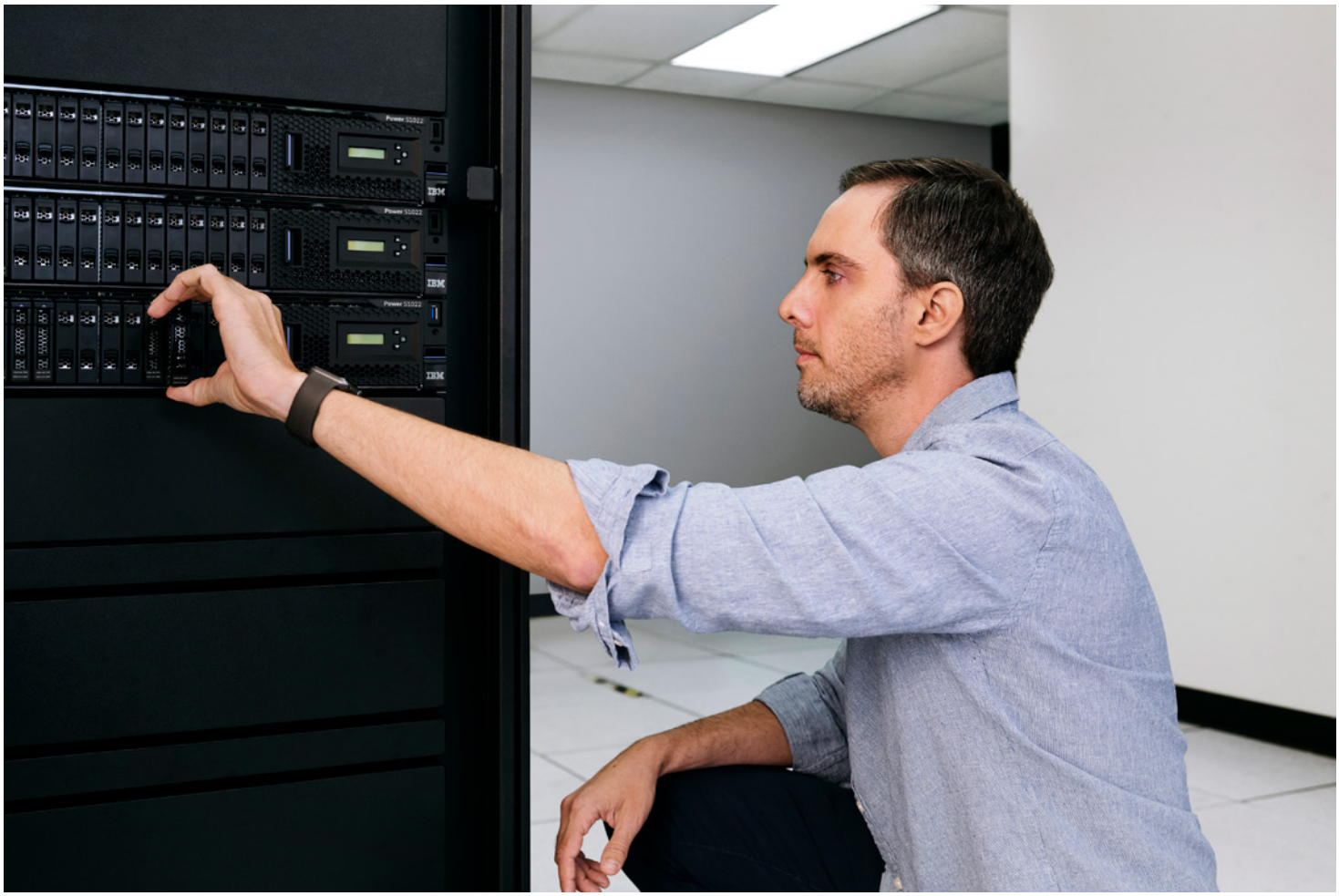
Uma abordagem de segurança em várias camadas com o IBM Power

