTICS (FBA)



Stats & Filters

End Date: 08/02/2017

Entity Filter: Select a Filter

Scenario: All Scenarios

Risk Level: ① ② ③ ④ ⑤

APPLY

last updated **00:50** 02/22/2019

24hr window 08/01/2017 - 08/02/2017 23:00

39 entities **61721** events

Top 39 Entities Of Interest

Entities	Risk Score	Risk Level
Chad Pursley Investments | New York	99	5
Richard Maclean Global Information Technology | Denver	98	5
Philip Zamudio Global Information Technology | Los Angeles	95	5
Chris Lenoir Operations | Denver	89	4
Tony Minard Operations | Los Angeles	82	4
Liam Smith Mergers & Acquisitions | Los Angeles	67	3
Albert Saucier Investments | New York	57	3
Luke Rogers Mergers & Acquisitions | Los Angeles	57	2
Ralph Heilman Investments | New York	56	2
Steven Pass Investments | Los Angeles	53	3
Christy Graff Operations | Los Angeles	50	3
Gerald Patterson Operations | New York	49	3
Nathan Wells Mergers & Acquisitions | Denver	49	3
Laura Stahl Global Information Technology | Denver	46	4
Daniel Cook	43	

Chad Pursley | July 26 - August 02, 2017

Risk Score 99 | Risk Level 5

In the 24 hours prior to 23:00 8/02/17, Chad Pursley's risk score is 99, which is higher than their average of 50 over the past week. Currently, their highest score is on the Compromised User (CU) scenario, with a score of 99.

DDP - Risk-Adaptive Protection

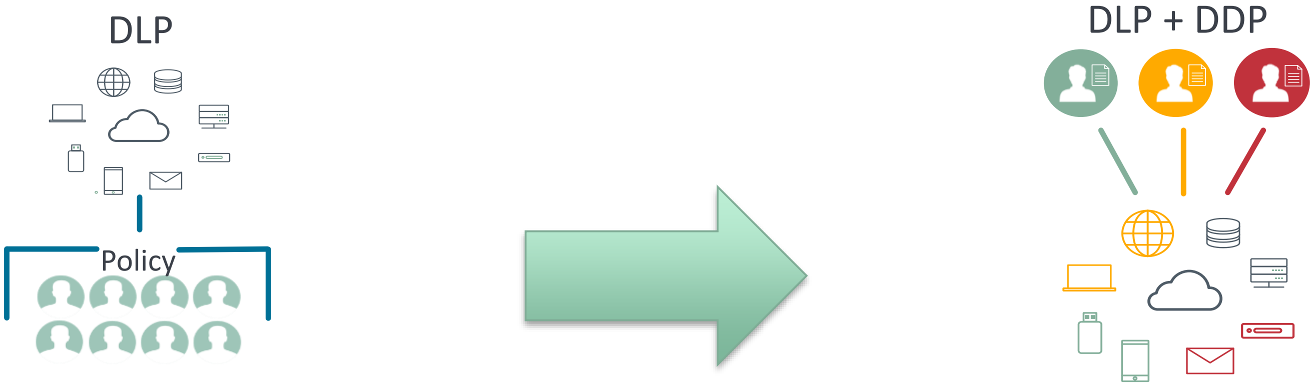
Risk-adaptive protection **dynamically applies monitoring and enforcement controls to protect data** based on the calculated behavioral **risk level of users** and **value of data** accessed.

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. Each user has a **unique and dynamic Risk Level**
2. Risk levels are driven up and down based on **changes in behavior**
3. Risk Levels drive **different outcomes**
4. **Security adapts** to Risk Levels as they fluctuate

Improved Visibility and Reduction of Noise



- Total Incidents (30 Days) - ~400,000
- Top 2 Policies ~ 65% of incidents
  - Office Files Sent over Time ~170,000
  - Large Files ~74,000
  - Requires thresholds

- Total Incidents (30 Days) - ~165,000
- Visibility into all file types
- Visibility into all file sizes
- Simplification of DLP policies

DDP Results In The Real World

	User 1 – Product Development Engineering	User 2 - Security Architecture
Summary	• User injected numerous DLP policy violations and exfiltration events over 12 hours • High Volume, important data	• User injected small amount of DLP policy violations and exfiltration events with critical data • Low volume, critical data
Risk Score / Level	95 / 5	93 / 4
Analytics		
DDP Matches Sum – Total amount of incident	1,378	158
DDP Incident Score – Type of data being moved	75	81 22 violations with “Confidential and Proprietary Content”
DDP Event Count – Total number of exfiltration events	~130,000	~9,000
DDP Bytes Sum – Total amount of data exfilled (GB)	75	9
DDP Event Score – non incident type of data being moved	85	85

Immediate Benefits of Dynamic Data Protection

Intelligent DLP

Reduce the amount of DLP alerts that need to be triaged; transition DLP from broad to individual policies.

