Fluency

Overview Paper

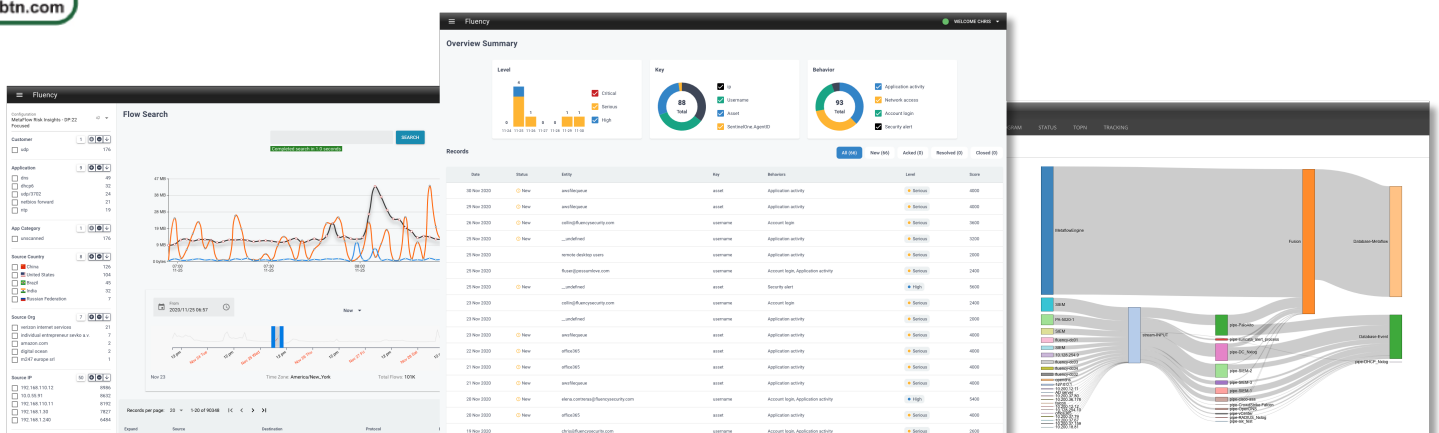
Fluency® SIEM

Designed for a Distributed World

Fluency SIEM has the ability to address highly distributed environments caused by mobile devices, cloud services, remote offices, software defined networks (SD-WAN), home users, and road warriors. Fluency SIEM enhances the telemetry of endpoint detection and response (EDR) to a level equal to XDR. It addresses the distributed network and its operational issues by scaling to the workload, enhancing cryptic messaging, clarifying issues, and reducing alert noise. Fluency's ease-of-use and automation is based on three simple phases:

- Fully leverage endpoint telemetry data (EDR)
- Establishing Infrastructure (IaaS) and Software as a Service (SaaS) awareness
- Transfer Expertise with Implementing behavioral analytics and rules
- Clear Alerting through Feedback and Priority Scoring

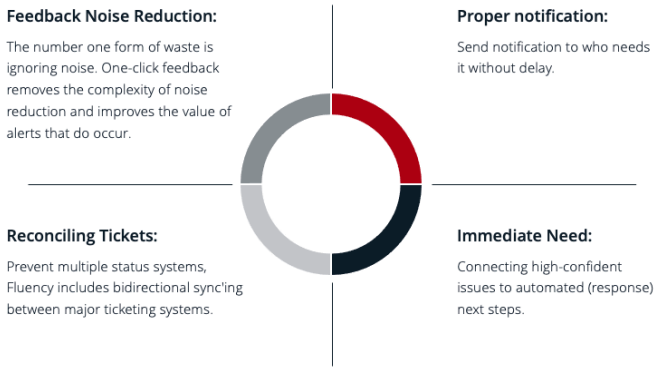
Fluency's big data foundation is "Collect All, Search All", referred to in Artificial Intelligence as Ground Truth. As companies' infrastructures grow both in complexity (diversity) and geo-graphical dispersion, the ability to collect audit activity becomes even more critical. In the past, Fluency SIEM users can see the network and provide support. It provides this network vision by extending visibility beyond the local network. Fluency also changes the dialogue from IP addresses to that of users, services and assets. This is more in tuned with how people think and results are achieved.



Fluency's **Behavior Watch Intelligence** provides the first phase of clarity by using live Lucene searches to select elements of interest. Streams of data are converted into understandable metrics displayed on customizable reports and dashboards. Each watch node generates histogram data for display and analysis. It leverages Fluency a list manager to change cryptic codes into plain language. Lists can also be updated by threat intelligence and used as an alternative to search live data.

Programable behavioral rules are unique to Fluency. These are agnostic rules that allow definable user entity behavioral analysis (UEBA) over any data source. This is the second phase of analytics, that changes basic metrics into correlated behavior. A behavioral node can change users' logins with IP addresses into geographical behavior informing operators when a specific user signs in from a new location. It can detect abnormal downloading, use of new commands, lateral movement, or determine when inactive users become active again. The agnostic rule capability supports both legacy technologies, such as IBMi, and new technology like Office365 or SentinelOne.

The Fluency case workflow engine protects analysts from overwhelming alerts by keeping them focused on what is being addressed and what is new. Incoming alerts are first compared to existing alerts to ensure that the user is not being confounded with variations of the same alert. Alert signals interact with the case workflow manager which ensures that incoming alerts are not a variant of a known case. Cases are also grouped, allowing a significantly higher view. Case workflow keeps analysts informed and focused on proactive results.



Fluency is the most advanced next generation SIEM. Each feature of Fluency, from its database to its disk filing system is new code, based on cloud optimization and efficiency. Innovation requires effort, not integration.

About Fluency

Fluency's goal is to augment and improve our clients' business security posture without incurring information overload. Our success is attributable to our unrelenting focus on client needs, satisfaction and security. Fluency continues to innovate, enhance client workflows, and address the demand for more timely and efficient security operations. Fluency is the only log manager that is focused on ground truth and fusing related data – harnessing streaming live data to perform real-time threat analysis and analytics to reduce overall dwell time and reduce business risk.