Forcepoint

Use Case

Advanced R&D Lab uses Forcepoint User Activity Monitoring and Behavioral Analytics to reshape security posture

Forcepoint Insider Risk Solutions provide the Insight needed to investigate and respond to insider and contractor behaviors that could lead to exfiltration or compromise of sensitive data

Challenge

- Accurate analysis of large amounts of user & worker data
- Visibility into user behaviors to determine risk to the organization
- Risk scoring and priority alerts for stakeholders needing to make quick and informed decisions

Solution

- **Collect** using comprehensive UAM endpoint sensor with policy-driven data collection and administration
- **Explore** UAM data with visualizations and flexible dashboards, reporting and link analysis
- **Insight** from behavioral analytic models to identify user risk. Integrate all available employee data, not just UAM.

Outcomes

- Retain both people and data through policy-driven data collection with less unusable analysis and more context
- Advanced analytics & investigations – at scale for harder-to-find risks
- Visibility into the how, where and when's of a potential breach

Reshaping security

It's not often that a product's feature set helps reshape an organization's entire security posture. The exception is when a product offers superior insight and visibility into how people are interacting with the organization's most sensitive data. Actionable intelligence that security analysts can use to better protect information, systems, and people. Shifting the approach from using basic data movement detection tools to engaging in a more effective behavioral analysis model useful to the entire interdisciplinary security teams.

Risk of workers interacting with sensitive data

Within the myriad of users that interact daily with critical information the risk associated with that access is enormous. To better protect information the lab needed real-time visibility into their collections of security related data. To know what might be hidden in the data that needed immediate attention or action.

The customer's lab had plenty of unsorted analysis data to review, but it required tedious and manual analysis to try and interpret. Was their data telling them that workers were in full compliance of policies or were there indicators within the data somewhere that was being missed? It was crucial to know the answer to the ensure they had the right access controls and security in place. Ensuring that only workers with the right security clearances had access and were using that access correctly. Instead of periodically sorting through collections to try and see what workers were up to they needed a more effective blend of technical indicators to help them identify a potential data breach.

In an environment where incoming analysis data was sporadic and non-standardized, the first challenge was to improve how data was analyzed and scored against potential risks. A shift to more rapid and streamlined methods of analyzing various types of collections. Thus establishing more meaningful, automated and accurate indicators and detections. This required a more efficient, accurate and frequent data analysis approach with better insight into user behaviors related to unauthorized and even authorized data migration and access.

Next, the lab needed to give analysts more decision-making power so they could determine and rank the types of user activities they considered risky. With such a system, analysts would be able to measure against established policy and determine whether incidents resulted from intentional violations or accidental user error.

The solution would need to provide these key capabilities:

- → **Flight Risk Detection:** Ability to identify users likely to leave the organization
- → **Espionage Exfil Mapping:** A focus on Exfil of data based on criteria of clearance level, foreign travel risk, and region of origin
- → **Job Search & Exfil Mapping:** Focus on Exfil of data based detection of individual job searching within a 90-day window
- → **Data Exfiltration Mapping:** Focus on Exfil of data based on entire population with a focal point of a pattern of backup actions.

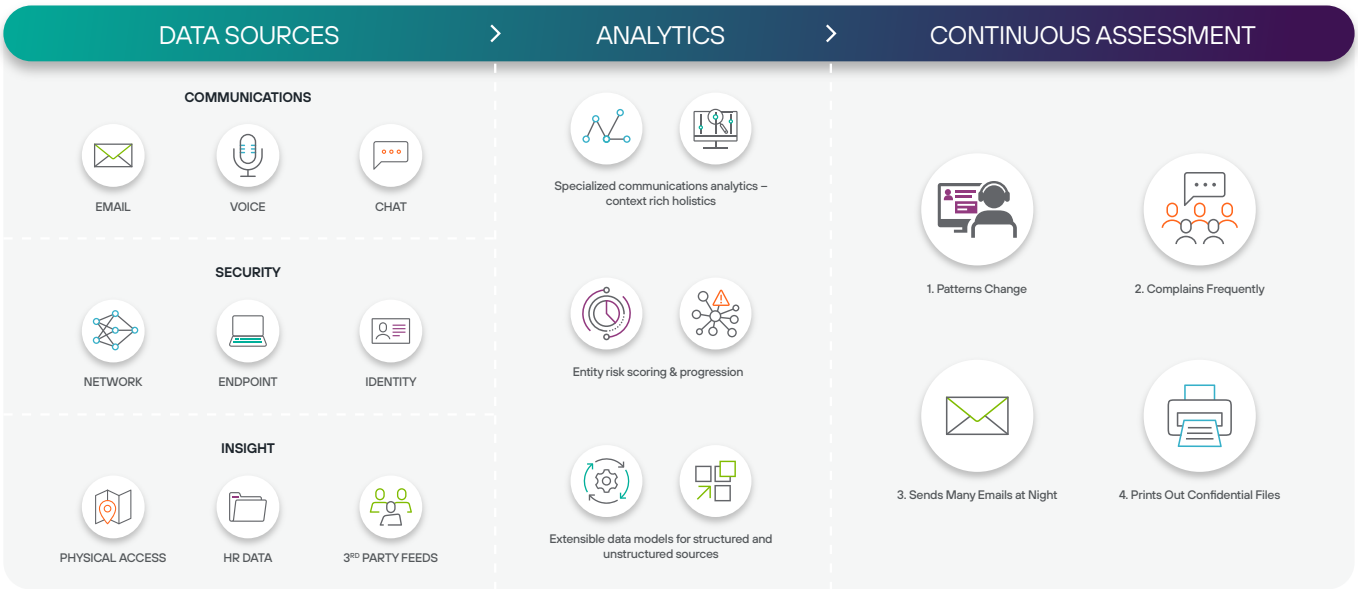
To achieve this, Forcepoint behavioral analysis and technology experts provided the following solutions.