Increased Productivity

Provide greater flexibility in policies, and adapt enforcement based on calculated risk.

Proactive Security Management

Detect and respond to high-impact events in a shorter amount of time.

Multilevel Risk Adaptive Protection

Problem:

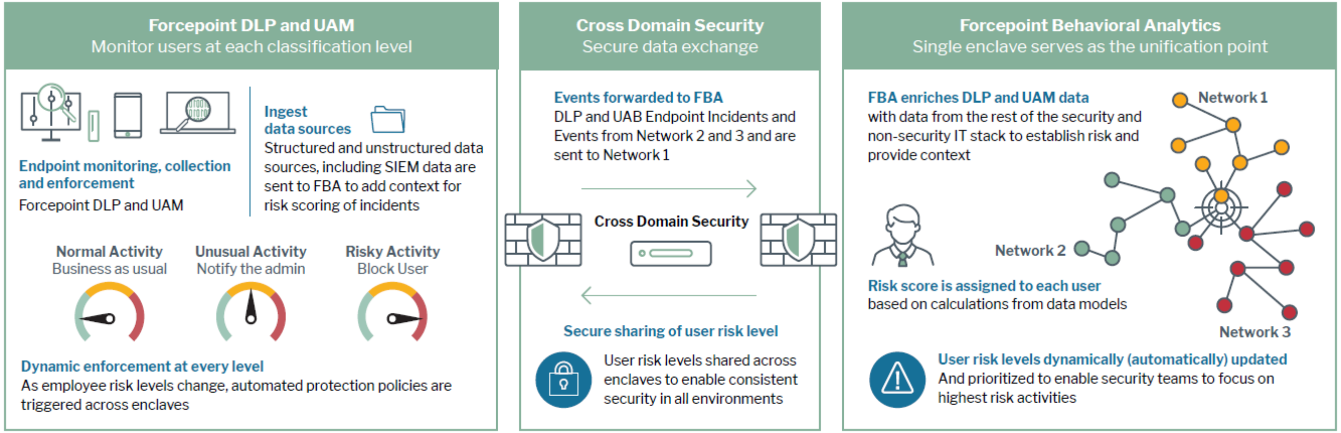
- Protect sensitive data across multiple networks
- Discover and inventory critical data and IP every place users collaborate.

Solution:

- Forcepoint’s Multilevel Risk Adaptive Protection Solution integrates the market’s most powerful data protection suite, user behavioral analytics, next generation firewall and cross domain transfer technologies to provide secure data sharing and comprehensive user visibility. The solution provides multilevel end-to-end security utilizing Behavior Analytics by and securely sharing user risk levels across multiple networks for adaptive and consistent enforcement.

Benefits:

- From a single pane of glass, multilevel Risk Adaptive Protection significantly reduces time to discovery, alerts and false positives, across domains to enable better use of resources for holistic forensic investigations, stronger security, and automated risk responses.



Forcepoint DLP and UAM
Monitor users at each classification level

Endpoint monitoring, collection and enforcement
Forcepoint DLP and UAM

Ingest data sources
Structured and unstructured data sources, including SIEM data are sent to FBA to add context for risk scoring of incidents

Dynamic enforcement at every level
As employee risk levels change, automated protection policies are triggered across enclaves

Cross Domain Security
Secure data exchange

Events forwarded to FBA
DLP and UAB Endpoint Incidents and Events from Network 2 and 3 and are sent to Network 1

Secure sharing of user risk level
User risk levels shared across enclaves to enable consistent security in all environments

