Enforcive™
Data respected.

Workers
INFORMÁTICA

CPA - Monitoração e auditoria de segurança

Uma única solução para múltiplas plataformas

Monitoração Real-Time

Central de Alertas

Evidências de Antes e Depois

Relatórios Personalizados

Muitos são os desafios que as empresas enfrentam e deverão superar com gerenciamento de dados de auditoria coletados de diferentes sistemas e plataformas em seu extenso ambiente de TI.

Aumentando o tamanho dos desafios, estão as exigências para manterem-se aderentes às políticas organizacionais e normas regulatórias tais como SOX, PCI, HIPAA, etc.

A Enforcive desenvolveu o CPA – "Cross Platform Audit", software que **trata de questões práticas da segurança organizacional**, independente do tamanho da empresa, **em uma única solução, simples e fácil de usar.**

Através da coleta e consolidação de dados dos sistemas corporativos, tais como Windows, Mainframe, IBM iSeries, DB2 (todos as plataformas), AIX, UNIX, Linux, Sybase, Solaris, SQL, Oracle e Progress, possibilita aderência às políticas de segurança definidas.

SOLUÇÃO SEM O CROSS-PLATFORM AUDIT™ (CPA)

1. Coleta e armazenamento de milhões de logs de auditoria produzidos por várias plataformas através de várias ferramentas específicas.
2. Muitas horas necessárias para análise dos dados coletados.

HAVENDO FALHA NO PROCESSO, PODE CAUSAR ATRASOS NA GERAÇÃO DE DADOS FORENSES OU COMPROMETER A PERFORMANCE DOS SISTEMAS.

SOLUÇÃO COM O CROSS-PLATFORM AUDIT™ (CPA)

1. Monitoração das atividades das bases de dados.
2. Gerência de logs, focando no fornecimento de informações práticas e relevantes dos sistemas críticos da empresa.
3. Consolidação de eventos de auditoria específicos de diversas plataformas em uma única console.
4. Apresentação intuitiva dos eventos, oferecendo recursos poderosos aos auditores e administradores de sistemas.

FÁCIL IDENTIFICAÇÃO DE PROBLEMAS CRÍTICOS QUE PODEM IMPACTAR O NEGÓCIO, EVITANDO PERDAS FINANCEIRAS E DE TEMPO DE PROFISSIONAIS.

Workers Informática | Sede: Avenida Presidente Wilson, 231 - 14º andar. Centro - Rio de Janeiro / RJ - CEP: 20030-905
Tel: 21 3554-6652 • E-mail: info@workers.com.br • Site: www.workers.com.br

Enforcive™
Data respected.

Workers
INFORMÁTICA

[VANTAGENS E BENEFÍCIOS]

EFICIÊNCIA
Console central para análise e depuração de informações críticas de auditoria.

OBJETIVIDADE
Somente eventos críticos selecionados serão registrados no repositório central de dados.

SIMPLICIDADE
A diversidade de dados coletados e armazenados em um formato padronizado.

VISIBILIDADE
Análise gráfica estatística dos dados de segurança.

FLEXIBILIDADE
Filtragem baseada em multicritérios ajuda a apontar eventos com características específicas.

UNIFORMIDADE
Correlação de similaridade dispara eventos para análise.

GRANULARIDADE
As alterações mais recentes de dados são destacadas para dar foco nas depurações de ocorrências.

MONITORAÇÃO REAL-TIME

A configuração e agendamento da extração de dados utiliza uma interface amigável e intuitiva configurada em minutos, permitindo investigar e responder ameaças em tempo real.

O **CPA** coleta itens críticos e os consolida num repositório central de eventos. Os dados resultantes podem ser apurados online ou através de relatórios, provendo informações significativas para os membros de diversas equipes da empresa que atuam nos projetos de auditoria e conformidade.

O **CPA** inclui um **Centro de Operações de Segurança** (SOC) que é um conjunto de telas customizáveis que proporcionam um sumário de alto nível das atividades através da empresa. As áreas de segurança utilizam esse recurso para iniciar um ponto de análise sobre o repositório central de dados.

Os eventos coletados nas diversas origens são filtrados e organizados em diferentes combinações, baseados na data, endereço IP, usuário e status da transação.

Gráficos são construídos dinamicamente através de uma fácil seleção de parâmetros.

O **CPA** também identifica atividades por usuário, "linkando" ao mesmo tempo todos os logons, rastreando cada passo dado (onde ele foi e o que ele fez).

Cada componente visualizado nos gráficos do SOC pode exibir eventos de auditoria mais recentes sobre as estatísticas.

Cada evento auditado pode exibir detalhes, como imagens do antes e depois, destacando o que é relevante.

