Benchmark Insights

IBM **Institute for Business Value**

Introdução à segurança de zero trust

Um guia para criar a resiliência cibernética

IBM

Como a IBM pode contribuir

A IBM Security está trabalhando com a zero trust em uma abordagem de segurança moderna e aberta que se alinha às prioridades de seus negócios. Para obter mais informações, acesse: ibm.com/security/zero-trust

Para entender melhor como as organizações estão implementando a segurança de zero trust, o IBM Institute for Business Value (IBV) fez uma parceria com a Oxford Economics para entrevistar mais de 1000 executivos de operações e segurança de organizações de quinze diferentes setores de todo o mundo (consulte “Metodologia de pesquisa” na página 16).

Por Chris McCurdy,
Shue-Jane Thompson,
Lisa Fisher
e Gerald Parham

Principais conclusões

Os novos modelos de negócios aceleram a transformação de segurança.
Conforme os riscos evoluem e novas ameaças surgem, os modelos de segurança tradicionais que contam com perímetros definidos e confiança implícita estão se tornando obsoletos. As organizações que transcendem as fronteiras funcionais e organizacionais tradicionais requerem um modelo de segurança mais abrangente, com diversas camadas e orientado por eventos.

A segurança de zero trust oferece benefícios operacionais claros.
"Zero trust" é uma abordagem dinâmica de segurança na qual as solicitações são validadas por uma combinação de controles de acesso, gerenciamento de identidade e dados contextuais. As organizações pioneiras em zero trust com os recursos mais maduros da área reduziram gastos, aumentaram a eficácia da segurança cibernética e desfrutam de taxas mais altas de retenção de recursos cibernéticos.

Os líderes de zero trust se destacam em quatro competências centrais.
A segurança de zero trust aumenta a resiliência cibernética, transformando a confiança em uma variável operacional. A proficiência em quatro competências centrais e em práticas associadas promove o sucesso da zero trust.

O preço do progresso

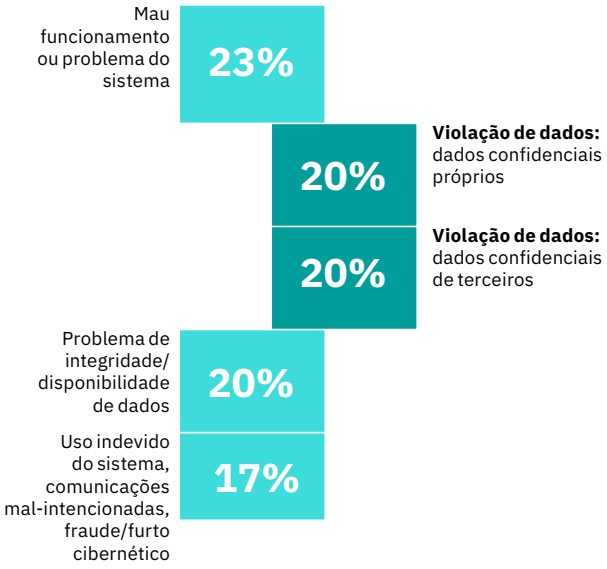
As organizações responderam à pandemia da COVID-19 acelerando a transformação dos negócios digitais, expandindo o espaço da nuvem, aumentando as forças de trabalho remotas e integrando suas cadeias de suprimentos. Como resultado, nossa pesquisa indica que a porcentagem de trabalhadores remotos atendidos pela função de segurança aumentou em 41% entre o final de 2019 e ao longo de 2020.

No entanto, ao realizar comunicações, negócios e interações pessoais on-line, também ocorreu uma ampliação significativa das superfícies de ataques em potencial, o que resulta em um aumento drástico de incidentes de segurança cibernética e registros expostos (veja a Figura 1).[1] À medida que as cargas de trabalho são migradas para a nuvem, as ameaças migram para ela também. Nossa pesquisa indica que em 2020, mais de 90% dos incidentes cibernéticos tiveram origem em ambientes de nuvem.

Figura 1

Exposição de dados

A expansão das interações on-line torna as violações de dados mais comuns



P. Do total de incidentes de segurança cibernética detectados por sua organização, qual foi a distribuição por tipo?

70% das organizações não conseguem proteger dados sendo movidos entre diversos ambientes de nuvem e locais, o que representa um grande problema para a realização de valor.

92% das organizações não têm capacidade de ativar e estender com segurança novos recursos nativos de nuvem para seus parceiros internos e externos.

150 dias para preencher vagas de talentos cibernéticos com candidatos qualificados, o que resulta em deficiências na conscientização e na responsabilização que podem elevar a exposição ao risco.

Embora os serviços compartilhados e os ambientes de trabalho colaborativo baseados na nuvem sejam vitais para a entrega de resultados de negócios, esses ambientes requerem uma nova abordagem mais flexível, ágil e cooperativa para as operações de segurança. Buscando capitalizar os méritos dessa nova abordagem, os líderes estão modernizando suas operações de TI e TO com base nos princípios de zero trust (veja "Perspectiva: quais são as diferenças da segurança de zero trust?").

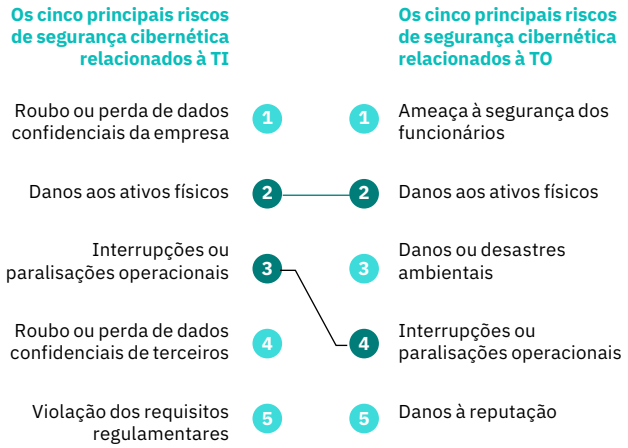
Valiosa, mas vulnerável: protegendo a infraestrutura crítica

A própria natureza da infraestrutura crítica implica um relacionamento dinâmico entre confiança e risco. À medida que as operações são realizadas on-line, tanto as redes de TI quanto as de tecnologia operacional (TO) estão sujeitas ao comprometimento. O ataque de ransomware da Kaseya de julho de 2021, por exemplo, afetou aproximadamente 2.000 organizações e causou pedidos de resgate superiores a US$ 70 milhões. Nossa confiança depositada nos ambientes de TI e de TO significa que a infraestrutura crítica está cada vez mais vulnerável a novas ameaças (veja a Figura 2).[2]

Figura 2

Risco interconectado

Os riscos de TI e TO são complexos e interdependentes



P. Como você classificaria os riscos de segurança cibernética acima? A figura mostra as respostas alta e muito alta.

As abordagens tradicionais de segurança cibernética dependem de permissões e limites de rede discretos, mas as redes atuais são definidas por serviços dinâmicos e limites difusos.