First, they introduced and utilized Forcepoint's Container Platform, a modernized management platform for integrating various types of data from multiple data sources. Accommodates changes in both data types and structures. The platform provides a foundation of data integration that can operate and scale in both on-prem and in cloud environments, allowing ingestion of billions of data objects within collections. Whether customer specific data sources or other data types.

In the process the data is redacted and cleaned so that it can be more accurately and easily analyzed. This includes data coming in from Forcepoint User Activity Monitoring solutions

As patterns emerge the tool communicates what is contained in the security data collections data and gives analysts contextual insight into those patterns. Analysts get a clear view of events, activities, behaviors, risks, threats, and potential violations of policy.

Analysts are then able to click to export what they see as a report in PDF, PowerPoint, and other shareable and visual reporting formats used to communicate situational analysis and mitigation needed. This gives stakeholders accurate and attributable information needed to take the most appropriate and immediate action. This has proven to be an extremely useful and beneficial capability of the Forcepoint solution.



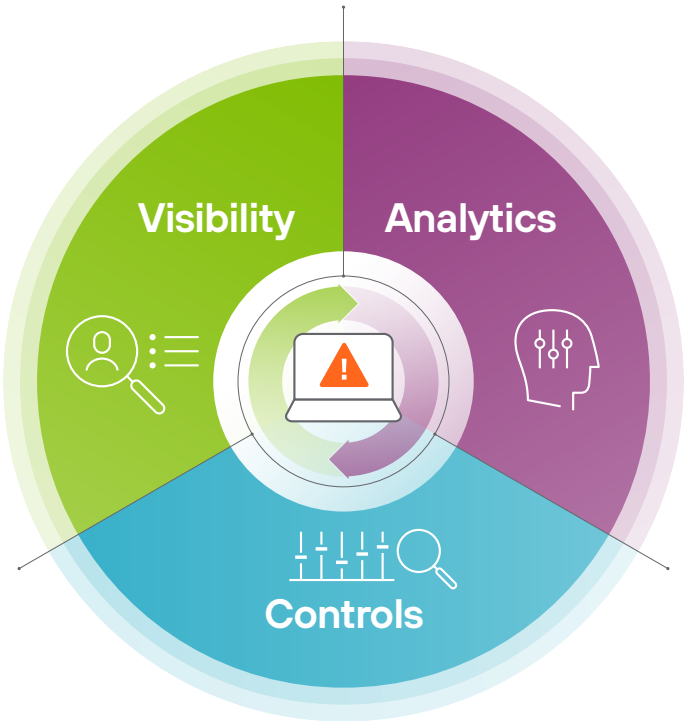
Previously, analysts were required to manually review data from multiple sources to find anything of risk or concern. Interpretation of data was often subjective rather than definitive as to whether or not violations of policy or risky behaviors were actually occurring.

The lab is now able to ingest multiple data sources and focus on the highest risk data and people to investigate, eliminating the need to manually review endless logs of non useful data.

