EVERFOX

DATASHEET

EverShield Behavioral Analytics

Intelligent Insight Into Risk Precursors

Features

- → No-Code Model Tuning to easily adapt threat detection to new behaviors
- → 100+ Configurable Analytic Models and indicators for scoring high-risk user activity
- → Predictive and Adaptive Risk Alerting flags precursors before critical events occur.

Benefits

- → Comprehensive visibility of business data
- → Deep Context of behaviors and anomalies
- → Flexibility to customize risk models
- → Efficiency of investigations with tunable analytic features, models and scenarios

EverShield Behavioral Analytics and Linguistic Analysis 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

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.

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.

EverShield 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 EverShield's proven tenets of: Diverse Data Sources, Hybrid Analytics, Configurability and Transparency

Gain Insight with smart visualizations

Behavioral Analytics Dashboards

Insight to understand and rapidly respond to risky behavior

EverShield provides insight into structured and unstructured data for a holistic view into nuanced activities, patterns, and risky behaviors.

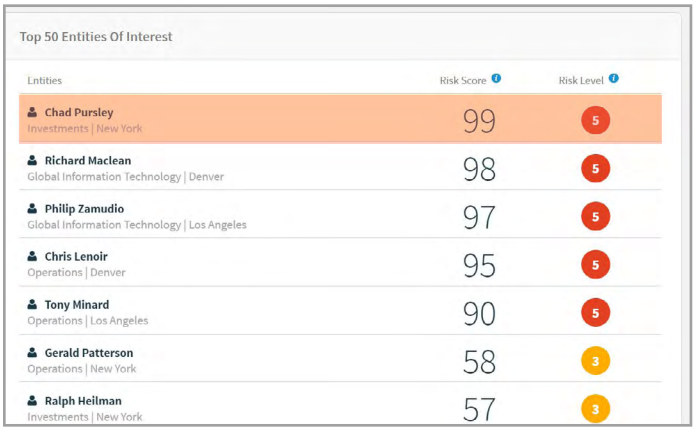

Figure 1: Behavioral Analysis Risk Scoring.

Proven tenets with diverse data sources

EverShield 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. EverShield open architecture delivers the ability to easily configure risk models for thesecustom use cases and their data sets. Further, EverShield 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.

Supporting diverse data sources and hybrid analytics for enhanced configurability and transparency within a wide variety of behavioral use cases.

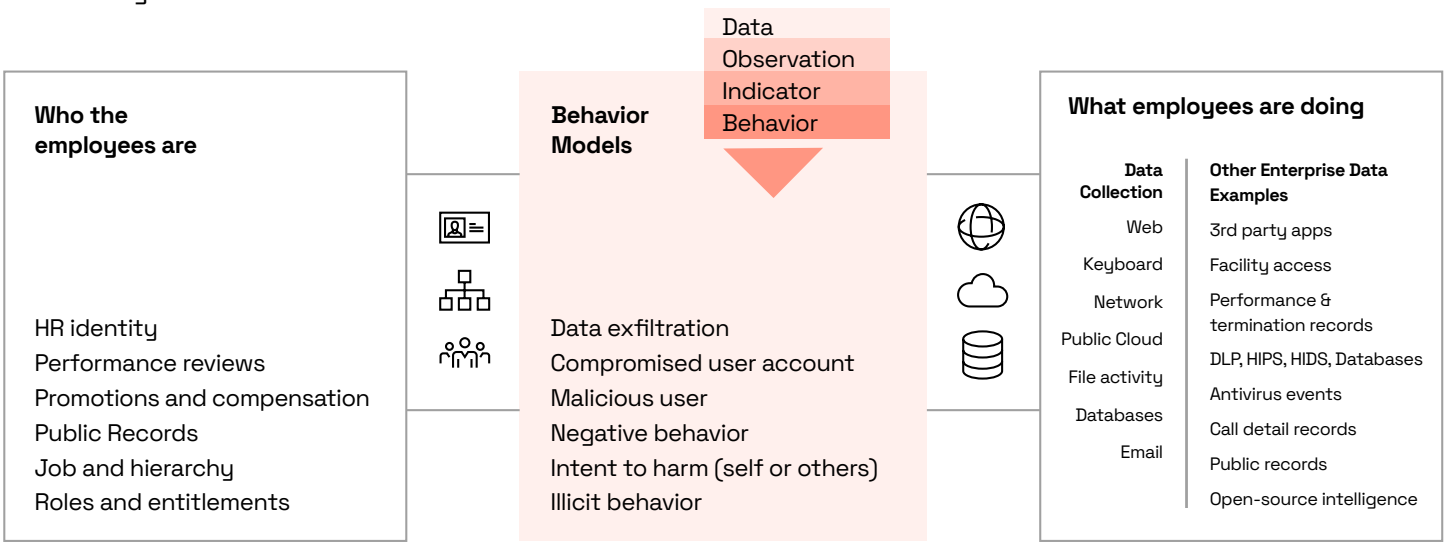

Figure 2: Analytics Driven Visibility, Baselining, Risk-Adaptive Controls, Modeling & Risk Scoring, Anomaly Detection

BENEFIT **Comprehensive Visibility**

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

Hybrid Analytics

EverShield Behavioral Analytics effectively leverages both rulebased and statistical methods by combining the two into a hybrid analytic approach.

