White Paper

Gerenciamento de informações e governança
Segurança

Solução Micro Focus Data Access Governance

Tradicionalmente, os principais produtos de Gerenciamento de Identidade e Acesso (IAM) e de Governança e Administração de Identidade (IGA) têm focado no gerenciamento do acesso aos dados dos aplicativos e dos dados hospedados e controlados por esses aplicativos. Mas e quanto aos dados fora do escopo dos aplicativos?

MICRO FOCUS

Índice

página

Quando se trata de acesso a arquivos confidenciais em dados desestruturados, a solução Micro Focus Data Access Governance fornece uma abordagem de produto integrada para geração de relatórios, correção e certificação de acesso adequado por meio de análises de acesso.

Os analistas concluíram que o "elefante na sala" é a falta de governança dos dados desestruturados das organizações, ou seja, dados baseados em arquivos que compõem mais de 80% dos dados totais das organizações. Quando se trata de acesso a arquivos confidenciais em dados desestruturados, a solução Micro Focus Data Access Governance fornece uma abordagem de produto integrada para geração de relatórios, correção e certificação de acesso adequado por meio de análises de acesso.

Introdução

Nos últimos anos, as violações de dados têm sido o assunto de várias notícias. Na verdade, a frequência das violações de dados e a exposição resultante de informações confidenciais tornaram-se tão comuns que essas histórias agora tendem a se concentrar nas ocorrências mais extremas. Para não esquecer ou perder alguns desses incidentes relatados, organizações como Business Insider, Wired, Digital Information World e outras encerraram o ano de 2018 com suas classificações dos piores casos de violação de dados do ano.

Os dados têm valor tanto para a organização que os detém, como para as pessoas de fora que desejam acessá-los e explorá-los. Mas o acesso não autorizado aos dados nem sempre se baseia em intenções nefastas. As permissões de acesso, por exemplo, são atribuídas temporariamente mas não removidas, as funções mudam, as afiliações a grupos são modificadas, e antes que você saiba, um usuário interno tem acesso aos dados que ele não deveria ter.

Com as ramificações do acesso não autorizado, que vão desde a perda de confiança do consumidor até multas severas, a segurança dos dados através de controles de acesso é um objetivo de alta prioridade de todas as organizações.

Comparação de riscos: dados estruturados e desestruturados

Para analistas, pessoal de segurança e legisladores, o foco tradicional na segurança de dados tem sido os registros armazenados em bancos de dados. Conhecidos como "dados estruturados", esses dados são uma fonte primária de informações de identificação pessoal (PII, *personally identifiable information*), registros de saúde, números de conta, senhas e outras informações confidenciais que, quando acessadas por indivíduos não autorizados, podem ter consequências potencialmente devastadoras. Para proteger as PIIs, informações de saúde e outros dados confidenciais, os governos estabeleceram regulamentos de privacidade para os quais as organizações devem estar em "conformidade" ou enfrentar consequências potencialmente graves. Por este motivo, as organizações são obrigadas a realizar periodicamente "análises de acesso" de quem pode acessar dados confidenciais.

A maioria dos aplicativos que possuem dados estruturados no back end possuem mecanismos de segurança inerentes ao aplicativo. Os fornecedores de software "Gerenciamento de identidade e acesso (Identity and Access Management – IAM)" e "Governança e Administração de Identidade (Identity Governance and Access – IGA)" fornecem softwares que autorizam, validam e reconciliam controles de acesso a esses aplicativos, controlando inerentemente o acesso aos dados.

Um conjunto de dados igualmente vulnerável, mas historicamente menos enfatizado, é o de "dados desestruturados". Dados desestruturados são os dados baseados em arquivos – processamento de texto, planilhas, mídia, imagens virtuais e outros arquivos que compõem mais de 80% dos dados armazenados de uma organização. Dados desestruturados são armazenados principalmente em servidores de arquivos, SANs (Storage Area Networks) e na nuvem. E como os dados estruturados, os dados desestruturados também podem conter informações confidenciais que precisam ser protegidas. Em alguns casos, podem ser IPIs exportadas de fontes de dados estruturados. Mas não se trata apenas de IPIs. Dados desestruturados podem ser as "joias da coroa" dos dados de uma empresa. Arquivos Excel podem conter dados de lucros e perdas, arquivos Word podem incluir informações jurídicas, e arquivos PowerPoint podem incluir previsões de vendas.

