Enforcive™
Data respected.

Enterprise Security CPA for IBM MF

CPA – What is it?

The CPA (Cross Platform Audit) is a comprehensive log management and critical data monitoring platform for the IBM mainframe. It allows you to collect a wealth of system and security audit events, analyze them and consolidate them with events from other computers in your organization, and in doing so, turn audit events into usable information, vital for correct tactical decision making.

Unique Benefits for Mainframes.

1. **FTP and Telnet Access Control**. You can restrict access from the network through FTP and Telnet.

2. **DB2 Log Records**. View data at the field level before and after record addition, update and deletion. Changes in field values are emphasized using different colors.

3. **SMF Audit**. Including Telnet, VSAM, FTP, RACF and DB2. View SQL statements,

Additional Benefits

- **Partition Management.** For fast and efficient retrieval of information without the headache of manual management.

- **Clear and Easy Display of Your Security Audit.** Intuitive and user-friendly audit trail of all SMF, SAFE/CICS and RACF events. The events are broken down into its appropriate parameters making it easy to understand each event.

- **Detailed Filtering Criteria.** The security auditor can view security events on-line and filter them on the screen without the need for additional applications or programming. Filtering can be done on date and time ranges, account type, user, event status, IP address and application event type. The application can be filtered down to highly granular levels such as record updates, FTP downloads, invalid passwords and user changes.

- **Dynamic Dashboards.** You can produce graphs to identify trends and pinpoint behaviour in your system activity. Events from across the enterprise can be combined, sorted and filtered into hundreds of different combinations of platform, application, IP address, user, identity management user, transaction status and date. The dashboards are built dynamically by the user selecting the sort parameter at each level

The dashboards include statistics views and time-line views of the audit events. The graphs and summary tables can be displayed on the screen, printed, sent by email and saved as files in various formats including PDF and MS Office-compatible HTML which can be opened by Excel and Word.

- **Offload Audit Data to Dedicated Database.** After you transfer your audit data to the PC-based database (MS SQL server) the original logs can be purged on the source system, freeing up valuable storage space. Once imported to the CPA, the information can be viewed and analyzed on your PC. You can schedule the transfers for unattended regular runs.

- **Report Generator.** Includes a report generator with the capability of exporting reports to MS Excel, PDF and other formats. Report runs can be scheduled to run periodically by day, week or month, to provide an informative view of your system information.

- **Consolidate Security Audit Data from Multiple Machines.** Consolidate security audit data from any number of machines all in one place. You can create logical users called IDM users, to audit activity of a user having different logon IDs. The IDM user doesn't require any pre-defined identity management requirements like the implementation of single user sign-on.

- **SYSLOG.** The audit data collected from the system by the CPA can be sent directly to a SYSLOG server, with option of SYSLOG NG encryption, or maintained and managed in the CPA database. NFX and CEF message format options.

Other Platforms

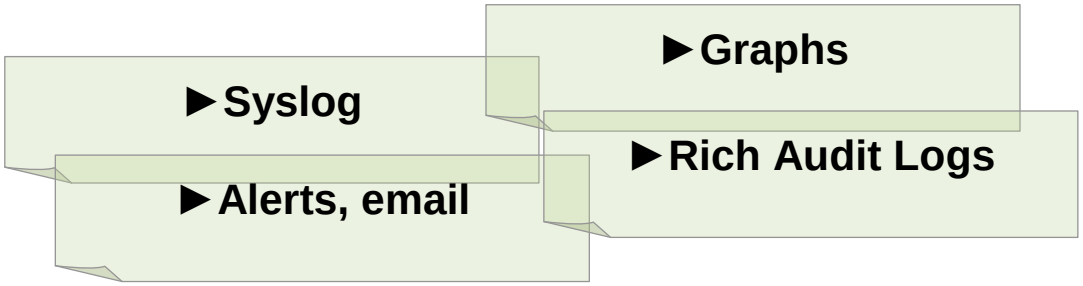
The CPA is a multi-platform product that can connect to many different environments. These include IBM mainframe, IBM i, MS Windows, AIX, Linux, Oracle, MS SQL Server and SAP Application.

