Cross-Platform Audit

Enterprise Log Management and Database Activity Monitoring (DAM)

Enforcive/ Cross-Platform Audit (previously Bsafe/ Cross-Platform Audit) is an Enterprise Log Management and Database Activity Monitoring (DAM) tool, aimed at organizations running multiple systems and disparate platforms. The Cross-Platform Audit (CPA) consolidates platform-specific audit events and makes them available to auditors and administrators in an intuitive and easy-to-use interface. It does this while maintaining a high level of granularity to filter events by platform-specific characteristics.

Monitored Platforms

- IBM i (AS400)
- IBM z (Mainframe)
- Windows
- SQL Server
- Unix/AIX
- Linux
- Oracle
- Sun Solaris

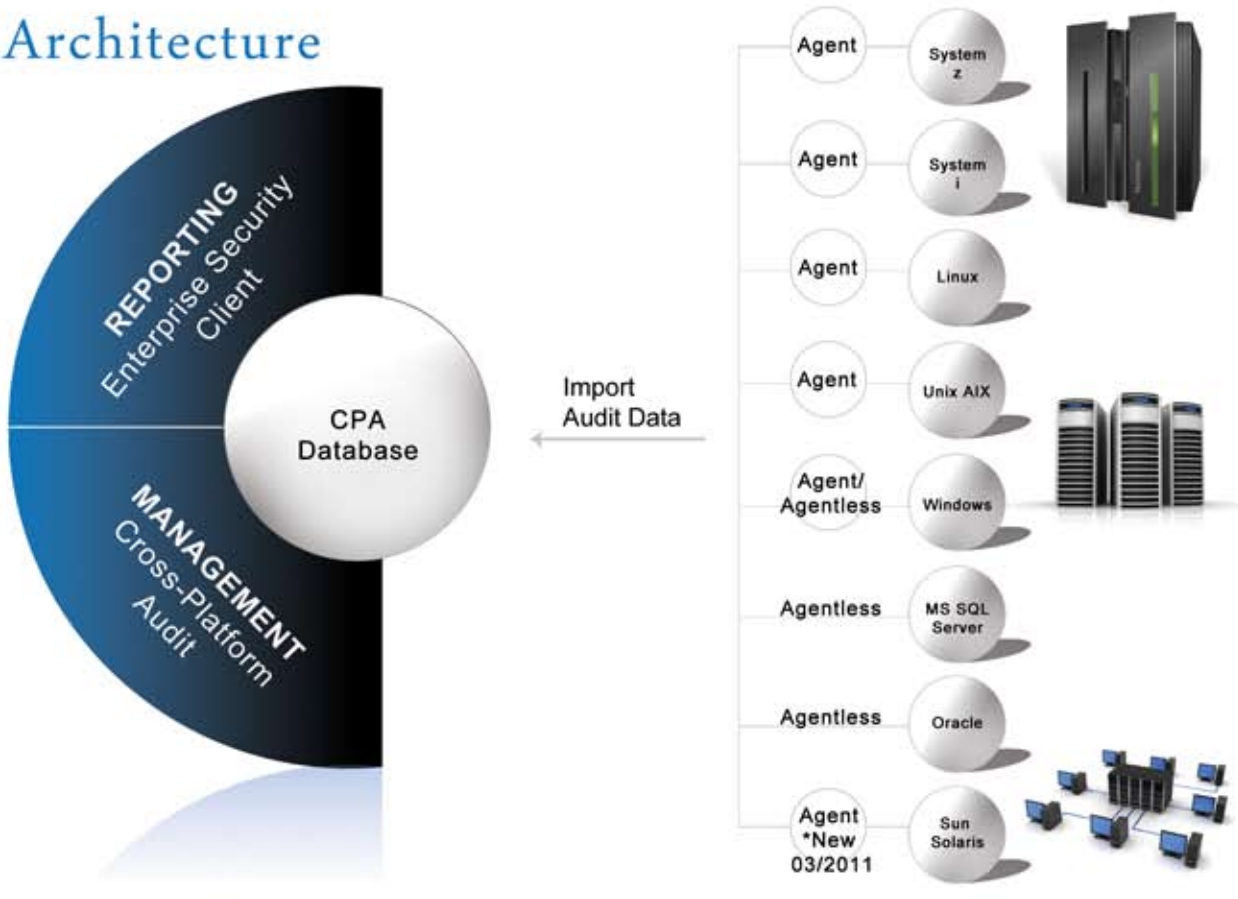
Critical and Sensitive Data Monitoring

The CPA lets you monitor the activity of a user across different computers on diverse platforms and present that activity on screen, in a single event log and graphical format.