Mas talvez nenhuma área de gerenciamento de dados tenha recebido atenção mais recente do que a segurança de dados. Isto inclui ameaças dentro e fora do firewall, desde acesso não autorizado a arquivos, até arquivos corrompidos através de um ataque de ransomware.

Como foi apontado em um artigo da Forbes, "A maioria das empresas não entende a quantidade de dados confidenciais que têm, e quando consideramos a quantidade de dados desestruturados (e-mails, PDFs e outros documentos) que uma empresa típica tem sob gerenciamento, as bandeiras vermelhas estão claras e presentes. ... Este é um problema de big data, para dizer o mínimo. Conforme o nível de dados desestruturados sobe e os hackers mudam seu foco para ele, dados desestruturados são um problema que não pode mais ser colocado no back burner de TI da empresa."[1]

Ao definir o mercado de DAG e os requisitos para lidar com ele, a Gartner afirma: "O DAG (Data Access Governance, governança de acesso a dados) fornece recursos de avaliação de acesso a dados, gerenciamento e monitoramento em tempo real para dados desestruturados e semiestruturados encontrados em repositórios de arquivos."

Data Access Governance

Reconhecendo a vulnerabilidade e os custos potenciais relativos ao acesso não autorizado de informações confidenciais em dados desestruturados, muitas empresas de pesquisa e consultoria estão reconhecendo um novo mercado de Governança de Acesso a Dados (Data Acess Governance – DAG).

Ao definir o mercado de DAG, Gartner afirma: "A governança de acesso aos dados (DAG) fornece recursos de avaliação, gerenciamento e monitoramento em tempo real de dados não-estruturados e semiestruturados encontrados em repositórios de arquivos". O objetivo principal do DAG é determinar quem tem acesso a quais dados nos repositórios de uma organização, como esses dados são classificados e qual foi o histórico de acesso a esses dados" [2]

Com este reconhecimento da Gartner e de outras organizações de pesquisa, acreditamos que é evidente que os regulamentos e objetivos de conformidade serão atualizados em breve para incluir a segurança e a proteção de acesso aos dados desestruturados.

1 *The Big (Unstructured) Data Problem, Juliette Rizkallah, Forbes, 05 de junho de 2017*
2 *Gartner, Hype Cycle for Data Security, 2018, Brian Lowans, 24 de julho de 2018*

Desde sua introdução inicial do produto em 2003, a equipe que desenvolve o que hoje é conhecido como Micro Focus File Reporter e Micro Focus File Dynamics tem continuamente abordado os objetivos do que anos mais tarde seria classificado como o mercado de DAG.

Detalhamento dos Requisitos de DAG

Práticas de segurança corporativa, pesquisa, práticas recomendadas, normas, legislação e as ideias de líderes de opinião estão contribuindo para uma lista evolutiva de requisitos para uma solução abrangente de DAG. Elas podem ser categorizadas da seguinte forma:

- Relatório de propriedade de dados
- Relatórios de segurança
- Notificações de mudanças
- Engajamento do proprietário dos dados da linha de negócio
- Abstração de segurança no nível de negócios
- Gestão do ciclo de vida
- Bloqueio de segurança
- Isolamento de segurança
- Revisão de acesso
- Atestado

Cada uma destas categorias é detalhada mais adiante neste artigo.

Figura 1. Uma solução completa do Data Access Governance inclui recursos oferecidos no Micro Focus File Reporter, File Dynamics, Identity Governance e Identity Manager.

Integração com o Identity Governance

Todas as organizações de pesquisa de segurança têm definições ligeiramente diferentes do Identity Governance, mas uma boa definição geral seria um sistema centralizado baseado em políticas de gestão de identidade de usuários e controle de acesso monitorado proativamente. Um componente do Identity Governance é a revisão de acesso. Como mencionado anteriormente, o Gerenciamento de Identidade e Acesso (Identity and Access Governance - IGA) ajuda a abordar a segurança de TI corporativa e a conformidade regulamentar através de revisões de acesso.