A confiança é a base da colaboração e da parceria. Como estes recursos estão se tornando essenciais para a entrega de valor, a forma de pensar a confiança está mudando rapidamente. Enquanto as abordagens tradicionais de segurança cibernética se baseavam em permissões e limites de rede discretos, as redes atuais são definidas por serviços dinâmicos e limites difusos. As plataformas digitais de hoje geram valor porque são interconectadas e compartilham informações entre diversas partes.

Os problemas podem ser inevitáveis. Muitos sistemas de TO tradicionalmente confiam no isolamento de sistemas, no entanto, a demanda por insights de dispositivos conectados e sistemas inteligentes torna essas práticas difíceis de sustentar. A falta de conectividade pode tornar as vulnerabilidades existentes mais difíceis de corrigir.

Para piorar as coisas, os riscos podem se multiplicar: uma falha em um sistema muitas vezes resulta na falha de outros. Os agentes de ameaças estão se tornando cada vez mais sofisticados em sua capacidade de explorar as falhas nos controles de segurança de TI e TO (veja "Perspectiva: a convergência dos sistemas de TI e TO eleva a exposição ao risco").[3] Embora os impactos potenciais sejam significativos, esses riscos podem ser difíceis de antecipar.

Cibercrime como um serviço é uma nova tendência preocupante.[4] Esses serviços, vendidos em fóruns de hackers, em vendas diretas na web e na dark web por meio de criptomoedas, dependem de explorações de crimes cibernéticos sofisticadas e frequentemente coordenadas, como botnets, ataques distribuídos de negação de serviço (DDoS), fraude de cartão de crédito, malware, spam e ataques de phishing.

Na verdade, devido ao ataque cibernético do Colonial Pipeline, o presidente dos Estados Unidos, Joseph Biden, emitiu uma ordem executiva para melhorar a postura de segurança cibernética de setores e infraestruturas essenciais. Nela, está incluída uma diretiva para que as agências federais elaborem planos para a implementação de arquiteturas de zero trust no prazo de 60 dias a partir do pedido.[6]

Perspectiva: o que torna a segurança de zero trust diferente?

Em princípio, a zero trust é uma abordagem de segurança preventiva que pressupõe que agentes maliciosos já tenham penetrado nas defesas da rede da organização. As operações de TI e de segurança cibernética são reconhecidas como funcionalmente interdependentes. Como resultado, a capacidade da organização de perceber, avaliar e responder a eventos é muito mais dinâmica, muitas vezes, ocorrendo praticamente em tempo real. Esse conhecimento abrangente das operações de TI e cibernéticas torna os recursos de zero trust verdadeiramente transformadores.

Na prática, a zero trust une os domínios operacional e de segurança cibernética ao requerer a autenticação e a verificação em cada troca de valor. Como um modelo operacional de zero trust não depende de perímetros seguros, ele é adequado para ecossistemas compartilhados nos quais as fronteiras organizacionais são difusas e o valor é trocado na forma de serviços. Ao tornar a confiança uma variável operacional e transacional, terceiros podem oferecer suporte até mesmo às cargas de trabalho mais sensíveis e aos recursos de missão crítica.

Perspectiva: a convergência dos sistemas de TI e TO eleva a exposição ao risco

As principais preocupações dos executivos relacionadas à TI são a exposição de dados confidenciais, as implicações de longo prazo de violações bem-sucedidas e a conformidade regulatória. Suas principais preocupações relacionadas à TO são a segurança dos indivíduos, dos ativos físicos e do ambiente, bem como os impactos resultantes nas operações e na reputação da organização.

Embora os riscos de segurança cibernética relacionados aos ambientes de TI e TO nem sempre sejam os mesmos, eles frequentemente se reforçam mutuamente. Como o hack da Colonial Pipeline demonstrou, uma falha em uma área, como uma senha comprometida em um sistema de TI, pode levar a falhas em outras, como a redução da disponibilidade e da confiabilidade da plataforma de TO.[5]

Os benefícios da zero trust

Nossa análise revela que 23% das organizações, um grupo ao qual nos referimos como “pioneiros da zero trust”, estão à frente de seus pares na implementação de recursos de zero trust em seus ambientes de TI e TO e em suas interações com parceiros do ecossistema.

Essas organizações moldaram suas operações de TI e de segurança como um único espólio. Elas são habilidosas no estabelecimento de parcerias internas e externas para gerenciar o risco da segurança cibernética. Elas modernizaram suas operações de segurança relacionadas às estruturas interdependentes de controle, risco e conformidade. Elas utilizam a nuvem, as análises de dados orientadas por IA e a automação extensivamente. E recrutam, desenvolvem e retêm recursos qualificados de segurança cibernética para possibilitar recursos de zero trust em seus espólios digitais.

Mais importante ainda, suas operações de segurança podem se adaptar à complexidade do ambiente de negócios atual, seja capacitando uma força de trabalho remota, monitorando terminais, aplicativos, dados e tráfegos de rede ou analisando o comportamento de funcionários, clientes e parceiros para identificar ameaças emergentes.

O que diferencia os pioneiros da zero trust?

Os pioneiros da zero trust nos dizem que dedicam uma porcentagem semelhante de seus orçamentos e recursos de TI à segurança cibernética, mas que estão recebendo benefícios de segurança e negócios significativamente maiores com sua abordagem de segurança.

Na verdade, o dobro dos pioneiros afirma ter reduzido significativamente o capital de segurança e as despesas operacionais, aumentando ao mesmo tempo a eficácia dos recursos de segurança cibernética. Em particular, eles:

- Melhoraram os recursos de detecção e resposta, reduzindo drasticamente a exfiltração de dados sensíveis. No caso de violações, sua capacidade de limitar a propagação de malware reduz o impacto na organização.
- Priorizaram a capacidade de estabelecer e manter conexões seguras entre os parceiros do ecossistema, o que permite que eles capitalizem melhor os investimentos em nuvem.
- Investiram mais do orçamento de segurança cibernética em recursos de requalificação. Como resultado, suas taxas de retenção de recursos cibernéticos são 10% maiores do que de outras organizações.

O sucesso dos pioneiros da zero trust oferece evidências convincentes dos méritos de uma estratégia abrangente de zero trust. Essas organizações estão favoravelmente posicionadas para alcançar maior eficiência operacional e melhores resultados de negócios. Outras organizações podem obter benefícios semelhantes ao entender e aplicar os recursos operacionais essenciais para o sucesso da zero trust.

Os pioneiros da zero trust dedicam uma porcentagem semelhante de seus orçamentos de TI à segurança cibernética, mas obtêm benefícios significativamente maiores.

Introdução: definindo um roteiro de zero trust

Os pioneiros da zero trust estão quase duas vezes mais à frente na implementação das quatro competências centrais:

1. Uma base sólida para operações de segurança de zero trust guiada por controles de governança, risco e conformidade e reforçada com análises orientadas por IA.

2. Recursos de automação e orquestração de segurança que aumentam o escopo, a escala, a visibilidade e a eficiência das operações de segurança em ambientes operacionais de nuvem híbrida.

3. Uma estrutura de controles de segurança de zero trust para monitorar, gerenciar e ajudar a proteger recursos críticos, que abrange usuários, dados, redes, dispositivos e cargas de trabalho.

