

whitepaper

Sentiment-based Analytics to Understand Employee Morale

One of the benefits of Forcepoint Behavioral Analytics is its ability to ingest and process unstructured data (e.g., email message text, chat logs, etc.), which helps to provide richer context around behavior and risk. Specifically, this enables greater visibility into user sentiment.

Definition of “sentiment”:

- ▶ A view of or attitude toward a situation or event
- ▶ An attitude, thought, or judgment prompted by feeling
- ▶ The emotional significance of a passage or expression as distinguished from its verbal context

Essentially, analysis of user sentiment is using inputs to infer how that user thinks and feels—a critical but difficult-to-measure factor in human behavior. Applied to the enterprise, measuring sentiment can provide valuable insight into employee morale, contributing to a more detailed assessment of digital and physical risk.

Sentiment-based analytics enables examination of communications and leverages lexicon libraries to infer a user’s underlying attitudes and/or intent. Lexicon libraries are collections of keywords that may be used in existing or customized data models to measure the risk associated with the user and events.

Ultimately, that measurement is factored into the user’s overarching risk level, greatly enhancing the ability to identify “persons of interest” that could potentially warrant further investigation or response.

Here’s an example of what that can look like in the enterprise environment. One employee begins making negative remarks to a colleague, sending communications like, “You’re a moron,” and “I’m disappointed you were the project lead.” Those statements include keywords in one of the lexicon libraries.

The appearance of these keywords triggers the risk models to score that employee’s sentiment toward their colleague or the workplace. The employee’s behavioral change, in this case, indicates an increased risk to the organization. That risk is quantified and used to adjust their risk score in Forcepoint’s platform.

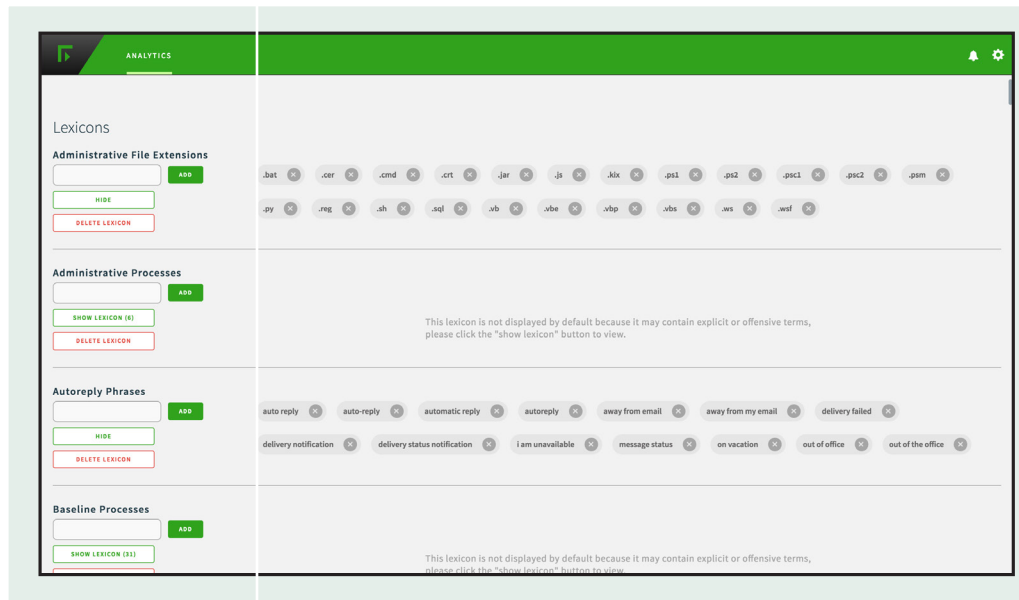
Visibility into exchanges like this one enables the organization to proactively address the problem with appropriate measures aligned with approved corrective actions. And this is just one example; the lexicon library also includes categories for flight risk, radicalization, violence, collusion, and suicide. The ability to calculate risk at this granular of a level doesn’t just protect the organization—it has the potential to save lives.

One of the biggest advantages Forcepoint provides with regard to sentiment-based analytics is its flexibility for customization. Organizations are given the ability to edit both the use of the lexicons and the associated risk impact of the words. This includes adding or removing words within categories, creating new categories, and adjusting category scoring.

To mitigate governance concerns, privacy protection comes built in. Organizations may implement controls to keep certain categories confidential through data masking or entitlement restriction. This ensures access to personally identifiable information only is available only when and to whom it is needed.

Forcepoint technologies provide deep visibility into and context around user behavior. Sentiment-based analysis is a powerful piece of the puzzle, vastly enhancing your ability to recognize behavior indicating potential violations of ethics, human resources, or security standards or policies.

For more information, visit the webpage on our [Behavioral Analytics](#) product or [contact us](#) to get in touch.



Forcepoint Behavioral Analytics Lexicon Library

About Forcepoint

Forcepoint is transforming cybersecurity by focusing on what matters most: people's behavior as they interact with critical data and systems. This human-centric approach to cybersecurity frees employees to innovate by understanding the normal rhythm of user behavior and the flow of data in and out of an organization. Forcepoint behavior-based solutions adapt to risk in real time and are delivered via a converged security platform to protect network users and cloud access, prevent confidential data from leaving the corporate network, and eliminate breaches caused by insiders. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.

forcepoint.com/contact

© 2019 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.

[SENTIMENT-BASED-ANALYTICS-GLOBAL-WHITEPAPER-US-EN] 200077.031319