Human Centric Security
Risk Adaptive Protection by User and Data Analytics

WILLIAM TAM
Director of Sales Engineering
Forcepoint LLC
wtam@forcepoint.com
HOW DO YOU SECURE A WORLD WHERE YOU OPERATE ON THE INTERNET BUT DON’T OWN THE INTERNET

Your Corporate Network

Internet

Employees

Suppliers

Partners

Customers

SFDC

AWS

BOX

O365

ZERO PERIMETER

FRAGMENTED TRUST

INFINITE NOISE
HOW DO YOU SECURE A WORLD WHERE YOU OPERATE ON THE INTERNET BUT DON’T OWN THE INTERNET?

Continuously Expanding Attack Surface
Do you know where all your data lives?

Lack of Visibility
You cannot secure what you cannot see

Disjointed Security Policy
From one perimeter to defend to many

Siloed Security Solutions
A patchwork of offerings that create unintended gaps

Signals Become Noise
An overload of events

Disparate Compliance Regulations
Things just got a lot more complicated
WHY TRADITIONAL CYBER FAILS IN NEW IT ENVIRONMENT
NOT BUILT FOR VIRTUALIZED, DISTRIBUTED CLOUD OPERATING ENVIRONMENTS

1990-2010

- Perimeter

- Employees

- Security vendors focus on monitoring north-south network traffic and aim to block suspicious traffic

2010 – Today

- Perimeter

- Employees

- The perimeter is increasingly penetrated by hackers
- CIOs focus on east-west traffic to block lateral movement

Today’s (and Tomorrow’s) IT Reality

- Traffic is now multi-directional across internal and external clouds, suppliers, mobile employees and customers
- CIOs lack visibility and control. Very difficult to understand threats and how to block them
- A new approach is needed
FOCUS ON MANAGING PEOPLE AND DATA
FOCUS ON MANAGING PEOPLE AND DATA

PEOPLE

NETWORKS

Internet

DATA
CHASING DATA WITHOUT UNDERSTANDING THE USER

Data in Motion

Data at Rest

Data in Use

Who

What

Where

How

Action

Human Resources

Customer Service

Marketing

Finance

Accounting

Sales / Marketing

Legal

Technical Support

Engineering

Source Code

Credit Card Data

Personal Data

M&A Plans

Employee Salary

Financial Report

Customer Records

Manufacturing Docs

Research

Evernote

Dropbox

Business Partner

Facebook

OneDrive

Malicious Server

Removable Media

Competitor

Customer

File Transfer

Web

Instant Messaging

Peer-to-Peer

Email

Print

File Copy

Print Screen

Copy/Paste

Block

Notify

Remove

Encrypt

Quarantine

Audit

Notify

Confirm

Block

Notify

Remove

Encrypt

Quarantine

Audit

Notify
USER BEHAVIOR WITHOUT CONTEXT
WHY CONTEXT MATTERS

User and Entity Behavior

Good

Threat

What?

Not Sure

Threat Determination
A NEW APPROACH NEEDED: HUMAN-CENTRIC SECURITY

the rhythm of your people

Human Centric Security

the flow of your data

VISIBILITY & CONTROL

Deep insight into user behavior and cloud application usage to assess & control risk

ENABLING USERS

Safeguards for users to be productive on any device while shielding corporations from risk

PROTECTING VITAL DATA

Advanced real-time protection to ensure data is not compromised

2018 臺灣資安大會 TAIWAN CYBER SECURITY SUMMIT 2018
THE HUMAN POINT SYSTEM

- Best in class capabilities in every category
- Any module can be your starting point
- Integrates together as a system with unified management and policy
- Works with customer existing environment
THE HUMAN POINT SYSTEM

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

100x reduction in malware incidents when deploying Forcepoint.¹

100x reduction in malware incidents when deploying Forcepoint.¹

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.