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

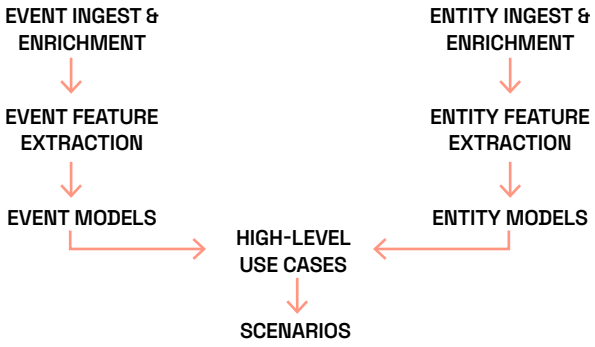

Figure 3: Everfox Analytic Hierarchy

- → **Features:** EverShield behavioral analytics automatically learns thedistribution 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:** EverShield'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 accessedor anomalous web search activity relative to organizationaland user baselines. It is then able to compare that with priornormalized observations.
- → **Scenarios:** Additionally, the technology incorporatesscenarios that correspond to high-level use cases suchas data exfiltration where a variety of model scores couldindicate an employee leaking proprietary information.

As part of these features, models and scenarios, EverInsight 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).

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

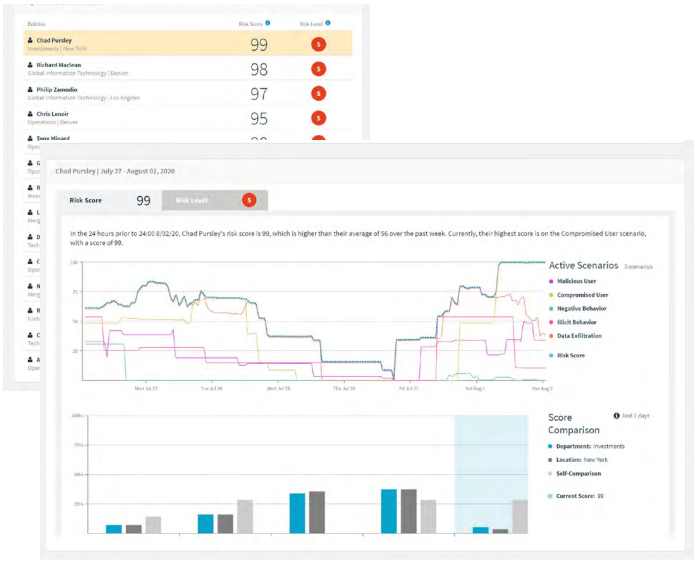

Figure 4: EverShield summary dashboards showing entities of interest, timeline and risk scores.

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.

EverShield 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.

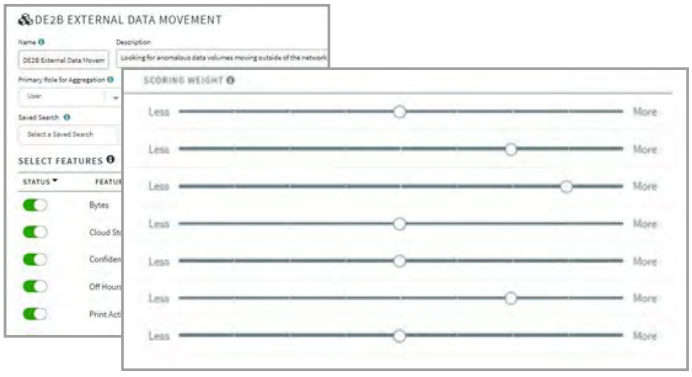

Figure 5: Analytic Content Management (ACM) for flexible data model tuning and configurability.

Transparency

The analytics in EverInsight behavioral analytics are simple and easy to understand, producing accurate and insightful results.

Unlike competitor products, EverInsight 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 organizationat risk. Enrich your insight into behavior with a full spectrum of available enterprise data sources and collections.

EverShield behavioral analytics protects sensitive client information and detects compromised accounts to gain insight and improve your organization's security posture.

→ **Comprehensive visibility** EverInsight behavioral analytics uniquely covers structured and unstructured business datasets 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 anyunique organization and support any risk use case.

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

EverShield Insider Risk Management Platform

User Activity Monitoring • Behavioral Analytics • Case Management

→ **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.

→ **Centralized case management and operations** designed for classified or sensitive environments. It supports collaborative investigations with built-in privacy enforcement, chain-of-custody tracking, and role-based access.

About Everfox

Everfox, formerly Forcepoint Federal, has been a trailblazer in defense-grade cybersecurity for more than two decades. Leading the way in delivering innovative, high-assurance solutions. But we're just getting started.