Otimize a segurança do Linux com a Red Hat

O valor de negócio do Red Hat Enterprise Linux

A IDC descobriu que as organizações que adotaram o Red Hat Enterprise Linux como padrão alcançaram benefícios de segurança significativos[1], incluindo:

- 33% de aumento na eficiência das equipes de segurança.
- 46% mais agilidade na conclusão de atualizações de segurança.
- 47% mais velocidade na resposta a vulnerabilidades de segurança.

Nem todas as distribuições Linux têm a mesma abordagem de segurança

Todos os dias, surgem novas ameaças à segurança da infraestrutura de TI, e há cada vez mais regulamentações de conformidade. Para proteger as aplicações, processos e cargas de trabalho, é essencial manter a padronização usando uma base que prioriza a segurança. Todas as distribuições Linux® são open source, mas cada uma tem uma abordagem de segurança diferente.

Ao escolher uma distribuição Linux para a padronização, é importante avaliar até que ponto sua empresa está preparada para mitigar novos riscos e atender aos requisitos mais recentes. Como os recursos de segurança da distribuição foram desenvolvidos? É possível aplicar as proteções da distribuição nos seus ambientes com eficiência? Fora do ponto de venda, a distribuição viabiliza e aprimora sua abordagem de segurança, protegendo sua infraestrutura contra ameaças atuais e futuras?

O Red Hat® Enterprise Linux é um sistema operacional reforçado, desenvolvido com base em mais de 30 anos de experiência em Linux por uma empresa líder em tecnologia confiável, segundo mais de 90% das organizações da Fortune 500[2]. Ele oferece uma estratégia de *defesa profunda* para o desenvolvimento, configuração, gerenciamento e suporte a soluções. Descubra nesta visão geral como cada um desses elementos contribui para oferecer uma abordagem de segurança sólida em um sistema operacional confiável.

O Red Hat Enterprise Linux proporciona segurança e confiabilidade essenciais aos negócios

A Red Hat usa software open source criado por uma comunidade global, descentralizada e transparente de engenheiros que priorizam a segurança da tecnologia. Esse é o foco do Red Hat Enterprise Linux, que facilita o uso de recursos de segurança no momento da compilação e oferece suporte aos usuários com a vigilância contínua e a correção de novas ameaças.

Segurança no ciclo de vida de desenvolvimento de software

Ao escolher uma distribuição Linux, analise os padrões seguidos na fase de desenvolvimento.

A Red Hat prioriza a segurança durante o ciclo de vida de desenvolvimento, alinhando-se aos padrões National Institute of Standards and Technology (NIST), Secure Software Development Framework (SSDF) e International Organization for Standardization (ISO), bem como às orientações do Open Worldwide Application Security Project (OWASP).

O Red Hat Product Security realiza melhorias contínuas na segurança dos pipelines de produção da Red Hat, permitindo que os sistemas e equipes acessem a confidencialidade, disponibilidade e integridade das nossas soluções e serviços. Para diversos clientes da Red Hat em setores altamente regulamentados, a garantia da segurança da cadeia de suprimentos de software é um requisito que antecede a implantação.

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

1 Whitepaper da IDC, patrocinado pela Red Hat. "O valor de negócio ao padronizar no Red Hat Enterprise Linux". Documento #US52594324, setembro de 2024.

2 Dados de clientes Red Hat e da lista da Fortune 500, junho de 2024.

Segurança integrada à produção

A melhor plataforma Linux para sua organização é aquela que capacita sua equipe a aplicar proteções com eficiência seguindo as práticas recomendadas de segurança. A plataforma Linux da Red Hat incorpora mecanismos de segurança em várias camadas. Por exemplo, configurações padrão de segurança, controles de acesso com privilégios mínimos e automação.