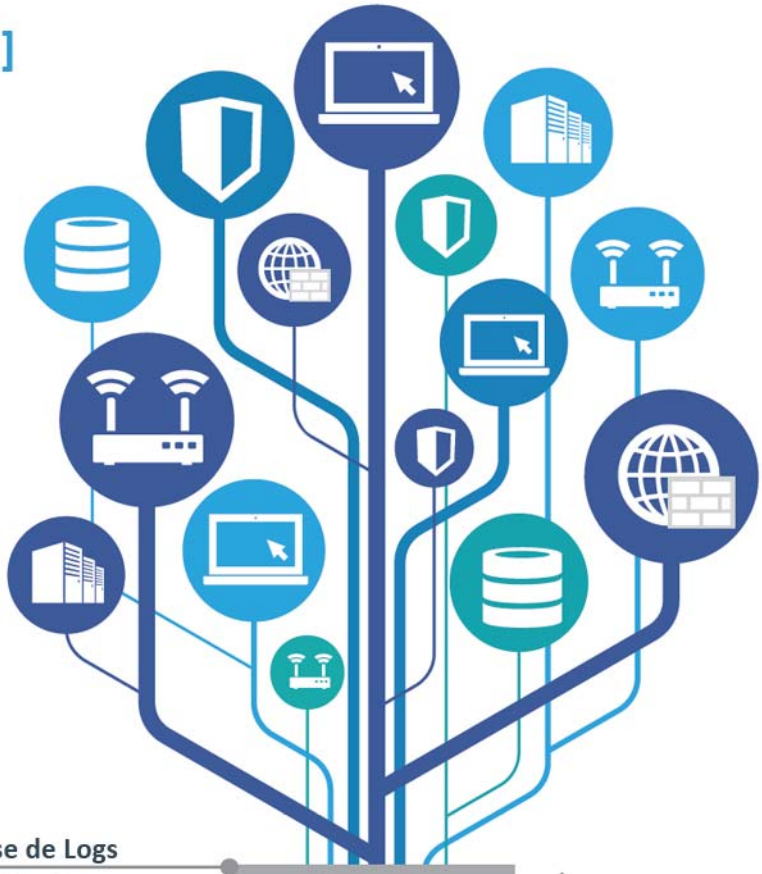
Os gráficos e os sumários podem ser exibidos na tela, impressos, encaminhados via e-mail ou armazenados em uma variedade de formatos.

Workers Informática | Sede: Avenida Presidente Wilson, 231 - 14º andar. Centro - Rio de Janeiro / RJ - CEP: 20030-905
Tel: 21 3554-6652 • E-mail: info@workers.com.br • Site: www.workers.com.br

Enforcive™
Data respected.

Workers
INFORMÁTICA

[ARQUITETURA CPA]



Análise de Logs
- Consolidação
- Classificação
- Correlação

Gerenciador de Eventos
- Monitoração Real-Time
- Central de Alertas
- Evidências de "Antes" e "Depois"

Relatórios
- Ditribuição Agendada
- Relatórios de Conformidade
- Customização de Relatórios

Análise de Logs

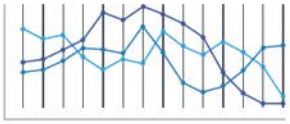
Gerenciador de Eventos

Relatórios

Repositório Central

CENTRO DE OPERAÇÕES DE SEGURANÇA

Tipo de Evento Breakdown



Visualização das Atividades Atuais

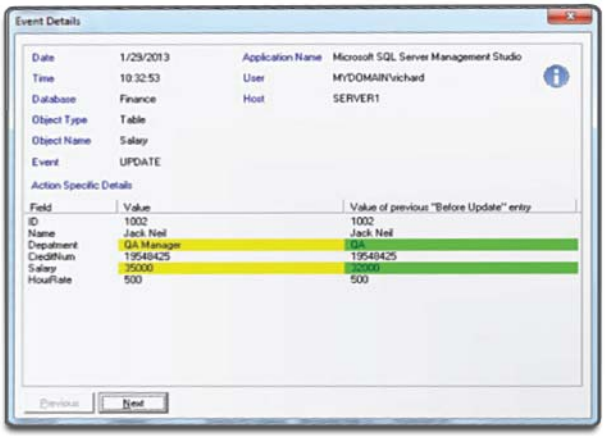
Painéis Aviso/Rejeitado

Workers Informática | Sede: Avenida Presidente Wilson, 231 - 14º andar. Centro - Rio de Janeiro / RJ - CEP: 20030-905
Tel: 21 3554-6652 • E-mail: info@workers.com.br • Site: www.workers.com.br

Enforcive™
Data respected.

Workers
INFORMÁTICA

EVIDÊNCIAS DE ALTERAÇÕES DE ANTES & DEPOIS



Além dos filtros e dos sumários de dados, os administradores se beneficiam da capacidade de análise através do highlight do "Antes" e "Depois" dos eventos alterados e registrados pela ferramenta.