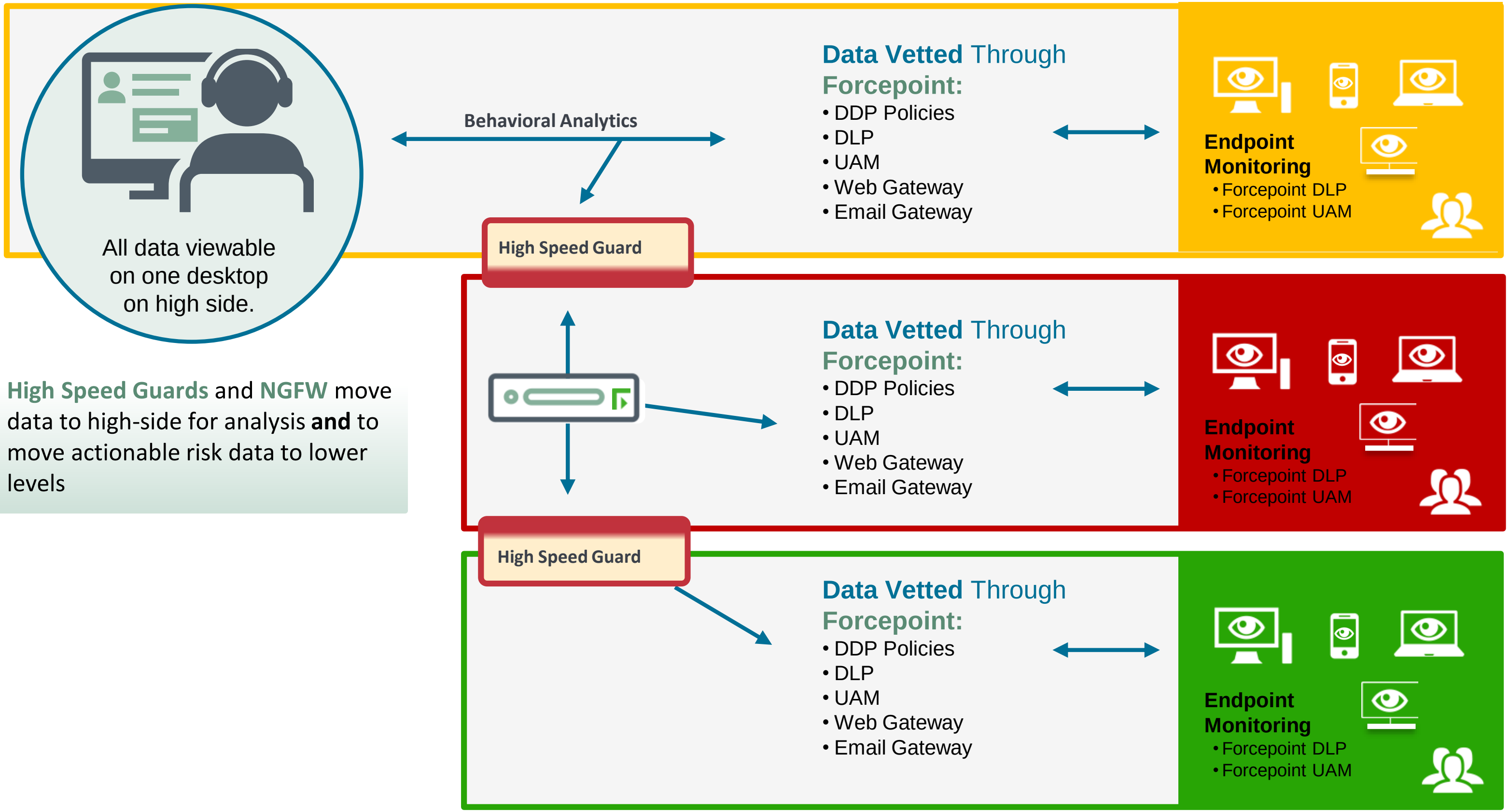
Forcepoint Behavioral Analytics
Single enclave serves as the unification point

FBA enriches DLP and UAM data
with data from the rest of the security and non-security IT stack to establish risk and provide context

Risk score is assigned to each user
based on calculations from data models

User risk levels dynamically (automatically) updated
And prioritized to enable security teams to focus on highest risk activities

Forcepoint’s Zero Trust Multilevel Risk Adaption Solution



All data viewable on one desktop on high side.

Behavioral Analytics

Data Vetted Through **Forcepoint:**
- DDP Policies
- DLP
- UAM
- Web Gateway
- Email Gateway

Endpoint Monitoring
- Forcepoint DLP
- Forcepoint UAM

High Speed Guard

Data Vetted Through **Forcepoint:**
- DDP Policies
- DLP
- UAM
- Web Gateway
- Email Gateway

