Product Datasheet

CorreLog Visualizer™ for IBM z/OS

Real-time Security Monitoring, Dashboards & Alerts for z/OS

The CorreLog Visualizer is an affordable Security Information & Event Management (SIEM) system especially designed and pre-configured for use by z/OS security administrators and system programmers. It provides point-and-click functionality from a standard web browser into z/OS security and operational events. Visualizer provides dashboard views, event message correlation, and can send text messages as alerts of security events generated from z/OS.

How does it work? The Visualizer for z/OS dashboard collection is a major advancement over the z/OS green screen most familiar to mainframe users. This mainframe SIEM system delivers a clean, web-based GUI with high speed search, and the capability to drill down to z/OS security messages with point-and-click functions. The solution is agent-based, residing on one or more LPARs, and collects a full range of mainframe security data from facilities like RACF, CICS, DFSMS, DB2 accesses/failed access attempts, and z/OS console messages, then presents the data in Visualizer dashboards.

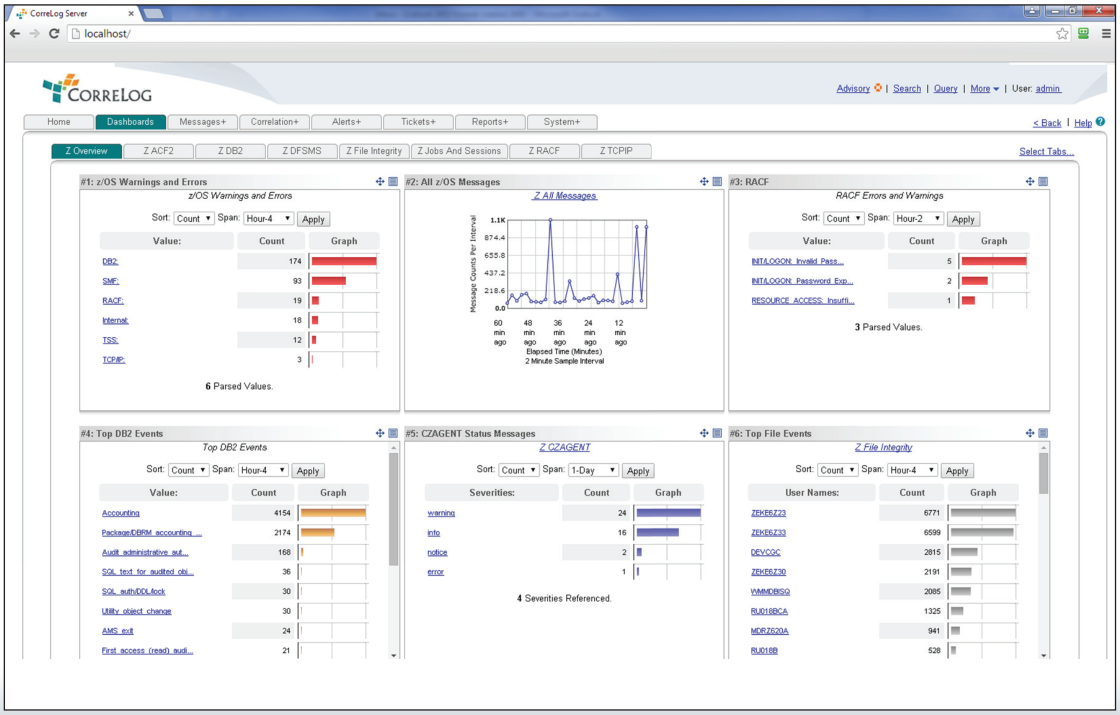
The Visualizer for z/OS is based on technology derived from CorreLog's leading SIEM Correlation Server log management product. Visualizer's correlation engine determines if messages are important and, in real time, alerts appropriate personnel of any security issues.

For integration, the API for Visualizer is certified for both IBM® Security QRadar® and HP ArcSight and CorreLog has a long-standing partnership with McAfee that includes several joint deployments. Additional field integrations have been completed with Splunk®, LogRhythm, Dell SecureWorks, and other well-known SIEM brands.

Business Partner IBM™

Ready for
Security Intelligence

hp ArcSight CEF Certified
2015



#1: z/OS Warnings and Errors

z/OS Warnings and Errors

Sort: Count Span: Hour-4 Apply

Value:	Count	Graph
DB2:	174	
SMF:	93	
RACF:	19	
Internal:	18	
TSS:	12	
TCP/IP:	3	

6 Parsed Values.

#2: All z/OS Messages

Z All Messages

#3: RACF

RACF Errors and Warnings

Sort: Count Span: Hour-2 Apply

Value:	Count	Graph
INIT/LOGON: Invalid Pass...	5	
INIT/LOGON: Password Exp...	2	
RESOURCE ACCESS: Insuffi...	1	