Sempre que possível, os dados para análise são apresentados em um formato que independe da tecnologia específica que o gerou, evitando assim a necessidade do usuário ser um especialista em todas as plataformas e aplicações.

CENTRAL DE ALERTAS

As áreas de segurança podem definir parâmetros específicos para serem monitorados, afim de que qualquer evento que se relacione a um critério particular gere um alerta. Essas notificações poderão ser enviadas por e-mail, ou telas de pop-up, ou ainda serem roteadas para Syslog.

Exemplos de alertas definidos pelo Administrador:

- **WINDOWS** – Alteração das políticas de auditoria
- **MAINFRAME DB2** – Falha na autorização do Database
- **MSSQL** – Uso de Delete no SQL

RELATORIOS PERSONALIZADOS

Os mais de 200 formulários de relatórios para múltiplas plataformas disponíveis na solução CPA garantem a capacidade de reduzir tempo e esforço aos administradores na geração e utilização dos relatórios necessários ao ambiente.

Esses relatórios ainda podem ser customizados de acordo com os requisitos específicos da empresa, incluindo a exibição do nome da empresa/departamento e também de logomarcas.

Os relatórios podem ser criados e executados em 'real-time', bem como visualizados online, impressos ou exportados para uma variedade de formatos de arquivos.

Uma vez criado o relatório, o CPA pode agendar sua execução em intervalos de tempo e automaticamemte distribuí-lo aos usuários previamente definidos.

Workers Informática | Sede: Avenida Presidente Wilson, 231 - 14º andar. Centro - Rio de Janeiro / RJ - CEP: 20030-905
Tel: 21 3554-6652 • E-mail: info@workers.com.br • Site: www.workers.com.br

Enforcive™
Data respected.

Workers
INFORMÁTICA

Os alertas disponíveis incluem:

- **WINDOWS**
  Tentativas Falhas de Login
- **WINDOWS**
  Contas Desativadas
- **SQL SERVER**
  Comandos Executados
- **SQL SERVER**
  Auditoria de Dados
- **LINUX**
  Falhas em Programas
- **AIX**
  Objetos Excluídos
- **IBM i**
  Falhas de Autorização
- **IBM i**
  Login de Acesso a Rede
- **MAINFRAME**
  Alterações de campo no DB2 “Antes” e “Depois”
- **MAINFRAME**
  Violações de RACF e DB2
- **ORACLE**
  Falhas de Login
- **ORACLE**
  Falhas de Criação de Index

SISTEMAS SUPORTADOS

AIX*
- System Audit

Windows
- Windows Event Logs: Security, Application, DNS and more
- Windows Active Directory Compliance
- ISA Server Logs
- DHCP Logs
- IIS Web Server Logs
- Exchange Server

Solaris*
- System Audit

Linux*
- System Audit X86
- System Audit 86_64
- System Audit IA64
- System Audit PPC64
- System Audit PPC
- System Audit S390X
- System Audit S390

SYSLOG Sources
- Routers
- Firewalls
- Antivirus
- Other SYSLOG Senders

Microsoft SQL Server
- SQL Statements
- SQL System Audit
- SQL Data Audit

Microsoft SQL Server
- SQL Statements
- SQL System Audit
- SQL Data Audit

ORACLE
- SQL Statements
- Oracle System
- Oracle Admin
- Oracle Profilles/Users
- Oracle Procedures
- Data Audit

DB2 LUW
- System Audit

MySQL
- Audit
- Connect
- Query
- Prepare
- Execute
- Shutdown
- Quit
- No Audit
- Init DB
- Other

Progress | Open Edge
- System Audit
- Data Audit

SYBASE
- System Audit

IBM i*
- System Audit
- File and Field Audit
- Alerts
- Application Audit
- SQL Statement
- IP Filter
- Compliance
- Message Queue
- History Log
- View Data

DB2-z/OS*
- DB2 SMF- MF
- DB2 LOG (Data Audit)- MF
- DB2 CICS (SQL Data Campture)- MF
- DB2 BATCH (SQL Data Capture)- MF
- DB2 System Audit- i, AIX, LUW
- DB2 SQL Statement Audit- i, AIX, LUW

z/OS*
- SMF TELNET
- SMF FTP
- SMF VSAM
- SMF RACF
- TCP/IP Application Audit (FTP and Telnet)
- DB2 SMF
- DB2 LOG (Data Audit)
- DB2 CICS (SQL Data Capture)
- DB2 BATCH (SQL Data Capture)

**** Requer Agente***

Workers Informática | Sede: Avenida Presidente Wilson, 231 - 14º andar. Centro - Rio de Janeiro / RJ - CEP: 20030-905
Tel: 21 3554-6652 • E-mail: info@workers.com.br • Site: www.workers.com.br