XpoLog Center is an End-To-End solution for log management and log analysis. Every single computing device and application in your organization generates log events. Some of the most critical and private information in your organization is stored in the endless haystacks of logged data. Log events contain valuable information on network errors, security risks, application problems, abuse of systems, frauds and more. Log events are characterized by unstructured data, hysteric generation ratio and usually it is very difficult to access logs scattered across the network. These problems make it impossible to efficiently correlate logs, track system problems, fix malfunctions and generate new reports for analysis. In the endless cryptic logs repositories, there is valuable information that you must use for root cause analysis, security needs, and analysis of business application malfunctions.

The Solution – XpoLog Log Analysis and Management
XpoLog Center is a non-intrusive, log analysis and management platform that can be integrated quickly and securely to ANY log type, device, or application in your organization. XpoLog provides analysis tools, report engine, monitoring engine, correlation capabilities, transaction tracking and monitoring, search engine for logs and many more features. XpoLog support a non-invasive both agent-less and agent-based architectures. That means XpoLog can access logs via standard protocols like SSH and make them ready for analysis. Deploying XpoLog is easy, as no changes to existing infrastructure or configuration is required. XpoLog simply access the logs and creates a single point of enterprise log management that an authorized user can access with a web browser from any where on the network.

Web Interface for remote Access
XpoLog application UI is web based. That means you can open a web browser on the log management server URL from any location and any machine in your secure network. Easily log-into the log analysis platform and start analyzing any of the logs in you organization both in real time and also historical data.

Log Collection made easy
Collecting logs from devices and servers to a central location is what log collection is all about. SysLog is very common for centralizing log events storage. XpoLog support both architectures. XpoLog can collect logs, store and analyze them, accessing SysLog repositories is also supported. That mean you will not have to change your existing SysLog infrastructure, you will just gain XpoLog analytical layer with minimal effort.

Reduce Troubleshooting Periods = Increasing system uptime
XpoLog reduces troubleshooting periods by 70%. This dramatic reduction is driven by XpoLog capabilities to quickly access logged data, running filters and search terms on it that help to quickly diagnose the root cause i.e. application problem, network faults or security risks. XpoLog TxExpo provides a clear graphical view of system behavior and help to pin point the location of faults. From TxExpo there is a drill down option that will present the log events recorded at the time the problem occur. This methodology brings the user directly to the root cause without spending long period in searching relevant log events.
XpoLog Center Solution

XpoLog delivers a leading enterprise log management platform that enables organizations to correlate, monitor, smart analyze and smart search logs across all security network, infrastructure and business applications domains.

Reports

Generating reports from logs is one of the key benefits organization gain from using XpoLog. As soon as XpoLog is installed and connected to the logs it enables generating any type of report on log events. Generating reports such as trend analysis, aggregation of security events, SOX, HIPPA and more is supported. XpoLog approach is to provide a generic all purpose data analysis board that enables the creation of any form of rules and filters. Once the rules are in place in matter of minutes you can generate reports and export them by email, or print them.

The power of Correlation – Transactions

Log events are constantly generated during IT systems activities. IT infrastructure is a collection of systems that are integrated together to execute business, system and security processes. Analyzing and monitoring one system log events will not provide the full picture regarding your IT process. In order to understand and monitor the behavior of complex processes in IT infrastructure, one must correlate different log events to isolate each and every instance of the process and then inspect it as a whole. Tracking and monitoring IT process through all devices, servers and applications is impossible task to do with existing technologies. XpoLog TxExpo will do just that and more. With XpoLog you can correlate IT log events with actual business process.

What is there in my logs?

One of the challenges there are in all that come to log analysis is the need to get information from logs. There are huge number of messages and events. In most cases you will be familiar only with a subset. XpoLog IT WIKI and external investigation tool helps to bridge over the information gaps.

👩‍💻 XpoLog

Management module for the log events environment, provided with a universal log viewer, simple correlation features, reporting, and data services. This module is also responsible on deployment management and log events collection.

🔍 XpoSearch

Searching terms in logs are one of the popular operations during log analysis. XpoLog Search patented technology indexes all live changing logs and makes it easy to search the needle in the data haystack. You can find an IP address with in gigs of logs in less then one second.

💡 XpoLogDashboard

XpoLog Dashboard gives Top level summary reports of systems status, transaction status, compliance reports, security filters and more.
XpoLog Center Provides an End-to-End solution for log management and analysis

- Business Application
- Network
- Security
- Transaction
- Root Cause Analysis
- Problem Isolation
- Monitoring
- SOA Troubleshooting

**XpoLog IT WIKI**

Very cool tool to share knowledge on top of live and changing data. Tag log events and create community know how base for technical problems. Another cool feature is the ability to drill out from the log analysis to remote technical knowledge web sites. By doing that you get automated access to huge number of technical support sites over the web.

**Analyst**

"Analysis and reporting of security logs is essential."

Mark Nicolett, VP Security Research, Gartner

**XpoLog Center Architecture**

- **XpoLog Center Applications**
  XpoLog Web interface enables user to access all application through web browser to view and configure monitoring, reports, log viewer, transactions, dashboard, analysis tools, search engine, IT WIKI on logs and more.

