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.

→ 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.
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

forcepoint.com
Gain Insight | Source Diagram

Behavioral Analytics

Who the employees are

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

DATA Observation

Indicator

BEHAVIOR MODELS

- DATA EXFILTRATION
- COMPROMISED USER ACCOUNT
- MALICIOUS USER
- NEGATIVE BEHAVIOR
- INTENT TO HARM (Self or Others)
- ILLICIT BEHAVIOR

What employees are doing

FIT Data Collection

Web

Keyboard

Facility access

Network

Performance & termination records

Public Cloud

DLP, HIPS, HIDS

File activity

Antivirus events

Databases

Call detail records

Email

Open-source intelligence

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

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

forcepoint.com/contact

© 2023 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners. [FP-Insider Risk Solutions Datasheet] JJan2023