Infraestrutura essencial para uma abordagem zero trust



Índice

03
O cenário de TI atual

04
Uma abordagem holística

06
Uma estratégia zero trust

07
Conheça o IBM Power

10
Tecnologia IBM PowerSC 2.0

12
Integração contínua

TI corporativa na era dos ataques cibernéticos sofisticados

O cenário de TI atual

Desde o início da pandemia do COVID-19, foi registrado um número impressionante de violações de dados devastadoras. O custo médio de uma violação de dados agora é de USD 4,24 milhões, um aumento de 10% em relação aos USD 3,86 milhões relatados no ano passado. Este é o maior aumento que a indústria testemunhou nos últimos sete anos[1], tornando a segurança uma das principais preocupações. Melhorar a estratégia de segurança e permitir que suas empresas se movam com rapidez, proteção e segurança neste mundo sempre ativo é o foco de muitos executivos hoje, resultando em maiores orçamentos de segurança. No entanto, o aumento dos gastos e as mudanças tecnológicas introduzem novas complexidades e riscos que continuam a ameaçar a segurança de TI. Uma das principais preocupações dos profissionais de segurança é o número crescente de vetores de ataques sofisticados que continuam a expor, mais do que nunca, aspectos dos negócios atuais.

Vulnerabilidades nos níveis de hardware e firmware podem não ter sido pontos de grande preocupação em um passado não muito distante. No entanto, agora eles são os principais alvos no cenário de ameaças de hoje.

De muitas maneiras, os desafios de cibersegurança que sua empresa deve superar hoje podem ser reduzidos a duas verdades empíricas:

- O stack de TI está se expandindo e os hackers estão ampliando seus horizontes.
- As organizações devem ficar à frente das ameaças futuras para proteger suas plataformas com o mais alto nível de segurança para proteger sua infraestrutura de nuvem híbrida.

USD
4,24 milhões

O custo médio de uma violação de dados agora é de **USD 4,24 milhões, um aumento de 10%** desde o último ano reportado USD 3,86 milhões.

As realidades do cenário de ameaças atual

Uma abordagem holística

As empresas confiam em seus sistemas de segurança para evitar ameaças atuais e futuras à propriedade intelectual, informações corporativas confidenciais, dados de clientes e privacidade da carga de trabalho.

A forma como os profissionais abordam estrategicamente a segurança de TI é fundamental para evitar violações de dados e ataques cibernéticos. As vulnerabilidades de segurança não apenas podem resultar em tempo de inatividade, mas também são caras para qualquer organização. Os ataques de ransomware representam a maior ameaça, custando às empresas USD 4,62 milhões por ataque em média[1]. A integridade da plataforma IBM® Power® pode reduzir o risco de ransomware implementando detecção e resposta de endpoint (EDR) e conceitos de zero trust, como autenticação multifator (MFA) contínua.

Adotar uma abordagem orientada aos negócios, à conformidade ou à monetização por si só não consegue oferecer proteção adequada para os processos de negócios contra o número crescente de riscos dos sistemas de TI. Abordagens solitárias podem ignorar os principais aspectos interdisciplinares de uma estratégia de segurança eficiente e integrada. O curso de ação ideal envolve planejamento e avaliação para identificar riscos em áreas-chave relacionadas à segurança. A tecnologia IBM Power e IBM® Power10 oferecem uma abordagem holística, zero trust e multicamadas para sua estratégia de segurança para garantir que sua organização esteja mais segura e em conformidade. Essa abordagem em várias camadas inclui:

- Hardware
- Sistema operacional
- Firmware
- Tecnologia IBM® PowerSC 2.0
- Hypervisor

A adoção de uma abordagem de segurança holística pode permitir que sua organização atenda às demandas das ameaças que afetam o cenário de segurança.

Os hackers estão cada vez mais sofisticados

Quanto mais uma organização sai das limitações dos data centers locais tradicionais e faz a transição para ambientes de nuvem híbrida ou multinuvem, mais os invasores cibernéticos precisam pensar fora da caixa. A implementação de privilégios mínimos e o aumento dos controles baseados em perímetro ajudarão a gerenciar o aumento do número de ameaças. Os métodos deles do passado não estão mais contidos no nível da rede, levando a horizontes mais amplos e ataques mais capazes.

