E-BOOK

Como proteger seus dados em um mundo onde pessoas trabalham de qualquer lugar

Mantenha suas informações críticas seguras com a Zscaler Data Protection

© 2024 Zscaler, Inc. Todos os direitos reservados.

Índice

© 2024 Zscaler, Inc. Todos os direitos reservados.

Principais desafios

Proteger seus dados nunca foi tão difícil

Com aplicativos em nuvem, seus dados agora estão amplamente distribuídos e seus funcionários estão se conectando de onde quer que estejam trabalhando, ou seja, de qualquer lugar. Abordagens tradicionais de proteção de dados não oferecem controle adequado sobre seus dados. Eis o porquê:

Não é possível seguir os usuários
Você não consegue fornecer proteção de dados de forma adequada porque seus aplicativos na nuvem são acessados pela internet, longe de sua rede e controles de dados.

Inspeção de TLS/SSL limitada
A maior parte do tráfego é criptografada, mas como as abordagens tradicionais de proteção de dados não conseguem inspecionar o tráfego em TLS/SSL em escala, você não enxerga os riscos potenciais.

Não se conhece o status de conformidade
Compreender o estado da sua conformidade tornou-se difícil porque seus aplicativos na nuvem estão espalhados por vários locais e grupos.

Perde-se o panorama geral
Os produtos para fins específicos e as abordagens complementares criam complexidade e impedem a visão unificada de que você precisa para entender a exposição.

© 2024 Zscaler, Inc. Todos os direitos reservados.

Solução Zscaler

Volte a ter controle de todos os seus dados com a Zscaler

A Zscaler Data Protection pode ajudar você a alcançar uma proteção de dados incomparável aderindo a estes princípios fundamentais:

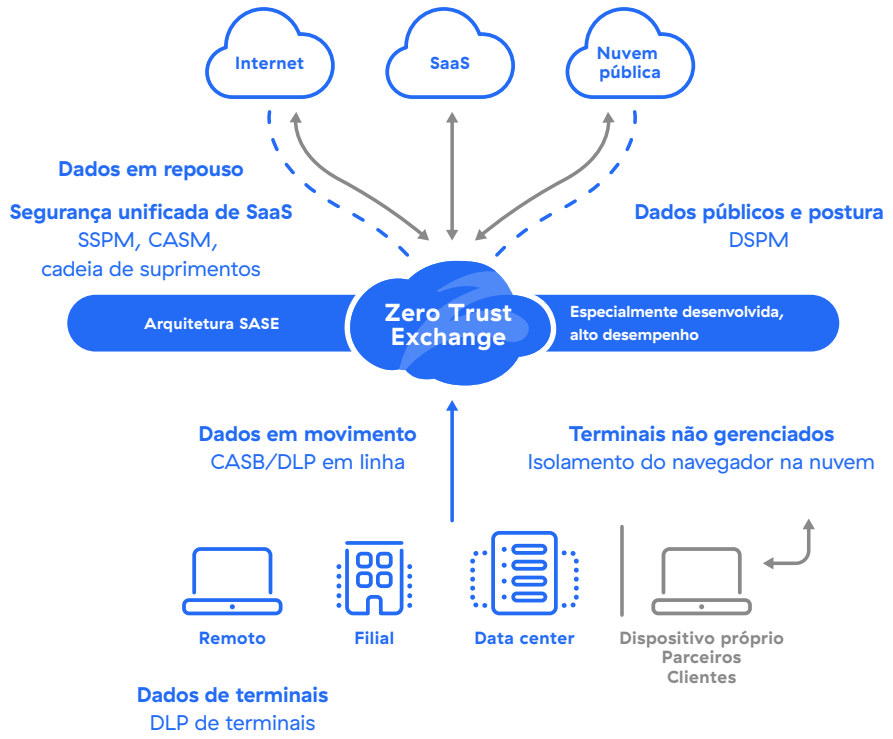
Arquitetura SASE desenvolvida para esse propósito
Forneça proteção em tempo real a todos os usuários a partir de uma nuvem em linha de alto desempenho distribuída por 150 data centers globais.

Inspeção de SSL em larga escala
Inspecione todo o tráfego em SSL para exposição de dados com capacidade de inspeção ilimitada por usuário.

Visibilidade da conformidade
Mantenha facilmente a conformidade verificando SaaS, Microsoft 365 e nuvens públicas em busca de violações e configurações incorretas.

Uma plataforma, uma política, visibilidade total
Proteja todos os seus canais de dados na nuvem (dados em trânsito, em repouso e entre terminais e nuvens) com uma plataforma simples e unificada.