The CPA logs raw transactional data and, through a variety of online filtering, reporting and dashboard tools, provides meaningful information that can give valuable insight to the organization. It has the ability to monitor activity on all the organization's computers and analyze it in a consolidated manner. For example, a user in one enterprise application might execute a series of transactions across different platforms – something which doesn't draw interest when looked at on the level of one computer, but could be seen in a different light when the entire audit trail is examined.

Using the CPA, system activity and user behavior can be analyzed as a consolidated chain of actions executed across different computers. The global user function allows tracking of a user's trail under various user IDs on different computers and platforms.

CPA Architecture



How It Works

The CPA monitors and collects security audit events as they occur on each computer. There, they can be viewed and sorted directly and are made ready to transfer to the consolidated central data repository when requested.

The importing of audit data from each computer to the central data repository can be executed at any time and also be scheduled to take place on pre-defined days and times. You also have the flexibility to specify specific groups of audit events for import.

The audit events imported from the different platforms are stored in the CPA in a uniform format so they can be filtered, reviewed and analyzed as if they originated on the same computer.

Managing Audit Policy

The security events logged on each computer are determined by the audit policy. The CPA provides you with a convenient way of viewing and changing the audit policy for each computer and defining what kinds of events will be included in the audit.

Main Features

One GUI based Management Console for all Platforms:
A single management console for all platforms from which you can manage the consolidated log, and also access all the different nodes monitored.

Multiple Event Types:
Including system events, field-level data before and after change, user actions, policy deviations, TCP/IP events, SQL statements, object-specific events and more.

CPA Alert Center:
Set up alerts that can be triggered when selected events are identified, based on specific event parameters. Alert events can be set to trigger notifications by email, screen pop-up and by routing the message to Syslog by specifying the IP address of a Syslog host.

SOC:
A graphical tool for the analysis of security audit events, trends and incidents (see detail later, in this document).

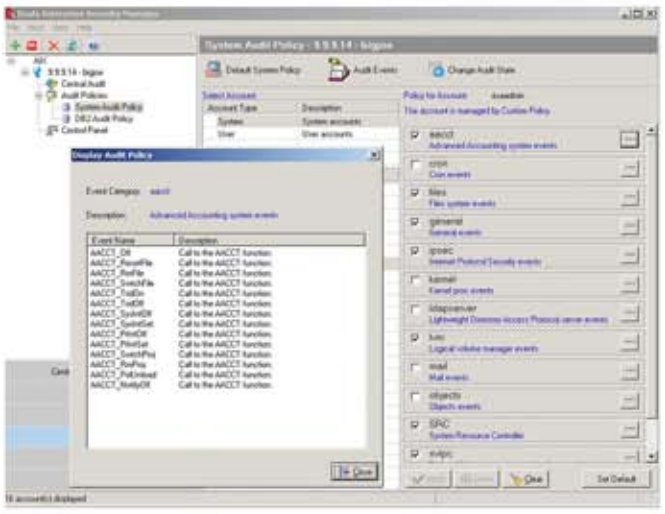
Audit Policy Management:
Define the types of events to be logged by your computers.

Compliance Tools:
Create template-based compliance policies with deviation checking and repair options. Ready-defined reports, alerts and templates for compliance.

Benefits

- Collection of diverse data formats into a uniform database
- Comprehensive monitoring in a multi-platform environment
- Efficiency. Audit data from different computers all in one place
- Powerful filtering to pinpoint events with specific characteristics
- Graphical analysis of security data statistics
- Correlation of seemingly disparate events into a uniform audit trail
- Rich comprehensive audit information for every event, showing exactly who did what, and when

AIX Audit Policy:



IBM i (AS400)

The CPA is tightly integrated with Enforcive/ Enterprise Security, the leading security and auditing product for the AS/400, allowing the import of audit events together with group and report definitions from the IBM i.

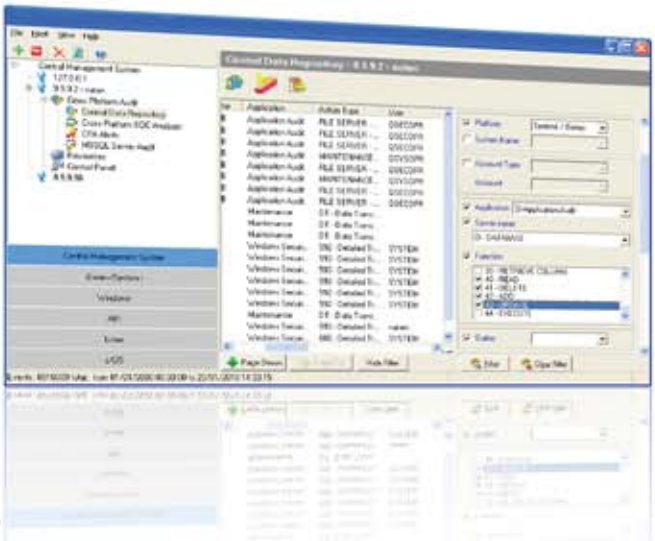
A large selection of IBM i system audit reports are provided, pre-defined and ready to run.

