IT Data streams as a Service for IT and Digital Teams. Create Smart Data pipelines across hybrid clouds. Reduce Splunk & ELK Cost.

PortX is a data streams management platform that seamlessly controls data pipelines with collectors, data parsing, transformation, filters, enrichment, and forwarding. PortX process IT data once and route intelligent optimized stream to the right service. Data filtering, masking and optimization help to reduce cost and TCO on Splunk, ELK, SIEM and more.

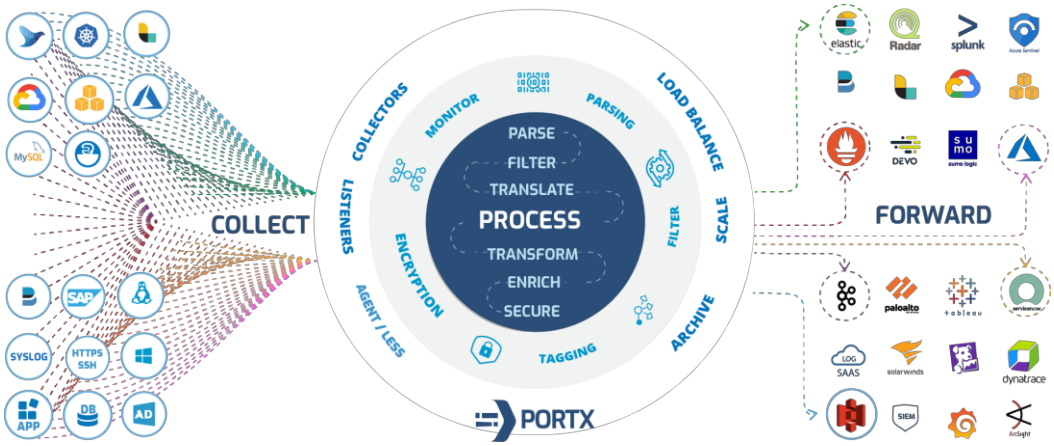
Optimize quality. Clean Noise. Focus. Reduce TCO | Improved Insights

PortX advanced tools saves manual work and infrastructure usage. Eliminates data management complexity. Saves storage volumes. Cuts annual license cost and TCO.

CUT 43%

Total Annual Saving by Adding PortX

		PortX + elastic	elastic
Infrasructure	49%	652K$	1.270K$
Storage	45%	181K$	313K$
Licenses and Support	34%	360K$	540K$
Operations	40%	390K$	650K$
Total Annual Saving	43%	1.58M$	2.77M$



Route Data to The Right Service
PortX filtering and forwarding services route data flows to the right place. Archives data to optimize cost. Only security events are routed to SIEM, observability data is routed to the specific tool or service.

Optimize Data Quality
Data filtered and cleaned to reduce volume. Transform. Restructure and filter events. Enrich, map, mask, extract, and forward only what matters.

Network
Load
Storage

Reduce Data Pipeline / TCO
Slash infrastructure requirements.
Reduce data by filtering noise and garbage.
Save storage space.
Define Data Once use this data for multiple services.

AUTOMATIC 95% MANUAL

AI/ML Automation Cuts 95% of Manual Work
Reduces cost of manual work involved in managing, AI parsing and normalizing IT data.

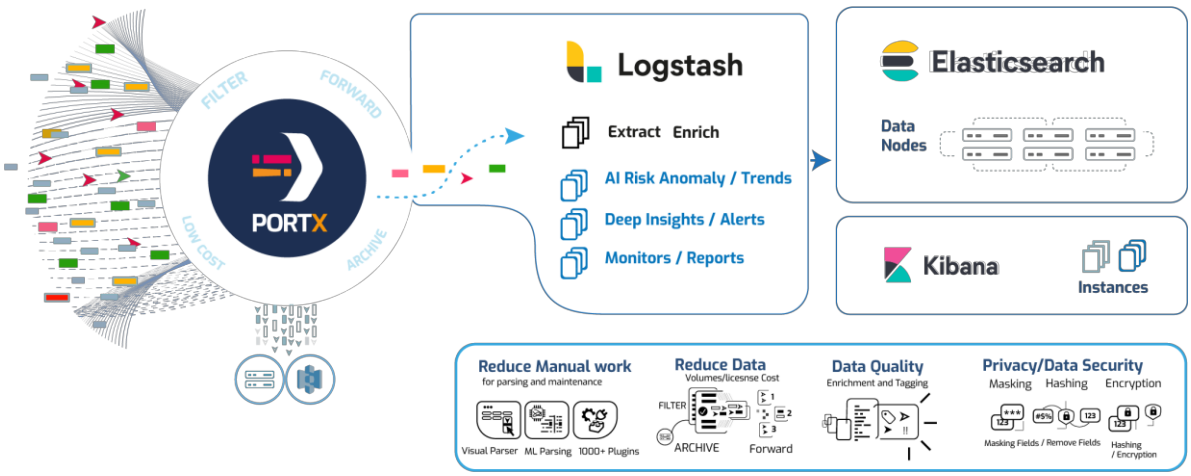
+TB DAY PROCESSING NODE×1

Performance at a New Scale
PortX processes terabytes of data/ day on day. Every 1xNode (on-prem or cloud). Built-in persistency, load balancing and more.