Key capabilities:

- → Export, communication, and collaborations tools
- → Behavioral Analytics that can link psychological and emotional factors within user activities
- → "Smart Lexicon" that takes context and word meaning into account
- → Ability to remove or 'mute' an entity from the dashboard
- → For example, users who have been authorized to perform an activity that might be alerting when performed by non authorized users.
- → Case management, policy management and risk management
- → Espionage Exfil Mapping: a focus on Exfil of data based on criteria of clearance level, foreign travel risk, and region of origin
- → Job Search & Exfil Mapping: focus on Exfil of data based detection of individual job searching within a 90 day window
- → Data Exfiltration Mapping: focus on Exfil of data based on entire population with a focal point of a pattern of backup actions.

Move beyond standalone User Entity Behavior Analytics (UEBA)



- → Gain a 360 degree view of intent and user actions across the enterprise.
- → Eliminate complexity for security analysts with Forcepoint Insider Threat (FIT) and Forcepoint Behavioral Analytics (FBA) automated policy enforcement and comprehensive user risk scoring.
- → Leverage out-of-the-box analytics or customize risk models to fit your unique organizational needs.

Risk of Sensitive Data Being Exfiltrated

Risk Factors used for Risk scoring:
Job Profile, Department, Foreign Travel, Security Clearance, Birth Country, Security Incidents, Adverse info. (These were the customer's criteria. Other customers may have different criteria and policies they might use to quantify risks.)

Up to 20% of a company's annual revenue is lost due to data breaches caused by insiders.

Points of exfiltration

Digital Routes

- → Web & Cloud
- → Email
- → Applications
- → Screenshots
- → Clipboard

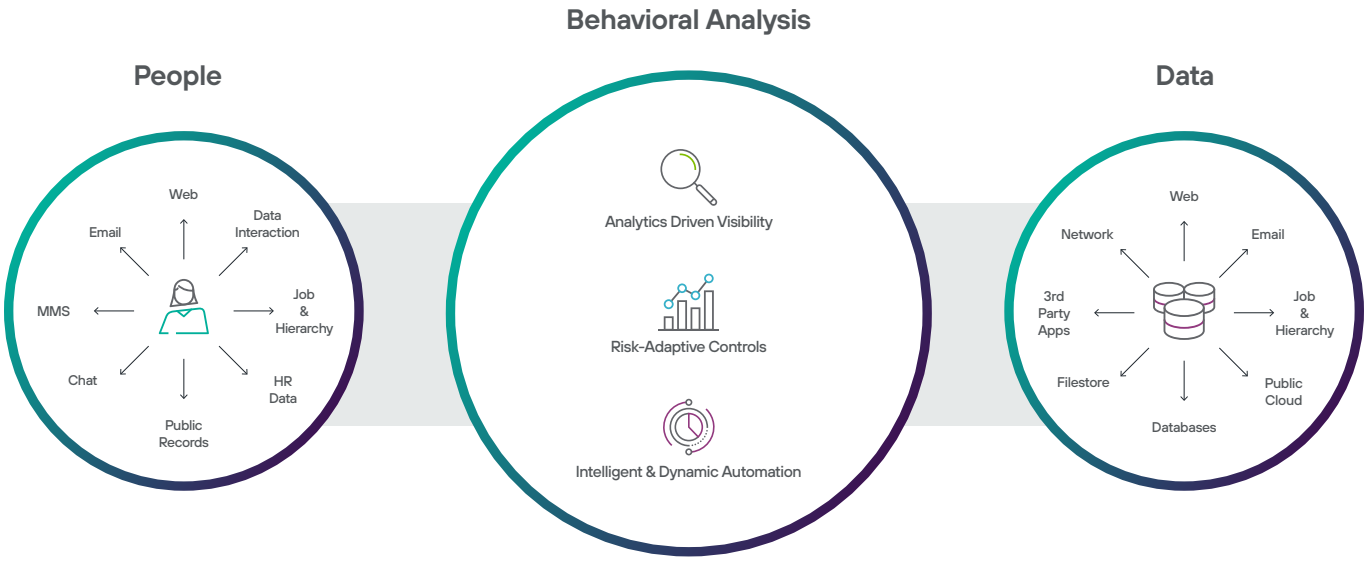
Physical Routes

- → Printing
- → Removable Media (USB, CD, DVD)

Data Types

- → Patents, Copyrights, Trademarks (e.g., inventions and discoveries, designs, written or recorded works, source code)
- → Confidential or Classified information, Trade secrets (e.g., processes, formulas, methods, sales and marketing plans, production schedules, merger and acquisition activities, customer lists)
- → Financial Data (e.g., forecasts, bookings, confidential pricing, contracts, securities, procurement data)
- → PII

Understanding user behaviors and data



forcepoint.com/contact

© 2022 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-FBA-FIT-Customer Use Case-LAB security version-US-EN] 10Jun2022