Audit data imported to the central data repository can originate in any of the monitored IBM i applications including:

- Application audit (like signon, TCP/IP, FTP and database reads)
- File audit (actual data changes on the field level value)
- Alerts (that have already been issued)
- View record data (information read)
- System audit events (such as system value changes, object management and authorization failures)
- Bsafe administrator audit (a trail of the actions taken by the Bsafe administrator)
- SQL statement audit
- IP filtering events
- Compliance deviations

Applications can be further filtered by event category, for example 'object authority' deviations only or 'database' application audit events, and even down to functions such as SQL read, add and/or delete.

Using the powerful custom application option, IBM i event reports can be produced for any combination of applications and event categories.

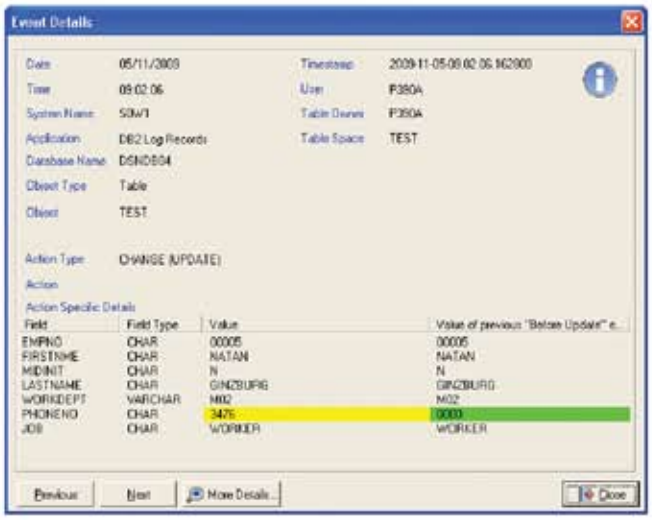


IBM z (Mainframe)

The CPA handles all mainframe system and data audit events from the leading security applications; RACF, Top Secret and SAFE and additionally, DB2, TCP/IP and SMF.

CPA SMF events for RACF and Top Secret are categorized into four categories: Security events (e.g. resource access, add volume, scratch), admin events (e.g. change password, change group profile), z-Unix (e.g. kill, link, open) and Kerberos events (e.g. grant ticket, PKI verify).

DB2 events collected by the CPA allow you to monitor data read and changed at the field level. In the case of changes, the before and after values of the changed fields are shown side by side.



Events from Enforcive's range of mainframe security products include SAFE/CICS security events such as program violations, user suspensions, SMF and non-SMF access via FTP and Telnet (e.g. logon, logoff, send, retrieve), and VSAM file operations (e.g. record open, close, append)

IBM z (Mainframe) continued

Shown below, is an example of one of the ready-defined MF reports included in the CPA. Other customizable standard report formats include: users who have submitted programs with another user's code, unauthorized access to system resources, unauthorized access to sensitive files and unused sensitive files.

MF Users at Multiple IP Addresses (PDF):

Enforcive

GENERAL CROSS PLATFORM AUDIT REPORT

Users which worked from multiple IP addresses-brief

Platform.....: System2 / Mainframe
System Name.....: *ALL
Application.....: 9 - SS-TCP/IP Application Audit
Service Name.....: *ALL
Account.....: *ALL
From Date.....: 5/15/2006 00:00:00
To Date.....: 5/15/2008 23:59:59
Sorted By.....: Date,Time
Report Style.....: BRIEF REPORT
Users which worked from multiple IP addresses on MF - TCP/IP Application Audit