A segurança é vital à medida que o acesso a dados aumenta

Os dados dentro de uma organização agora podem ser armazenados e acessados por funcionários de praticamente qualquer lugar – em servidores, ambientes de nuvem híbrida e vários dispositivos móveis e de edge. Esse cruzamento inextricável de servidor e dispositivo é o subproduto da contínua transformação e modernização digital. Como resultado, isso cria de forma acessível uma infinidade de vetores de ataque prontos para serem explorados.

Uma regulamentação mais rígida está afetando os perfis de risco

Os processos que estão sendo implementados para ajudar a garantir a conformidade regulatória também podem levar à exposição não intencional a riscos. O Regulamento Geral de Proteção de Dados (RGPD) é apenas um desses desenvolvimentos recentes de uma tendência crescente. As entidades governamentais estão prestando muito mais atenção em como as organizações usam os dados. No entanto, eles também adicionam camadas de complexidade às operações de negócios diárias.

Os funcionários são vulnerabilidades esperando acontecer

As credenciais comprometidas dos funcionários são responsáveis por 20% de todas as violações de dados no ano passado[1]. Além das informações de login, os golpes de phishing e o comprometimento de e-mail são outras maneiras pelas quais os funcionários colocam em risco, sem saber, as informações da empresa. Sua força de trabalho sempre apresentará algum nível de risco — não importa quais controles de segurança você implemente ou o quanto você lida bem com vulnerabilidades. Na era do crime cibernético, é imperativo treinar os funcionários sobre essas ameaças de segurança comuns e ter um sistema de relatórios em vigor. Seu trabalho árduo para proteger os endpoints e aderir à conformidade pode ser discutível por um erro ou um ataque malicioso inteligente.

Enquanto isso, muitas organizações lutam para encontrar e reter uma equipe competente de cibersegurança e se veem presas a uma escassez perpétua de habilidades. Para combater essa escassez de habilidades, as organizações podem implementar o gerenciamento de segurança simplificado que automatiza as operações, a conformidade, a aplicação de correções e o monitoramento. Beneficie-se da segurança de ponta a ponta projetada para proteger com detecção de endpoint adicional sem os recursos adicionais.

O volume, a variedade e a velocidade do cenário de ameaças cibernéticas de hoje só se multiplicarão à medida que as arquiteturas de TI continuarem a evoluir e a se adaptar às mudanças nas marés da tecnologia, cultura de trabalho e conformidade. Isso significa que sua estratégia de segurança também deve evoluir para ir além do nível da rede.

Uma estratégia zero trust é essencial

Uma abordagem holística

A implementação de conceitos de zero trust pode ajudar as organizações a abordar a segurança em um ambiente de TI frequentemente complexo. Os profissionais de TI enfrentam dificuldades com a visibilidade e o controle em ambientes de nuvem híbrida e multinuvem. Zero trust gerencia os riscos mudando para uma estratégia mais abrangente que restringe os controles de acesso sem afetar o desempenho ou a experiência do usuário. A construção de segurança em todos os níveis de seu stack pode ser alcançada com a implementação de várias soluções de segurança de fornecedores terceirizados.
No entanto, essa abordagem piora a complexidade que já existe — e introduz ainda mais vulnerabilidades e pontos de exposição em sua rede. Seu melhor recurso é adotar uma abordagem zero trust em várias camadas. Isso protege todos os dados e sistemas da sua organização, além de minimizar a complexidade.
Com isso em mente, o IBM® Information Security Framework ajuda a garantir que todos os aspectos de segurança de TI possam ser abordados adequadamente ao usar uma abordagem holística para a segurança orientada aos negócios.