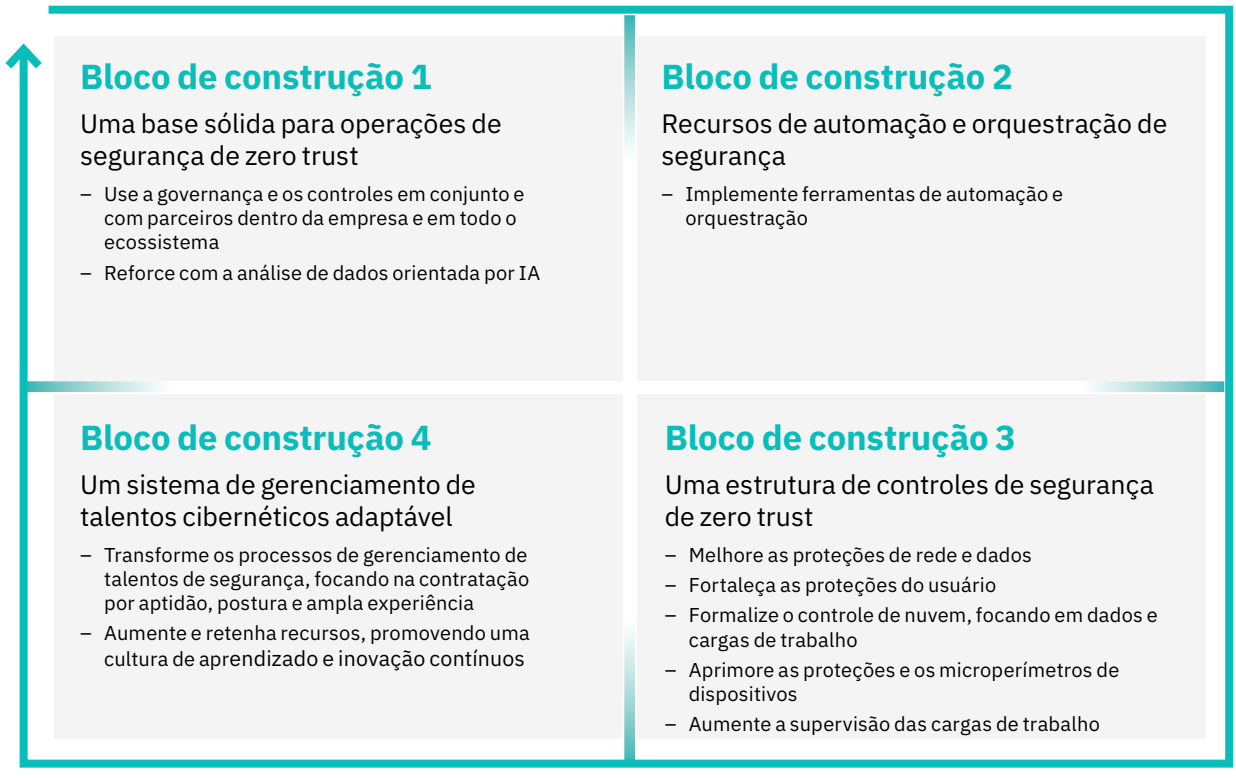
4. Um sistema adaptável de gerenciamento de talentos cibernéticos que prioriza a combinação de talentos e tecnologias para obter resultados de segurança melhores.

Cada um desses blocos de construção é realizado por meio de uma série de práticas e atividades de consolidação. Nossa análise de dados ressalta até que ponto essas práticas e atividades dependem umas das outras, o que é de particular importância. Em outras palavras, todas as quatro competências centrais trabalham em conjunto para alcançar os benefícios associados à zero trust (veja a Figura 3).

Figura 3

Design com foco em segurança

Os recursos de zero trust se reforçam mutuamente



Fonte: análise de dados do IBM Institute for Business Value.

O aumento da conscientização sobre os riscos e dos controles de propagação de malware reduz significativamente a exposição a ataques cibernéticos.

Como a TI e os espólios cibernéticos de cada organização refletem necessidades distintas, cada jornada de zero trust será única. Os fatores que influenciarão a jornada de uma organização incluem sua estratégia de negócios e seus modelos operacionais, a disponibilidade de orçamento e de recursos, a amplitude e a profundidade das relações com os parceiros, as implementações e as restrições de tecnologia existentes e as demandas regulatórias e competitivas geográficas e do setor.

Reconhecendo a diversidade desses fatores, nossa abordagem prioriza a praticidade, a flexibilidade e a possibilidade de desenvolver os recursos existentes. Nossas recomendações, derivadas de insights de desempenho operacional, são baseadas em resultados reais de uma variedade de ambientes operacionais, abrangendo desde organizações novas com foco no crescimento até organizações maduras com foco na transformação.

Para cada bloco de construção, fornecemos uma explicação, os benefícios associados e as práticas e atividades necessárias para realizá-lo.

Bloco de construção 1: estabelecer uma base sólida para operações de segurança de zero trust

Os pioneiros da zero trust integraram recursos de zero trust em suas arquiteturas e operações de segurança existentes. Os recursos incrementam, em vez de substituir, as tecnologias, os processos e as capacidades existentes.

Essas organizações desenvolveram uma cultura de reconhecimento de segurança baseada em práticas modernas de segurança e em controles de segurança automatizados. Essa cultura aumenta a conscientização sobre os riscos de segurança por meio de políticas que definem quem e o que pode acessar ativos comuns de rede, aplicativo e dados.

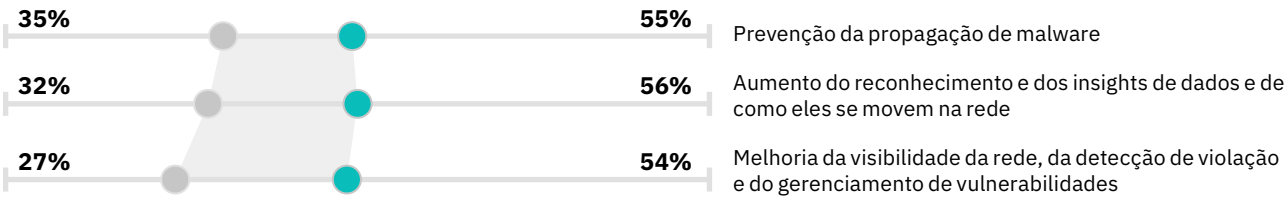
Essas políticas são complementadas por soluções técnicas de segurança que as aplicam sistematicamente. Esse ambiente pode ajudar a identificar dispositivos, aplicativos, serviços e comportamentos sujeitos a comprometimento e, em seguida, usar controles automatizados para ajudar a corrigir ameaças e vulnerabilidades.

No caso de violações, a capacidade de um pioneiro evitar a propagação de malware ajuda a conter os riscos, limitando a probabilidade de falhas subsequentes (veja a Figura 4). Juntos, o aumento da conscientização sobre riscos e os controles de propagação de malware reduzem significativamente a exposição a ataques cibernéticos.