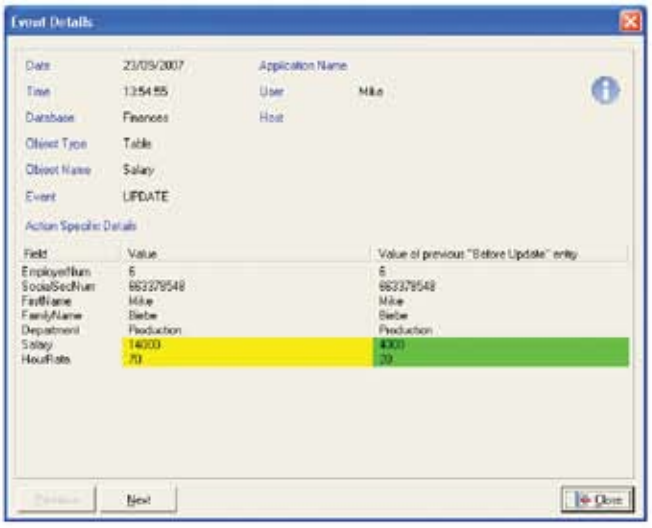
DATE	TIME	SYSTEM NAME	APPLICATION	USER	IP ADDRESS	DESCRIPTION
5/4/2007	14:07:44	MF-ADCS	MF Appl.Audi	ADCDA	9.9.9.200	FTP Server - USER LOGON
5/15/2007	15:30:25	MF-ADCS	MF Appl.Audi	ADCDA	9.9.9.67	FTP Server - USER LOGON
5/15/2007	15:28:48	MF-ADCS	MF Appl.Audi	ADCDMST	9.9.9.67	FTP Server - LIST FILE
10/18/2007	12:24:34	MF-ADCS	MF Appl.Audi	ADCDMST	9.9.9.159	TELNET
5/4/2007	14:08:10	MF-ADCS	MF Appl.Audi	IBMUSER	9.9.9.200	FTP Server - USER LOGON
5/8/2007	09:08:36	MF-ADCS	MF Appl.Audi	IBMUSER	9.9.9.67	FTP Server - USER LOGON
5/14/2007	13:45:28	MF-ADCS	MF Appl.Audi	HAITHAM	9.9.9.96	FTP Server - USER LOGON
5/14/2007	13:57:19	MF-ADCS	MF Appl.Audi	HAITHAM	9.9.9.67	FTP Server - USER LOGON
5/14/2007	13:59:55	MF-ADCS	MF Appl.Audi	HAITHAM	9.9.9.200	FTP Server - USER LOGON
11/15/2007	11:56:13	MF-ADCS	MF Appl.Audi	HAITHAM	9.9.9.106	FTP Server - GET DIRECTORY
10/16/2007	15:55:50	MF-ADCS	MF Appl.Audi	SYSADM	9.9.9.200	TELNET
10/16/2007	12:33:55	MF-ADCS	MF Appl.Audi	SYSADM	9.9.9.67	TELNET

The CPA shares the same GUI as Bsafe's leading CICS security products such as Enforcive/Security for CICS which allows complete access control by user for resources such as files, programs and transactions and provides field level protection and masking.

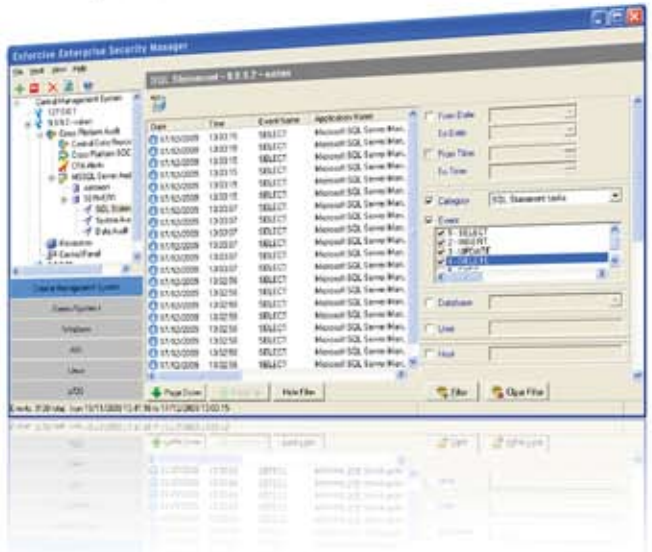
SQL Server

The CPA includes a host of powerful auditing functions for SQL server. Full-featured audit policy definition includes specification of categories of system audit events, SQL statements, databases, users and applications.

The CPA's SQL Server audit capabilities incorporate auditing directly on the database with three powerful audits: SQL Statement Audit that displays full-length SQL statement detail, System Audit showing activity such as login and database management events and Data Audit showing data changes in tables at the field level.



SQL Server audit data can be imported to the CPA's central data repository for integrated auditing alongside audit events from other platforms.