Zscaler Data Protection: Visão geral da solução



© 2024 Zscaler, Inc. Todos os direitos reservados.

CASB para dados em repouso

Gerencie aplicativos autorizados com segurança com CASB fora de banda

Aplicativos em nuvem possibilitam uma melhor colaboração, principalmente com muitos funcionários trabalhando remotamente, mas também podem expor seus dados. Os funcionários muitas vezes fazem mau uso desses aplicativos inadvertidamente, o que pode levar a atividades maliciosas.

Como você pode proteger seus aplicativos e dados na nuvem com o CASB fora de banda da Zscaler:

- **Proteja os dados em repouso expostos**
  Identifique dados críticos em aplicativos na nuvem, e-mail e compartilhamentos de arquivos. Aplique políticas de DLP para controlar o acesso e a exposição.

- **Evite o compartilhamento indevido de dados**
  Aplique uma política granular sobre dados sigilosos em repouso para garantir que eles não sejam compartilhados fora da organização.

- **Corrija ameaças**
  Examine repositórios de dados em serviços de hospedagem de arquivos, como OneDrive ou Box, para encontrar e colocar em quarentena rapidamente conteúdo malicioso.

- **Simplifique a proteção de dados**
  Evite a complexidade de produtos específicos com uma plataforma unificada que fornece uma única política de dados e ameaças para todos os dados em trânsito e em repouso.

© 2024 Zscaler, Inc. Todos os direitos reservados.

Ofereça visibilidade e controle em tempo real com o CASB em linha

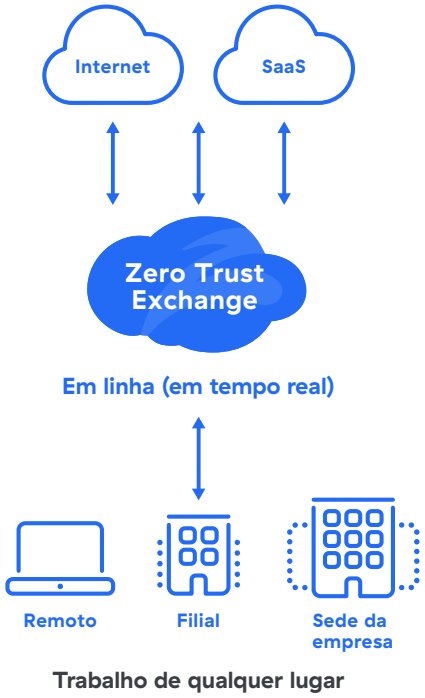
Embora o CASB fora de banda ajude a proteger os dados em repouso, ainda é necessário ter controle em tempo real sobre os aplicativos em nuvem. Como o CASB em linha permite que você migre com segurança para a nuvem?

- **Reduz o risco de TI invisível**
  Entenda rapidamente quais aplicativos na nuvem, seguros ou inseguros, estão sendo usados em toda a organização.

Exemplo: bloqueie a atividade de aplicativos perigosos que acessam seus dados, como conversores de PDF on-line ou sites de compartilhamento de arquivos.

- **Garante o uso de aplicativos oficialmente aprovados**
  Limite a atividade do usuário aos aplicativos na nuvem aprovados pela TI e pela organização.

Exemplo: melhore o compartilhamento e a produtividade do Microsoft 365 permitindo apenas o uso do OneDrive enquanto bloqueia o Box.



Trabalho de qualquer lugar

- **Evita perda de dados com controles de tipo de arquivo**
  Restrinja a transferência de dados por tipo de arquivo com bloqueio condicional e alertas.

Exemplo: impeça o upload ou download de arquivos do Word, Excel ou PowerPoint por usuário ou grupos.

- **Impõe restrições de uso**
  Controle os fluxos de dados permitindo apenas instâncias específicas de aplicativos na nuvem.

Exemplo: evite o vazamento de dados em instâncias pessoais do Microsoft 365, permitindo apenas o acesso ao Microsoft 365 for Business.

© 2024 Zscaler, Inc. Todos os direitos reservados.

DLP de terminais

Simplifique a forma como você controla os dados de dispositivos com a Endpoint DLP

Uma ótima proteção de dados requer uma estratégia de terminais. Com a DLP de terminais você obtém proteção total para os dispositivos, sem a complexidade das abordagens tradicionais.