- **XpoLog Agent**
  XpoLog center can communicate with remote agents to reduce network traffic and machine resources. Providing unlimited log management scalability.

- **SysLog Analysis & Collection**
  Newer and security devices report SysLog events to a SysLog server. XpoLog agent access the SysLog server for analysis and collection.
# XpoLog Center Leading Technology

<table>
<thead>
<tr>
<th>Feature</th>
<th>XpoLog</th>
<th>Competitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non - Intrusive, no changes to IT configuration</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Low Network Traffic, only log delta on network.</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>No Obligatory DB for logs, can work on files and DB</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Fast Deployment period, minutes to days</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>No need for additional Hardware</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Cross OS, Web Interface - Pure Java</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Agent-less for distributed deployment</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>No Data Replication, less then 5% overhead on data</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Transaction Analysis – online and for postmortem</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Interactive Dashboard – Statistics, diagnostics, anomaly detection</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Transaction Monitoring – With Alerts of any type</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Log Correlation Visualization – of any type</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Security and Network Event Management built in</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Merge multi data sources to a single view for analysis</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Automatic Problems Isolation through RCA process</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Parse any type of Log – Multi-vendor or homegrown</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Detect Rolling Files, changes in sources format</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Connection Via SSH – secure agent less access</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Deployed as J2EE Apps – WAR,EAR to Portal</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Support J2EE standard – Portals, App Servers</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Support SSO – LDAP,CA SiteMinder</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Support JAAS security – Open to integration</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Meta Data Reports – Audit, Compliance</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Distributed architecture - for large deployment</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Log Management – Security, Network &amp; Applications</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Troubleshooting tools – End-to-End</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Search Engine for Logs and other data types</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Technical Knowledge on filters and rules</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>System Health Dashboard for Executive Summary</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Audit Reports for Compliance and System Analysis</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Open for new Reports definition – SOX, HIPPA etc.</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Support any type of JDBC supported DB</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Send alerts via SNMP, JMS, email, scripts, URL etc.</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Log Monitoring, Rules Monitoring</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Automatic discovery wizard – add apps within minutes</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Out-of-the-box support for many types of logs</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Structured root cause analysis process</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Report Engine for any type of log format</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Manage Enterprise configuration from one location</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Merge several logs into one view</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Integration to Sys Log format for log collection</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Tail logs in real time, normalize time zone</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Integration to external Workflow system</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Validated by blue chip reference customers</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>High Experience with Enterprise deployments</td>
<td>✔️</td>
<td>✗</td>
</tr>
</tbody>
</table>
XpoLog Center Features

- Enterprise Log Viewer for all type of logs
- Merge logs to one combined view
- Filters over time, regular expression, priorities
- Filter numbers, Boolean operators
- Quick Search, Search Engine
- Transaction and Correlation of events
- Track changing files automatically
- Define many patterns on log data for parsing
- Normalize date according to time zone
- Monitor logs in real time with alerts
- Built in Scheduler for tasks
- Scheduled log collection
- Export Logs via email, via SSH or file system
- Export, transform and inject logs to database
- Run SQL queries on all type of logs
- Detect log data pattern automatically
- Detect new log files in directories
- Parse multiple text line events i.e. Exceptions
- Support XML files
- Support database logs and tables
- Support for binary file and char stream file
- Support Windows Event viewer
- Support any type of data pattern
- Non-Intrusive read of log events
- Templates and Out-of-the-Box wizards
- Aggregation of log data: data, filters, count
- Graphical reports
- Transaction tracking, monitoring, analysis
- Transaction search and reports
- Log event correlation by id, time, heuristics
- Search engine indexes all live data
- Fast search over huge amount of data
- Tag events and manage knowledge
- WIKI in logs for IT know how
- Rule engine on logs for verification
- Web interface
- HTTP/S connection between agents
- Tail logs for real time view
- Tail with filter like Unix/Linux tail grep
- Monitoring with alerts notification
- Enterprise log configuration management
- Full Audit support for user operation
- Audit reports
- Meta data support for logs
- Search logs across distributed environment
- Index log over time or data changes
- Build virtual modules and logs tree
- One click to access any log through browser
- Support Clusters

XpoLog Center Security

- JAAS standard
- Authentication – built-in, SSO, LDAP
- Authorization – limit users for viewing logs
- Authorization – limit users by application
- Authorization – limit users by policy
- Authorization – limit users from operations
- Groups and Policies for user management
- Integration to enrollments database
- Connection encryption by SSL
- Private/Public key cryptography

XpoLog Center J2EE

- BEA Weblogic
- IBM Websphere
- Sun Application Server
- Oracle Application server
- SAP Net Weaver
- Red-Hat JBoss
- Apache Tomcat/Catalina
- Geronimo
- Jetty
- Raisin
- Macromedia JRun
- And other J2EE Application servers

XpoLog Center Supported Platforms

- Linux
- Unix
- Windows
- AIX
- Solaris
- Red-Hat
- Any Java JVM 1.4.1+ supported OS

Contact XpoLog

Get FREE trial now at www.xpolog.com
Call +972 3 6343884
Online Support http://www.xplg.net/support
Corporate Website www.xplg.com