Figura 4

Visualizando e entendendo

Quanto melhor a visibilidade da rede, melhores serão os resultados



Todos os outros | **Pioneiros da zero trust**

P. Até que ponto sua organização obteve cada um dos benefícios acima com sua abordagem de segurança? As porcentagens são baseadas na escolha dos entrevistados com relação a uma escala significativa ou muito grande.

Além disso, os pioneiros da zero trust trabalham com parceiros para aperfeiçoar o gerenciamento e o relatório de riscos cibernéticos. Guiados por estruturas de controle, risco e conformidade, eles comunicam de forma proativa novas ameaças em toda a empresa e se relacionam com parceiros estratégicos e fornecedores terceirizados. Seu uso de metodologias de ciclo de vida de desenvolvimento de sistema padrão (SDLC) e de DevSecOps padroniza recursos críticos para operações de segurança e controle, facilitando ainda mais a eficiência.

Por meio da ampla aplicação de análises avançadas de segurança cibernética para detecção e resposta a incidentes, os pioneiros da zero trust monitoram uma porcentagem maior de comunicações de rede (55%) e dispositivos de terminal (68%) quanto a vulnerabilidades e violações de políticas, em comparação com 45% e 60% dos concorrentes, respectivamente. Quanto mais uma empresa observa o tráfego de comunicações de rede e os dispositivos de terminais, por exemplo, maior é a sua capacidade de identificar e corrigir potenciais ameaças. Uma maior visibilidade aumenta a probabilidade de sucesso.

A maioria dos pioneiros indica que aumentou significativamente os insights sobre como os dados se movem em suas redes. Os pioneiros melhoraram seus recursos de visibilidade de rede, detecção de violações e gerenciamento de vulnerabilidades em 1,5x em comparação aos concorrentes (veja a Figura 4).

Bloco de construção 1

Estabeleça uma base sólida para operações de segurança de zero trust

Monitore as comunicações de rede em busca de atividades suspeitas

45% Todos os outros

55% Pioneiros da zero trust

Monitore os dispositivos de terminal em busca de vulnerabilidades e violações de política

60% Todos os outros

68% Pioneiros da zero trust

Como fazer isso

Use os controles e a governança de TI com parceiros dentro da empresa e em todo o ecossistema

Use análises orientadas por IA para sinalizar exceções e acionar controles automatizados

Os modelos automatizados de segurança de IA podem reconhecer comportamentos anormais, avaliar vulnerabilidades e sinalizar novas ameaças.

1

Em particular, duas práticas pioneiras podem ajudar as organizações a estabelecer uma base sólida para operações de segurança de zero trust:

1. **Use os controles e a governança de TI com parceiros dentro da empresa e em todo o ecossistema para aumentar a visibilidade e a eficácia dos esforços de mitigação do risco cibernético:**

   – Ofereça educação em segurança e treinamento de reconhecimento para funcionários: o conhecimento, os recursos e as habilidades necessários para proteger a organização.

   – Aplique os programas e as estruturas de controle, gerenciamento de riscos e conformidade para identificar, avaliar e mitigar o risco cibernético. Equilibre os níveis de risco aceitáveis com os objetivos comerciais e os requisitos de conformidade. Coordene esses esforços com os parceiros do ecossistema para obter melhor economia de escala.

   – Implemente uma política de prevenção de perda de dados (DLP). Defina como a sua organização pode compartilhar e proteger dados para orientar a implementação de ferramentas que evitem que os usuários enviem informações sensíveis ou críticas para fora da rede principal. Coordene esses esforços com parceiros usando a infraestrutura compartilhada.

   – Integre a segurança no processo de desenvolvimento de software. As metodologias nativas de nuvem, como DevSecOps, permitem que as organizações trabalhem com parceiros de forma mais eficiente, notavelmente por meio da adoção de abordagens comuns para operações de segurança e controle.[7]

2. **Use a análise de dados orientada por IA para sinalizar exceções, acionar controles de correção e evitar que agentes de ameaça utilizem técnicas de varredura e exploração automatizadas:**

   – Implemente recursos avançados de telemetria de segurança cibernética, incluindo o monitoramento e a análise de dados para detecção e correção de incidentes. Reduza a dependência da detecção manual de ameaças usando processos de investigação automatizados e orientados por IA em dados de alto valor, ativos, segmentos de rede e serviços de nuvem.

   As ameaças podem ser classificadas e priorizadas para acionar alertas baseados em assinaturas de ataque e indicadores de comprometimento (IOC). Para melhorar a eficiência operacional, as organizações podem complementar as soluções de telemetria existentes com recursos de detecção e resposta de terminal (EDR) e detecção e resposta de camada cruzada (XDR).

   – Aplique a IA para automatizar a criação de modelos, controlar o comportamento normal e sinalizar atividades anômalas. Os modelos automatizados de segurança de IA podem reconhecer comportamentos normais (em comparação com os anormais), avaliar vulnerabilidades de maneira dinâmica e sinalizar atividades anômalas que possam indicar novas ameaças. Em seguida, eles podem usar essas entradas para qualificar e quantificar a exposição ao risco potencial.

Bloco de construção 2

Crie operações robustas com recursos de automação e orquestração de segurança

Redução significativa do capital de segurança e dos custos operacionais

61%
Pioneiros da zero trust

Redução drástica do escopo e do custo de iniciativas de conformidade

50%
Pioneiros da zero trust

Como fazer isso

Estabeleça um centro de operações de segurança (SOC) em todo o ecossistema

Implemente uma única plataforma de nuvem independente com visibilidade dos provedores

Aplique a inteligência de segurança ativada para a IA a fim de detectar comportamentos anormais

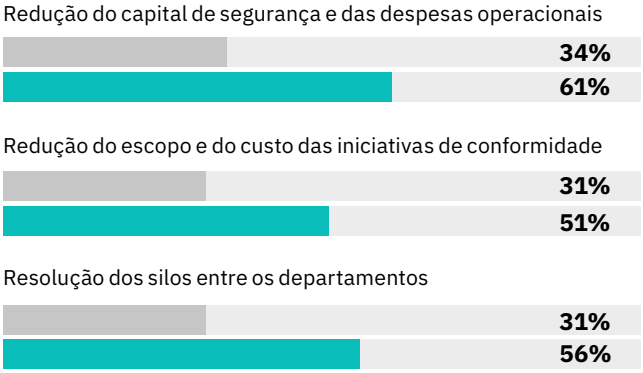
Bloco de construção 2: crie operações robustas com recursos de automação e orquestração de segurança

Os pioneiros da zero trust adotaram a automação e a orquestração de segurança e aumentaram o escopo, a escala e a eficiência das operações de segurança. Um total de 61% dos pioneiros da zero trust indicam que isso reduziu significativamente o capital de segurança e os custos operacionais. Metade deles diz que isso reduziu drasticamente o escopo e o custo das iniciativas de conformidade (veja a Figura 5).

Figura 5

A vantagem do custo

A automação e a orquestração aumentam o escopo, a escalabilidade e a eficiência



P. Até que ponto sua organização obteve cada um dos benefícios acima com sua abordagem de segurança? As porcentagens são baseadas na escolha dos entrevistados com relação a uma escala significativa ou muito grande.

