Insight

Powerful behavioral analytics to detect, understand
and rapidly respond to risky behavior.

Key Advantages

Tunable analytic features, models
and scenarios.

› User-centric risk models and
  indicators for scoring high-risk
  user activity.

› Configurable analytic models and
  scenarios that can be tuned without
  additional programming or scripting
  to address new and emerging insider
  threat use cases.

› Basic and advanced search features
  for flexibility in deeper investigations
  and improved workflow.

› Weighted risk models that are
  customizable for producing
  usable reports.

› Open architecture that gives data-
  agnostic insight into potential
  risky behavior.

Insight into user behavior

As the threat landscape continues to evolve, security leaders are turning to behavioral
analytics to gain better insight into accidental, malicious and high-risk behavior.

Forcepoint Behavioral Analytics (FBA) is a powerful platform that provides unrivaled
visibility into user behavior to manage risks from within. Identify anomalous behaviors and
mitigate adverse activities before they can cause harm.

Analyst-designed

Gain a better understanding of your organization's security posture with structured
analytics developed by analysts to enhance case readiness models for risk scoring,
anomaly detection, focused analysis and risk-adaptive controls.

FBA offers greater insight into insider risks using models such as: Data Exfiltration,
Compromised Access, Malicious Users, Negative Behavior, Illicit Behavior and Intent to
Harm (self/others).

The solution offers intuitive controls for adjusting out-of-the-box threat models, giving
analysts the ability to customize and adjust them according to your organization's
requirements. Detect anomalous behavior utilizing customizable dashboards displaying
risk scores, anomalies and reports.

The open architecture fuses structured and unstructured data to provide enriched insight
into nuanced patterns, human activity and trends that comprise human risk. The solution
incorporates Forcepoint's proven tenets of: Diverse Data Sources, Hybrid Analytics,
Configurability and Transparency

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	97	5
Chris Lenoir Operations | Denver	95	5
Tony Minard Operations | Los Angeles	90	5
Gerald Patterson Operations | New York	58	3
Ralph Heilman Investments | New York	57	3

Figure 1: Forcepoint Behavioral Analytics risk scoring

Behavioral Analytics

Who the employees are

What employees are doing

Data
Observation
Indicator
Behavior

BEHAVIOR MODELS

DATA EXFILTRATION

COMPROMISED USER ACCOUNT

MALICIOUS USER

NEGATIVE BEHAVIOR

INTENT TO HARM
(Self or Others)

ILLICIT BEHAVIOR

HR identity
Performance reviews
Promotions and compensation
Public Records
Job and hierarchy
Roles and entitlements

**UAM
Data Collection**

Web
Keyboard
Network
Public Cloud
File activity
Databases
Email

**Other
Enterprise
Data Examples:**

3rd party apps
Facility access
Performance and termination records
DLP, HIPS, HIDS,
Antivirus events
Call detail records
Public records
Open-source intelligence

Figure 2: Understand and rapidly respond to risky behavior with powerful insight of data, Indicators and behavior.

Proven tenets

Diverse Data Sources

Forcepoint Behavioral Analytics collects and analyzes raw data from a variety of enterprise sources, including communications, physical access, endpoint and network activity:

→ Behavioral indicators are available in facility access, HR, performance and termination records, call detail records, DLP data, HIPS, HIDS, antivirus events and common enterprise records such as Security Information and Event Management (SIEM) and more.

→ Organizations often have unique risk use cases. FBA's open architecture delivers the ability to easily configure risk models for these custom use cases and their data sets. Further, FBA delivers a framework that allows the simplified integration of emerging analytic techniques without the need for expensive development.

→ External threat sources such as consumer data, public records and other open-source intelligence. This allows security organizations to obtain the maximum benefit of these vital data sets by enriching risk models for greater insight into behavior.

BENEFIT Comprehensive Visibility
Covers structured and unstructured business data in addition to communications to leave no detection gaps.

Hybrid Analytics

Forcepoint Behavioral Analytics effectively leverages both rule-based and statistical methods by combining the two into a hybrid analytic approach.

Forcepoint's analytic hierarchy is made up of features, models and scenarios as shown in the following diagram.
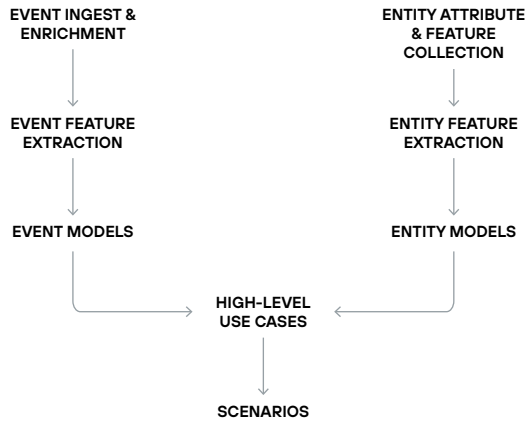

Figure 3: Forcepoint Analytic Hierarchy

→ **Features:** Forcepoint's solution automatically learns the distribution of feature values (e.g., the hour of day, destination domain, applications used, file type, file size or sentiment across event data sets). This enables it to recognize anomalies and calculate risk.

→ **Models:** Forcepoint's models are unique in that they provide access to the underlying analytics and engines. For example, a model may measure the number of bytes uploaded to a cloud storage site, the number of unique printers accessed or anomalous web search activity relative to organizational and user baselines. It is then able to compare that with prior normalized observations.

→ **Scenarios:** Additionally, the technology incorporates scenarios that correspond to high-level use cases such as data exfiltration where a variety of model scores could indicate an employee leaking proprietary information.

BENEFIT Deep Context

Focus on behaviors, not just anomalies, with precise narratives that indicate unwanted behavior.

