Melhore a segurança e a conformidade

Reduza os riscos com uma plataforma Linux open source e robusta

Red Hat

Conteúdo

O Linux é a base para o futuro

O Linux® é um dos sistemas operacionais mais usados no mundo todo, sendo adotado por empresas de diversos setores econômicos e tecnologias emergentes.[1] Normalmente, é o sistema operacional preferencial para processar cargas de trabalho altamente disponíveis, confiáveis e críticas em datacenters e ambientes de cloud computing, além de ser compatível com uma grande variedade de casos de uso, sistemas de destino e dispositivos. Todos os principais provedores de nuvem pública oferecem várias distribuições do Linux em seus marketplaces.

Porém, você precisa escolher a distribuição do Linux e as ferramentas de gerenciamento ideais para seu ambiente de TI, pois elas podem impactar significativamente a eficiência, segurança e interoperabilidade do ambiente. Neste ebook, analisamos as principais considerações e oferecemos orientações sobre o gerenciamento de vulnerabilidades de segurança e riscos de conformidade em ambientes Linux.

Segurança e conformidade são duas das principais preocupações de TI

O gerenciamento de riscos de segurança e conformidade na TI é uma preocupação constante de todas as organizações. Sabemos que 33% dos CEOs consideram os ciberataques como a principal ameaça à perspectiva de crescimento de suas organizações.[2] E as violações de segurança podem custar caro. O prejuízo médio de uma violação de dados é de US$ 3,86 milhões.[3]

Além disso, as regulamentações governamentais e do setor também estão mudando. Acompanhá-las é desafiador. As falhas de conformidade aumentam em cerca de 6% o prejuízo causado por uma violação de dados.[3]

Impactos da segurança ineficaz

Velocidade é a palavra-chave para reduzir o risco e o impacto das violações.

US$ 3,86 milhões
é o prejuízo médio de uma violação de dados em 2020[3]

280 dias
é o tempo médio para identificar e conter uma violação de dados em 2020[3]

US$ 1,12 milhão
são economizados quando uma violação é identificada e contida em até 200 dias[3]

Desafios comuns de segurança e conformidade

Vários fatores dificultam o gerenciamento da conformidade e das vulnerabilidades de segurança.

Mudanças nos cenários de conformidade e segurança

As ameaças à segurança evoluem rapidamente e exigem respostas imediatas aos novos riscos e alterações nas regulamentações.

Ambientes híbridos e de multicloud distribuídos

É mais difícil ter uma visão completa da TI quando os ambientes são distribuídos de acordo com a geografia e a lógica.

Ambientes grandes e complexos

Infraestruturas de grande porte geralmente usam várias ferramentas de segurança e conformidade, o que dificulta o gerenciamento de riscos.

Equipes limitadas e instruções remotas

A maioria das organizações não tem funcionários suficientes para gerenciar manualmente as tarefas de segurança e conformidade.

1 *The Linux Foundation.* "**Linux is the most successful open source project in history**", *acessado em 24 de setembro de 2020.*

2 *PWC.* "**23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty**", *2020.*

3 *IBM Security.* "**Cost of a Data Breach Report 2020**", *2020.*

Adote uma abordagem efetiva para o gerenciamento de riscos de segurança e conformidade

O gerenciamento de conformidade e vulnerabilidades de segurança inclui monitorar e avaliar os sistemas para que eles estejam em conformidade com as políticas regulatórias e de segurança. Uma abordagem ideal permite desenvolver processos consistentes e repetíveis no ambiente inteiro para:

Avaliar
Identifique sistemas vulneráveis ou fora de conformidade. Avalie com facilidade o estado real da segurança do ambiente, da infraestrutura às cargas de trabalho. Entenda quais das várias orientações de segurança realmente se aplicam aos sistemas e ambiente da sua empresa.

Priorizar
Organize as ações de correção de acordo com o esforço demandado, o impacto e a gravidade do problema. Aplique técnicas de gerenciamento de riscos para determinar o que é um risco real para os negócios em cada problema e planeje a correção devidamente. O risco abrange a probabilidade de um problema resultar em uma violação, sua gravidade em potencial e as implicações de corrigi-lo. Um problema que talvez não valha a pena ser corrigido nos sistemas de desenvolvimento e teste pode ser de alta prioridade nos sistemas de produção.