Os diferentes perfis de segurança com configurações padrão do Red Hat Enterprise Linux oferecem segurança às suas imagens desde o início. Conforme práticas recomendadas, essas linhas de base de segurança permitem que os administradores apliquem a configuração no momento da compilação. Assim, a implantação atende aos requisitos de conformidade e das políticas de segurança corporativa. Isso reduz os riscos e mitiga os erros humanos nas tarefas que seriam realizadas manualmente após a compilação.

O Red Hat Enterprise Linux ajuda os clientes a alcançarem suas metas de segurança

Quando a Universidade de Sussex precisou migrar servidores críticos para os negócios para um sistema operacional com suporte completo, ela trabalhou com a empresa de consultoria de TI WM Promus para adotar o Red Hat Enterprise Linux. Assim, ela reduziu o risco de um ataque cibernético e conquistou uma certificação governamental significativa por demonstrar um alto grau de segurança operacional.

"O patrimônio de TI da universidade é imenso. Migrar para o Red Hat Enterprise Linux minimizou as interrupções e permitiu reduzir os riscos rapidamente."[3]

Eileen O'Mahony,
Gerente geral, WM Promus

Roadmap para combater ameaças futuras

Ter uma abordagem de segurança forte envolve a preparação para lidar com ameaças futuras e a capacidade de manter a conformidade com novos requisitos. Em algumas distribuições Linux, os usuários precisam se preparar sozinhos, o que os leva a procurar soluções da comunidade.

O Red Hat Enterprise Linux conta com uma equipe de soluções e desenvolvimento que monitora novas ameaças e cria métodos para enfrentá-las ativamente. Os experts da Red Hat são membros ativos da comunidade de segurança, e muitos deles participam do projeto OpenSCAP: um framework open source para monitorar a segurança e a conformidade em sistemas Linux.

Suporte às demandas regionais de conformidade ao redor do mundo

Outro fator importante para sua escolha é considerar se a distribuição Linux atende aos diferentes requisitos de conformidade das suas equipes e clientes. Ela é compatível com validações e certificações comuns de cibersegurança, ou sua equipe precisará resolver isso depois?

Ao longo dos anos, a Red Hat fez investimentos significativos para garantir que o Red Hat Enterprise Linux ajudasse as organizações a atender aos rigorosos requisitos globais de segurança em suas regiões e adotar as práticas recomendadas com a maior eficiência possível. Com mais de 100 escritórios em mais de 40 países, a equipe da Red Hat sabe que inúmeras regulamentações de conformidade variam de país para país.

Para atender às demandas regionais de conformidade, a Red Hat obteve uma grande variedade de validações e certificações para suas soluções, como o Red Hat Enterprise Linux.

Métodos de implantação eficientes

Atender aos requisitos de segurança e seguir as práticas recomendadas pode sobrecarregar as equipes encarregadas. Os processos de verificação, validação e certificação podem ser demorados e envolver várias equipes.

O image mode, método de implantação do Red Hat Enterprise Linux, é uma abordagem nativa em container para desenvolver, implantar e gerenciar o sistema operacional. Assim, é muito mais fácil para as equipes aplicar as ferramentas de segurança de container, como verificação, validação, criptografia, atestados de proteção e elementos básicos do sistema operacional. Essa abordagem reduz os riscos e aumenta a eficiência.

3 Estudo de caso da Red Hat. "WM Promus ajuda universidade a aumentar a eficiência e a segurança". 23 de outubro de 2024.

Gerenciamento de riscos proativo

O sistema operacional deve ser simples e eficiente, permitindo que suas equipes estejam sempre cientes das possíveis ameaças e problemas de segurança.

O Red Hat Insights é uma solução de gerenciamento de sistemas de ponta a ponta integrada ao Red Hat Enterprise Linux. Com ele, os usuários identificam e relatam problemas, priorizam os riscos com base no possível impacto nos negócios e até mesmo acionam a próxima ação em uma cadeia de ferramentas de automação. O Red Hat Insights verifica as Vulnerabilidades e Exposições Comuns (CVE) e ajuda a priorizar as ações de correção considerando o tipo de risco, a gravidade e o impacto.

