Forcepoint

Datasheet

Forcepoint Behavioral Analytics

Information security: Protect IP, detect compromised accounts, and reduce insider risk

Forcepoint Behavioral Analytics enables security teams to proactively monitor for high-risk behavior inside the enterprise. Our security analytics platform provides unparalleled context by fusing structured and unstructured data to identify and disrupt malicious, compromised, and negligent users. We uncover critical problems such as compromised accounts, corporate espionage, intellectual property theft, and fraud.

Why Forcepoint Behavioral Analytics for security?

Our clients rely on us to deliver context about human behavior inside the enterprise. Only Forcepoint Behavioral Analytics offers configurable analytics to help security analysts tackle the problems that matter most to the business. We are built to scale while helping security teams:

- → Reduce the time to detect insider attacks
- → Surface relevant alerts at a time when security teams are drowning in noise
- → Get granular about insider activity, going beyond SIEM and other tools in your stack
- → Improve investigation efficiency for incident response and post-breach forensics

Platform pillars

Forcepoint Behavioral Analytics provides insight into high-risk behaviors and individuals, not just anomalous alerts. By evaluating nuanced interactions between people, data, devices, and applications, Forcepoint prioritizes timelines for security teams. Our software is built upon four pillars:

- → **Rich context ›** Fuses disparate data sources into a single narrative, combining communications content to decipher intent alongside SIEM, endpoint, and employee enrichment feeds.
- → **Hybrid analytics ›** Applies multiple types of rigorous behavioral and content-based analytics focused on change, pattern, and anomaly detection to better detect sophisticated attacks.
- → **Search and discovery ›** Exposes powerful forensic search-and-discovery tools through a context-rich user interface for ongoing monitoring and deep-dive investigations.
- → **Intuitive workflow ›** Delivers proactive reporting that fully integrates with human workflow and existing client information architectures to streamline operational efficiency.