Corrigir
Aplique patches e reconfigure sistemas que demandem alguma ação com rapidez e facilidade. Automatize os processos de configuração e aplicação de patches para acelerar as correções, manter a consistência entre sistemas e reduzir os riscos de erro humano. Quando usadas com eficácia, as ferramentas automatizadas ajudam a remediar problemas rapidamente, aumentando a segurança do ambiente e dos negócios.

Informar
Valide as alterações aplicadas e automatize a geração de relatórios de correção para otimizar o trabalho de auditoria. A elaboração de relatórios eficazes ajuda a fornecer informações com o nível certo de detalhamento para executivos, auditores e equipes técnicas entenderem os atuais riscos e pontos fracos de segurança.

Além disso, esse tipo de abordagem é um dos primeiros passos para preparar sua organização para a adoção de técnicas rápidas e modernas de desenvolvimento e gerenciamento, como o **DevSecOps**. Na verdade, 38% das organizações consideram que a avaliação de vulnerabilidades é o fator mais crítico na segurança dos fluxos de trabalho DevOps.[4]

Nas seções a seguir, você verá as principais considerações e ações para gerenciar riscos de segurança e conformidade com mais eficiência.

4 451 Research, grupo pertencente à S&P Global Market Intelligence. "Voice of the Enterprise, DevOps H2 2019".

Identificação e correção de vulnerabilidades em ambientes Linux

Identificação e correção de vulnerabilidades é o processo de avaliar a infraestrutura para localizar e corrigir os sistemas que estão vulneráveis a ataques. Essas vulnerabilidades podem ser causadas por novas ameaças, patches desatualizados e não aplicados ou configurações incorretas do sistema. As ações de correção muitas vezes incluem aplicação de patches, atualização e reconfiguração dos sistemas para eliminar as vulnerabilidades.

Por que isso é importante?

As vulnerabilidades de segurança podem resultar em violações caras e prejudicar a confiança dos clientes, a reputação da empresa e a receita. Na verdade, a perda de negócios é responsável por 39,4% do prejuízo médio de uma violação de dados.[5]

Desafios para identificar e corrigir vulnerabilidades com eficiência

A maioria das organizações não tem uma estratégia de segurança consistente para operações em escala.

- Os poucos funcionários geralmente estão sobrecarregados e não têm as habilidades necessárias para desenvolver e executar uma estratégia de segurança completa.
- As ferramentas genéricas de verificação de segurança geram listas infindáveis de vulnerabilidades em potencial que nem sempre são aplicáveis ao seu ambiente. Como resultado, a equipe precisa desperdiçar muito tempo investigando possíveis problemas e ações corretivas.
- Processos manuais de identificação, correção e acompanhamento tornam as operações lentas e, com isso, vulnerabilidades conhecidas muitas vezes ficam sem patches ou correções.
- Os métodos de correção ad hoc resultam na aplicação inconsistente de patches e aumentam os possíveis riscos de segurança.

Funcionalidades essenciais em ferramentas de gerenciamento de segurança

Para ser mais eficaz, você precisa identificar e corrigir as vulnerabilidades do sistema o mais rápido possível, antes de elas resultarem em uma violação. Prefira ferramentas de gerenciamento de segurança unificadas que:

Realizem uma análise completa para identificar os riscos (tanto no nível do sistema operacional quanto das cargas de trabalho) em todos os sistemas e as instâncias no ambiente.

Automatizem a correção de riscos identificados para que equipes de segurança e TI sejam mais rápidas, precisas e eficientes.

Incorporem o know-how do fornecedor para oferecer orientações sobre correções para suas soluções (talvez existam ações mais simples para reduzir os riscos).

Acessem regularmente os dados mais recentes sobre vulnerabilidades e riscos de segurança disponibilizados pelos fornecedores do sistema operacional e das aplicações.

Gerem relatórios sobre possíveis riscos, ações corretivas e auditoria com os detalhes adequados para cada público.