Isso permite que suas equipes auditem a conformidade regulatória com as políticas do OpenSCAP, corrijam sistemas fora dos padrões e gerem relatórios de conformidade proativamente. O Red Hat Insights também permite detectar rapidamente os sinais de malware ativos nos sistemas do seu ambiente de nuvem híbrida.

Suporte contínuo à segurança

A plataforma Linux escolhida para a padronização trará reflexos para sua organização por muitos anos. Por isso, é essencial entender o suporte que você terá logo após a implantação e mais adiante.

O Red Hat Enterprise Linux garante dez anos de atualizações e suporte para os lançamentos principais, além de acesso ao Portal do Cliente Red Hat, onde os usuários encontram informações sobre vulnerabilidades de segurança contínuas e etapas para mitigar seus impactos. A equipe de resposta a incidentes de segurança em soluções (PSIRT) da Red Hat ajuda os usuários a entenderem os riscos e implicações das novas CVE, além de oferecer orientações para correção.

Parceiros de confiança e histórico de colaboração

A Red Hat participa de vários programas de divulgação coordenada e responsável do setor. Com um longo histórico de participação em organizações de segurança, como o Forum of Incident Response and Security Teams (FIRST), Open Source Security Foundation (OpenSSF), Oasis e outras, a Red Hat continua sendo parceira global de colaboração na segurança.

A Red Hat fez uma parceria com o CVE.org para viabilizar a missão de identificar, definir e catalogar as vulnerabilidades de cibersegurança divulgadas publicamente, sendo uma das seis organizações do mundo que tem a função especial Root. Além disso, a Red Hat é uma autoridade de numeração CVE (CNA), podendo atribuir IDs às vulnerabilidades e publicar registros de CVE. Em outras palavras, quando um usuário do Red Hat Enterprise Linux é notificado sobre uma nova CVE, uma equipe de experts em segurança que conhece bem a plataforma já iniciou a pesquisa, avaliação e investigação das etapas de correção necessárias.

Colaboração da comunidade

Até mesmo usuários de outras distribuições Linux podem se beneficiar das práticas de segurança da Red Hat. Seguindo a filosofia open source, a Red Hat acredita na colaboração da comunidade para proporcionar respostas rápidas, aplicação de patches e estratégias de mitigação para as vulnerabilidades que afetam o sistema Linux, mantendo a reputação do sistema operacional de ser altamente focado em segurança.

A equipe da Red Hat colabora com equipes do mundo todo para desenvolver práticas de segurança open source. Alguns exemplos são a criação do OpenSCAP, a associação ao OpenSSF e as contribuições para o OSV.dev.

A colaboração também abrange o código da Red Hat, que pode receber inspeção, auditoria, revisão e contribuição dos membros da comunidade.

Otimize a segurança do Linux com a Red Hat

Ao padronizar o seu ambiente com o Red Hat Enterprise Linux, você conta com o suporte de uma empresa que vê a segurança como prioridade. Descubra como a Red Hat ajuda sua organização com uma plataforma Linux que prioriza a segurança.

Sobre a Red Hat

A Red Hat é líder mundial no fornecimento de soluções de software open source empresarial, realizando parcerias com as comunidades para oferecer tecnologias confiáveis e de alto desempenho para Linux, nuvem híbrida, containers e Kubernetes. A Red Hat ajuda os clientes a desenvolver aplicações nativas em nuvem, integrar aplicações de TI novas e existentes e automatizar e gerenciar ambientes complexos. Parceira de confiança das empresas da Fortune 500, a Red Hat oferece serviços de consultoria, treinamento e suporte premiados, compartilhando os benefícios da inovação open source com todos os setores. A Red Hat é um hub que conecta uma rede global de empresas, parceiros e comunidades, ajudando as organizações a se transformarem, crescerem e se prepararem para o futuro digital.

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

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

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

br.redhat.com