



NEW RELEASE: **XPLG Released LogX**

LogX Deep ML|AI Insights on Log Data Streams. Monitor 1.5+ million ML|AI based patterns on log data.

XPLG LogX automatically identifies and alerts on complex insights found in log data. LogX was fine-tuned for logs, observability, security, apps, and IT data based on comprehensive research and algorithmic breakthrough. LogX create a unique profile for each log event, this profile is then aggregated into a new data model with systems behavior profiles, complex risk patterns, and more. LogX detects anomalies and clustering Insight within those new data models. LogX meets today's Apps, DevOps, IT, CI/CD, and Cloud architecture which are subject to frequent changes with this new ML|AI paradigm.

Deep Insights Monitoring for Apps, DevOps, DevSecOps Cloud Applications, IT Data

LogX combines AI and DTI that read and profile textual data, complex flows, and data patterns. Those new models are fine-tuned to meet the modern applications release cycle. DevSecOps needs and addresses the needs in an automated approach that will understand risk and avoid false alerts.

Today's Log data Anomaly detection & ML doesn't meet modern Apps | IT Needs!

Logging solutions like Xpolog, ELK, Splunk, and others provide anomaly detection and ML tools for log data, but those solutions fail to meet today's **frequent code and apps release cycles changes**. Technical experiences and endless manual work are required in order to define anomalies detection rules. In most cases, anomalies and ML fails due to ongoing changes and errors.



LogX New DTI/AI/ML Models



Deep text inspection engine (DTI) inspects every log event payload and compute risk, signs it, enriches, and tags it. ML behavior profile is built on the correlated risk and KPIs,

Data | Events | Stream Anomalies



Data Volumes anomaly detection.
Events Volume flow anomaly detection.
Correlated risk on streams flow & patterns.

High-Risk Behavior Pattern Anomaly



LogX cross-correlates multiple data points and risk factors for each source. Deep insights based on clustering and anomaly detection trigger alerts only for changes in the risk model.

New Errors | High Risk Errors Detection



Every 24 hours LogX generates a new detected errors report, grouped by source and risk level. Weekly reports on risk factors and events that were removed.

AI/ML Automation Cuts



95% of Manual Work

No parsing, No custom rules, no complex anomaly rule definition. No experts in ML work. LogX cuts manual work with real-time adaptive automation for every source.

Optimize Business Quality and Security

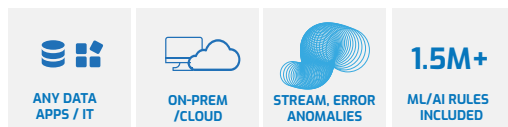


LogX deep insights discover risk patterns, IT problems, and anomalies detected in any system logs behavior profile and context.

LogX as automated Service to Applications DevOps, DevSecOps, IT, Security

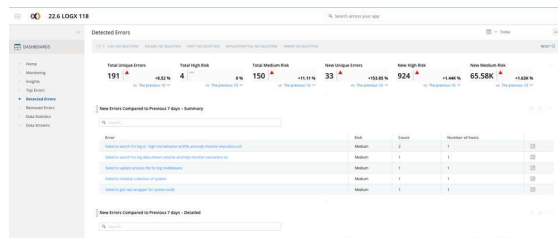
Simply stream data to LogX, tag the sources by context and deploy LogX. LogX will scan and automatically identify risk patterns. Each Application| IT Context team will get Insights within minutes of deployment.

LogX works well and is fully Integrated with ELK and Splunk, for more Information, contact us.



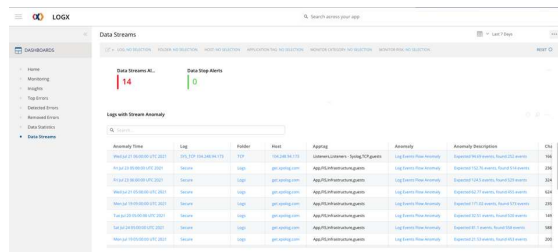
New Errors and Risk Discovery Reports

Deep insights and DTI auto-discover new errors, patterns, and risks in each data set. Every 24 hours, the owner will get reports by email or alerts.



No Need In Parsing Rules | No Manual Rules | Open Simply Route Data Streams

LogX unique technology is based on deep insights and data inspection. Working on every log data source without the need to create search rules, parsing rules, monitors, etc.



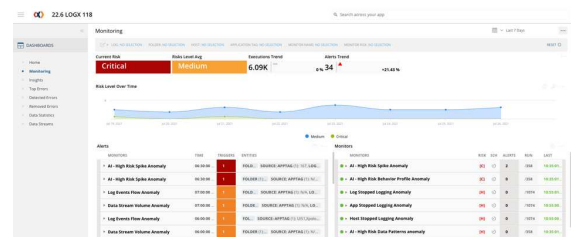
ELK | Splunk | ServiceNow | Dynatrace Integration

Stream log data from Splunk forwarder or Logstash to LogX and gain immediate insights. Alerts and Reports can be forwarded back to any system.



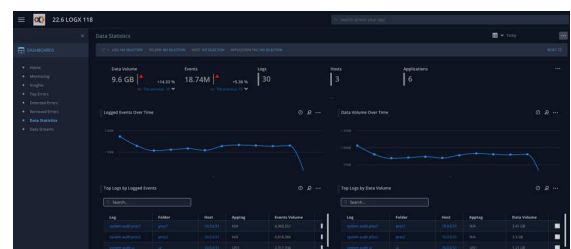
Anomalies, Insights, Risk, Alerts by Application | Context

LogX analytical app provides a summary of all errors, insights, anomalies, and alerts. Quickly navigate and zoom into each alert or search the data for the root cause.



ML-Powered Risk model Pattern Detection and Anomalies

Automated reports and real-time alerts will be sent to ITOM, Ops, NOC rooms, and application teams.



DevSecOps Security and Audit

LogX monitor every log source, IT stream, Cloud source and application log. LogX unique engines provide deep insights that help detect

Monitor patterns in IT, Apps streams and report to SIEM

Monitor Audit logs for anomalies, profile risk and abnormal changes.

Deep insights on application Audit access and changes data manipulation.

Monitor streams, events, correlation and risk on every security system and log source.



Try LogX on your data.
Our Team is available at any time.

US Office 1250 Broadway, 36th Floor
Manhattan, NY 10001, USA
Phone: +1 888.482.4770
Email: sales@xplg.com