Windows

Comprehensive capturing of event and server logs, without the need for an agent on the end point. Including:

- Windows Event Logs: Security, DNS, system, application and others
- Microsoft DHCP log
- Microsoft ISA Server logs
- Microsoft IIS Web Server logs
- Microsoft Exchange Server log
- IBM Lotus Domino log

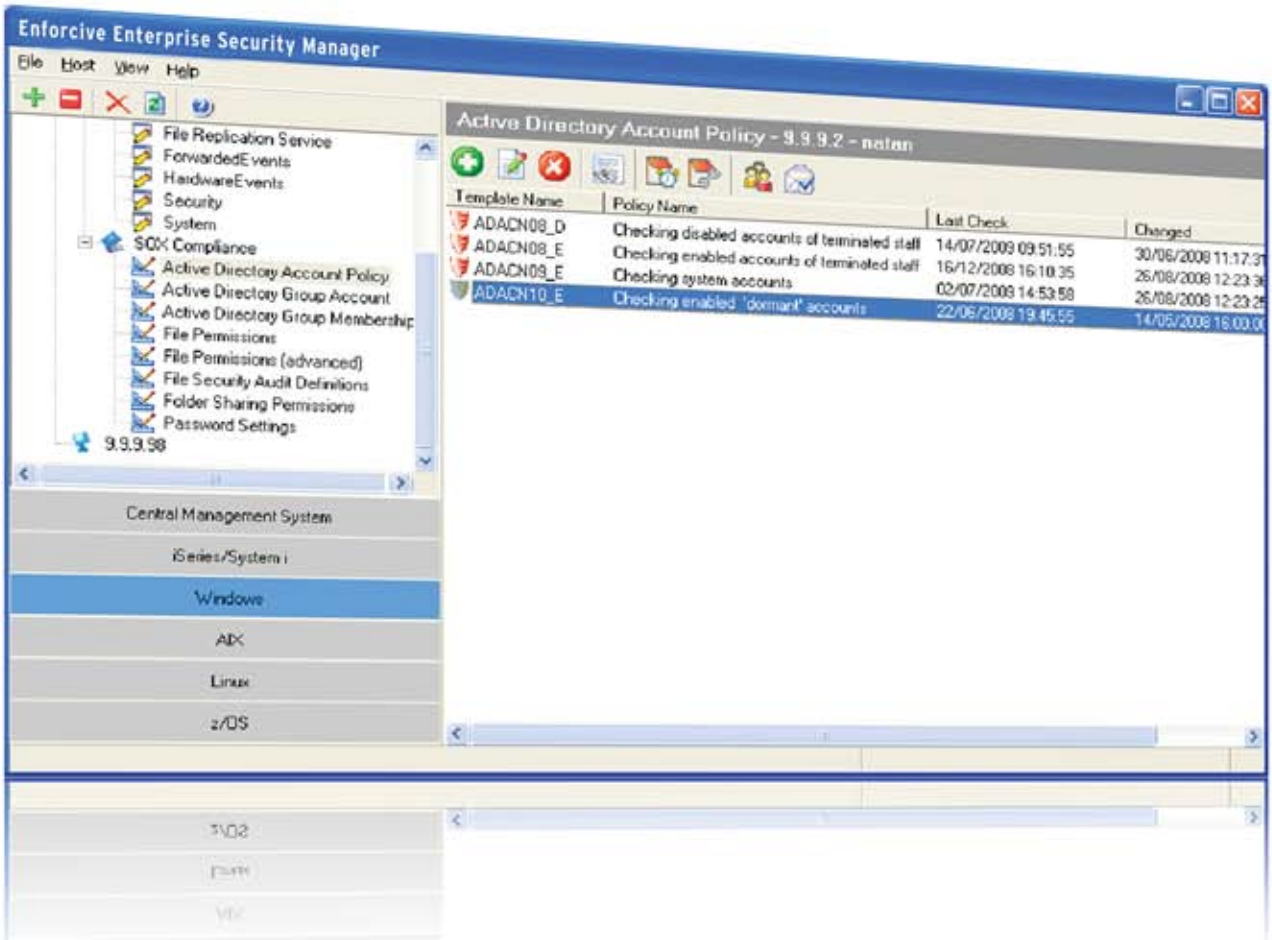
Parameters such as log size and overwrite policy can be changed directly on the host computer through the CPA interface.

Windows Domain Server and Active Directory - SOX Compliance

The Windows SOX Compliance Manager is a tool to create, document and maintain a clear security policy for Windows PCs and servers in your organization. The policy details are defined through templates specific to different categories pertaining to local PC and Windows Active Directory definitions. The template categories are:

- Active Directory Account Policy
- Active Directory Group Account
- Active Directory Group Membership
- File Permissions
- File Permissions (advanced)
- File Security Audit Definitions
- Folder Sharing Permissions
- Password Settings

The policy can be checked against the actual definitions in the system, producing a report showing any deviations from that policy.