*5 IBM Security. "**Cost of a Data Breach Report 2020**", 2020.*

Gerenciamento de conformidade em ambientes Linux

O gerenciamento de conformidade é o processo de manter os sistemas continuamente em conformidade com políticas empresariais, padrões do setor e regulamentações aplicáveis. Esse processo usa a avaliação da infraestrutura para identificar sistemas que estejam fora de conformidade devido a alterações em regulamentações, políticas ou padrões, configurações incorretas ou outros motivos.

Por que isso é importante?

A falta de conformidade pode resultar em multas, prejuízos para os negócios e perda de certificações, além de facilitar as violações de segurança. E esse tipo de falha ainda aumenta os prejuízos nas violações de dados.[6]

Desafios para gerenciar a conformidade com eficiência

Muitas organizações ainda usam operações manuais e scripts personalizados para gerenciar a conformidade. Esses processos são muito lentos e limitados em escala para dar conta de operações e iniciativas de desenvolvimento rápidas e modernas.

- Com a infinidade de linhas de base e padrões genéricos, fica mais difícil de entender a importância e o impacto no seu ambiente.
- Os processos manuais atrasam as operações de monitoramento, correção e auditoria, resultando em desperdício do tempo dos funcionários, inconsistência na aplicação de políticas e maior risco de problemas de conformidade.
- Muitas organizações usam ferramentas diferentes para gerenciar a segurança e a conformidade. Isso leva a operações menos eficientes e dificulta a configuração de políticas consistentes e personalizadas.

Funcionalidades essenciais em ferramentas de gerenciamento de conformidade

Para ser mais eficiente, você deve ser capaz de definir e aplicar políticas contextuais, manter sistemas em conformidade com essas políticas e gerar rapidamente relatórios gerenciáveis usados em auditorias. Prefira ferramentas de gerenciamento de conformidade unificadas que:

Usem inteligência analítica para identificar riscos de conformidade o quanto antes e de maneira consistente.

Corrijam automaticamente os sistemas fora dos padrões de conformidade.

Forneçam uma visão total da situação de conformidade do ambiente como um todo.

Gerem relatórios de conformidade automaticamente, de acordo com seus requisitos de auditoria e as necessidades de quem receberá as informações.

Ofereçam recomendações especializadas e orientações contextualizadas para a correção de sistemas fora de conformidade no ambiente.

6 *IBM Security. "Cost of a Data Breach Report 2020", 2020.*

Práticas recomendadas

Analise os sistemas regularmente

O monitoramento diário ajuda a identificar vulnerabilidades e riscos de conformidade antes que suas operações de negócios sejam interrompidas ou ocorra alguma violação. Use sempre os dados de segurança mais recentes dos seus provedores de sistema operacional e aplicações para melhorar a precisão da análise. E configure políticas de segurança personalizadas ao ambiente e às operações da sua organização para ter resultados da análise de conformidade mais precisos.

Encontrar e eliminar uma violação em até **200 dias** pode reduzir substancialmente os prejuízos decorrentes.[7]

Aplique e teste patches com frequência

Manter os sistemas atualizados é uma maneira de aumentar a segurança, a confiabilidade, o desempenho e a conformidade. Aplique patches regularmente para manter seu ambiente atualizado com a correção de problemas importantes em geral. Aplique o quanto antes os patches para bugs e defeitos críticos. Teste a aceitação dos sistemas que receberam patches antes de recolocá-los em produção.

Uma ferramenta eficaz de gerenciamento de patches pode acelerar a correção de problemas em até **88,9%**.[8]

Implante a automação

À medida que o tamanho e a complexidade da sua infraestrutura aumentam, torna-se cada vez mais difícil gerenciá-la manualmente. Use a automação para otimizar o monitoramento, acelerar a correção, melhorar a consistência e gerar relatórios regularmente.