O IBM Information Security Framework foca em:

1. Infraestrutura — proteja-se contra ataques sofisticados com insights sobre usuários, conteúdo e aplicações.
2. Segurança avançada e pesquisa de ameaças — adquira conhecimento sobre vulnerabilidades e metodologias de ataque e aplique esses insights por meio de tecnologias de proteção.
3. Pessoas — gerencie e estenda a identidade corporativa em todos os domínios de segurança com inteligência de identidade abrangente.
4. Dados — proteja a privacidade e a integridade dos ativos mais confiáveis da sua organização.
5. Aplicações — reduza o custo de desenvolvimento de aplicações mais seguras.
6. Inteligência e análise de dados de segurança — otimize a segurança com contexto, automação e integração adicionais.
7. Filosofia zero trust – Conecte e proteja os usuários certos aos dados certos enquanto protege sua organização.

Saiba mais sobre o IBM Security Framework (PDF, 25.2 MB) e como você pode acrescentar mais detalhamento.

Como a tecnologia IBM Power protege o stack

Conheça o IBM Power

Com a tecnologia IBM Power, você pode aumentar a resiliência cibernética e gerenciar riscos com segurança abrangente de ponta a ponta que se integra em todo o stack — do processador e firmware ao sistema operacional e hypervisors, às aplicações e recursos de rede, até o gerenciamento do sistema de segurança.

Hardware, firmware e hypervisor

Aceleradores no chip
O chip do processador IBM Power10 foi projetado para aprimorar o desempenho de mitigação de canal lateral e é equipado com isolamento de CPU aprimorado dos processadores de serviço. Este processador de 7nm foi projetado para oferecer um aumento de até 3x na capacidade resultando em maior desempenho[2].

Criptografia de ponta a ponta
A criptografia de memória transparente das soluções IBM Power foi projetada para permitir segurança de ponta a ponta que atende aos exigentes padrões de segurança que as empresas enfrentam hoje. Ele também foi projetado para auxiliar na aceleração de criptografia, criptografia de segurança quântica e criptografia homomórfica completa para proteção contra ameaças futuras. A criptografia acelerada para o mais novo modelo de sistema IBM Power tem desempenho de criptografia AES (Advanced Encryption Standard) 2,5 vezes mais rápido por núcleo do que a tecnologia IBM Power E980[3]. As organizações podem se beneficiar da criptografia de memória transparente sem configuração de gerenciamento adicional.

Software EDR
O aumento de ameaças externas torna a segurança de endpoints crítica quando se trata de proteger dados de clientes e ativos digitais. Ao detectar quaisquer ameaças potenciais no endpoint, as organizações podem agir rapidamente e resolver incidentes sem interromper a continuidade dos negócios. Uma abordagem integrada elimina complicações e protege sua organização até mesmo dos ataques mais perigosos.

2,5 vezes

A criptografia acelerada para o mais novo modelo de sistema IBM Power tem **desempenho de criptografia AES (Advanced Encryption Standard) 2,5 vezes mais rápido por núcleo** do que a tecnologia IBM Power E980[3].

Princípios de habilitação, como autenticação multifator e privilégio mínimo, trazem proteção adicional, protegendo todas as APIs, endpoints, dados e recursos de nuvem híbrida.

Princípios zero trust
As organizações estão evoluindo para adotar princípios zero trust para ajudar a gerenciar essas ameaças crescentes. Princípios de habilitação, como autenticação multifator e privilégio mínimo, trazem proteção adicional, protegendo todas as APIs, endpoints, dados e recursos de nuvem híbrida.

A estrutura zero trust da IBM dá vida a esse conceito.

- **Colete insights** – entenda os usuários, dados e recursos para criar as políticas de segurança necessárias para garantir proteção completa.
- **Proteção** – proteja a organização validando o contexto de forma rápida e consistente e aplicando políticas.
- **Detecção e resposta** – resolva violações de segurança com impacto mínimo nas operações de negócios.
- **Analise e aprimore** – aprimore continuamente a postura de segurança ajustando políticas e práticas para tomar decisões mais informadas.