Devido à preocupação com violações de dados direcionadas a repositórios de dados desestruturados, os analistas estão agora observando os desejos das organizações de expandir as análises de acesso para incluir o acesso a dados desestruturados. Segundo a Gartner, "O acesso a dados desestruturados está despertando interesse na integração do IGA com produtos de gerenciamento de acesso a dados... para organizações mais maduras."[3] "Como as ferramentas de DAG fornecem um contexto relevante, sua inclusão será importante para as organizações que procuram fazer uso da inteligência de segurança para melhorar suas capacidades de detecção e resposta."[4]

Com foco em relatórios de identidade, gerenciamento e revisões de acesso combinados com mais de 30 anos de desenvolvimento e aprimoramentos contínuos, os produtos que compõem a solução Micro Focus Data Access Governance estão exclusivamente equipados para atender aos requisitos abrangentes de uma solução de DAG.

A abordagem da Micro Focus para uma solução DAG abrangente

Desde sua introdução inicial do produto em 2003, a equipe que desenvolve o que hoje é conhecido como Micro Focus File Reporter e Micro Focus File Dynamics tem continuamente abordado os objetivos do que anos mais tarde seria classificado como o mercado de DAG. Através de uma abordagem orientada por identidade, estes produtos relatam e controlam o acesso a dados desestruturados localizados no sistema de arquivos de rede, ajudando a garantir que somente as pessoas certas tenham as informações certas no momento certo.

Com a eventual identificação do mercado de DAG, a equipe de produto constatou que os relatórios, resultados e projeções dos analistas associados para a direção do mercado estavam em alinhamento com a pesquisa independente da equipe. Logo, houve uma interação regular entre a equipe e os analistas de DAG, à medida que a equipe começou a desenvolver requisitos de produtos, roteiros e novas iniciativas.

Uma das primeiras dessas iniciativas foi a integração entre File Reporter e o Micro Focus Identity Governance, oferecendo a este último a capacidade de realizar revisões de acesso sobre dados desestruturados (além de revisões de acesso sobre aplicativos que o produto já poderia fazer).

3 *Gartner, Magic Quadrant for Identity Governance and Administration, Felix Gaehtgens, Kevin Kampman, Brian Iverson, 21 de fevereiro de 2018*
4 *Ibid*

Para cada meta de alto valor, o File Dynamics permite designar proprietários de dados que, dependendo do tipo de política envolvida, são notificados quando as permissões de acesso são alteradas, revisam os logs de permissões, determinam quem deve ter acesso e que tipo de acesso, bloqueiam as permissões de acesso, e muito mais.

Esta integração de produtos é parte de uma solução global de Gerenciamento de Dados, que é composta pelos seguintes produtos:

- **File Reporter.** Faz o inventário da segurança do sistema de arquivos de rede juntamente com informações de identidade e funções para fornecer a inteligência detalhada de armazenamento de arquivos necessária para otimizar e proteger sua rede, atenuar riscos e garantir a conformidade.
- **File Dynamics.** Oferece amplos serviços de gerenciamento de dados através de administração automatizada e baseada em políticas. Os serviços incluem provisionamento de armazenamento, gerenciamento do ciclo de vida do armazenamento, migração de dados, remediação, limpeza, notificação de segurança, proteção contra corrupção de dados e tempo de inatividade e muito mais.
- **Identity Governance.** Fornece uma interface amigável ao negócio construída sobre um modelo de governança comum que abrange todos os seus processos de negócios relacionados à identidade, acesso e certificação. Demonstra conformidade proporcionando a você confiança de que suas campanhas de recertificação de acesso são feitas corretamente.

Metas e riscos de alto valor

A abordagem Micro Focus para Governança de Acesso a Dados permite que você implemente a solução em uma abordagem prioritária baseada na identificação e proteção das "metas de alto valor" em sua rede. Uma meta de alto valor é uma pasta de rede ou compartilhamento onde arquivos contendo informações sensíveis ou confidenciais são armazenados. Pastas ou ações contendo informações financeiras, jurídicas e de saúde são exemplos de metas de alto valor, mas na realidade, pode ser qualquer pasta da rede que armazene dados que sua organização possa considerar valiosos.

Uma vez identificadas essas metas, você pode verificar ou corrigir as permissões de acesso e então protegê-las através de políticas (detalhadas mais adiante neste documento). Esta abordagem não precisa ser um empreendimento monumental e pode ser feita em fases. Com a simples criação de políticas sobre algumas metas de alto valor, você verá benefícios imediatamente.

Atendendo aos requisitos de DAG

Com foco em relatórios de identidade, gerenciamento e revisões de acesso combinados com mais de 30 anos de desenvolvimento e aprimoramentos contínuos, os produtos que compõem a solução Micro Focus Data Access Governance estão exclusivamente equipados para atender aos requisitos abrangentes acima mencionados de uma solução de DAG.

