Red Hat
Enterprise Linux

# Simplifique a segurança na nuvem

O Red Hat Enterprise Linux oferece recursos de segurança consistentes em todos os ambientes.

**Tenha operações consistentes em todos os ambientes de nuvem**

O Red Hat Enterprise Linux inclui otimizações variadas para garantir um desempenho confiável e com foco na segurança na nuvem. Ele oferece uma base de operações consistente para ambientes híbridos e de multicloud. Assim, você pode executar suas aplicações onde for necessário.

Obtenha mais informações sobre o valor do Red Hat Enterprise Linux na nuvem.

## A segurança na nuvem é uma grande preocupação

À medida que a adoção da nuvem cresce, a segurança permanece uma das principais preocupações de organizações de todos os portes. Na verdade, 85% das organizações citam a segurança como um dos principais desafios da nuvem.[1] E essa preocupação tem fundamento: em 2022, 45% das violações ocorreram na nuvem.[2]

Em qualquer ambiente, a consistência é fundamental para as práticas recomendadas de segurança e conformidade. Para proteger sua empresa, o nível da política de segurança e os controles de acesso na nuvem devem ser os mesmos presentes no data center local. Com um sistema operacional padronizado que tenha controles de segurança consistentes em todas as áreas de ocupação da infraestrutura, é possível aumentar a segurança e a conformidade em toda a sua organização. Quando você usa o Red Hat® Enterprise Linux® como sua base operacional em todos os ambientes, propicia a consistência necessária para manter a segurança e a conformidade na nuvem.

## Adote uma base consistente de segurança e conformidade em todos os ambientes

Com o Red Hat Enterprise Linux, é mais simples manter a segurança e a conformidade em ambientes locais, de nuvem e edge. A segurança é essencial na arquitetura e no ciclo de vida do Red Hat Enterprise Linux. As funcionalidades de segurança integradas e a conformidade com os regulamentos da indústria e do governo protegem seus sistemas na nuvem. As melhores configurações padrão baseadas nas práticas recomendadas configuram seus sistemas para aumentar a segurança desde o início. Conjuntos de pacotes minimizados de imagens de nuvem pré-construídas reduzem a superfície de ataque de ameaças à cibersegurança. Os upgrades de segurança e os patches em tempo real também fazem parte da subscrição do Red Hat Enterprise Linux.

O Red Hat Enterprise Linux permite reduzir os riscos de segurança e implementar e manter a segurança em camadas, além de simplificar a conformidade em ambientes híbridos e de multicloud. Esta visão geral descreve as principais funcionalidades e recursos para adotar uma abordagem de segurança consistente em ambientes híbridos e de multicloud.

## Detecte e corrija vulnerabilidades em escala com o Red Hat Insights

Em 2022, o tempo médio para identificar e conter uma violação de dados foi de 277 dias.[2] Encontrar e interromper a violação em 200 dias ou menos pode reduzir o custo decorrente, em média, em 24%.[2] Realizar o monitoramento consistente todos os dias ajuda você a identificar as vulnerabilidades e riscos de conformidade antes que eles interrompam as operações de negócios ou resultem em uma violação.



1 Flexera. "Flexera 2022 State of the Cloud Report", março de 2022.
2 IBM Security. "Cost of a Data Breach Report 2022", 2022.

Red Hat
Enterprise Linux

**Acelere as operações de segurança e conformidade**

O Red Hat Insights ajuda você a acelerar as operações de segurança e conformidade:

- **91%** de redução no tempo para detectar vulnerabilidades de segurança[3]
- **69%** de redução no tempo para detectar violações de política[3]

Obtenha mais informações sobre como gerenciar a segurança e a conformidade com o Red Hat Enterprise Linux:

- Resumo sobre como gerenciar riscos de segurança com o Red Hat Insights
- Demonstração de como resolver problemas com o Red Hat Insights
- Demonstração ao vivo de como usar o OpenSCAP para verificações de vulnerabilidade e conformidade de segurança

O Red Hat Enterprise Linux inclui o Red Hat Insights, um conjunto de soluções de serviços hospedados no Hybrid Cloud Console que analisa continuamente plataformas e aplicações para ajudar você a gerenciar e otimizar melhor seus ambientes de nuvem híbrida. O Red Hat Insights usa análises preditivas e conhecimento profundo para identificar, avaliar e recomendar a correção de riscos de segurança e conformidade, bem como outros riscos operacionais. Ele também ajuda a priorizar as ações de correção com base no tipo de severidade, risco e impacto da mudança. O Red Hat Insights funciona em ambientes locais e de nuvem, permitindo que você gerencie todos os sistemas Red Hat Enterprise Linux usando uma única interface. Você pode até mesmo vincular sua conta da Red Hat à conta do seu provedor de nuvem para conectar automaticamente seus sistemas e cargas de trabalho baseados na nuvem ao Red Hat Insights e a outros serviços da Red Hat ao provisioná-los.