Ao implementar princípios zero trust, as empresas podem inovar e escalar com segurança.

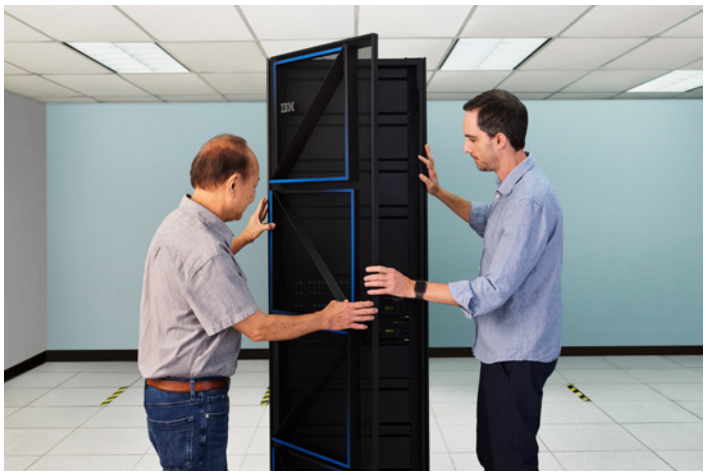
Inicialização mais segura em soluções IBM Power10
A inicialização mais segura foi projetada para proteger a integridade do sistema, verificando e validando todos os componentes de firmware por meio de assinaturas digitais. Todo firmware lançado pela IBM é assinado digitalmente e verificado como parte do processo de inicialização. Todos os sistemas IBM Power vêm com um módulo de plataforma confiável que acumula medições de todos os componentes de firmware carregados em um servidor, permitindo sua inspeção e verificação remota.

Hypervisor corporativo IBM PowerVM
O hypervisor corporativo IBM PowerVM® tem um excelente histórico de segurança quando comparado aos principais concorrentes, para que você possa proteger com confiança suas máquinas virtuais (VMs) e ambientes de nuvem.

Sistema operacional

Os sistemas IBM Power oferecem recursos de segurança líderes para uma ampla variedade de sistemas operacionais, tais como IBM® AIX®, IBM i e Linux®. A tecnologia EDR para IBM Power oferece segurança adicional para cargas de trabalho de VM, garantindo proteção completa em cada endpoint na rede. Para sistemas que dependem de senhas para serem seguros, os sistemas operacionais AIX e Linux utilizam a autenticação multifator (MFA) IBM PowerSC que requer níveis de autenticação para todos os usuários, protegendo contra malware de quebra de senha. Os recursos variam dependendo do sistema operacional, mas os exemplos desses recursos incluem:

- Atribua funções administrativas normalmente reservadas para o usuário root sem comprometer a segurança
- Criptografe dados em nível de arquivo por meio de armazenamentos de chaves individuais
- Obtenha maior controle sobre os comandos e funções disponíveis para os usuários, além de controle sobre quais objetos eles podem acessar
- Registre o acesso a um objeto no diário de auditoria de segurança usando os valores do sistema e os valores de auditoria do objeto para usuários e objetos
- Carregue a criptografia em uma unidade inteira, primeiro criptografando um objeto e depois gravando no formato criptografado
- Meça e verifique cada arquivo antes de abrir para o usuário solicitante