Relatórios de Propriedade de Dados

Os repositórios de dados não estruturados são um alvo natural para estranhos e pessoas não autorizadas devido à imensa quantidade de conteúdo ali armazenado. Embora haja muitos dados redundantes, desatualizados e triviais (ROT) que provavelmente deveriam ser excluídos, certamente existem muitos arquivos contendo informações sensíveis também.

Ao gerar relatórios de propriedade usando o File Reporter, você pode identificar os proprietários de cada arquivo e então se referir a esses proprietários sobre se o arquivo deve ser mantido onde ele está, se deve ser excluído, arquivado ou movido para um local mais seguro. Para aqueles arquivos que são mantidos ou protegidos, uma revisão de acesso aos arquivos pode determinar se o proprietário do arquivo está correto ou se um novo proprietário precisa ser designado.

Relatórios de segurança

Antes de implementar medidas para controlar o acesso a dados desestruturados, você deve primeiro determinar quem tem permissões de acesso aos dados. Com esse conhecimento, você pode fazer as alterações necessárias nas permissões de acesso atribuídas diretamente ou nas associações de grupo.

O desafio está no fato de que identificar permissões de dados desestruturados é muito mais complexo do que identificar permissões de aplicativos. Contribuem para esta complexidade todos os tipos de permissão NTFS, princípios de segurança, identificadores de segurança, herança, filiação a grupos, listas de controle de acesso ao Active Directory, entre outros fatores. A dificuldade em determinar permissões de acesso precisas é um dos principais motivos pelos quais a maioria dos fornecedores de IG não oferece a capacidade de fornecer análises de acesso para dados desestruturados.

Desde sua introdução, o File Reporter tem sido capaz de relatar permissões de usuário atribuídas e efetivas do sistema de arquivos para todas as pastas e subpastas a partir de um caminho específico do sistema de arquivos. Além disso, você pode identificar todos os usuários que possuem qualquer tipo de permissão de acesso a uma pasta de rede especificada, bem como todas as pastas de rede que um usuário especificado pode acessar.

Desde sua introdução, o File Reporter tem sido capaz de relatar permissões de usuário atribuídas e efetivas do sistema de arquivos para todas as pastas e subpastas a partir de um caminho específico do sistema de arquivos. Além disso, você pode identificar todos os usuários que possuem qualquer tipo de permissão de acesso a uma pasta de rede especificada, bem como todas as pastas de rede que um usuário especificado pode acessar.

Notificações de mudanças

Uma vez gasto o tempo para rever as permissões de acesso, fazer os ajustes necessários, participar de uma auditoria e demonstrar conformidade com quaisquer políticas corporativas ou regulamentações governamentais, a última coisa que você deseja é comprometer essa conformidade através de uma mudança não autorizada nas permissões de acesso.

O File Dynamics permite que você crie políticas de Notificação de Segurança atribuídas a metas específicas de alto valor em sua rede para que os "proprietários dos dados" – usuários designados e familiarizados com o conteúdo e segurança da meta de alto valor – possam rever as mudanças nas permissões de acesso.

As alterações de permissão de acesso podem ocorrer diretamente através de uma atribuição de usuário individual ou indiretamente através de uma mudança na filiação em grupo.

Os recursos da solução Micro Focus Data Access Governance oferecem a você os meios para fornecer aos auditores e gerentes de linha de negócios processos e relatórios de certificação de acesso intuitivos, de fácil utilização e automatizados para demonstrar a conformidade e fornecer atestados.

As políticas de Notificação de Segurança são granulares o suficiente para proporcionar o nível de controle desejado. Por exemplo, se uma política de Notificação de Segurança fosse atribuída à pasta Finanças e um novo membro fosse adicionado a um grupo que tivesse permissões de acesso a essa pasta, uma notificação seria enviada ao proprietário dos dados para que o proprietário dos dados pudesse então decidir se alguma ação responsiva precisaria ser realizada.

Proprietários dos dados da linha de negócios

Pessoas que trabalham na empresa com os dados...