AIX

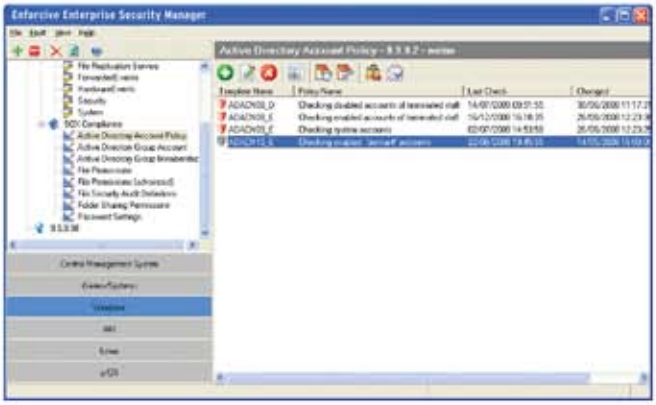
The CPA provides direct control of AIX audit policy with event logging including system and Unix DB2 events.

The main system audit events are categorized as follows:

1. System events (devices, time changes...)
2. Kernel procedure (execution, loads...)
3. Audit (audit policy changes)
4. File system (opens, reads, ownership...)
5. SVIPC system (msg reading, writing...)
6. TCP/IP user level (connect, data in/out...)
7. TCP/IP kernel level (bind, listen, receive...)
8. Unix commands (cron jobs, group changes...)

Plus 12 other event categories including shell, objects and secureway directory server.

Audit Events- Filtered Display:



The DB2 audit events are categorized as follows:

1. DB2 audit control (start, stop, config...)
2. Checking (function, object, transfer...)
3. Object maintenance (rename, alter...)
4. Security maintenance (grant, revoke...)
5. System admin (drop DB, start DB2...)
6. Validation (authentication, group mbr...)
7. SQL statements (connect, drop, execute...)

Linux

Linux events on all the main hardware platforms are handled in the CPA including: X86, X86 64-bit, IAX 64-bit, PPC, PPC 64-bit and system 390 / 390X).

Linux events are categorized as follows:

- Audit system commands (list, login, user...)
- User space trusted application messages (user command, user login, add group...)
- Messages internal to the audit daemon (config, start, abort...)
- Audit event messages (config change...)
- Kernel SE Linux use (AVC path, MAC sts)
- AppArmor (allowed, denied, error...)
- Kernal crypto events (first / last message)
- Kernal anomaly (append, promiscuous)
- User space anomaly and response (crypto fail, login failure, alert, kill proc...)
- User space LSPP (device allocation, role assign/ remove, user role change...)
- User space crypto (first / last messages)

The currently-defined audit policy for each machine can be viewed and changed through the CPA.

Oracle Server

Agentless monitoring of Oracle database events including inquiries, administrative operations on the database and actual data changes at the field level:

- SQL Statements
- Oracle System
- Oracle Admin
- Oracle Profiles/Users
- Oracle Procedures
- Data Audit (Before/After Changes)

Sun Solaris

Monitoring and logging of all system audit events for the Solaris operating system.

CPA Security Operations Center (SOC)

The Cross Platform Audit Security Operations Center (CPA SOC) makes the events consolidated in the CPA available through easy-to-configure dashboards. Events from across the enterprise can be combined, sorted and filtered into hundreds of different combinations of platform, application, IP address, user, global users, transaction status and date. The graphs are built dynamically by the user, selecting the sort parameter at each level.

Every component of the on-screen graphs can be expanded at the click of a mouse, to show the actual audit events behind the statistics and each event can be drilled down upon to show its detail including the name and value of each event parameter.

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

Report Scheduling and Exporting

The CPA's full power of multi-platform auditing is realized through its reports. They include the CPA correlation reports that automatically match events from different audit sources, the CPA special MF reports such as the unauthorized access to sensitive files report, and the CPA contents reports – for the display of database changes on different platforms.

Over 200 ready-defined reports complement the ability to create custom reports to meet most any requirement.

Create and run reports instantly on-screen, print them, email them or save them in different file formats such as PDF, Microsoft Word, Excel, text and more. Report runs can then be scheduled to run periodically by day, week or month.

Enforcive/Cross-Platform Consolidated Audit

The Enforcive/Cross-Platform Audit (CPA) offers both the administrator and auditor a comprehensive solution for enterprise auditing. It provides the convenience of auditing, investigating or just browsing your enterprise activity in a consolidated and easy to understand format, in a single application. It empowers administrators to analyze behavior on their systems to pinpoint activity that might otherwise have passed unnoticed and to investigate incidents quickly and thoroughly.

It gives auditors the freedom to look into the activity of all the organization's systems and to produce their own reports without IT department assistance.

The CPA saves time in preparing management reports and saves expensive server disk space, by offloading enterprise audit data onto a consolidated database.