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

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

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

ENFORCE POLICIES TO PREVENT DATA LOSS
IDENTIFY RISKY INSIDER BEFORE DATA EXFILTRATION HAPPEN

start with
Forcepoint DLP

add
Forcepoint UEBA
THE FLOW OF YOUR **DATA** : DATA MOVEMENT BY FORCEPOINT DLP

**INVENTORY**
PERSONAL DATA

**MAP, MANAGE & CONTROL**
PERSONAL DATA FLOWS

DLP: Discover, Cloud, Endpoint

DLP: Network, Endpoint
Web & Email Security modules
THE RHYTHM OF YOUR PEOPLE - USER BEHAVIOR ANALYTICS

DATA SOURCES

COMMUNICATIONS
- EMAIL
- VOICE
- CHAT

SECURITY
- NETWORK
- ENDPOINTS
- IDENTITY

ENRICHMENT
- PHYSICAL ACCESS
- HR DATA
- 3RD PARTY FEEDS

ANALYTIC ENGINE

COMMUNICATIONS
Specialized Communications Analytics - Content & Meta

DATA MODEL
Extensible Data Module for All Structured & Unstructured Sources

RISK SCORING
Identity Risk Scoring & Progression Along Cyber Risk Chain

VISUALIZATIONS
Behavioral Analytics Visualization

INFORMED NARRATIVE

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

FORCENET Ueba

2018 臺灣資安大會 TAIWAN CYBER SECURITY SUMMIT 2018
HUMAN CENTRIC SECURITY IN ACTION

DATA SOURCES

COMMUNICATIONS
- EMAIL
- VOICE
- CHAT

SECURITY
- Fortpoint LIF
- Fortpoint CASB
- Fortpoint IMS/W
- Fortpoint Web/Email Security
- Fortpoint Insider Threat

ENRICHMENT
- PHYSICAL ACCESS
- HR DATA
- 3RD PARTY FEEDS

ANALYTIC ENGINE

DATA MODEL
Extensible Data Module for All Structured & Unstructured Sources

RISK SCORING
Incy Risk Scoring & Progression Along Cyber Risk Chain

INFORMED NARRATIVE

COMMUNICATIONS
Specialized Communications Analytics - Content & Meta

VISUALIZATIONS
Behavioral Analytics Visualization

Risk Adaptive Protection
Protect Data & Assets Adaptively by Understanding Risk to the Business

**High Risk Group**
Policy: **observe** Kate’s every user & machine detail and **block** all data transfers or copies anywhere
Kate hordes SECRET files slowly in various places and attempts to copy to Google drive.
The Analytics Platform will aggressively increase Kate C’s risk score when she accesses SECRET fingerprinted files & classified data.

**Medium Risk Group**
Policy: **observe** Kate much more closely with video from local cache.
Kate begins to copy files to her local machine at off hours.
The Analytics Platform will determine Kate C’s risk score by user anomalies.

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

**HUMAN CENTRIC SECURITY IN ACTION : RISK ADAPTIVE PROTECTION**

Actions vary based on the risk level of actors & value of data.
DLP TODAY: APPLYING ACTIONS TO POLICY RULES

Action plan (response) is applied based on sensitive data matches

Incident severity is based on sensitive data matches
DLP RAP : APPLYING ACTIONS TO POLICY RULES

Action plan (response) is applied based on user risk level (1 – 5)

Incident severity is based on sensitive data matches

Applies to all DLP components: Endpoint; Network and Cloud Apps
RISK LEVEL CALCULATION BASED ON USER ACTIVITY

User risk score is calculated hourly by UEBA

User risk level (1 - 5) is computed by UEBA

Current risk levels computed by UEBA are are synced with DLP management system
Tier 2 analyst moves into Human Point UI to investigate employee

Incident is escalated out-of-application (e.g., email or chat) from Tier 1 to Tier 2 analyst
Employee risk level 2. Sensitive data copied onto USB drive

RAP applies file encryption action
Employee risk level 3. Sensitive data copied onto USB drive

RAP applies block action
OUR JOURNEY TOGETHER

SECURITY EFFECTIVENESS

- Anti-Virus
- Firewall
- Secure Web Gateway
- NGFW
- CASB
- DLP
- UEBA

THE HUMAN POINT SYSTEM

- Forcepoint UEBA
- Forcepoint DLP
- Forcepoint Insider Threat
- Forcepoint NGFW
- Forcepoint CASB
- Forcepoint Web/Email Security
- Forcepoint Data Guard

Source: Gartner, Cybersecurity Maturity Curve
THANK YOU

wtam@forcepoint.com
linkedin.com/in/willitam/