30th Nov 2011

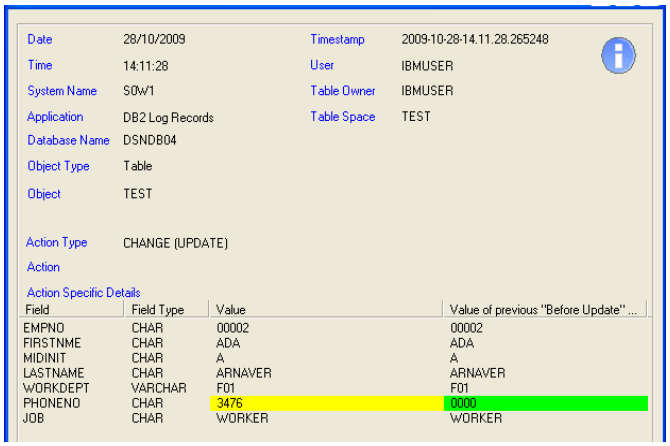
Enforcive Enterprise Security

CPA for Mainframe

Critical Data Monitor for mainframe data,
security and system events in a graphical UI



DB2 Data Before / After ● SMF TELNET ● SMF FTP
SMF VSAM ● SMF RACF
TCP/IP FTP / Telnet ● SMF DB2 ● SAFE/CICS



Date	28/10/2009	Timestamp	2009-10-28-14.11.28.265248
Time	14:11:28	User	IBMUSER
System Name	S0W1	Table Owner	IBMUSER
Application	DB2 Log Records	Table Space	TEST
Database Name	DSNDB04		
Object Type	Table		
Object	TEST		
Action Type	CHANGE (UPDATE)		
Action			

Action Specific Details

Field	Field Type	Value	Value of previous "Before Update" ...
EMPNO	CHAR	00002	00002
FIRSTNME	CHAR	ADA	ADA
MIDINIT	CHAR	A	A
LASTNAME	CHAR	ARNAVER	ARNAVER
WORKDEPT	VARCHAR	F01	F01
PHONENO	CHAR	3476	0000
JOB	CHAR	WORKER	WORKER

DB2 record update showing before and after field values

Clear and Easy Display of Your Security Audit
Intuitive and user-friendly audit trail of SMF and other audit data events produced by DB2, RACF, FTP and Telnet activity. The events are broken down into the appropriate parameters making them easy to understand.

Detailed Filtering Criteria to Analyze Security Audit Events
The security auditor can view security events on-line and filter them on the screen without the need for additional applications or programming. Filtering can be done on date and time ranges, platform, account type, user, event status, IP address and application event type.

Filter events by application: DB2 log records, SMF RACF, SMF DB2, TCP/IP application audit, SMF telnet, SMF FTP, Bsafe/Security for CICS.

Filter events further by application, event category, type and even sub-type. Examples include:

- DB2 log records > change audited table > delete/insert/update
- SMF DB2 > authorization failures > database privileges > display database

Dynamic Graphs
You can produce graphs to identify trends and pinpoint behavior in your system activity. Dynamically drill down from your chosen starting point until you have reached the desired selection. Print the graphs, save them in PC file format or email them as you wish. Events from across the enterprise can be combined, sorted and filtered into hundreds of different combinations of platform, application, IP address, user, identity management user, transaction status and date. The graphs are built dynamically by the user selecting the sort parameter at each level

