Forcepoint

Datasheet

Insider Risk Solutions

Unrivaled User Activity Monitoring

Advantages

- Enable deep visibility and identify your riskiest users
- Protect your workforce, organization, and customers
- Simplify exploration and analysis
- Optimize your workflows and customize your program
- Safeguard your investigations

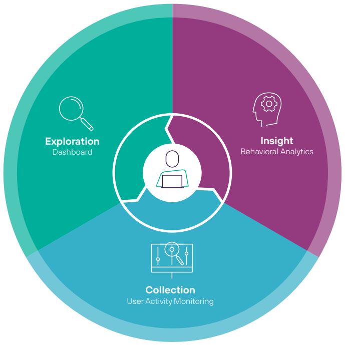
Key Capabilities

- Robust endpoint sensor for policy-driven data collection
- Collect behavioral data from multiple endpoint channels for full context of user activity
- In-depth analytics to ensure rapid response to risky behaviors
- Enterprise ready for centralized management and monitoring
- Transparent to the end-user, preserving the user experience
- Trusted data source for behavioral analytics and security event management solutions
- Secure UAM solution with end-to-end encryption of data through FIPS 140-2 compliant communications and hardware based data-at-rest encryption of on-prem stored data

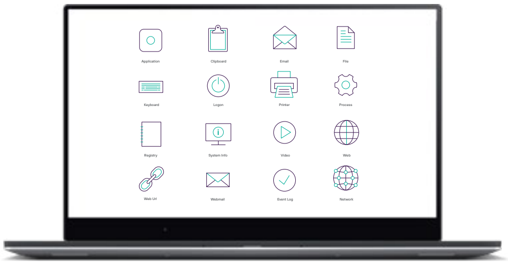
Forcepoint Insider Risk Solutions is a User Activity Monitoring (UAM) and Analytics platform that provides analysts and investigators with deep visibility into all user endpoint activity for effective detection programs and resolving anomalous behavior.

Collection, Exploration, and Insight

Forcepoint has the tools to help you collect, explore, and gain insight into how users are interacting with your most sensitive data and the information systems processing and protecting it.



Collections Channels



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

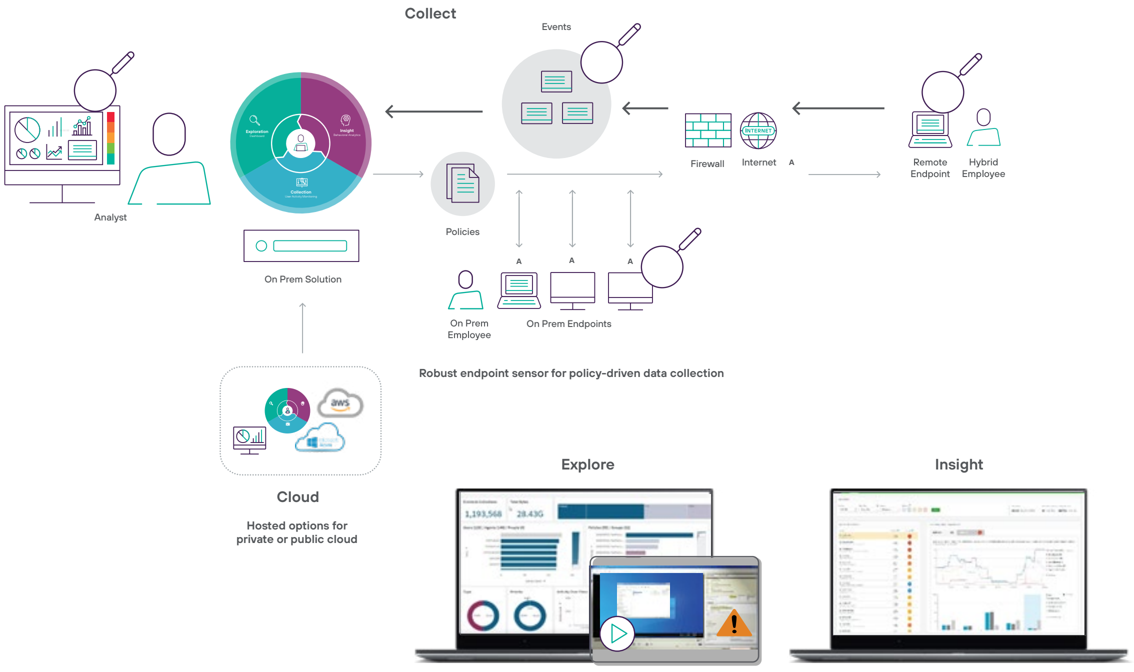
→ **Explore** meaningful data using a powerful dashboard built for analysts, by analysts.

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

→ **Optimize Operations** with centralized analyst audit, maintain privacy, comply with best practices such as role-based access.