A automação da segurança pode reduzir o prejuízo médio de uma violação em **93%**.[7]

Conecte as ferramentas e alinhe os processos

Os ambientes distribuídos geralmente têm uma ferramenta de gerenciamento diferente para cada plataforma. Integre essas ferramentas por meio de interfaces de programação de aplicações (APIs). Use suas interfaces preferidas para executar tarefas em outras ferramentas. Tenha menos interfaces para melhorar as operações e a visibilidade do status de segurança e conformidade de todos os sistemas do seu ambiente. Por fim, alinhe seus processos nos ambientes para ter mais consistência e confiabilidade.

52% das organizações estão otimizando a infraestrutura de TI e os processos para melhorar a segurança.[9]

Adote uma estratégia de segurança consistente e contínua

A eficácia das medidas de segurança depende de uma abordagem holística que incorpore pessoas, processos e tecnologias. Uma estratégia de segurança contínua deve ser baseada no feedback e na adaptação do ambiente para dar suporte a técnicas modernas de desenvolvimento, ao DevSecOps e a necessidades de negócios digitais. Adote uma abordagem de segurança em camadas com defesa em profundidade para aproveitar os recursos de cada camada no seu ambiente, incluindo sistemas operacionais, plataforma de aplicações em container, ferramentas de automação, ativos de software como serviço (SaaS) e serviços em nuvem.

Adotar uma abordagem de DevSecOps pode reduzir o prejuízo médio de uma violação de dados em **5%**.[7]

7 *IBM Security. "**Cost of a Data Breach Report 2020**", 2020.*

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

9 *Qualtrics e Red Hat. Estudo sobre otimização da TI, fevereiro de 2020.*

Ferramentas recomendadas

As ferramentas ideais de segurança e conformidade incluem vários recursos e funcionalidades essenciais.

Análise proativa

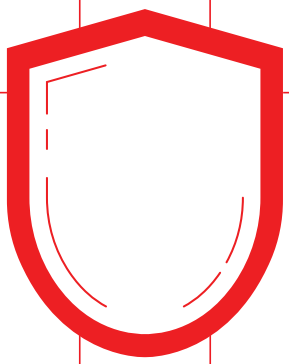
Entender a situação de segurança e conformidade do seu ambiente é o primeiro passo para aprimorá-lo. Ferramentas que oferecem análise automatizada ajudam a monitorar o sistema em intervalos regulares e emitem alertas sobre os problemas, sem desperdício de tempo e esforço da equipe.

Correção priorizada

Ferramentas que oferecem instruções de correção prescritivas acabam com a necessidade de pesquisar as ações necessárias por conta própria, economizando tempo e reduzindo o risco de erros. A priorização de ações com base no possível impacto e nos sistemas afetados ajuda a não perder tempo na aplicação de patches.

Resultados personalizáveis

Algumas verificações de conformidade e de vulnerabilidades não se aplicam a determinados sistemas devido a características específicas de configuração, utilização ou carga de trabalho. As ferramentas ideais são aquelas que permitem definir o contexto de negócios para reduzir falsos positivos, gerenciar os riscos e oferecer uma visão mais realista do status de segurança e conformidade do ambiente.



Relatórios intuitivos

Ferramentas que geram relatórios intuitivos e claros sobre sistemas já receberam patches, os que ainda precisam receber e aqueles que não estão em conformidade com as políticas de segurança facilitam a realização de auditorias e ajudam a entender melhor o status do ambiente.

Interface unificada

Ferramentas que vão além do gerenciamento de apenas um componente ou camada do ambiente ajudam a simplificar as operações de proteção e entender melhor a situação de segurança e conformidade do ambiente. As ferramentas unificadas também dão mais contexto para as verificações e orientações sobre correções.

Insights úteis

Ferramentas que oferecem informações personalizadas para o ambiente ajudam a identificar rapidamente os problemas de conformidade e as vulnerabilidades de segurança que realmente estão ocorrendo, além dos sistemas afetados e dos possíveis impactos. Essas ferramentas também são úteis para priorizar e planejar ações corretivas.

Melhore a segurança e a conformidade com a Red Hat

A Red Hat adota uma abordagem holística no gerenciamento dos riscos de segurança e conformidade. Essa abordagem ajuda a aumentar a velocidade, a escalabilidade e a estabilidade no ambiente de TI inteiro, incluindo servidores bare-metal ou virtualizados e infraestruturas de nuvem privada, pública ou híbrida. Ao incorporar pessoas, processos e tecnologias, as plataformas Red Hat® são ideais para alcançar a eficiência operacional, impulsionar a inovação e melhorar a satisfação dos funcionários.