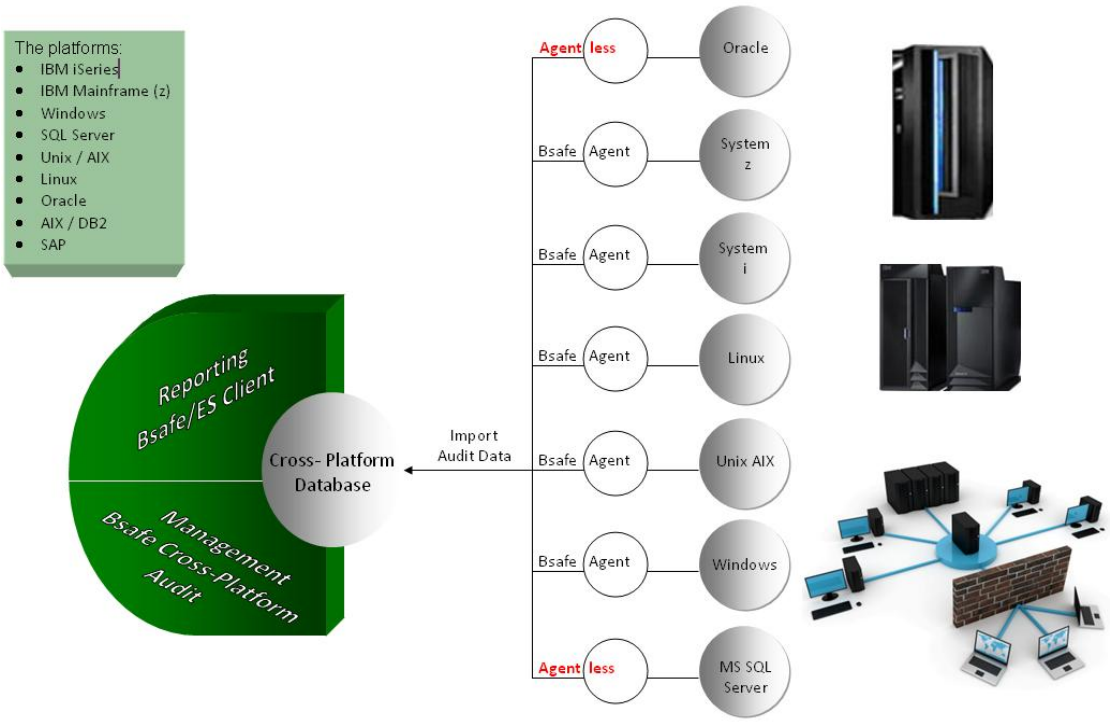
Each component of the on-screen graphs can be expanded at the click of the mouse to show the actual audit events behind the statistics and each event can be drilled down to show all related information including the name and value of each event parameter.

The graphs include statistical and time-line views of the audit events. The graphs and summary tables can be displayed on the screen, printed, sent by email and saved as files in various formats including PDF and MS Office-compatible HTML which can be opened by Excel and Word.

Offload audit data from MF to PC-based database
After you transfer your mainframe audit data to the PC-based database (MS SQL server) the files can be automatically purged on the MF, freeing up valuable storage space. Once imported to the CPA (Cross-Platform Audit) the information can be viewed and analyzed on your PC. You can schedule the transfers for unattended regular runs.

Report Generator
Includes a report generator with the capability of exporting reports to MS Excel, PDF and other formats. Report runs can be scheduled to run periodically by day, week or month.

Consolidate Security Audit Data from Multiple Machines
Consolidate security audit data from any number of MF computers and also from IBM i, MS Windows, MS SQL Server, Linux, AIX, Oracle and more. The importing of audit data from other computers requires installation of appropriate Bsafe agents on those machines too. You can create logical users called IDS users to audit activity of a user having different logon IDs. The IDS user doesn't require any pre-defined identity management requirements like the implementation of single user sign-on.



USA New Jersey	Tel: 877-237-8024 toll free	salesusa@enforcive.com
Canada	Tel: 905-9434042	info-ca@enforcive.com
Europe & R.O.W.	Tel: +972-9-9610400	info-eu@enforcive.com

A list of local resellers can be found on our website

24th Nov 2011