Endpoint Monitoring
- Forcepoint DLP
- Forcepoint UAM

High Speed Guard

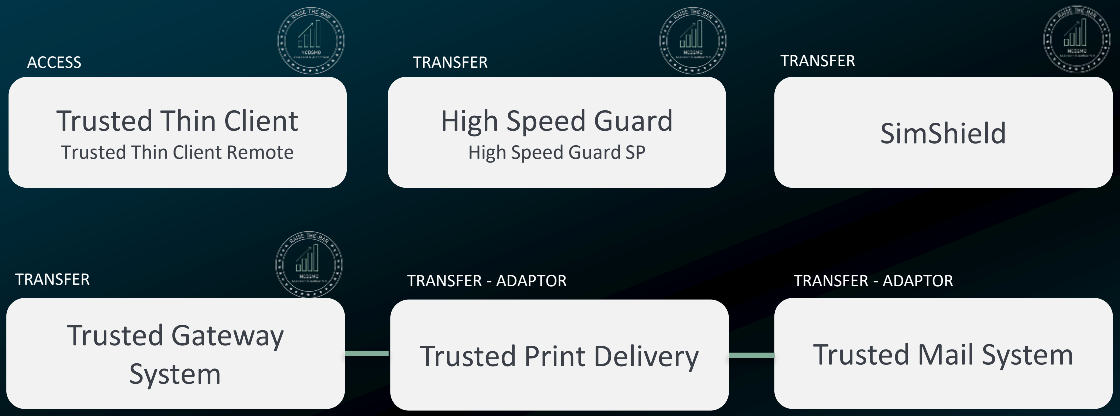
Data Vetted Through **Forcepoint:**
- DDP Policies
- DLP
- UAM
- Web Gateway
- Email Gateway

Endpoint Monitoring
- Forcepoint DLP
- Forcepoint UAM

High Speed Guards and **NGFW** move data to high-side for analysis **and** to move actionable risk data to lower levels

Cross Domain Solutions Suite

Facilitating your mission while maintaining the highest degree of network and data security



ACCESS

Trusted Thin Client
Trusted Thin Client Remote

TRANSFER

High Speed Guard
High Speed Guard SP

TRANSFER

SimShield

TRANSFER

WebShield

TRANSFER

Trusted Gateway System

TRANSFER - ADAPTOR

Trusted Print Delivery

TRANSFER - ADAPTOR

Trusted Mail System

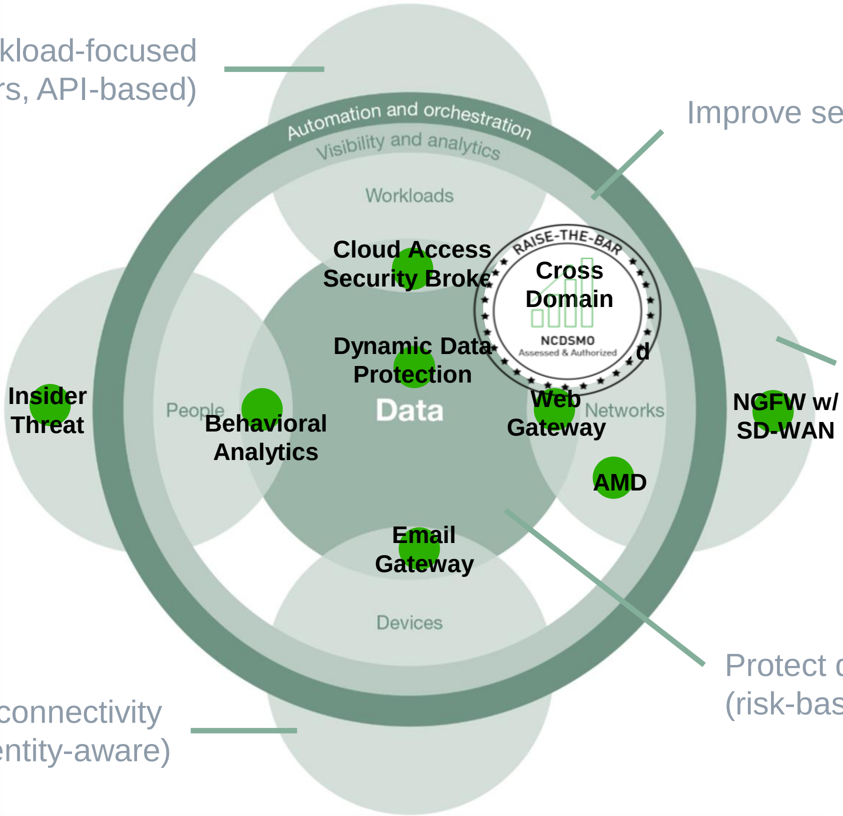
RAISE-THE-BAR
NCDSMO
Assessed & Authorized

Zero Trust – Forcepoint Portfolio Today

Workload-focused
(virtualized, containers, API-based)

Improve security detection and response
(analytics and automation)

Limit excessive user privileges
(risk-based, identity-aware)



Highly distributed networks
(micro-segmentations, perimeters)

Enable secure connectivity
(scalable, identity-aware)

Protect data where it resides and in use
(risk-based, frictionless)

● Forcepoint

Thank you!

Patricia.Colpitts@forcepoint.com

Data at the Center

Everywhere—
cloud, on-prem, endpoint

Behavior-based Controls

Automated ZT protection via risk-adaptive enforcement

Unified Cloud Solution

Dynamic Security Platform