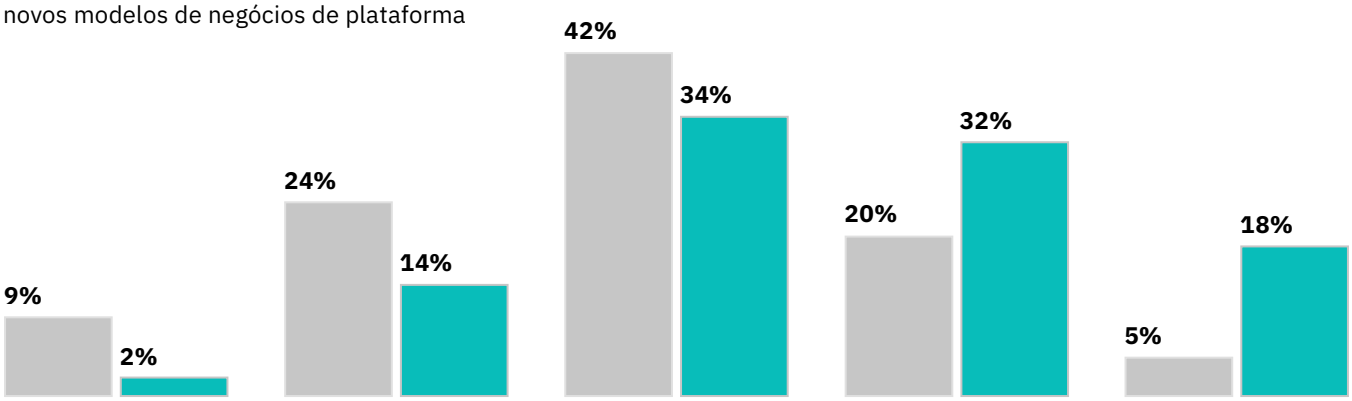
As soluções de automação e orquestração, como o gerenciamento de eventos e incidentes de segurança (SIEM), a orquestração, automação e resposta de segurança (SOAR) e o XDR, fornecem uma visão abrangente das ameaças. Ao ver as ameaças no contexto de dados, aplicativos, redes e dispositivos corporativos, essas soluções aprimoram as investigações de segurança, facilitando para os pioneiros o aumento da agilidade de suas operações de segurança e a melhora de seus recursos de resposta a incidentes.

Além disso, os recursos de segurança de nuvem dos pioneiros da zero trust são abrangentes. Um em cada três fornece suporte a ambientes de nuvem híbrida e aproveita a vantagem integral do fluxo de dados seguro em diversos ambientes de nuvem e locais. Um em cada cinco pode desenvolver ainda mais esse processo (veja a Figura 6). Eles têm capacidade de ativar e estender com segurança novos recursos de negócios e operacionais nativos de nuvem para parceiros internos e externos.

Figura 6

A vantagem da nuvem

Os recursos maduros de segurança de nuvem possibilitam novos modelos de negócios de plataforma



Todos os outros | **Pioneiros da zero trust**

P. Qual afirmação descreve melhor a maturidade dos recursos de segurança de nuvem de sua organização? Selecione uma.

60% dos pioneiros concordam que a abordagem de segurança adotada possibilitou a transformação digital de forma significativa, e 54% dizem que ela aumentou a confiança e as conexões seguras com parceiros externos.

Mas o que realmente diferencia os pioneiros da zero trust? O grau de resiliência cibernética e a capacidade de capitalizar sobre as eficiências operacionais e a economia de escala. Eles aproveitam todo o alcance de seus ambientes de nuvem para permitir novos recursos e modelos de negócios com seus parceiros do ecossistema.

Uma prática pioneira, em particular, pode ajudar as organizações a alcançar maior resiliência de segurança e eficiência operacional:

1. **Implemente ferramentas de automação e orquestração para melhorar o escopo, a escala, a visibilidade e a eficiência das operações de segurança de zero trust:**
   - Avalie continuamente a postura de segurança da organização usando um centro de operações de segurança (SOC) que abrange todo o ecossistema com um gerenciamento coordenado de incidentes e recursos de resposta a crises.[8] Priorize as ferramentas que fornecem visibilidade em todo o SOC. Permita a visibilidade em tempo real em todos os ambientes locais e de nuvem, incluindo redes, dispositivos, aplicativos, usuários e dados. Isso pode ajudar os responsáveis pelas decisões a entender o estado atual dos ativos e serviços críticos.
   - Implemente soluções de segurança que funcionem entre diversas nuvens e que se integrem a soluções de diversos fornecedores. A equipe do SOC deve ter uma única plataforma com abrangência de nuvem e visibilidade dos provedores para iniciar investigações de qualquer incidente baseado em nuvem em qualquer lugar do ecossistema.
   - Implemente a inteligência de segurança ativada para IA e analise fluxos de dados a fim de detectar comportamentos anormais. Combine as informações de segurança de diversos domínios, bem como fontes externas, para enriquecer os dados/metadados contextuais das interações e aplicar políticas de segurança. Amplie os recursos de captura de log aplicando os mesmos procedimentos nos ambientes de nuvem, procurando por configurações irregulares que podem apontar para indicadores de comprometimento.

Bloco de construção 3: Implemente uma estrutura de controles de segurança de zero trust

Os pioneiros da zero trust estão integrando controles de zero trust em suas operações de segurança existentes. Os pioneiros usam recursos de telemetria de segurança, de análise de tráfego em tempo real e de automação e orquestração para melhorar os insights de segurança.

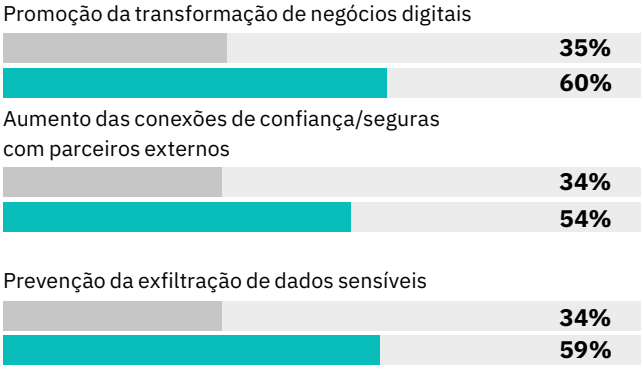
Isso engloba recursos críticos, como usuários, dispositivos, dados, redes e cargas de trabalho. Como esses recursos operam em conjunto, geralmente com parceiros do ecossistema, os pioneiros estão mais bem posicionados para agir com base em insights. Isso aumenta a resiliência cibernética e a capacidade de estimular novas propostas de valor.

Os benefícios associados são evidentes. Dos pioneiros da zero trust, 60% concordam que essa abordagem ajudou significativamente as transformações digitais de suas organizações, enquanto 54% concordam que ela aumentou a confiança e as conexões seguras com parceiros externos (veja a Figura 7).

Figura 7

O poder da confiança

A zero trust melhora a resiliência e os esforços de transformação digital



P. Até que ponto sua organização obteve cada um dos benefícios acima com sua abordagem de segurança? As porcentagens são baseadas na escolha dos entrevistados com relação a uma escala significativa ou muito grande.

