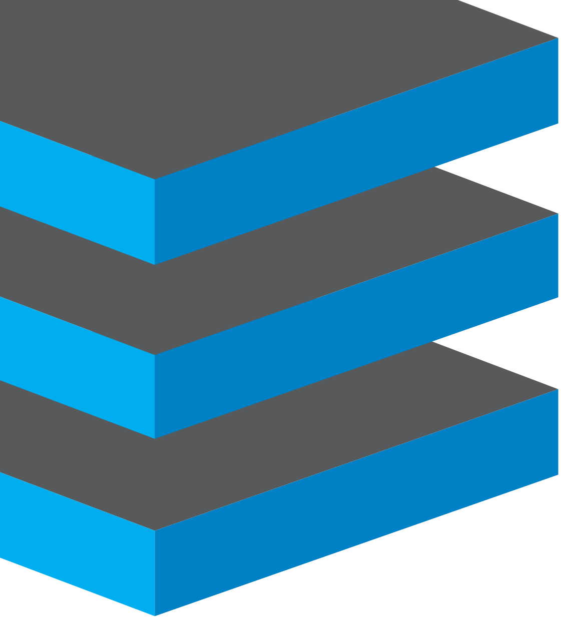
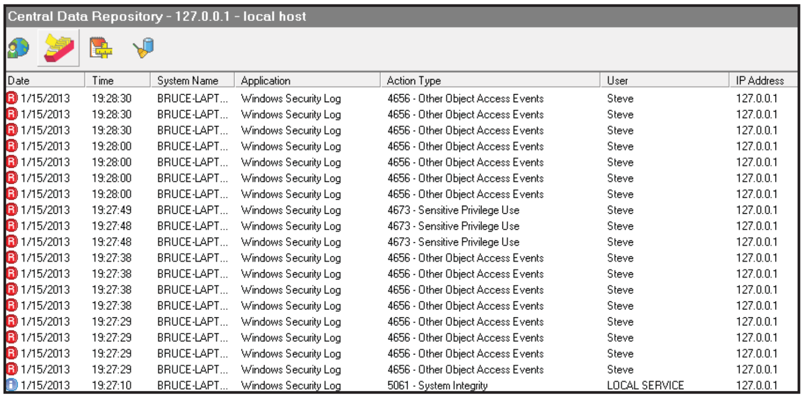


February 2013

Datasheet:
Enforcive™/Cross-Platform Audit
for Windows

The Cross-Platform Audit (CPA) is an enterprise-wide Compliance Event Monitor, built on the principles of database activity monitoring and log management, but focused on providing practical and relevant information about an organization's critical systems. The CPA analyzes the raw transactional data from user activity and, through a variety of filtering, reporting and dashboard tools, correlates seemingly unconnected events into a clear and uniform audit trail of critical information.

CPA will collect all of the critical security events from all of your important platforms and databases, filter them, then store them in a Central Data Repository. Once this important information is in CPA it can then be analyzed statistically, viewed on-screen, reacted to (if selected criteria are satisfied), and administrator and auditors reports produced.



Central Data Repository - 127.0.0.1 - local host

Date	Time	System Name	Application	Action Type	User	IP Address
R 1/15/2013	19:28:30	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:28:30	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:28:30	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:28:00	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:28:00	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:28:00	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:28:00	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:27:49	BRUCE-LAPT...	Windows Security Log	4673 - Sensitive Privilege Use	Steve	127.0.0.1
R 1/15/2013	19:27:48	BRUCE-LAPT...	Windows Security Log	4673 - Sensitive Privilege Use	Steve	127.0.0.1
R 1/15/2013	19:27:48	BRUCE-LAPT...	Windows Security Log	4673 - Sensitive Privilege Use	Steve	127.0.0.1
R 1/15/2013	19:27:38	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:27:38	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:27:38	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:27:38	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:27:29	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:27:29	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:27:29	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
R 1/15/2013	19:27:29	BRUCE-LAPT...	Windows Security Log	4656 - Other Object Access Events	Steve	127.0.0.1
i 1/15/2013	19:27:10	BRUCE-LAPT...	Windows Security Log	5061 - System Integrity	LOCAL SERVICE	127.0.0.1

Figure 1: Windows Event Logs in the Central Data Repository

Windows Log Monitoring using Cross-Platform Audit:

Event Collection Policy. In order to minimize the data collected CPA provides a way to define the level of granularity of collected data. The CPA administrator can select which Windows event categories to collect, and even which event types within those categories.