1

Entenda melhor

(melhor do que TI)

2

Saiba:

- o valor dos dados e/ou o risco associado a eles
- quem deve poder acessá-los (e quem não deve)

3

"Possuem" os dados

e (por extensão) são responsáveis por eles

4

São "especialistas no assunto"

(PMEs) sobre os dados

Figura 2. Os proprietários dos dados são especialistas no assunto que conhecem o valor dos dados e sabem quem deve ter e não ter acesso aos mesmos.

Engajamento do proprietário dos dados da linha de negócio

Em organizações de qualquer porte, ninguém sabe a relevância, o valor ou a confidencialidade dos dados do que aqueles que trabalham com os dados. Um usuário no departamento de RH de uma organização, por exemplo, será um juiz muito melhor sobre quais dados de RH armazenar, excluir e proteger através de acesso limitado em comparação a um administrador de rede regular.

Para cada meta de alto valor, o File Dynamics permite designar proprietários de dados que, dependendo do tipo de política envolvida, são notificados quando as permissões de acesso são alteradas, revisam os logs de permissões, determinam quem deve ter acesso e que tipo de acesso, bloqueiam as permissões de acesso, e muito mais.

Abstração de segurança no nível de negócios

Ao realizar uma análise de acesso, os auditores devem determinar quais permissões de acesso um usuário tem e se essas permissões estão em conformidade com a política corporativa ou com os regulamentos governamentais. Um usuário, por exemplo, pode ter acesso de gravação a um aplicativo quando deve ter apenas acesso de leitura, ou outro usuário pode ter controle total quando deve ter acesso de gravação.

Infelizmente, as permissões do sistema de arquivos NTFS do Windows são muito mais amplas do que essas três designações, de modo que, como parte da integração entre o File Reporter e o Identity Governance, o File Reporter executa a abstração em nível comercial das permissões NTFS para que as pessoas de nível comercial que executam revisões de acesso em dados desestruturados (e não familiarizados com permissões NTFS) possam revisá-las com classificações que eles entendem. Por exemplo, o sinalizador de máscara de acesso NTFS do Excluir Subpastas e arquivos torna-se Gravação, enquanto Apropriar-se torna-se Alterar Permissões.

Gerenciamento do ciclo de vida

Muitas organizações utilizam software de Gerenciamento de Identidade (IDM) para gerenciar o acesso aos aplicativos com base no papel do usuário. Por exemplo, um novo usuário do departamento de RH pode receber automaticamente permissões de acesso ao aos aplicativos de RH e dados associados.

Enquanto o sistema IDM pode conceder direitos de acesso a aplicativos e dados baseados em funções, ele não pode conceder acesso ao sistema de arquivos de rede baseado em funções – é aí que entra o File Dynamics.

Como ele usa o mesmo serviço de diretório do seu sistema de gerenciamento de identidade, o File Dynamics pode tomar ações de armazenamento de usuários enquanto o sistema de gerenciamento de identidade toma ações de conta do usuário.

Enquanto o sistema de gerenciamento de identidade cria uma nova conta de usuário no Active Directory, torna o usuário um membro de um ou mais grupos e define o acesso do usuário à rede, o File Dynamics pode estabelecer uma pasta inicial da rede, permissões de acesso e cota de armazenamento de acordo com a função do usuário. Além disso, ele pode estabelecer acesso a áreas de armazenamento colaborativo baseado em funções.

Bloqueio de segurança

Dados confidenciais devem ser acessíveis com base na "necessidade de saber", o que significa que apenas um conjunto limitado de indivíduos, com base em suas funções, deve ter acesso a esses dados confidenciais. Além disso, os proprietários dos dados - os mais familiarizados com a confidencialidade dos dados e quem deve ter acesso aos mesmos - devem ter poderes para se tornarem os tomadores de decisão finais.

Uma vez estabelecidas as permissões de acesso adequadas para uma meta de alto valor, você pode estabelecer o arquétipo de permissões de acesso para a meta de alto valor que será rigorosamente aplicado através de uma política de bloqueio. Quando são feitas alterações de permissão de acesso não autorizado à meta de alto valor, as novas permissões são excluídas e as permissões especificadas na política de bloqueio são restauradas.

Isolamento de Segurança

Pode haver algumas metas de alto valor em que você pode não querer colocar o mesmo nível de restrições que uma política de Bloqueio de Segurança, mas pode, no entanto, querer garantir o acesso apenas a usuários ou funções autorizados.