Cargas de trabalho, VMs e contêineres

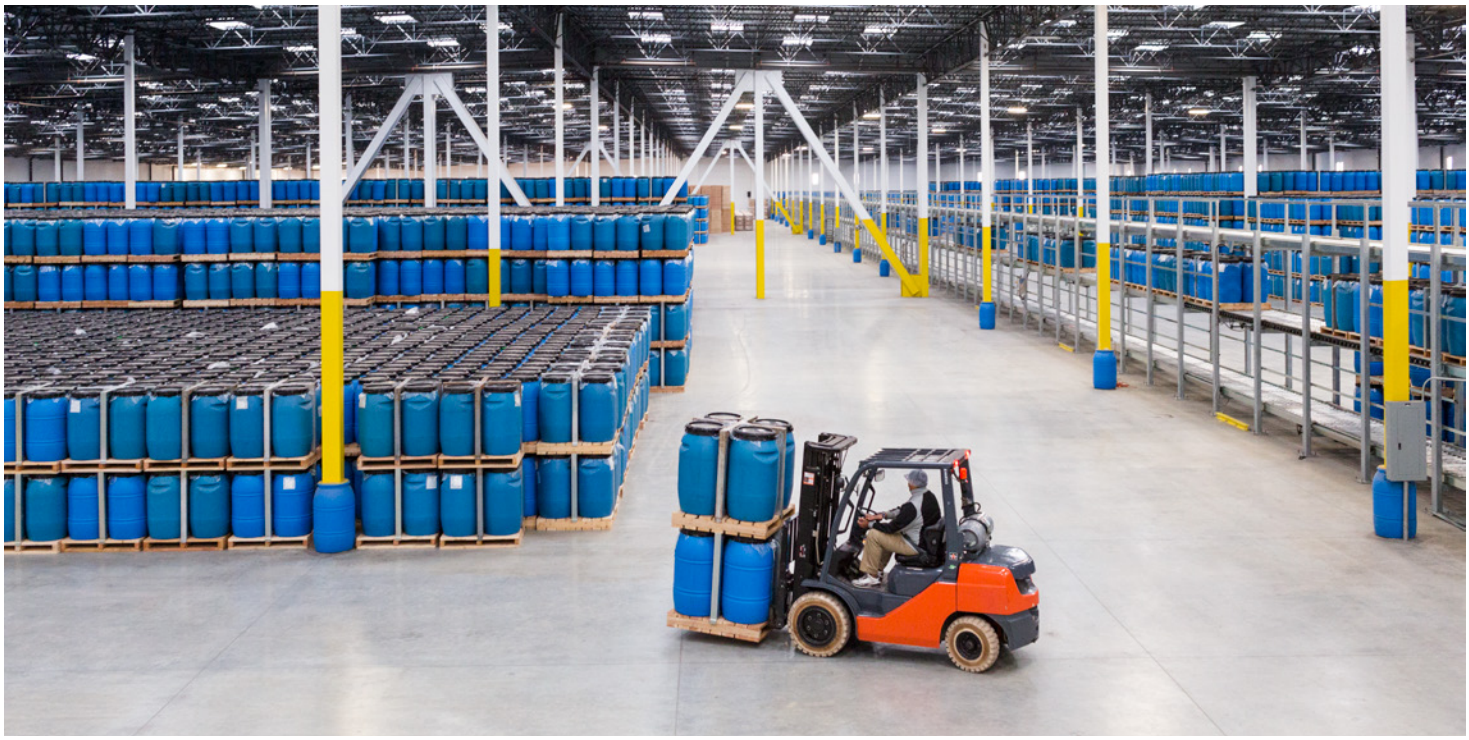
As cargas de trabalho não estão mais restritas a data centers locais; elas estão migrando continuamente para ambientes de nuvem híbrida e multinuvem virtualizados. Como exemplo, muitas organizações estão adotando contêineres para implementar aplicações novas e existentes em infraestruturas híbridas.

Esses ambientes e cargas de trabalho cada vez mais dinâmicos exigem recursos de segurança igualmente versáteis. As soluções IBM Power podem atender às necessidades de segurança preservando a privacidade da carga de trabalho com aceleração de algoritmo criptográfico, armazenamento seguro de chave e auxílio de CPU para criptografia pós-quântica e algoritmos criptográficos de criptografia totalmente homomórfica (FHE).

Para atender aos requisitos de segurança exclusivos de implementações em contêineres, a IBM também fez parceria com fornecedores de software independentes (ISVs) como Aqua Security, que desenvolve com a tecnologia IBM Power e Red Hat® OpenShift® Container Platform para proteger ainda mais os contêineres ao longo de seu ciclo de vida.