Bloco de construção 3

Implemente uma estrutura de controles de segurança de zero trust

Promoção da transformação de negócios digitais

Aumento da confiança e das conexões seguras com parceiros externos

60%
Pioneiros da zero trust

54%
Pioneiros da zero trust

Como fazer isso

Melhore as proteções de rede e dados

Controle o acesso aos dados e gerencie as identidades digitais

Formalize o controle da nuvem

Estenda a visibilidade a todos os terminais que tentem acessar recursos críticos

Aumente a supervisão das cargas de trabalho

Transformar a confiança em uma variável transacional melhora a integridade do ambiente de operações. Com maior visibilidade dos recursos críticos, os pioneiros operam de forma mais eficiente. Colocando os controles de segurança mais próximos dos recursos críticos, por exemplo, criando microperímetros em torno de ativos e serviços específicos, eles podem estender os controles de autenticação e validação sem introduzir tensões desnecessárias. Isso aumenta a resiliência, evitando o acesso não autorizado e a exfiltração de dados confidenciais (veja a Figura 7).

Quando considerada como um todo, essa mudança nas operações é sutil, mas significativa. Ao estabelecer a confiança em intervalos predefinidos, usando controles de validação e autenticação para eventos e comportamentos específicos, a capacidade de negociar a confiança torna-se um recurso dinâmico e em tempo real. Como a confiança pode ser ajustada com base nas circunstâncias ou no contexto, ela pode permitir novas formas de colaboração e novas trocas de valor.

As cinco práticas e atividades associadas a seguir são fundamentais para estabelecer uma estrutura de controles de zero trust:

1. **Melhore as proteções de rede e de dados, começando com o estabelecimento de um gateway de segmentação para ativar controles de acesso mais granulares:**

– Use firewalls de nova geração (NGFWs) para aumentar os controles de segurança de nuvem. Defina as regras e políticas para NGFWs, e-mails e gateways de segurança de nuvem, além de soluções de DLP para aplicar políticas de acesso e segurança de dados. Elas devem ser capazes de operar em modelos de hospedagem, locais, usuários e dispositivos.

– Execute regularmente a descoberta e a classificação de dados sensíveis, tanto no local quanto no terminal, em trânsito e na nuvem. Capture dados e metadados suficientes para recriar o contexto completo de qualquer interação.

Entenda onde estão seus dados mais sensíveis, quem tem acesso a eles (e como), quem está acessando esses dados (e quando) e o que estão fazendo com eles. Isso pode ajudar você a cumprir as normas de privacidade de dados e conformidade regulamentar, bem como monitorar e controlar o acesso a dados altamente sensíveis.

À medida que surgem técnicas para contornar a autenticação, especialmente o abuso dos mecanismos de confiança, é preciso examinar o gerenciamento de identidade como uma origem potencial de vulnerabilidades.

3

2. Fortaleça as proteções do usuário, controlando o acesso aos dados e gerenciando as identidades digitais:

– Revise regularmente as autorizações de acesso do usuário. Estabeleça controles baseados em funções para o acesso aos dados. Opere com base no princípio do privilégio mínimo, com acesso restrito às informações e aos recursos necessários para executar uma tarefa específica com base em uma necessidade legítima reconhecida.

  Instrua os usuários privilegiados sobre os controles e as práticas relevantes de segurança cibernética. Documente quem tem autorizações para acessar recursos sensíveis, em seguida, monitore comportamentos e realize auditorias para melhorar a visibilidade e sinalizar anomalias e ações potencialmente maliciosas.

– Implemente a autenticação de diversos fatores (MFA) para aplicativos e ativos de dados críticos. Os funcionários devem usar a autenticação de dois fatores (2FA) ou a MFA para identificar áreas nas quais a equipe de segurança deve focar, bem como para evitar ataques internos.9 Elas devem ser complementadas por uma solução de gerenciamento de identidade privilegiada (PIM) e por processos rígidos de controle e gerenciamento de identidade (IMG).

  À medida que surgem técnicas para contornar a MFA, especialmente o abuso de mecanismos de confiança como OAuth e SAML, dê maior ênfase no gerenciamento de identidade como origem potencial de vulnerabilidades.[10] Melhore as políticas e os controles relacionados ao gerenciamento de credenciais e de segredos.

3. Formalize o controle da nuvem para promover a abertura e a interoperabilidade:

– Estabeleça um processo formal de controle de nuvem. Crie seu modelo de controle de nuvem com base em políticas e estruturas de controle padronizadas para ajudar as despesas de segurança relacionadas à nuvem a impulsionar os objetivos de negócios relacionados à adoção da nuvem.

– Estabeleça o controle e a supervisão dos dados e das cargas de trabalho da nuvem. Ao migrar para a nuvem, defina claramente como as responsabilidades são distribuídas entre sua organização e seus provedores de nuvem.

  Em um modelo de responsabilidade compartilhada, o provedor geralmente é responsável por proteger e gerenciar a infraestrutura e o cliente por proteger os dados e as cargas de trabalho que operam nela. Para mitigar o risco de perda de dados, bem como a não conformidade com os regulamentos, use serviços de segurança especializados de seus provedores de nuvem.

4. Aprimore as proteções e os microperímetros de dispositivos, estendendo a visibilidade a cada terminal que tenta acessar recursos críticos:

– Conduza verificações de funcionamento nos terminais antes de permitir que eles se conectem à rede de TI corporativa ou acessem os sistemas. Use soluções automatizadas que varrem e fazem o inventário de novos dispositivos de terminal.

  Inclua novos terminais em um registro, com dados contextuais detalhando usuários, recursos e eventos associados. É preciso identificar os usuários não autorizados e os dispositivos não gerenciados, definir um perfil para eles e impedi-los de obter acesso.

5. Aumente a supervisão das cargas de trabalho:

– Faça o inventário e monitore as configurações de carga de trabalho. Implemente uma solução de segurança multicloud que forneça supervisão centralizada de instâncias de plataforma em nuvem, cargas de trabalho, definições de configuração, serviços autorizados e credenciais.

Bloco de construção 4

Desenvolva um sistema de gerenciamento de talentos cibernéticos adaptável

Os pioneiros da zero trust têm taxas de retenção de talentos cibernéticos 10% mais altas do que os concorrentes

60%
Pioneiros da zero trust

50%
Todos os outros

Como fazer isso

Contrate por aptidão, postura e ampla experiência

Promova uma cultura de aprendizagem contínua e inovação que valorize a vontade de aprender

Bloco de construção 4: desenvolva um sistema de gerenciamento de talentos cibernéticos adaptável

Independentemente de como as organizações escolherem implementar seus recursos de zero trust, elas poderão enfrentar desafios para oferecer resultados de segurança e de negócios duradouros se não tiverem os recursos cibernéticos qualificados.[11] No entanto, muitas organizações estão se esforçando para recrutar e reter essas capacidades. Em média, leva 150 dias para preencher uma vaga com um candidato qualificado.

Em resposta, os pioneiros da zero trust estão usando um sistema de gerenciamento de talentos cibernéticos mais dinâmico e capaz de se adaptar às mudanças nas capacidades e na demanda. Mais notavelmente, eles contratam tendo em vista o potencial do candidato, reconhecendo a importância de ter tanto pessoas que possam aprender quanto pessoas com habilidades específicas.