3 Parsed Values.

#4: Top DB2 Events

Top DB2 Events

Sort: Count Span: Hour-4 Apply

Value:	Count	Graph
Accounting	4154	
Package/DBRM accounting ...	2174	
Audit administrative aut...	168	
SQL text for audited obj...	36	
SQL auth/DDL/lock	30	
Utility object change	30	
AMS exit	24	
First access (read) audi...	21	

#5: CZAGENT Status Messages

Z CZAGENT

Sort: Count Span: 1-Day Apply

Severities:	Count	Graph
warning	24	
info	16	
notice	2	
error	1	

4 Severities Referenced.

#6: Top File Events

Z File Integrity

Sort: Count Span: Hour-4 Apply

User Names:	Count	Graph
ZEKE6Z23	6771	
ZEKE6Z33	6599	
DEVCGC	2815	
ZEKE6Z30	2191	
WMMDBISQ	2085	
RU018BCA	1325	
MDRZ620A	941	
RU018B	528	

CORRELOG®

Visualizer™ for IBM z/OS

Additionally, the Visualizer for z/OS can act as a general-purpose collector and SIEM Syslog forwarder in a larger enterprise SIEM strategy. Visualizer can simply provide live mainframe security data to key resources within your organization – that may or may not have access to your enterprise SIEM – utilizing a standard web browser. The solution compliments the functionality that exists within your SIEM system, expanding your team's visibility to data currently generated from your z/OS.

Frequently Asked Questions

Q: Is the CorreLog Visualizer for z/OS required to use CorreLog's mainframe product SIEM Agent for z/OS?

A: The Visualizer for z/OS is NOT REQUIRED to fully use SIEM Agent for z/OS. Visualizer is most useful for providing visibility to the mainframe data outside an organization's SIEM system (such as to select administrators, or mainframe operators.)

Q: Is the Visualizer for z/OS considered a replacement for our current SIEM system?

A: Visualizer for z/OS is a comprehensive dashboard and mainframe security system that includes search, correlation, alerting, and reporting. However, it is not intended to replace the SIEM of your organization. Its intent is mostly to provide mainframe IT security visibility in a more functional display than traditional green screens.

Q: How is the Visualizer for z/OS licensed?

A: CorreLog Visualizer for z/OS is licensed separately from the CorreLog SIEM Agent for z/OS program (or other CorreLog products). Visualizer is licensed for a certain number of LPARS that are each running a CorreLog agent.

Q: Can I upgrade the Visualizer for z/OS to a full CorreLog Correlation Server license?

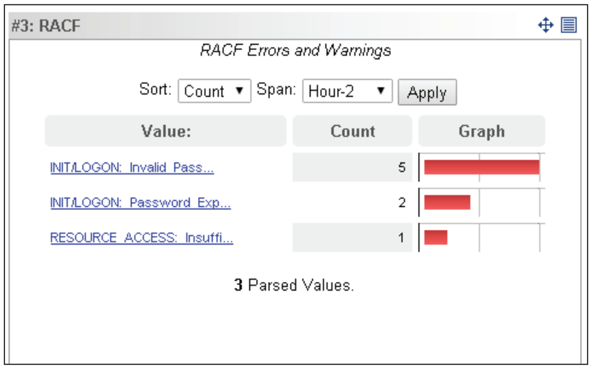
A: If you have the CorreLog Visualizer for z/OS installed, you can upgrade to the full CorreLog Correlation Server system with minimal effort, while keeping your existing configurations. You would simply license more devices. CorreLog team support is available to assist.

Q: Where can I find more information on CorreLog Visualizer for z/OS?

A: Because the CorreLog Visualization system is based on the CorreLog Correlation Server and CorreLog Framework, you can find an abundance of information (such as system requirements, administrative configuration, internal security concepts, and other documents) by consulting standard CorreLog Correlation Server documentation found on our website at www.correlog.com.

Extended Mainframe Visibility via Standard Web Browser

- **z/OS Dashboard Views: Data can be depicted using a suite of pre-configured dashboards that show mainframe activity related to system-wide security.**
- **The software comes with out-of-the-box correlation rules for monitoring a multitude of z/OS security events, including RACF, CICS, DB2 and DFSMS.**
- **High-speed Mainframe Message Search: Mainframe security messages are collected by Visualizer and indexed for rapid search**



RACF Errors and Warnings

Value:	Count	Graph
INIT/LOGON: Invalid Pass...	5	
INIT/LOGON: Password Exp...	2	
RESOURCE ACCESS: Insuffi...	1	

3 Parsed Values.

About CorreLog, Inc.

CorreLog, Inc. is the leading independent software vendor (ISV) for IT security log management and event correlation spanning both distributed and mainframe platforms. CorreLog's flagship products are CorreLog Correlation Server™, CorreLog SIEM Agent™ for z/OS, CorreLog Visualizer™ for z/OS, and CorreLog dbDefender™ for DB2.

For more information about CorreLog products for IBM z/OS, please visit www.correlog.com/products or scan the QR code on the right.