Os servidores IBM Power são projetados para proteger dados do local à nuvem com criptografia de memória de ponta a ponta e desempenho criptográfico acelerado. As políticas incorporadas para cargas de trabalho nativas da nuvem, incluindo VMs, contêineres e funções sem servidor, são criadas para ajudar os clientes Red Hat OpenShift e IBM Power ao integrar seus requisitos de segurança e conformidade para modernização de aplicações.

Mobilidade de partição em tempo real (LPM)
A tecnologia IBM Power permite proteger dados em movimento. LPM protege VMs por meio de criptografia quando você precisa migrar de um sistema para outro. Se você virtualizou data centers local, ambientes de nuvem híbrida ou ambos, esse recurso é fundamental.



Produtos de segurança integrados em soluções IBM Power

IBM PowerTecnologia SC 2.0

A tecnologia IBM® PowerSC 2.0 é uma oferta do portfólio integrada para segurança e conformidade corporativa em ambientes virtuais e na nuvem. Ela fica no topo de seu stack enquanto apresenta uma UI baseada na web para gerenciar os recursos de segurança da tecnologia IBM Power que residem nas soluções de nível mais baixo.

Com seus recursos de simplificação e automação, a tecnologia IBM PowerSC 2.0 pode reduzir tempo, custo e risco ao otimizar o monitoramento e o cumprimento da conformidade. Essa solução é compatível com processos de auditoria e permite que os clientes obtenham certificações de conformidade com mais eficiência. Ele também pode reduzir os riscos de segurança aumentando a visibilidade em todo o stack.

Recursos do IBM PowerSC 2.0 Standard Edition

Tecnologia de autenticação multifator (MFA)
A MFA agora está integrada às soluções IBM PowerSC 2.0. Isso simplifica a implementação de mecanismos de MFA seguindo o princípio de zero trust de “Nunca confie, sempre verifique”. Essa abordagem é compatível com fatores alternativos para que os usuários façam login com a autenticação baseada em RSA SecurID e opções de autenticação de certificado, incluindo cartão de acesso comum (CAC) e cartões de verificação de identificação pessoal (PIV). O IBM PowerSC MFA aumenta os níveis de garantia dos sistemas exigindo fatores de autenticação adicionais para os usuários.

A tecnologia IBM PowerSC 2.0 pode reduzir tempo, custo e risco

Recursos de EDR
As soluções IBM PowerSC 2.0 introduzem EDR para Linux em cargas de trabalho IBM Power, oferecendo os mais novos recursos padrão do setor para gerenciar a segurança do endpoint, incluindo detecção e prevenção de intrusão, inspeção e análise de log, detecção de anomalias e resposta a incidentes.

Automação de conformidade
A família IBM Power vem com perfis pré-construídos compatíveis com uma infinidade de padrões de mercado. Você pode personalizar esses perfis e mesclá-los com regras corporativas sem precisar tocar em Extensible Markup Language (XML).

Conformidade em tempo real
Detecta e alerta você quando alguém abre ou interage com arquivos críticos de segurança.

Conexão de rede confiável
Alerta você quando uma VM não está no nível de correção prescrito. Também o notifica quando as correções ficam disponíveis.

Inicialização confiável
Permite a inspeção e verificação remota da integridade de todos os componentes de software em execução em partições lógicas AIX.

Firewall confiável
Protege e encaminha o tráfego de rede interno entre os sistemas operacionais AIX, IBM i e Linux.

Registro confiável
Cria logs de auditoria centralizados, fáceis de fazer backup, arquivar e gerenciar.

Relatórios pré-configurados e linha do tempo interativa
O IBM PowerSC Standard Edition aceita auditoria com cinco relatórios pré-configurados. Você também tem uma linha do tempo interativa para ver a vida e os eventos de uma VM.