Como as organizações estão competindo pelo mesmo talento de alto valor, aquelas que tiverem um talento mais específico ou diverso terão uma vantagem decisiva. Em vez de falhar e não preencher as vagas essenciais, os programas de desenvolvimento de conhecimento podem fornecer perspectivas viáveis, ajudando uma empresa a manter uma atitude de segurança efetiva.[12]

Os pioneiros da zero trust dedicam uma porcentagem maior de seu orçamento de segurança cibernética para desenvolver as capacidades dos recursos cibernéticos por meio de uma cultura de aprendizado contínuo. Isso é refletido em suas taxas de retenção de talentos cibernéticos, que são 10% mais altas do que de outras organizações (60% vs. 50%).

Promova uma cultura que valorize não só o conhecimento, mas a vontade de aprender.

4

Duas práticas podem informar um sistema de gerenciamento de talentos cibernéticos adaptável:

1. **Transforme os processos de gerenciamento de talentos de segurança para focar na contratação por aptidão, postura e ampla experiência:**

- Defina requisitos para capacidades, aptidões e habilidades com relação a cada função de segurança cibernética. Essa prática, combinada com objetivos de gerenciamento de desempenho mais amplos, pode facilitar para os gerentes a identificação de falta de habilidades que devem ser abordadas por meio de iniciativas de recrutamento e treinamento. Considere investir em soluções de talento que forneçam atualizações regulares para critérios de habilidades, funções e desenvolvimento a fim de que as variáveis de talento sejam atualizadas com novas tecnologias e requisitos operacionais.
- Ao contratar, priorize a avaliação do comportamento e da competência, em vez da experiência. Com o advento da nuvem, os eventos de segurança estão se multiplicando muito além da capacidade de gerenciamento de muitas equipes. Os profissionais de segurança cibernética devem ser flexíveis e desenvolver suas habilidades para se adaptar aos riscos emergentes. Eles também devem ser proficientes no trabalho com soluções automatizadas de segurança. Para novas ameaças, a familiaridade com táticas, técnicas e processos de negócios pode substituir a experiência em operações de segurança cibernética.
- Aplique testes de aptidão cibernética para identificar o potencial latente das pessoas no processo de seleção de candidatos. Avalie as habilidades, atitudes e comportamentos de segurança cibernética subjacentes dos candidatos bem-sucedidos e use esses insights para expandir o conjunto de talentos em potencial além da organização de segurança. Isso pode agregar maior diversidade à força de trabalho, introduzir novas maneiras de pensar e expandir as opções para enfrentar os desafios de maneiras diferentes.

2. **Desenvolva e retenha pessoas, promovendo uma cultura de aprendizado e inovação contínuos. Aprimore as operações de segurança de zero trust, envolvendo talento de novas maneiras:**

- Estabeleça um programa de treinamento para ensinar à equipe de segurança sobre outras partes do negócio. Forneça insights operacionais mais profundos sobre os processos críticos do negócio para que a equipe entenda melhor os riscos associados.
- Implemente ferramentas de IA e outras para informar os esforços de aprendizado contínuo ao longo do ciclo de vida de recursos humanos. Reconheça os talentos potenciais identificados durante o recrutamento e os otimize por meio de aprendizagem e desenvolvimento customizados. Isso pode atrair rapidamente novos funcionários, estimular o trabalho em equipe em áreas especializadas, criar um conjunto de recursos secundários para cobertura de backup e manter as equipes de operações de segurança atualizadas à medida que surgem novas ameaças e tecnologias.
- Promova uma cultura que valorize não só o conhecimento, mas a vontade de aprender. Proporcione oportunidades de desenvolvimento e crescimento profissional para melhorar a retenção da equipe. Defina critérios de sucesso e planos de carreira para funções específicas. Crie incentivos que encorajem os principais talentos a compartilhar conhecimentos com outros e a crescer com a empresa.

Leve em conta estas questões ao se tornar um pioneiro da zero trust:

- Como complementar nossa arquitetura de segurança existente com recursos de zero trust? O que é fundamentalmente diferente e requer uma nova abordagem?
- Por meio de quais métodos nossa organização está desenvolvendo uma visão integrada das ameaças para melhorar a visibilidade, aumentar a agilidade de nossas operações de segurança e melhorar os recursos de resposta a incidentes?
- Como incorporamos controles de zero trust em todo o nosso espólio digital, incluindo redes, dados, usuários, cargas de trabalho e dispositivos?
- De que formas é possível adaptar as práticas de talentos cibernéticos para aproveitar ao máximo nossa estratégia de zero trust?

Metodologia de pesquisa

No quarto trimestre de 2020, o IBM Institute for Business Value, em colaboração com a Oxford Economics, entrevistou mais de 1.000 líderes de segurança e operações de diversos setores e regiões para compreender em detalhes o que constitui uma estratégia de segurança de zero trust e como esses recursos estão sendo implementados.

Para entender as ameaças à infraestrutura crítica, a pesquisa de opinião coletou dados sobre os riscos de segurança cibernética relacionados à TI e à TO e sobre a maturidade, o desempenho e a eficácia dos recursos das organizações no gerenciamento e na minimização desses problemas. Isso incluiu a adoção de práticas de liderança, bem como prioridades e iniciativas futuras. A pesquisa também analisou os benefícios dos entrevistados com suas abordagens de operações de segurança.

A análise dos dados revelou que 23% das organizações, um grupo que denominamos de “pioneiros da zero trust”, estão à frente de seus concorrentes na implementação de recursos de zero trust para proteger recursos críticos em ambientes operacionais. Ao avaliar as medidas de desempenho e as práticas atuais, concluímos que essas empresas estão obtendo benefícios comerciais e de segurança significativos com a abordagem.

Uma análise fatorial de confirmação (CFA) forneceu insights sobre quais fatores estão impulsionando esses benefícios. Eles incluem práticas operacionais de segurança e risco cibernético, análises e automação orientadas por IA e práticas de zero trust para proteger dados, redes, usuários, dispositivos e cargas de trabalho. Com base nisso, derivamos uma abordagem de operações de zero trust fundamentada em quatro blocos de construção essenciais e em um conjunto de práticas que se reforçam mutuamente.

Sobre os autores

Chris McCurdy
Vice President and General Manager
IBM Security Services
cmccurdy@us.ibm.com

Chris tem experiência de mais de 25 anos em consultoria de TI e tem ajudado grandes empresas e clientes governamentais com o design, a implementação e o gerenciamento de programas de tecnologia da informação complexos. Ele lidera a estratégia de entrada no mercado mundial na IBM Security e é responsável pelo gerenciamento global de vendas. Nos últimos cinco anos, ele aumentou a receita comercial da IBM Security em dois dígitos. Chris é bacharel em administração de negócios na área de sistemas de informação pela Universidade Baylor e é auditor certificado em sistemas de informação.