O Red Hat Insights inclui serviços que ajudam a proteger ambientes híbridos e de multicloud.

- **Serviço de vulnerabilidade:** avalie os sistemas em busca de vulnerabilidades e exposições comuns (CVEs), colete informações de varredura e confira orientações sobre correção por meio de uma única interface.
- **Serviço de malware:** identifique rapidamente os sistemas que contêm assinaturas de malware ativas para evitar a exposição em longo prazo.

## Garanta a conformidade com verificação e correção integradas

A falta de conformidade pode resultar em multas, prejuízos para os negócios e perda de certificações, além de facilitar as violações de segurança. Em 2022, o custo médio de uma violação de dados para organizações com altos níveis de falha de conformidade foi de US$ 5,57 milhões.[2] Além disso, no mesmo ano, os altos níveis de falhas de conformidade aumentaram o custo da violação de dados, em média, em US$ 258.293.[2]

O Red Hat Enterprise Linux é certificado pelos principais padrões do governo e da indústria, podendo ser usado com confiança em ambientes altamente regulamentados. O Red Hat Insights inclui serviços que ajudam a manter a conformidade mais facilmente em ambientes híbridos e de multicloud.

- **Serviço de conformidade:** audite conformidades com as políticas do OpenSCAP, corrija os sistemas que não estão conformes e gere relatórios de conformidade normativa e auditorias de segurança. Além disso, é possível ajustar as políticas padrão para seu ambiente e operações a fim de gerar resultados mais precisos. As principais linhas de base integradas incluem:
  - Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI-DSS).
  - Perfil de Proteção Avançada do Sistema Operacional (Common Criteria).
  - Oito fundamentos essenciais do Centro Australiano de Cibersegurança (ACSC).
  - Referência do Center for Internet Security (CIS).
  - Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA).
  - Diretrizes de implementação técnica de segurança da Agência Americana de Sistemas de Informação de Defesa (DISA STIG).
- **Serviço de políticas:** defina políticas de segurança personalizadas, monitore a conformidade dos sistemas e alerte as equipes quando um sistema não está conforme.

3 Principled Technologies (patrocinado pela Red Hat). "Poupe tempo e trabalho de administração automatizando o monitoramento com o Red Hat Insights", setembro de 2020.

Red Hat
Enterprise Linux

## Implante imagens consistentes e reforçadas em todas as nuvens com o serviço de image builder

Atualmente, 89% das organizações têm uma estratégia multicloud.[1] Apesar de permitir escolher a nuvem certa para cada carga de trabalho, a abordagem multicloud gera complexidades e aumenta o risco de inconsistências que podem levar a problemas de segurança e conformidade.

O serviço de image builder do Red Hat Insights ajuda você a criar, gerenciar e implantar as imagens do sistema operacional Red Hat Enterprise Linux nos ambientes de nuvem híbrida com mais rapidez e facilidade. Ele permite criar imagens personalizadas com segurança reforçada, salvá-las como templates e enviá-las para vários inventários de provedores de nuvem, simplificando o provisionamento. Assim, você tem a certeza de que seus sistemas estão configurados de forma consistente nas diversas nuvens.

## Verifique a integridade do sistema nos diversos ambientes com atestado remoto

Em ambientes altamente distribuídos de larga escala, é essencial garantir a integridade do sistema. Quando os sistemas não são confiáveis ou estão comprometidos, sua organização fica vulnerável a ataques de agentes maliciosos.

O Red Hat Enterprise Linux conta com funcionalidades de atestado remoto, que verificam o estado dos sistemas na inicialização e monitoram continuamente a integridade dos sistemas remotos. Com base no projeto de open source Keylime, o atestado remoto usa o hardware Trusted Platform Module (TPM) incorporado e a Integrity Measurement Architecture (IMA) do kernel Linux para monitorar os sistemas em escala. Também é possível enviar arquivos criptografados para os sistemas monitorados e especificar ações automatizadas para serem executadas quando um sistema monitorado falha no teste de integridade.