Redefining security analytics

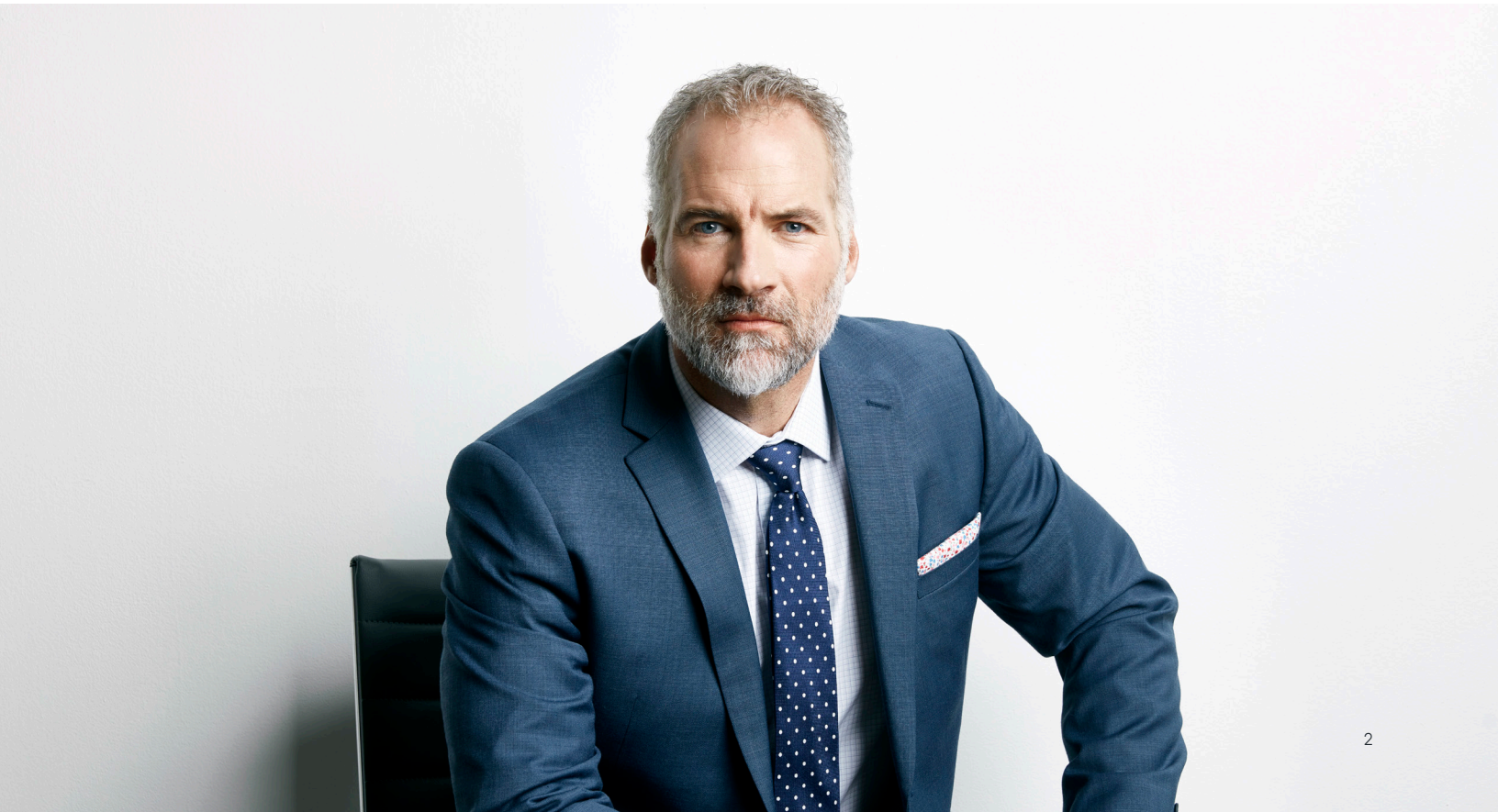
- **Context-driven visibility ›** Forcepoint Behavioral Analytics uniquely delivers visibility into employee activities, behaviors, and relationships by integrating unstructured, context-rich data streams with structured data. Our analytic models allow entities and events to be scored and prioritized through multiple lenses across all data streams—previously unavailable to security teams. We also integrate with Active Directory, SIEM, EDRs, and key data sources to offer true situational awareness, and a powerful forensic platform that radically enhances internal investigations.
- **Configurable analytics ›** Traditional, black-box UBA tools are often limited to structured data sources, analyzed in disparate systems, with a fixed configuration of analytics. Forcepoint, in contrast, delivers powerful analytic capabilities that allow Forcepoint Behavioral Analytics security teams to address evolving security use cases and perform real-time ad hoc analysis, including advanced search across all data sets. Our analytics can be tuned without additional programming, allowing a more nimble response to security threats.
- **Scale ›** We are fundamentally built to scale. Only Forcepoint uses ElasticSearch to power instant access to massive amounts of data. Our platform seamlessly stores both structured and unstructured data and scales horizontally to grow with our clients. Forcepoint also provides variable levels of access and administrative controls so you can rely on our technology to work for your business in any type of deployment.

Enterprise capabilities

- **Roles-based dashboards and workflows ›** Enable rapid review of non-compliant activity through an intuitive user interface so analysts and managers can quickly investigate, review, escalate, and take action.
- **Robust data entitlements ›** Fully support complex data entitlements required by both internal controls and externally driven data privacy concerns.
- **Extensible platform ›** Configurable analytics, dashboards, usergroups, and workflow support out-of-the-box security use cases with full capability to expand to any risk use case. Flexible privacy controls provide confidentiality between workgroups. Delivers advanced data science models without a heavy professional services commitment.
- **Flexible deployment options ›** Readily deploy on-premises, in a virtual private cloud, or even using a Forcepoint appliance.

Key benefits:

- **Precursor activities**
- **Content-aware DLP**
- **Compromised account detection**
- **Data reconnaissance**
- **Privileged user abuse**
- **Security analytics**



Advanced functionality

- → **Behavioral insights ›** Identify changes in behavior that may indicate current or potential illegal, unwanted, or non-compliant activity by employees using sentiment and content analysis.
- → **Intelligent prioritization ›** Prioritize events of interest and alerts based on the analysis of content and metadata patterns.
- → **Natural Language Processing (NLP) ›** Significantly reduce false positives through a smart, practical application of NLP, complex lexicons for any language, and text identification technology that recognizes disclaimers and quoted text from threaded emails.
- → **Tailored visualizations ›** Visualizations are specifically developed to unlock an analyst's own inference capabilities and deliver maximum context around relevant activities. Quickly understand the who, what, when, and how of employee actions.
- → **Content classification ›** Supercharge DLP deployments using Forcepoint's content classification engine to identify and filter out non-relevant communications like bulk mail, third-party mailers, and more.