Dr. Shue-Jane Thompson
Senior Partner, Security Strategy & Growth — Distinguished Industry Leader
IBM Global Business Services
shuejane@us.ibm.com
linkedin.com/in/shuejane

Shue-Jane supervisiona a entrega e a venda de serviços, inovações e integrações de soluções de segurança cibernética para clientes no mundo inteiro. Ela tem mais de 30 anos de experiência em ambientes acadêmicos, comerciais, governamentais e internacionais de tecnologia e gerenciamento de negócios, incluindo o gerenciamento de muitos programas de larga escala de TI, área cibernética, nuvem e operações críticas.

Lisa Fisher
Global Benchmark Research Leader — Industrial, EE&U, T&T and MEA
IBM Institute for Business Value
linkedin.com/in/lisa-giane-fisher
lfisher@za.ibm.com

Lisa é responsável por produzir pesquisas de benchmarking para todos os setores e regiões, a fim de exibir e articular o impacto das tecnologias nos negócios a partir das perspectivas de risco cibernético e segurança cibernética. Lisa está atualmente na África do Sul.

Gerald Parham
Global Research Leader — Segurança e CIO
IBM Institute for Business Value (IBV)
linkedin.com/in/gerryparham/
gparham@us.ibm.com

Gerald lidera os portfólios de pesquisa de segurança e CIO no âmbito do IBM Institute for Business Value. Ele se concentra em estratégias de segurança e em cadeias de valor cibernético, em particular, na relação entre estratégia, risco, operações de segurança, identidade, privacidade e confiança. Ele tem mais de 20 anos de experiência em liderança executiva, inovação e desenvolvimento de propriedade intelectual.

Relatórios relacionados do IBV

Parham, Gerald, Shue-Jane Thomson, Shawn DSouza e Shamla Naidoo. “The new era of cloud security: Use trust networks to strengthen cyber resilience.” IBM Institute for Business Value. 26 de março de 2021. http://ibm.co/cloud-security-cyber-resilience

Comfort, Jim, Blaine Dolph, Steve Robinson, Lynn Kesterson-Townes e Anthony Marshall. “A vantagem da plataforma de nuvem híbrida”. IBM Institute for Business Value. 2020. https://www.ibm.com/thought-leadership/institute-business-value/report/hybrid-cloud-platform

“Estudo do CEO de 2021: Encontre o essencial: como prosperar em uma realidade pós-pandêmica”. IBM Institute for Business Value. 2021. https://www.ibm.com/thought-leadership/institute-business-value/c-suite-study/ceo

Payraudeau, Jean-Stéphane, Anthony Marshall e Jacob Dencik. “Aceleração digital”. IBM Institute for Business Value. 2021. https://www.ibm.com/thought-leadership/institute-business-value/report/digital-acceleration

IBM Institute for Business Value

O IBM Institute for Business Value (Instituto IBM de Valor de Negócios), parte do IBM Services, desenvolve insights estratégicos baseados em fatos para executivos seniores de negócios em questões críticas dos setores público e privado.

Mais informações

Para saber mais sobre este estudo ou sobre o IBM Institute for Business Value, entre em contato conosco pelo e-mail iibv@us.ibm.com. Siga @IBMIBV no Twitter, e para obter um catálogo completo de nossas pesquisas ou para se inscrever na nossa newsletter mensal, acesse:ibm.com/ibv.

Notas e fontes

1 "IBM 2021 X-Force Threat Intelligence Index." IBM Security. 24 de fevereiro de 2021. https://www.ibm.com/security/data-breach/threat-intelligence

2 Paul, Kari. "Quem foi o responsável pelo ataque de ransomware da Kaseya e por que ele foi tão perigoso?" *The Guardian*. 7 de julho de 2021. https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers; Kenny, Caroline e Pamela Brown. "É necessário ter um foco maior na defesa da infraestrutura crítica contra ataques cibernéticos, diz o presidente da agência cibernética." CNN. 27 de junho de 2021. https://www.cnn.com/2021/06/27/politics/brandon-wales-cyber-security-cnntv/index.html

3 Marks, Joseph "The Cybersecurity 202: The Kaseya attack is a revolution in sophistication for ransomware hackers" *The Washington Post*. 8 de julho de 2021. https://www.washingtonpost.com/politics/2021/07/08/cybersecurity-202-kaseya-attack-is-revolution-sophistication-ransomware-hackers/; Caltagirone, Sergio, Dr. Tom Winston e Kyle O'Meara. "2020 ICS Cybersecurity Year in Review." Dragos. https://www.dragos.com/year-in-review/

4 Kramer, Andrew E., Michael Schwirtz e Anton Troianovski. "Secret Chats Show How Cybergang Became a Ransomware Powerhouse." *The New York Times.* 29 de maio de 2021. https://www.nytimes.com/2021/05/29/world/europe/ransomware-russia-darkside.html

5 Osborne, Charlie. "Colonial Pipeline attack: Everything you need to know." ZDNet (Edição dos EUA). 13 de maio de 2021. https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

6 "Executive Order on Improving the Nation's Cybersecurity." O site The White House Briefing Room. 12 de maio de 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

7 Parham, Gerald, Shue-Jane Thomson, Shawn DSouza e Shamla Naidoo. "The new era of cloud security: Use trust networks to strengthen cyber resilience." IBM Institute for Business Value. 26 de março de 2021. http://ibm.co/cloud-security-cyber-resilience

8 Ibid.

9 Pollard, Jeff e Stephanie Balaouras. "Craft Zero Trust Security Metrics That Matter - Performance Management: The Zero Trust Security Playbook." Forrester. 24 de março de 2020. https://www.forrester.com/report/Craft+Zero+Trust+Security+Metrics+That+Matter/-/E-RES136188?objectid=RES136188

10 O Auth, ou Open Authorization, é um processo de autorização. Ele permite que serviços de terceiros troquem informações sobre o usuário sem que ele precise revelar suas senhas. O SAML, ou Security Assertion Markup Language, é um processo de autenticação. Ambos os aplicativos podem ser usados para conexão única (SSO) na web, mas o SAML tende a ser específico para um usuário, enquanto o OAuth tende a ser específico para um aplicativo. Ambos são necessários e trabalham juntos.

11 Johnson, David, Samuel Stern, et al. "Focus On Employees' Daily Journeys To Improve Employee Experience." Forrester. 20 de abril de 2018. https://www.forrester.com/report/Focus+On+Employees+Daily+ Journeys+To+Improve+Employee+Experience/-/E-RES126042?objectid=RES126042

12 Parham, Gerald, Shue-Jane Thomson, Shawn DeSouza e Shamla Naidoo. "The new era of cloud security: Use trust networks to strengthen cyber resilience." IBM Institute for Business Value. 26 de março de 2021. http://ibm.co/cloud-security-cyber-resilience

Sobre o Benchmark Insights

O Benchmark Insights oferece insights para executivos sobre importantes tópicos de negócios e relacionados à tecnologia. Elas são baseadas na análise de dados de desempenho e em outras referências comparativas. Para obter mais informações, entre em contato com o IBM Institute for Business Value pelo e-mail iibv@us.ibm.com.

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – SP
Brasil
Produzido nos Estados Unidos da América
Julho de 2021

BRLA2XP4-BRPT-00