## Proteja seus dados na nuvem com criptografia de disco vinculada à rede

Seus dados são um ativo essencial para os negócios, por isso protegê-los na nuvem é fundamental.

O Red Hat Enterprise Linux inclui suporte para criptografia de disco vinculada à rede (NBDE) para simplificar a proteção de dados em repouso. O NBDE desbloqueia automaticamente os volumes de armazenamento por meio de conexões com um ou mais servidores de rede. Isso permite descriptografar volumes sem gerenciar manualmente as chaves de criptografia, além de garantir que eles estejam disponíveis apenas quando estiverem protegidos. O Red Hat Enterprise Linux também é compatível com NBDE por TPM, que garante a integridade do sistema antes de desbloquear os volumes criptografados.

## Implemente arquiteturas de confiança zero mais facilmente com o gerenciamento integrado de identidade e acesso

As abordagens tradicionais de segurança, baseadas em perímetro, não protegem ambientes de nuvem novos e amplamente distribuídos de modo eficiente. As arquiteturas de confiança zero podem ajudar aplicando a segurança a cada ativo, em vez de somente a um perímetro da rede. Na verdade, a implementação de confiança zero reduz o custo das violações de dados em 20,5%, em média.[2] O principal elemento das arquiteturas de confiança zero é o gerenciamento de identidade e acesso.

### Crie uma base de confiança zero em ambientes Linux

A arquitetura de confiança zero protege melhor seu ambiente e organização de TI.

- Obtenha mais informações sobre como implementar a confiança zero com o Red Hat Enterprise Linux.
- Assista a uma demonstração ao vivo de gerenciamento de usuários no Red Hat Enterprise Linux

**Gerencie a segurança em diferentes versões em menos tempo**

A automação ajuda a reduzir os erros manuais e a gerenciar os sistemas mais rapidamente.

Assista a uma demonstração ao vivo de funções do sistema no Red Hat Enterprise Linux

Incluso no Red Hat Enterprise Linux, o Red Hat Identity Management centraliza o gerenciamento de identidades, impõe os controles de segurança e garante a conformidade com os padrões de segurança em todo o ambiente. Ele oferece os recursos necessários para implementar as práticas recomendadas de confiança zero enquanto simplifica a infraestrutura de gerenciamento de identidades. Autentique os usuários e implemente controles de acesso baseado em função (RBAC) ou política usando uma única interface escalável que engloba todo o data center. O Red Hat Identity Management se integra ao Microsoft Active Directory, ao protocolo lightweight de acesso a diretórios (LDAP) e a outras soluções de terceiros usando interfaces padrão. Além disso, o Red Hat Identity Management é compatível com a autenticação baseada em certificado e técnicas de autorização.

## Simplifique a configuração e o gerenciamento da segurança com funções do sistema

À medida que o tamanho e a complexidade da sua infraestrutura aumentam, torna-se cada vez mais difícil gerenciá-la manualmente. O vetor de ataque inicial de 15% das violações de dados foi a configuração incorreta da nuvem, resultando em um custo médio de US$ 4,14 milhões por violação em 2022.[2] Com a automação, você configura e gerencia seus sistemas com mais rapidez e consistência e menos esforço.

As funções do sistema Red Hat Enterprise Linux, com tecnologia do Red Hat Ansible® Automation Platform, usam a automação para ajudar você a instalar e gerenciar as configurações de segurança em escala em menos tempo. As funções do sistema são compatíveis com várias versões do Red Hat Enterprise Linux nas diferentes áreas de ocupação da infraestrutura. Assim, é possível definir novas configurações de segurança e mantê-las em todos os sistemas com um único comando ou fluxo de trabalho.

## Mais informações

Com uma abordagem consistente de segurança e conformidade em ambientes híbridos e de multicloud, você protege melhor sua organização. O Red Hat Enterprise Linux propicia uma base com foco em segurança para executar aplicações em todas as áreas de ocupação da infraestrutura, em seu data center, na nuvem ou edge.

Obtenha mais informações sobre a abordagem da Red Hat para a segurança em nuvem híbrida.



AMÉRICA LATINA
+54 11 4329 7300
latammktg@redhat.com

BRASIL
+55 11 3629 6000
marketing-br@redhat.com

facebook.com/redhatinc
@redhatbr
linkedin.com/company/red-hat-brasil

br.redhat.com
275099_0323_KVM