Datasheet

Forcepoint Behavioral Analytics

Discover and stop insider threat: Forcepoint's uniquely powerful analytics find malicious insiders no matter how they try to hide

Overview

The insider threat spans an overwhelming landscape. It is nearly impossible to achieve situational awareness while at the same time quickly identifying specific threats. The Forcepoint Behavioral Analytics platform leverages a uniquely powerful analytic framework that pierces through the fog by looking across all insider activity, factoring in the intrinsic risk of each insider and supplementing activity streams with value-add information from across a company's security and compliance ecosystem.

The unique power of Forcepoint Behavioral Analytics

Synthesize across all human activity

- Forcepoint Platform takes all human activity—communications, financial, physical, systems/digital—and analyzes it to identify unwanted activity.
- Forcepoint leverages raw activity data as well as value-add signals from other security tools in the ecosystem, including DLP alerting.

Fully incorporate intrinsic human risk

- Each insider has their own level of intrinsic risk, given attributes such as their role, tenure, location, performance, and more. Leverage these data to raise or lower the risk assessment across each insider's activity.
- In addition to internal stores of knowledge on people, Forcepoint can leverage ongoing assessments and information from outside sources (e.g., public records).

Leverage "out-of-the-box" and refine and extend with ease

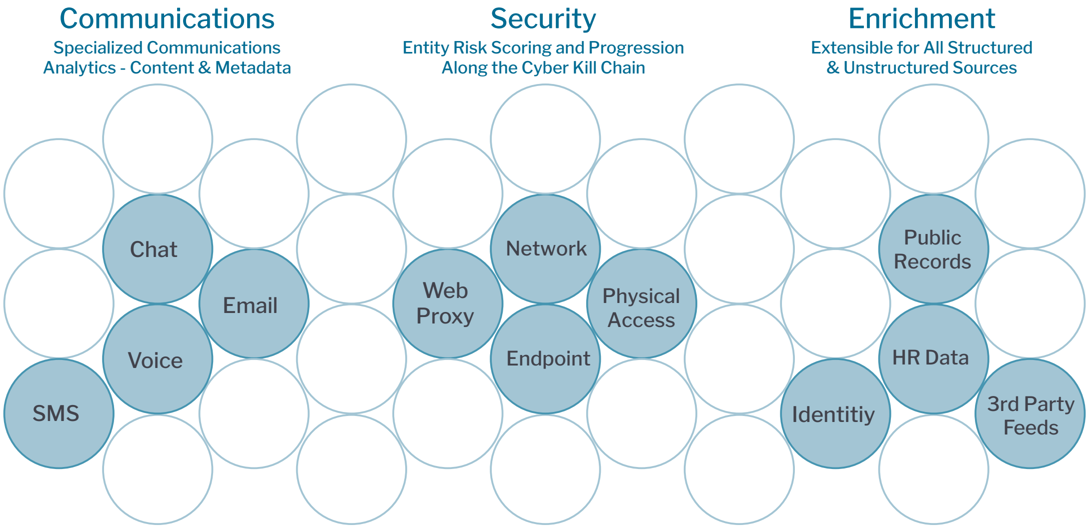
- Forcepoint Behavioral Analytics ships with its industry-leading analytic models for identification of threats such as data exfiltration, malicious users, compromised users, negative behavior, and more. Each model has been developed and successfully deployed against real world threats.
- Forcepoint customers are able to leverage these off-the-shelf models and can refine and extend them as use cases and threats evolve. These capabilities are available without the need for data scientists, engineers, or expensive professional services.

Analytics are understandable and explainable

- Today's insider threat teams need the ability to fully understand and explain the analytics that identify potentially malicious insiders. Forcepoint's analytics are fully explainable to support discussions with Legal and Compliance, ultimately enabling swift investigation and action.

Operational Overview

Forcepoint integrates readily with communications, security, and other enterprise applications currently in use. Forcepoint's built-in, proprietary analytics models analyze information from across the across the enterprise to generate a holistic view of behavioral risk:


Communications
Specialized Communications Analytics - Content & Metadata
Security
Entity Risk Scoring and Progression Along the Cyber Kill Chain
Enrichment
Extensible for All Structured & Unstructured Sources
Chat
Email
Voice
SMS
Web Proxy
Network
Physical Access
Endpoint
Public Records
HR Data
Identitiy
3rd Party Feeds

SELECTED DATA SOURCES

Email: Exchange, Office 365
Chat: Lync/Skype

DLP Alerts: Symantec, McAfee ePOC
Proxy: Bluecoat, Cisco Web Security, F5 BIG-IP
Physical Data Movement: Print Logs, Removable Device Logs
Endpoint: Forcepoint, Veriato, Digital Guardian

Authentication: Windows event logs, *nix authentication logs, Application server logs
Systems Administration: Windows event logs, Privileged account security logs

Public Records: Criminal history, Financial distress
HR Data: Performance reviews
Identity: Privileges and permissions
Security Incidents: SIEM, Vulnerability management

FORCEPOINT BEHAVIORAL ANALYTICS MODEL - SELECTED ELEMENTS

DE-1 Internal Data Movement
DE-2 External Data Movement
DE-3 Email Data Movement
DE-4 File Operations
DE-5 File Share Cardinality
DE-6 Data Reconnaissance

MU-1 Network Reconnaissance
MU-3 Malicious Authentication
MU-4 Destination Cardinality
MU-5 Explicit Account Cardinality
MU-9 Configuration Deviation
MU-11 Access Request

CU-3 Remote Login
CU-4 Source Country Cardinality
CU-7 Configuration Deviation
CU-8 Redirected Internet Traffic
CU-9 Port Cardinality
CU-10 Destination IP Cardinality

NB-1 Sexual Harassment
NB-2 Workplace Violence
NB-3 Obscene Content
NB-7A Financial Distress Comms
NB-7B Financial Distress Web
NB-9 Oversight Evasion

IB-1 Espionage
IB-2 Corporate Espionage
IB-4 Clearance Evasion

EXAMPLE SCENARIOS

DATA EXFILTRATION (DE)

Illicit attempts to discover, gather, obfuscate, exfiltrate sensitive and/or classified data, and remove all auditable traces of exfiltration event

MALICIOUS USER (MU)

Disgruntled privileged users who are attempting to inflict virtual or physical harm to an organization's infrastructure through malicious, intentional acts of sabotage

COMPROMISED USER (CU)

Individuals whose credentials have been taken over by malicious, third-party actors, and whose network identities are used surreptitiously to cause significant harm to an organization's security

NEGATIVE BEHAVIOR (NB)

Individuals in violation of corporate policy for an array of reasons, such as workplace violence, sexual harassment, corporate espionage, and at risk of leaving

ILLICIT BEHAVIOR (IB)

Individuals putting the corporation at risk through unlawful behaviors, such as insider trading, espionage, market manipulation, conflicts of interest, legal malpractice, and PII leakage