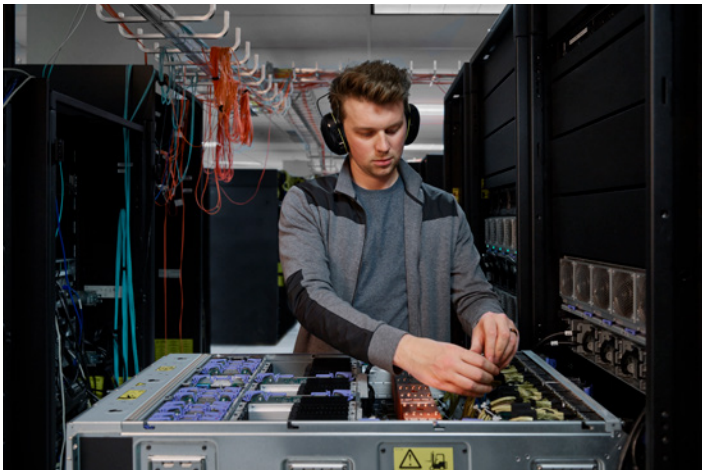
Saiba como simplificar o gerenciamento de segurança e conformidade de TI com IBM PowerSC em ambientes de nuvem e virtualizados

A abordagem mais poderosa para a segurança é aquela integrada continuamente

Integração contínua

À medida que os cibercriminosos continuam avançando em seus métodos e a evolução tecnológica introduz novas vulnerabilidades nos negócios de hoje, é fundamental integrar uma solução de segurança em várias camadas, zero trust e que não aumenta a complexidade organizacional. As soluções IBM Power podem proteger todos os níveis de seu stack, desde edge até a nuvem e ao núcleo, com as soluções detalhadas e totalmente integradas de um único fornecedor. Trabalhar com vários fornecedores apresenta complexidades que podem acabar sendo caras — de várias maneiras. A tecnologia IBM Power é compatível com criptografia de ponta a ponta no nível do processador sem afetar o desempenho. A integração de sua infraestrutura coloca todas as camadas do stack em foco.

A segurança de um único fornecedor pode oferecer vantagens naturais que simplificam e fortalecem sua estratégia de segurança. Com base em três décadas de liderança em segurança, a tecnologia IBM Power traz consigo extensas parcerias com outras organizações dentro e fora da IBM que aprofundam e ampliam ainda mais sua experiência em segurança. Essas parcerias podem permitir que a tecnologia IBM Power acesse uma comunidade ainda maior de profissionais de segurança e garanta que os problemas possam ser identificados rapidamente e tratados com confiança. E com o apoio das unidades de negócios IBM Security® e IBM Research®, juntamente com o portfólio PowerSC 2.0, os servidores Power10 podem impedir várias ameaças, incluindo ataques internos, de cima para baixo.



Agende uma consulta para explorar o potencial das soluções IBM Power

Fale conosco →

Notas

1. Cost of a Data Breach Report 2021, IBM Security, julho de 2021 (PDF, 3.6 MB)
2. O desempenho 3X é baseado na análise de engenharia pré-silício de ambientes Integer, Enterprise e Floating Point em uma oferta de servidor de soquete duplo POWER10 com módulos de 2 × 30 núcleos versus oferta de servidor de soquete duplo POWER9 com módulos de 2 × 12 núcleos. Ambos os módulos têm o mesmo nível de energia. A melhoria na inferência de IA 2 10-20X é baseada na análise de engenharia pré-silício de várias cargas de trabalho (Linpack. Resnet-50 FP32, Resnet-50 BFloat16 e Resnet-50 INT8) em uma oferta de servidor de soquete duplo POWER10 com módulos de 2 × 30 núcleos em comparação com a oferta de servidor de soquete duplo POWER9 com módulos de 2 × 12 núcleos.
3. O AES-256 nos modos GCM e XTS é executado cerca de 2,5 vezes mais rápido por núcleo ao comparar o IBM Power10 E1080 (módulos de 15 núcleos) com o IBM POWER9 E980 (módulos de 12 núcleos) de acordo com medições preliminares obtidas no RHEL Linux 8.4 e na biblioteca OpenSSL 1.1.1g

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo, SP

Produzido nos
Estados Unidos da América
junho de 2022