This functionality contributes greatly towards fulfilling legal and industry regulatory compliance requirements for auditing such as view-data monitoring, as required by the Health Insurance Portability and Accountability Act (HIPAA), or maintaining an audit trail for several years, as required by Sarbanes-Oxley (SOX).

Cross Platform Audit Report (Examples)

DB2Log records report

Platform	System/Z / Mainframe
System Name	SYS1
Application	SZ DB2 Log Records
LIBRARY	*ALL
FILE NAME	*ALL
From Date	01/10/2009 07:00:00
To Date	31/10/2009 08:00:00

DATE	TIME	SYSTEM NAME	APPLICATION	STATUS	LIBRARY	FILE NAME	USER
20091023	131431	SYS1	SZ DB2 Log Records	UPDATE	SYSDB04	TEST	SYSUSR

Field Name	Value	Previous value
PHONENO	3478	9400

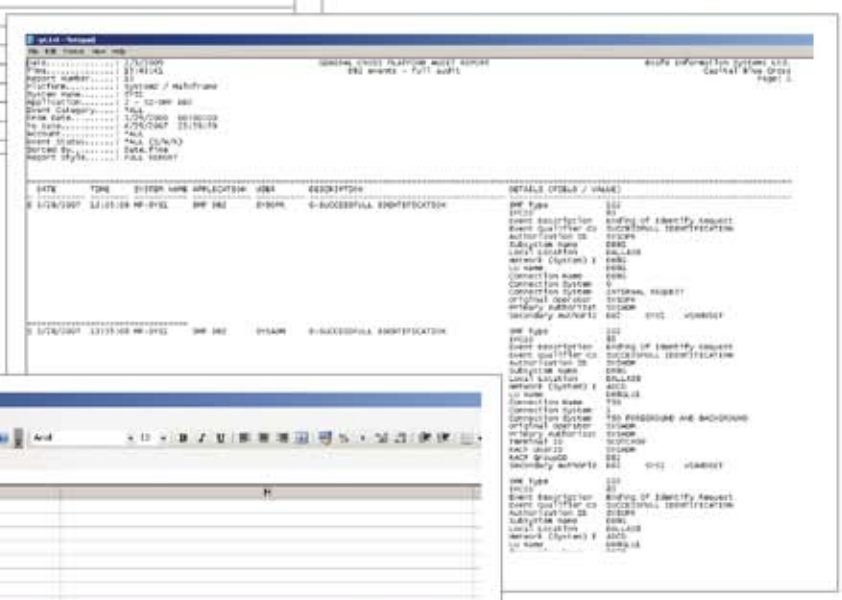
DATE	TIME	SYSTEM NAME	APPLICATION	STATUS	LIBRARY	FILE NAME	USER
20091023	131431	SYS1	SZ DB2 Log Records	UPDATE	SYSDB04	TEST	SYSUSR

Field Name	Value	Previous value
PHONENO	3478	9400

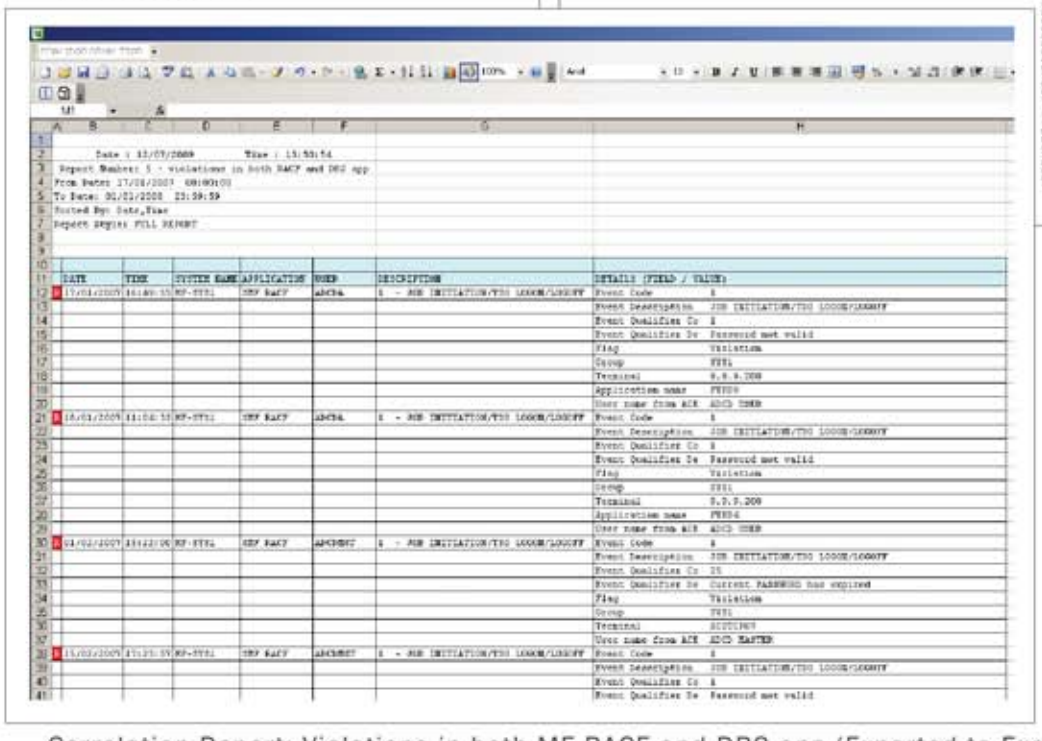
DATE	TIME	SYSTEM NAME	APPLICATION	STATUS	LIBRARY	FILE NAME	USER
20091023	135425	SYS1	SZ DB2 Log Records	DELETE	SYSDB04	TEST	SYSUSR