Avoid Vendor Lock-In
Control and shift streams of data to your preferred service provide or tool at any time in an agnostic fashion.

Data Pipelines under Control. Collect, Parse Enrich. Transform, Clean, Route and Forward.

PortX platform provide end to end data collection tools, listeners, and seamless Integration to existing data collection tools. Once data Is moving through PortX platform teams can have full control and tools to optimize the data quality, cost, and events destination.



Integration & Control

Simply collect, parse and forward data to Splunk components. During that process, since ELK cost Is based on data and Instances, putting a mechanism that can control stream volume help to control cost. Forward specific data events to other services on demand. PortX Is agnostic and will not require Infrastructure changes.

Collect and listen with Plugins & Connectors

100+ systems, services, and applications available plugins and connectors out-of-the-box.

Forward Data: Filter and Route Data Streams

Filter events and reduce data volume. Transform and customize data. Mask sensitive fields. Stream data to analytics, monitoring, SIEM, cloud archive and More.

ML-Powered Pattern Detection

Verify and manage parsing and data structures at parsing level. Monitor data parsing and integrity.

Visual Data Parsing

|UI-based management |Pattern sharing |Log templates repositories |Open integrations and more

Administrate Data With Log Viewer and Tags

Data sources |Permissions | Structures |Tags |Patterns.

Security and Audit

PortX' built-in enterprise-grade security features simplify regulatory compliance and cybersecurity requirements

Enterprise scale security.

Audit log on the administration and configuration for compliance.

Audit access and changes to data manipulation.

Authentication and Authorization of management console integrated to AD and SSO.

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

LogX provide Data Science Insights on any IT and Business Apps Log Streams. Detecte over 1.5+ million AI based Insight on IT data.

XPLG LogX automatically identify and alert 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 unique profile for each log event, this profile is than aggregated into a new data model with systems behaviour profiles, complex risk patterns and more. LogX detect 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) inspect every log event payload and compute risk, sigh it, enrich, and tag 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 correlate 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 generate new detected errors report, grouped by source and risk level. Weekly reports on risk factors and events that were removed.

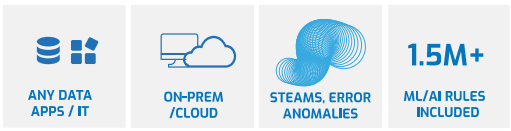
AI/ML Automation Cuts 95% of Manual Work
No parsing, No custom rules, no complex anomaly rule definition. No experts ML work. LogX cuts manual work with real time adaptive automation for every source.

Optimize Business Quality and Security
LogX deep insights discover risk pattern, IT problems and anomalies detect in any system logs behavior profile and context.

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

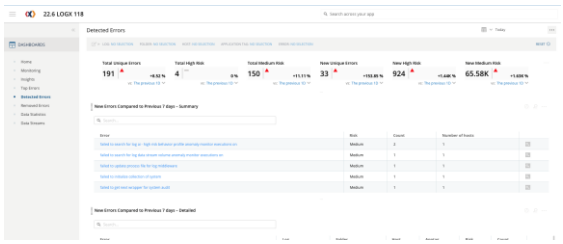
Simply stream data to LogX, tag the sources by context and deploy LogX. LogX will scan and automatically identify risk patterns. Each Application| IT Context team will get Insights within minutes of deployment.

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



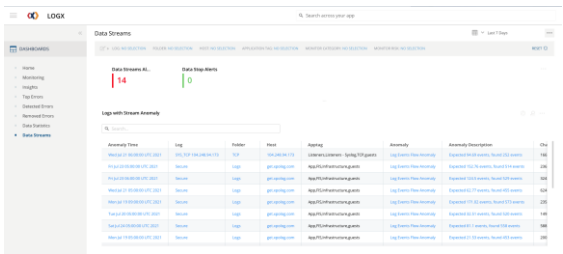
New Errors and Risk Discovery Reports

Deep insights and DTI auto discover new error, patterns, and risk 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.

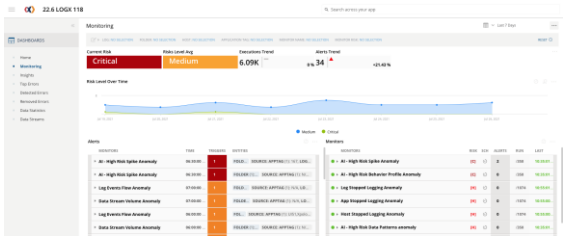


ELK | Splunk | ServiceNow | Dynatrace Integration

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

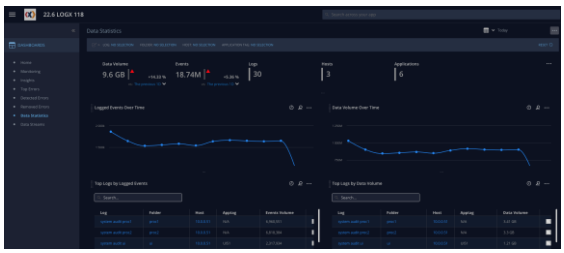
Anomalies, Insights, Risk, Alerts by Application | Context

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

Monitor patterns in IT, Apps streams and report to SIEM

Monitor Audit log 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.

LogX

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.comt