As políticas de isolamento no File Dynamics permitem que você estabeleça limites sobre como as permissões de acesso podem mudar ao longo do tempo. Usando um conjunto de declarações de PERMISSÃO/NEGAÇÃO para definir um "isolamento", a política especifica os contêineres, usuários ou grupos do Active Directory que podem concebivelmente receber permissões para uma meta de alto valor no futuro sem um problema ou que nunca devem receber direitos no futuro, como nas restrições especificadas na GDPR.

Família de políticas de segurança orientadas por meta

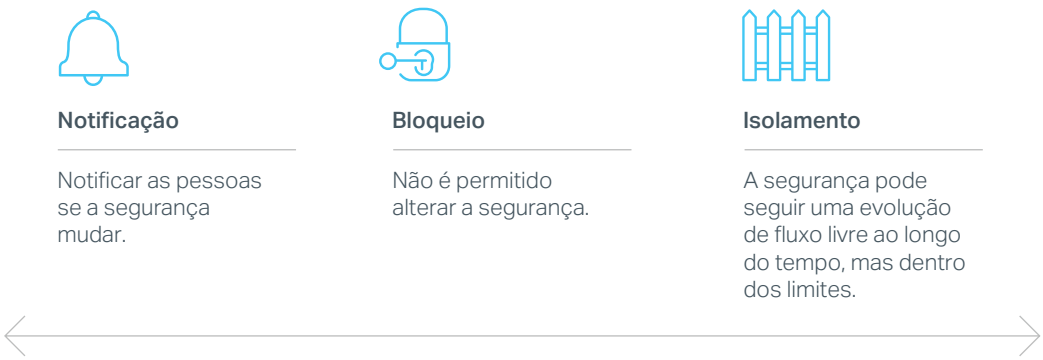

Figura 3. As políticas de segurança orientadas por metas incluem as políticas de Notificação de Segurança, Bloqueio e Isolamento. Cada uma é desenvolvida para ajudar os proprietários de dados a limitar o acesso a dados confidenciais somente a usuários autorizados.

Access Review

Muitas indústrias regulamentadas exigem revisões periódicas de acesso, que são o meio de fornecer certificação (também chamada de "atestação") para o cumprimento de regulamentos específicos. Para a maioria dessas organizações, as revisões de acesso são o meio de:

- Capacitar as organizações para gerenciar a adesão de grupos
- Revisão e conciliação de acesso a aplicativos empresariais
- Conciliando atribuições de funções

A solução Micro Focus Data Access Governance permite não só atender a esses requisitos, mas também realizar análises de acesso sobre talvez o repositório mais vulnerável a violações de dados - o sistema de arquivos de rede.

A integração entre o File Reporter e o Identity Governance permite a importação de permissões de varreduras realizadas no File Reporter para o Identity Governance, onde podem ser realizadas revisões de acesso sobre a meta de alto valor.

Fale conosco:
www.microfocus.com.br

Gostou do que leu? Compartilhe.

Atestado

Como uma simples definição, "atestado" é o processo de validação de que algo é verdade. Quando se trata de revisões de acesso, atestado é a certificação de que uma organização está em conformidade com os regulamentos ou políticas de segurança e acesso. Dependendo do regulamento, o atestado depende de uma série de especificações, incluindo quando a revisão é realizada, por quem, como a revisão é conduzida, e muito mais.

Os recursos da solução Micro Focus Data Access Governance oferecem a você os meios para fornecer aos auditores e gerentes de linha de negócios processos e relatórios de certificação de acesso intuitivos, de fácil utilização e automatizados para demonstrar a conformidade e fornecer atestados.

Conclusão

Abrangendo mais de 80% dos arquivos armazenados de uma organização, os dados desestruturados e a informação confidencial contida dentro dela são alvos de violações de dados internos e externos, representando riscos para organizações de todos os tamanhos e em todos os setores. O objetivo do Data Access Governance é proteger as organizações contra o acesso não autorizado através de um extenso conjunto de requisitos definidos.

A solução Micro Focus Data Access Governance, com suas capacidades de geração de relatórios, gerenciamento e revisão de acesso, é exclusivamente equipada e qualificada para atender aos requisitos abrangentes de uma solução DAG completa. À medida que as ameaças de violação de dados se tornam mais sofisticadas, à proporção que novas regulamentações são introduzidas e que os armazenamentos de dados continuam a crescer exponencialmente, você pode se sentir confiante de que está enfrentando esses desafios e todos os demais com a expertise de um reconhecido líder do setor na Micro Focus.