Field Name	Value
EMPNO	10001
FIRSTNME	NATHAN
MIDINIT	B
LASTNAME	KRUSHEVSKI
WORKDEPT	B02
PHONENO	3478
JOB	DESIGNER

MF DB2 Log Records
(Exported to HTML format)
Shows DB2 table field values before and after change



SMF DB2 Events Full Audit (exported to text file)
Full description of events showing user, connection, network, and result of action



	A	B	C	D	E	F	G	H
1								
2		Date : 11/07/2009		Time : 15:53:54				
3	Report Number: 5 - violations in both RACF and DB2 app							
4	From Date: 17/06/2009 08:00:00							
5	To Date: 30/11/2009 23:59:59							
6	Sorted By: Date,Time							
7	Report Style: FULL REPORT							
8								
9								
10								
11	DATE	TIME	SYSTEM NAME	APPLICATION	USER	DESCRIPTION	DETAILS (FIELD / VALUE)	
12	17/06/2009	16:40:55	MF-SYS1	DB2 RACF	ADMIN4	1 - JOB INITIATION/TSO LOGON/LOGOFF	Event Code	1
13							Event Description	JOB INITIATION/TSO LOGON/LOGOFF
14							Event Qualifier Co	0
15							Event Qualifier De	Password not valid
16							Flag	Violation
17							Group	SYS1
18							Terminal	9.9.9.200
19							Application name	FTSO4
20							User name from ACE	ADCD USER
21	18/06/2009	11:06:55	MF-SYS1	DB2 RACF	ADMIN4	1 - JOB INITIATION/TSO LOGON/LOGOFF	Event Code	1
22							Event Description	JOB INITIATION/TSO LOGON/LOGOFF
23							Event Qualifier Co	0
24							Event Qualifier De	Password not valid
25							Flag	Violation
26							Group	SYS1
27							Terminal	9.9.9.200
28							Application name	FTSO4
29							User name from ACE	ADCD USER
30	01/07/2009	13:12:05	MF-SYS1	DB2 RACF	ADMIN07	1 - JOB INITIATION/TSO LOGON/LOGOFF	Event Code	1
31							Event Description	JOB INITIATION/TSO LOGON/LOGOFF
32							Event Qualifier Co	25
33							Event Qualifier De	Current PASSWORD has expired
34							Flag	Violation
35							Group	SYS1
36							Terminal	SCOTCH07
37							User name from ACE	ADCD EASTED
38	15/07/2009	17:25:35	MF-SYS1	DB2 RACF	ADMIN07	1 - JOB INITIATION/TSO LOGON/LOGOFF	Event Code	1
39							Event Description	JOB INITIATION/TSO LOGON/LOGOFF
40							Event Qualifier Co	1
41							Event Qualifier De	Password not valid

Correlation Report: Violations in both MF RACF and DB2 app (Exported to Excel)
The correlation report automatically matches events from different selected audit sources.

About Our Services

Our Professional Services team combines years of security experience and expertise to add value to your IT team. Whether you are preparing for a single-site audit or a multifaceted enterprise implementation, our Professional Services enables you to:

- Avoid Regulatory Pitfalls by Applying Proven Best Practices
- Accelerate Compliance Implementation
- Step Up Security
- Mitigate Security Risks
- Enhance your IT Team's Value and Expertise
- Reduce Cost of Ownership

For more information:

USA	Tel: 877-237-8024 (toll free) salesusa@enforcive.com
Canada	Tel: 905-943-4042
Europe & R.O.W.	Tel: (+972) 9-9610400 info-eu@enforcive.com

Enforcive™
Data respected.