No coração dessa estratégia está o **Red Hat Enterprise Linux**. Por ser uma base operacional consistente e inteligente para a TI moderna e implantações em nuvem híbrida empresarial, o Red Hat Enterprise Linux oferece benefícios excelentes para sua organização. A consistência na infraestrutura permite que você implante aplicações, cargas de trabalho e serviços usando as mesmas ferramentas, independentemente do local.

A segurança é essencial na arquitetura e no ciclo de vida do Red Hat Enterprise Linux. As proteções em várias camadas contra violações usam controles de segurança automatizados e repetíveis para diminuir os riscos de exposição a vulnerabilidades. Os upgrades de segurança e os patches dinâmicos (Live Patch) críticos fazem parte da subscrição do Red Hat Enterprise Linux e ajudam a manter seu ambiente atualizado e protegido.

As ferramentas de gerenciamento da Red Hat podem ser integradas ao Red Hat Enterprise Linux para que você tenha todos os recursos necessários para gerenciar vulnerabilidades de segurança e riscos de conformidade com mais eficiência.

- Ferramentas configuráveis e linhas de base reduzem a ocorrência de falsos positivos e dão uma visão precisa do status da infraestrutura.
- Recursos de automação aumentam a precisão da configuração e da aplicação de patches, além de reduzir os erros humanos.
- Visualizações personalizáveis oferecem rapidamente as informações certas no momento ideal.
- A correção automatizada e proativa acelera a reparação de problemas, sem a necessidade de entrar em contato com o suporte.
- Uma extensa biblioteca de recursos dá acesso ininterrupto a informações direcionadas e detalhadas.
- Opções locais e de software como serviço (SaaS) permitem implantar ferramentas de acordo com suas preferências.

"Criar servidores adaptados, prontos para o uso e mais seguros desde o início é uma necessidade obrigatória da nossa TI. Com o Red Hat Enterprise Linux associado ao Red Hat Insights temos o poder de implantar servidores que possam ser usados imediatamente e atendam às nossas necessidades específicas assim que ativados."[10]

Steve Short
Gerente de plataformas, Unix, Kingfisher PLC

10 *Comunicado à imprensa da Red Hat. "**Red Hat oferece multiplicador de força para a TI empresarial com monitoramento inteligente aprimorado na apresentação da versão mais recente do Red Hat Enterprise Linux 8**", 21 de abril de 2020.*

Descubra os benefícios das ferramentas de gerenciamento integradas

As ferramentas de gerenciamento da Red Hat são baseadas em anos de experiência em desenvolvimento e suporte do Linux. Juntas, elas otimizam a administração da TI para poupar o tempo e os esforços da sua equipe, e tornam seu ambiente mais seguro, otimizado e confiável.

Red Hat Insights

Análises preditivas de riscos de TI

Todas as subscrições ativas do Red Hat Enterprise Linux incluem o **Red Hat Insights**, uma solução que ajuda as equipes de TI a identificar e corrigir proativamente várias ameaças para evitar interrupções, downtime não planejado e riscos de segurança e conformidade.

- Faça uma análise profunda dos sistemas para detectar proativamente vulnerabilidades de segurança, problemas de conformidade e violações de política.
- Prescreva e priorize ações corretivas e gere Playbooks do Red Hat Ansible® Automation Platform que possam ajudar.
- Compare sistemas com linhas de base, históricos e outros sistemas.
- Implante com facilidade em ambientes locais e de nuvem.

96%
mais rápido na detecção de problemas específicos de aplicações.[11]

91%
mais rápido na identificação de vulnerabilidades de segurança.[11]

89%
mais rápido na detecção de desvios na configuração.[11]

Mais informações

Red Hat Smart Management

Gerenciamento e correção acionáveis

o **Red Hat Smart Management** combina os recursos avançados de infraestrutura do Red Hat Satellite com a simplicidade de gerenciamento da nuvem para aprimorar e complementar o Red Hat Insights.

