Enforcive™
Data respected.

Workers
INFORMÁTICA

Enforcive Enterprise Security
CPA para MS Windows

CPA – O QUE É?

O **CPA (Cross Platform Audit)** é uma plataforma abrangente para o gerenciamento de logs e de monitoração de dados críticos para o ambiente MS Windows. Permite a coleta de uma vasta gama de eventos de auditoria de segurança e do sistema, a análise e a consolidação deles com eventos de outros computadores de uma organização e, deste modo, transformar tais eventos em informações úteis, o que é vital para um processo correto de tomada de decisões.

BENEFÍCIOS EXCLUSIVOS PARA O WINDOWS

1. **Gerenciador de IDs**
   Controla a política de autorizações do administrador a nível organizacional. Permite a definição de níveis comuns de privilégios do administrador entre os ambientes IBM i Access for Windows e Active Directory, bem como, a criação de senhas comuns entre as plataformas.

2. **Funcionamento sem Agentes (Agentless)**
   Não há necessidade de instalação de software nas estações monitoradas.

3. **Auditoria de Dados MS SQL**
   Permite a visualização dos campos de dados antes e depois da adição, atualização e exclusão dos registros. Alterações de valores dos campos são destacadas através do uso de cores diferentes.

4. **Conformidade com o Active Directory**
   Verifica a segurança do sistema, de acordo com a política definida, e produz relatórios sobre os desvios encontrados.

5. **Política de Auditoria**
   Define os tipos de eventos que devem ser gravados no log.

Enforcive™
Data respected.

Workers
INFORMÁTICA

BENEFÍCIOS ADICIONAIS

Exibição Fácil e Clara da Auditoria de Segurança.

Trilha de auditoria intuitiva e amigável de todos os tipos de log: eventos, servidor ISA, DHCP e servidores web IIS. Os eventos são decompostos em função dos parâmetros definidos, facilitando a compreensão de cada evento.

Gerenciamento de Partições

Recuperação eficiente e rápida das informações sem os complicadores do gerenciamento manual.

Critérios de Filtragem Detalhada

O auditor de segurança pode visualizar eventos de segurança on-line e filtrá-los na tela, sem a necessidade de aplicativo ou programação adicional. A filtragem pode ser efetuada por data e horário, tipo de conta, usuário, status do evento, endereço IP e tipo de evento de aplicativo. Este último pode ser filtrado em níveis granulares, tais como, atualizações de registros, downloads de FTP, senhas inválidas e alterações de usuário.

Painel de Instrumentos Dinâmico

Gráficos podem ser gerados para observar as tendências e identificar o comportamento da atividade do sistema. Eventos oriundos de toda a empresa podem ser combinados, classificados e filtrados, gerando centenas de combinações diferentes por plataforma, aplicação, endereço IP, usuário, status e data da transação.

Os painéis incluem visões estatísticas e ao longo do tempo dos eventos de auditoria. Os gráficos e sumários podem ser exibidos na tela, impressos, enviados por e-mail e armazenados em vários formatos, incluindo PDF e HTML compatível com o MS Office.

Exportação dos Dados de Auditoria para Database Dedicado

Após a transferência dos dados de auditoria para um banco de dados em um servidor MS SQL, os logs originais podem ser deletados do sistema, liberando assim um valioso espaço em disco. Uma vez importados para o CPA (Cross-Platform Audit), as informações podem ser visualizadas e analisadas a partir de um PC. As transferências podem ser agendadas para ocorrerem automaticamente.

Gerador de Relatórios

Tem a capacidade de exportar relatórios para o MS Excel, PDF e outros formatos. A geração de relatórios pode ser agendada periodicamente com frequência diária, semanal ou mensal, proporcionando uma vista informativa do sistema.

Consolidação de Dados de Segurança de Múltiplos Sistemas

Os dados de auditoria de segurança provenientes de qualquer número de sistemas podem ser consolidados em um único lugar. Usuários lógicos, chamados de usuários IDM, podem ser criados para auditar a atividade de um usuário com diferentes identificações de logon. O usuário IDM não requer uma identidade pré-definida como no caso da implementação de sign-on único.

SYSLOG

Os dados do sistema coletados pelo CPA podem ser enviados diretamente para um servidor de SYSLOG, com opção de criptografia SYSLOG NG, ou mantidos e gerenciados no database do CPA.

OUTRAS PLATAFORMAS

O CPA é um produto multi-plataforma que pode se conectar a diversos ambientes, tais como, mainframe IBM, IBM i, MS Windows, AIX, Linux, Oracle, MS SQL Server e SAP.