Windows Events. Relevant entries can be collected from the Security, System, Application and DNS event logs.

Windows Server Logs. Depending on your configuration CPA may also be able to collect logs relating to DHCP, ISA Server, IIS Web Server, Exchange Server and Lotus Domino.

SQL Server. Windows machines running Microsoft SQL Server will also benefit by CPA's ability to monitor system actions and data changes at the record level. Field level data changes are presented in a way to highlight the 'before' and 'after' values. **NOTE:** For more details of SQL Server monitoring a separate CPA Data Sheet is available.

Agentless. No need to install software on the Windows Servers to be monitored. The CPA configuration process simply links to the Windows Server; saving time and manpower. An added benefit is that the overall architecture is more robust due to the fact that there are fewer components.

Windows event log monitoring is available for:

Windows Server – 2000 / 2003 / 2008
Windows XP
Windows 7 / 8

Please note that as there are a wide variety of releases, service packs and configuration options for the above Operating Systems, not all CPA functionality will apply to all releases. We recommend you discuss your architecture and auditing requirements in detail with a CPA specialist.

February 2013

Features of Cross-Platform Audit:

A Single GUI Management Console. The same intuitive and user-friendly interface can be utilized for monitoring areas such as log records, compliance deviations, critical database changes and SQL commands. Administrators can view events and filter them on screen without the need for additional applications or programming. Filtering and sorting can be done by date and time, user, event status, IP address, application event type and other source specific selection criteria.

Correlate Audit Information from Multiple Platforms and Partitions. With the CPA, you can create logical identities, called Global Users, to cross reference all of the different logon IDs and aliases for a person. The resulting filtered views give a simple way to interrogate real user activity wherever they have been.

Dynamic Dashboards. Graphs can be used to identify trends and pinpoint behavior by aggregating the system activity. The dashboards can be used as a launching point for drill downs and filtered investigations.

Customizable Reports. The CPA's full power is realized through its reports. Over 200 ready-to-run reports are included, along with the ability to create custom reports to meet your organization's unique needs. Reporting can be scheduled and output produced in various file formats, in addition distribution by email is available. Windows specific reporting is available related to:

- Sarbanes Oxley compliance
- PCI DSS Compliance
- Correlation of activities; for example all activities performed by a user across many systems
- Login auditing
- General events; for example "changes to security policy"

Offload Audit Data to Dedicated Database. After transferring your audit data to the CPA Central Data Repository, the original logs can be archived and purged from the source system, freeing up valuable storage space.

SYSLOG integration. Any item of audit information collected by the CPA can be sent directly to a SYSLOG server, with the option of SYSLOG NG encryption.

Alerts. Real time alerts can be defined for the critical events which may occur on the source systems, including user maintenance and unexpected logon attempts.

Administrator Roles. Many levels of CPA Administrator can be defined so that separation of duties can be enforced.

Regulatory Compliance. Most current regulations call for the monitoring of critical event activities across the enterprise. CPA can fulfill those requirements without imposing unrealistic administrative workloads on an organization.

Other Platforms

The CPA is a multi-platform product that can connect to many different environments. In addition to the above Windows Servers CPA can collect logs from IBM mainframe, IBM i, AIX, Linux, selected databases and more.

About Enforcive, Inc.

Enforcive provides comprehensive security solutions to help businesses reduce workloads, satisfy auditors and improve responsiveness to security threats. For over two decades, Enforcive has been providing solutions within mission critical environments using platforms including IBM i, System z, AIX, Linux and Windows. Our expertise and commitment to innovation enables us to offer the best of breed solutions to our customers.