- Provisione, aplique patches e controle seus hosts do Red Hat Enterprise Linux e gere relatórios gerais detalhados usando o Red Hat Satellite.
- Identifique e corrija problemas no cloud.redhat.com junto com o Red Hat Insights.
- Corrija os problemas identificados pelo Red Hat Insights com apenas um clique usando o Cloud Connector.

56%
mais eficiente na aplicação de patches de sistema.[12]

14%
a mais de eficiência para equipes de segurança de TI.[12]

23%
a mais de produtividade para equipes de conformidade.[12]

Mais informações

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

12 *Whitepaper da IDC (patrocinado pela Red Hat).* "**Red Hat Satellite ajuda as empresas a otimizar a infraestrutura com ferramentas de automação**", *março de 2020. Documento #US46109220.*

Caso de sucesso

Metalloinvest

Garanta o desempenho dos sistemas críticos usando insights de dados e análises preditivas de riscos

Desafio

A Metalloinvest é uma das principais produtoras e fornecedoras de ferro briquetado a quente (HBI) e derivados de minério de ferro do mundo, além de produzir aço de alta qualidade para o mercado regional. Após décadas de operações, a Metalloinvest se deparou com um novo desafio: a Indústria 4.0 ou a Quarta Revolução Industrial, que tornou as operações automatizadas e voltadas para dados. A empresa decidiu automatizar e digitalizar a produção para operar e usar recursos com mais eficiência. O objetivo da empresa é não somente se tornar a maior mineradora do mundo, mas também a mais produtiva. Para criar uma base para a Indústria 4.0, a empresa buscou integrar e otimizar seu complexo ambiente SAP®.

Solução

Com a ajuda do JSA Group, um fornecedor de serviços gerenciados, a Metalloinvest adotou o Red Hat Enterprise Linux for SAP Solutions para criar uma base empresarial robusta para seu ambiente SAP S/4HANA®. Desenvolvido em colaboração pela **Red Hat e a SAP**, o Red Hat Enterprise Linux for SAP Solutions inclui o Red Hat Insights para análises de dados preditivas e o Red Hat Smart Management para simplificar o gerenciamento de ambientes Red Hat Enterprise Linux usando o Red Hat Satellite e serviços de gerenciamento de nuvem. Trata-se de uma subscrição que combina os recursos de confiabilidade, escalabilidade e alto desempenho do Linux com a tecnologia para requisitos específicos das aplicações SAP.

A Metalloinvest agora executa seu ambiente de produção SAP S/4HANA inteiro no Red Hat Enterprise Linux for SAP Solutions. A empresa pode se beneficiar dos insights de dados completos e análises preditiva de riscos para manter um desempenho estável e confiável em seus sistemas críticos, enquanto se prepara para digitalizar o ambiente de produção.

"Com a Red Hat, temos as ferramentas que tornam nossas operações e funcionários mais produtivos."

Konstantin Zelenkov
CTO, JSA Group

Melhor confiabilidade e desempenho em sistemas operacionais críticos

Insights de dados completos com melhor integração com soluções SAP

Riscos reduzidos no gerenciamento da segurança e suporte abrangente

Leia o caso de sucesso

Quer melhorar a segurança e a conformidade da sua empresa?

Seus negócios dependem das suas aplicações e infraestrutura de TI. Adotar abordagens e ferramentas eficientes para o gerenciamento das vulnerabilidades de segurança e dos riscos de conformidade é um dos principais passos para proteger sua organização. A Red Hat oferece a plataforma Linux e as ferramentas de gerenciamento integradas necessárias para inovações e operações que priorizam a segurança.

Apresente o Red Hat Insights para sua equipe agora mesmo:

red.ht/insights-br

Descubra como acelerar os fluxos de trabalho de TI com o Red Hat Insights:

red.ht/insights_savetime

Leia este resumo sobre como gerenciar riscos de segurança com o Red Hat Insights:

red.ht/insights-security-brief

Assista à demo sobre gerenciamento de riscos com o Red Hat Insights:

red.ht/insights-security-demo

F26049_1120_KVM

Red Hat