Red Hat Enterprise Linux | Segurança e Conformidade

Uma base segura para a execução de cargas de trabalho em nuvem híbrida aberta

O Red Hat Enterprise Linux oferece suporte aos requisitos fundamentais de segurança e conformidade em um sistema operacional:

- Recursos de segurança modernos e em várias camadas para reduzir o risco
- Automação da aplicação de patches e correção para minimizar o downtime
- Segurança dos processos e da validação do ciclo de vida de desenvolvimento
- Ferramentas de conformidade integradas para atender aos padrões de segurança
- Controles de segurança consistentes em toda a nuvem híbrida
- Segurança da carga de trabalho em ambientes de nuvem pública

Proteger o sistema operacional é fundamental

As falhas de segurança estão cada vez mais frequentes e sofisticadas. Por isso, é essencial integrar a segurança a todas as partes da infraestrutura. Os sistemas operacionais (SO), que servem de base para a execução de todas as aplicações, precisam de recursos de segurança profundos e abrangentes para se proteger contra vulnerabilidades e atender aos requisitos de conformidade.

O Red Hat® Enterprise Linux® oferece uma base mais segura para escalar aplicações existentes e implementar novas tecnologias, de maneira consistente, em infraestruturas bare-metal, virtuais, em nuvem e na edge. Os recursos integrados de segurança e conformidade do Red Hat Enterprise Linux ajudam a:

- **Mitigar:** gerencie a segurança e diminua o risco de falhas antes que seus dados, seus sistemas e sua reputação fiquem vulneráveis.
- **Proteger:** automatize e mantenha os controles de segurança em escala e com downtime mínimo.
- **Estar em conformidade:** simplifique os padrões de conformidade de organizações com ambientes altamente regulados.

Reduza o risco de expor seus dados, sistemas ou sua reputação

Upgrades e patches de segurança críticos: aumente o uptime e a resiliência com aplicação de patches de kernel e correção de vulnerabilidades de segurança em tempo real. Solucione problemas de segurança críticos e importantes sem reinicializações para assegurar o uptime das aplicações críticas.

Listas de permissões de aplicações (fapolicyd): impeça o acesso não autorizado com listas de permissões para que programas confiáveis sejam executados em uma máquina ou rede. Aproveite políticas pré-definidas ou personalize suas próprias políticas para identificar ou impedir a execução de aplicações modificadas.

Segurança da cadeia de suprimentos: diminua o risco do ciclo de vida do software com práticas de desenvolvimento mais seguras que incluem análise de código estático em toda a base de códigos. Isso pode reduzir falhas de segurança antes do envio, além de melhorar os projetos open source upstream.

Gerenciamento de vulnerabilidade escalável: use o Red Hat Insights para integrar a configuração de segurança escalável e o gerenciamento de vulnerabilidades. Personalize e aplique políticas de segurança nos sistemas, monitore e corrija as exposições, se necessário.

Automatize controles de segurança em escala

Proteção da raiz de confiança do hardware: use uma raiz de confiança baseada no hardware para assegurar a integridade do software nos sistemas. Use tokens de hardware externos para oferecer configurações consistentes de segurança do hardware, incluindo cartões inteligentes e módulos de segurança de hardware (HSMs).

Criptografia de disco vinculada à rede (NBDE): automatize a liberação de sistemas criptografados on-premise ou na nuvem híbrida sem gerenciar as chaves de criptografia manualmente. Com essa camada extra de proteção dos dados, eles ficam disponíveis apenas quando estão seguros.

Criptografia modernizada e escalável: use configurações de criptografia personalizáveis e que abrangem todo o sistema para proteger seus dados e atender aos requisitos de conformidade. Gerencie a criptografia do sistema com um método fácil, de apenas um comando.

Controles de acesso obrigatórios do Security-Enhanced Linux (SELinux): equipe arquivos, processos, usuários e aplicações com controles de acesso granulares para minimizar o risco de escalação inadequada de privilégios. Use aplicações ou containers para personalizar o acesso. Esse nível de controle assegura a integridade e confidencialidade dos dados, além de proteger os processos de entradas não confiáveis.

Gerenciamento de identidade centralizado: gerencie a autenticação e a autorização de usuários no ambiente com controle de acesso em escala baseado em políticas e funções. Faça a integração fácil com outra identidade e acesse diretórios ou soluções de gerenciamento.

Atenda aos requisitos de conformidade e otimize as auditorias

Certificações de segurança verificadas: suporte a mandatos de conformidade do cliente. O objetivo da Red Hat é que os upgrades de manutenção do Red Hat Enterprise Linux tenham validação independente em comparação com os padrões FIPS e que cada versão do EUS obtenha a certificação Common Criteria.

Ferramentas de conformidade integradas: faça varreduras de configuração e vulnerabilidade em um sistema local para validar a conformidade. Gere relatórios e linhas de base OpenSCAP e, em seguida, use a automação para corrigir sistemas que não estejam em conformidade. Faça a integração com o Red Hat Smart Management e o Red Hat Insights para gerenciar a conformidade em escala.

Gravação de sessões: grave as atividades administrativas como arquivos visualizáveis para atender aos requisitos de auditoria de segurança ou ofereça reproduções para auxiliar a solução de problemas após o incidente. Personalize com facilidade quais usuários ou grupos terão autorização para gravar.

Funções do sistema: automatize a configuração de segurança e mantenha a consistência nos sistemas ao longo do tempo para assegurar segurança e conformidade em escala. Implante e gerencie a segurança do Red Hat Enterprise Linux com menos recursos do que nunca. Para isso, use as funções do SELinux, certificados, NBDE, gravação de sessões, SSH, política de criptografia e mais.

Experimente tudo o que o Red Hat Enterprise Linux tem a oferecer

Entre em contato com seu representante de vendas da Red Hat ou descubra como o Red Hat Enterprise Linux pode ajudar a gerenciar a segurança e a conformidade em toda sua infraestrutura de nuvem híbrida.

SOBRE A RED HAT

A Red Hat ajuda os clientes a definir padrões entre diferentes ambientes, desenvolver aplicações nativas em nuvem, integrar, automatizar, proteger e gerenciar ambientes complexos com serviços de consultoria, treinamento e suporte premiados.

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
#F29077_0621