Forcepoint Insider Risk | Architecture

Unrivaled User Activity Monitoring and Behavioral Analytics



Robust endpoint sensor for policy-driven data collection

Hosted options for private or public cloud

Visualize, explore and investigate

Powerful analytics to understand and rapidly respond to risky behaviors

Investigative Tools

→ Investigator / Case management workbench

→ Comprehensive video replay – flexible resolution and frame rates

→ Proven authentic, relevant, and original records for use in legal proceedings

→ Native integrations to Forcepoint Behavioral Analytics, SIEMs, Remedy, Jira or ServiceNow, and others.

Endpoint Capabilities

→ Mature and robust endpoint (self-throttling)

→ Wide spectrum of collection capabilities

→ Enterprise-grade endpoint management

→ Privileged user resilient with anti-tampering features

→ Flexible UAM data inspection for insightful discovery and privacy compliance

→ Persistent monitoring while off-network

Enterprise Ready and Scalable

→ Governance controls / Segregation of duties

→ Enterprise scalable to over 200K endpoints

→ Built-in redundancy

→ Intelligent management of data

→ Highly customizable fine grain policies

Privacy and Governance Features

→ Granular policy controls examine and collect only the information and channels authorized

→ Do Not Collect' policies simplify protecting employee privacy

→ AES encryption safeguards UAM data at rest and in transit to preserve confidentiality

→ Two-person authorization for analysts enforces supervised access & administration

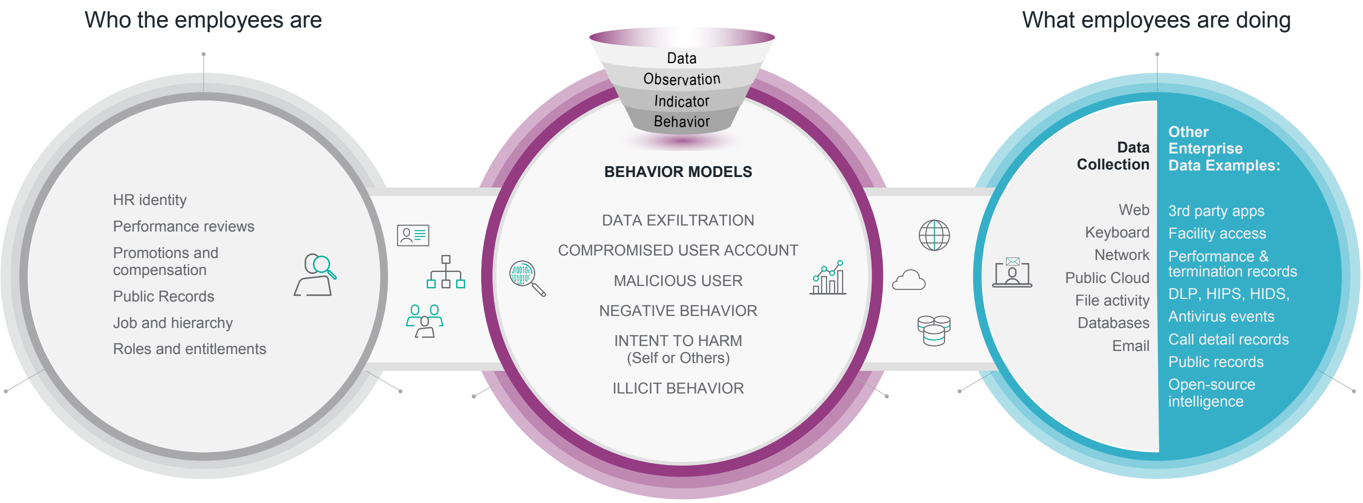
→ Role-based access allows separation of duties control over operator privileges

→ Immutable audit trail records access and memorializes policy and configuration changes

→ Centralized case management for comprehensive governance and oversight

Gain Insight | Source Diagram

Behavioral Analytics



Insight to understand and rapidly respond to risky behavior

Forcepoint's Behavioral Analytics provides insight into structured and unstructured data for a holistic view into nuanced activities, patterns, and risky behaviors. Supporting diverse data sources and hybrid analytics for enhanced configurability and transparency within a wide variety of behavioral use cases.

Professional Services Experts

SPECIALISTS	EXPERTISE
Subject Matter Experts	Experienced and certified Insider Threat Program Managers and Evaluators to support program development and assist in the use of technical and organizational controls to manage insider risk.
Product Field Engineers	Deep product knowledge for installation, integration, and operation of servers, agents, and consoles including developing and optimizing Forcepoint Insider Threat policies.
Database Administrators	Oracle experts ensure the central database remains optimized over time.
Data Scientists and Engineers	Data ingestion, risk model development, and optimization of analytics.
Developers	Reach back support to assist in issue resolution and to gather requirements and feedback for new features and enhancements.
Customer Support	Provide issue management and response, deliver on Enterprise and Enhanced Support commitments
Training	Deliver expert product knowledge transfer for operators and technical support staff
Technical Account Managers & Project Leads	Advise on product best practices, installations, and upgrades; advocate for customer requirements; coordinate Forcepoint resources for issue resolution and task accomplishment

Forcepoint

forcepoint.com/contact

18Sept2023