Q Software para JD Edwards EnterpriseOne 9.x

Audit Manager

Analise o acesso e Implemente a Segregação de Funções: Controle seus Principais Riscos de Fraude

ATÉ QUE PONTO O SEU SISTEMA É SEGURO?

Se a sua principal preocupação é evitar atividades fraudulentas ou satisfazer as demandas de seus auditores, a capacidade de aplicar e manter controles efetivos de Segregação de Funções (SoD) é uma ferramenta importante para ter em seu kit de ferramentas.

Infelizmente, o JD Edwards EnterpriseOne nativo não contém nenhuma funcionalidade para ajudar você a gerenciar a SoD ou a facilitar o relatório de conformidade. Muitas pessoas tentam gerenciá-lo usando planilhas e verificações manuais, mas além de serem complicadas e demoradas, esta abordagem não é confiável. As planilhas são notoriamente propensas a erros; é difícil aplicar o controle de versão; e quaisquer alterações feitas nas planilhas não podem ser auditadas.

GERENCIAMENTO DE SOD INTEGRADO

O Gerenciador de Auditoria permite que você mantenha um modelo de SoD no seu ambiente JD Edwards EnterpriseOne e execute verificações regulares para identificar os usuários que têm permissões de acesso que os habilitariam a violar sua política de SoD. Onde os conflitos de SoD forem encontrados, você pode pesquisar para investigar e corrigir os problemas, ou, se apropriado, aplicar controles de mitigação totalmente documentados.

COMO ISTO FUNCIONA

Audit Manager compreende:

- Programas e tabelas personalizados mantidas no seu ambiente JD Edwards, que permitem que você a mantenha as suas regras de SoD
- Um modelo inicial de SoD da regra "Risco Crítico", conforme recomendado por auditores experientes, que você pode adaptar ou estender para refletir a sua própria política de SoD
- Um poderoso mecanismo de varredura que analisa a sua tabela de segurança em tempo real F00950 e armazena os resultados em tabelas personalizadas
- Um conjunto de consultas e relatórios padrão
- Com resultados todos armazenados em tabelas dentro do seu ambiente JD Edwards, você também pode criar seus próprios relatórios usando o Relatório de Insight para a Q Software ou sua solução de relatório de terceiros preferida

BENEFÍCIOS

- **O gerenciamento automatizado de Segregação de Funções economiza tempo e melhora a precisão**
- **Reduz o risco de fraude ou erro dispendioso devido ao acesso inapropriado**
- **As regras pré-configuradas aceleram o processo de implementação**
- **Controles de mitigação eliminam muitos falsos positivos**
- **Acesso rápido às informações que você e seus auditores precisam**
- **Ajuda a manter o seu sistema em boa forma e reduz o tempo necessário para se preparar para auditorias**

PRINCIPAIS CARACTERÍSTICAS

Integrado no seu ambiente JD Edwards

Todos os processos e arquivos usados e produzidos pelo Gerenciador de Auditoria são mantidos de forma segura em seu ambiente ERP, que tem benefícios importantes:

- O acesso aos programas de manutenção de regras de SoD e suas próprias regras podem ser restritas a usuários autorizados
- Todas as alterações feitas são totalmente auditáveis
- As regras de SoD e os resultados de análise produzidos pelo mecanismo de verificação são armazenados como tabelas personalizadas e podem ser reportadas ao usar as nossas ferramentas ou sua solução de relatório preferida
- Nunca há a necessidade de procurar a planilha correta ou de se preocupar com o controle de versão

Então você pode ter certeza de que seus relatórios são sempre baseados em informações precisas e atuais ao invés de planilhas exportadas.

Quatro tipos de regras de SoD

Nós reconhecemos que as organizações diferem amplamente nas suas necessidades de conformidade. Audit Manager oferece quatro tipos diferentes de regras para que seus controles possam ser tão detalhados quanto necessário para satisfazer os requisitos específicos de seus auditores:

Nível de Função

O nível mais alto da regra permite que você estipule que combinações de funções especificas não devem ser atribuídas ao mesmo usuário.

Nível de Serviço

Permite que você agrupe uma série de programas em conjunto como uma Função e, em seguida, defina regras que estipulam que combinações específicas de Funções não devem ser atribuídas ao mesmo usuário (por exemplo, registro de ordem de venda / registro de ordem de compra).

Nível de Objeto

Permite a você especificar programas individuais que sempre devem ser segregados.

Objeto Crítico

Estes tipos de regras permitem que você monitore o acesso a Objetos Críticos - programas de alto risco que, mesmo usados dentro de seus limites, permitem que um usuário cometa uma fraude (por exemplo, acesso à conta bancária ou Next Numbers).

Quando usado em conjunto com o Gerenciador de Segurança Pro ou o Gerenciador de Segurança Expresso, as Regras de SoD podem ser usadas para verificar de forma proativa os conflitos antes de serem incorporados à sua segurança em tempo real.

Regras pré-configuradas

Para ajudar a acelerar a implementação, fornecemos regras de Segregação de Funções pré-configuradas, conforme recomendado por auditores experientes, as quais você pode adaptar ou estender para refletir sua própria política de SoD.

Mitigações Totalmente Documentadas

Para atender às circunstâncias em que você precisa conceder permissões que transgridem sua política de SoD, por exemplo, quando a equipe precisa assumir responsabilidades adicionais para cobrir férias, doença ou outra ausência temporária, Audit Manager permite que você aplique mitigações com datas de início e término efetivas . As mitigações atuais serão levadas em consideração quando você executar as análises de SoD, reduzindo a ocorrência de falsos positivos e o desperdício de tempo investigando-os.

Os detalhes das mitigações são documentados para que você e seu auditor possam ver quem os aplicou, por que e por quanto tempo eles permaneceram em vigor.

Consultas e Relatórios

Com o JD Edwards EnterpriseOne nativo, é preciso muito mais esforço do que deveria para responder a perguntas como:

- Quem pode acessar um dado programa e com quais permissões?
- Quais programas um usuário específico pode acessar e como eles chegam lá?

Audit Manager inclui 24 relatórios padrão para fornecer respostas rápidas às questões comuns que os auditores fazem.

Por exemplo, as perguntas dos nossos Aplicativos de Segurança de Efeito Prático e da Segurança de Linha de Efeito Prático permitem que você descubra rapidamente se um usuário pode acessar aplicativos ou itens de dados específicos e em que nível a segurança prevalecente é mantida.

Eles exibem as configurações de segurança aplicáveis em todos os níveis (ou seja, * público, função e usuário) e calculam o resultado final para mostrar se o usuário pode acessar o item especificado ou não.

Onde é necessário um relatório mais flexível ou personalizado, você pode criar seus próprios relatórios usando o Relatório de Insight para a Q Software ou a sua solução de relatório de terceiros preferida.

Você pode manter as análises históricas, bem como as atuais, permitindo que você monitore as tendências ao longo do tempo para monitorar as melhorias ou detectar um aumento nas violações que talvez necessitem de uma investigação.

Q Software

US Headquarters
5889 Greenwood Plaza Blvd, Suite 401
Greenwood Village, CO 80111
Tel: 720-390-7970

UK & EMEA Headquarters
Connect House, Kingston Road
Leatherhead KT22 7LT United Kingdom
Tel: +44 (0)1372 700850

ORACLE Validated Integration
JD Edwards EnterpriseOne

ORACLE Gold Partner

www.qsoftware.com