As part of these features, models and scenarios, FBA dashboards include insights to quickly score and visualize risks and timelines at-a-glance (as seen in figure 4). Also available are the configurable data models for ease of Analytic Content Management (as shown in figure 5).
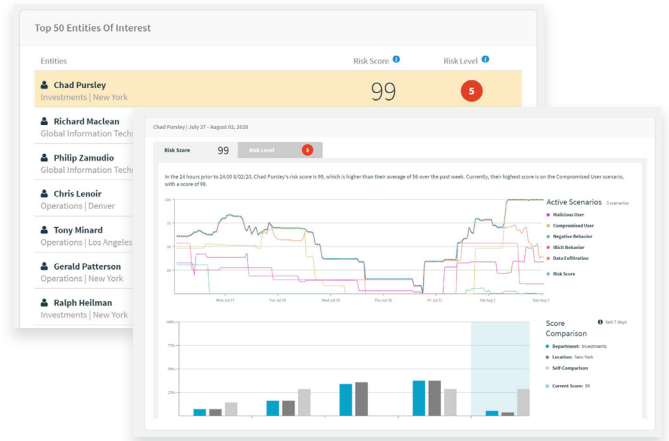

Figure 4: FBA summary dashboards showing of entities of interest, timeline and risk scores.

Configurability

Security risks vary across different organizations, depending on industry, region and standard business practices. Raw event model scores contributing to an entity scenario's risk score are shown on an entity timeline and the events that contribute the most to those model scores are shown clearly.

Forcepoint Insight empowers security analysts to leverage their expertise and easily configure use cases, analytics models and analytical scenarios.

BENEFIT Flexibility

Easily build or customize risk models to fit any unique organization and support any risk use case.
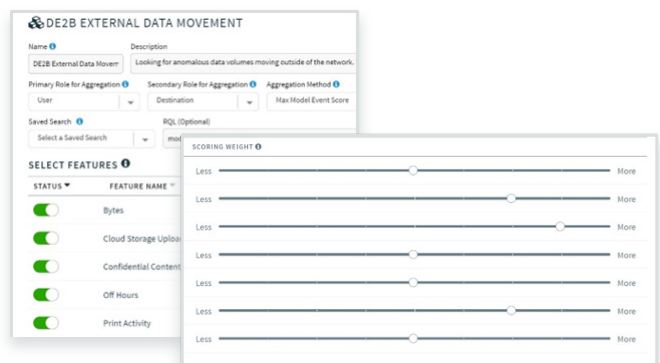

Figure 5: Analytic Content Management (ACM) for flexible data model tuning and configurability.

Transparency

The analytics in Forcepoint Behavioral Analytics are simple and easy to understand, producing accurate and insightful results. Unlike competitor products, FBA provides transparency by exposing enhanced detail so analysts can understand how the user community operates and then add their own expertise to the features and models.

For example, an analytics administrator can change the scoring weight of a cloud storage upload or weekend activity based upon the data feeds from various data sources, such as the organization's SIEM or DLP tool set.

When the analyst investigates a user of interest, they do so through the user-friendly entity timeline, which provides analytic explanations and context, allowing the analyst to make informed judgments and take appropriate actions as they assess possible security threats.

> **BENEFIT Efficiency**
> In-depth analytics within a single platform allows investigators to pivot from alert to investigation.

Summary

Understand at-a-glance behavior that could put your organization at risk. Enrich your insight into behavior with a full spectrum of available enterprise data sources and collections.
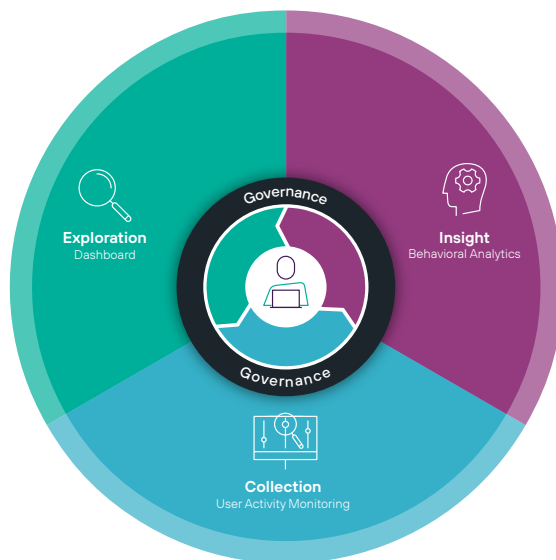
Forcepoint Behavioral Analytics protects sensitive client information and detects compromised accounts to gain insight and improve your organization's security posture.

→ **Comprehensive visibility** Forcepoint Behavioral Analytics uniquely covers structured and unstructured business data sets to close detection gaps.

→ **Deep context** Focus on behaviors, not just anomalies, with precise narratives that indicate unwanted behavior.

→ **Flexibility** Easily build or customize risk models to fit any unique organization and support any risk use case.

→ **Efficiency** Pivot from alert to investigation with in-depth analytics within a single platform.

Forcepoint Insider Risk Solutions
Collection • Exploration • Insight

→ **Collect** behavioral data from channels such as web, file operations, keyboards and email.

→ **Explore** meaningful data using a powerful dashboard built for analysts, by analysts.

→ **Gain insight** with powerful analytics to understand and rapidly respond to risky behaviors before harmful events occur.

→ **Governance** to ensure the integrity and effectiveness of the insider risk inquiry and response processes.

→ **Operations –** Employ a centralized analyst audit, maintain privacy and comply with best practices such as Role Based Access.

Exploration — Dashboard
Insight — Behavioral Analytics
Collection — User Activity Monitoring
Governance

Forcepoint