- **Política e visibilidade unificadas**
  Com um mecanismo de DLP centralizado, você obtém alertas consistentes em terminais, em linha e na nuvem.
- **Agente único e leve**
  Integrado ao agente da Zscaler, você obtém uma melhor experiência do usuário, reduzindo os agentes necessários em seu terminal.
- **Implantação rápida**
  Aproveite suas políticas de DLP da Zscaler existentes para implementar rapidamente.
- **Gerenciamento de incidentes mais veloz**
  Responda com mais rapidez a incidentes, com automação do fluxo de trabalho e painéis e análises forenses detalhados.

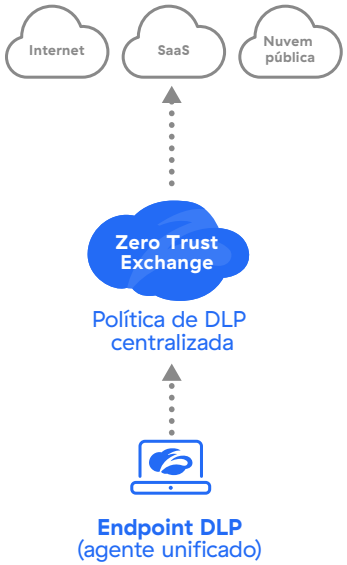
Principais casos de uso da Endpoint DLP

Melhore a cobertura de dados
Garanta que dados valiosos sejam devidamente rastreados e protegidos em qualquer lugar, sem falhas

Proteja-se contra demissões de funcionários
Garanta que os funcionários que estão saindo não copiem dados do dispositivo e os levem para a próxima empresa

Descontinue a DLP de terminais legada
Livre-se de produtos específicos e complicados e forneça uma plataforma unificada

Melhore a conformidade
Mantenha a conformidade regulatória em arquivos e dispositivos



Proteção dos canais

Midia removivel	Sincronização de armazenamento em nuvem pessoal
Compartilha-mentos de rede	Impressão

© 2024 Zscaler, Inc. Todos os direitos reservados.

Reduza a complexidade com uma abordagem unificada para DLP de e-mail em tempo real

Um dos maiores riscos para os dados é o e-mail. Com a DLP de e-mail da Zscaler, as organizações obtêm uma abordagem poderosa para adicionar controle completo de DLP sobre os dados de e-mail.

As abordagens legadas para proteger dados de e-mail podem ser complicadas e complicadas. Com a adoção da SSE, as equipes de TI buscam abordagens unificadas para proteger dados em canais de e-mail que reduzam a complexidade.

Com a DLP de e-mail da Zscaler aproveitando o Smarthost, a proteção de dados pode ser facilmente dimensionada para o e-mail em tempo real. Utilizando SMTP Relay, a Zscaler oferece integração fácil a arquiteturas de e-mail existentes, com controle completo sobre dados e anexos de e-mail.

Vantagens da DLP de e-mail da Zscaler:

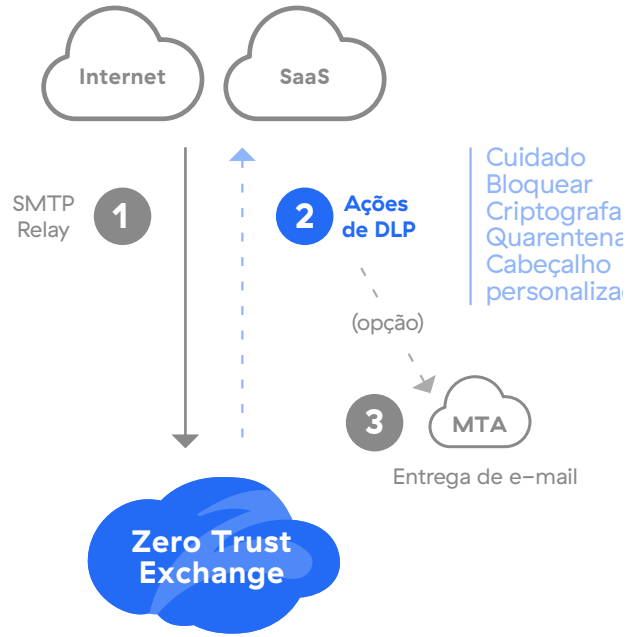
Independente de protocolo
Funciona em dispositivos gerenciados, não gerenciados e até mesmo em dispositivos móveis

Implantação fácil
Não são necessárias alterações no registro MX

Política flexível
Definições de políticas ajustáveis e avaliações granulares de políticas

Centralizada e unificada
Interface única e mecanismos de DLP para todos os canais

DLP de e-mail em tempo real



© 2024 Zscaler, Inc. Todos os direitos reservados.

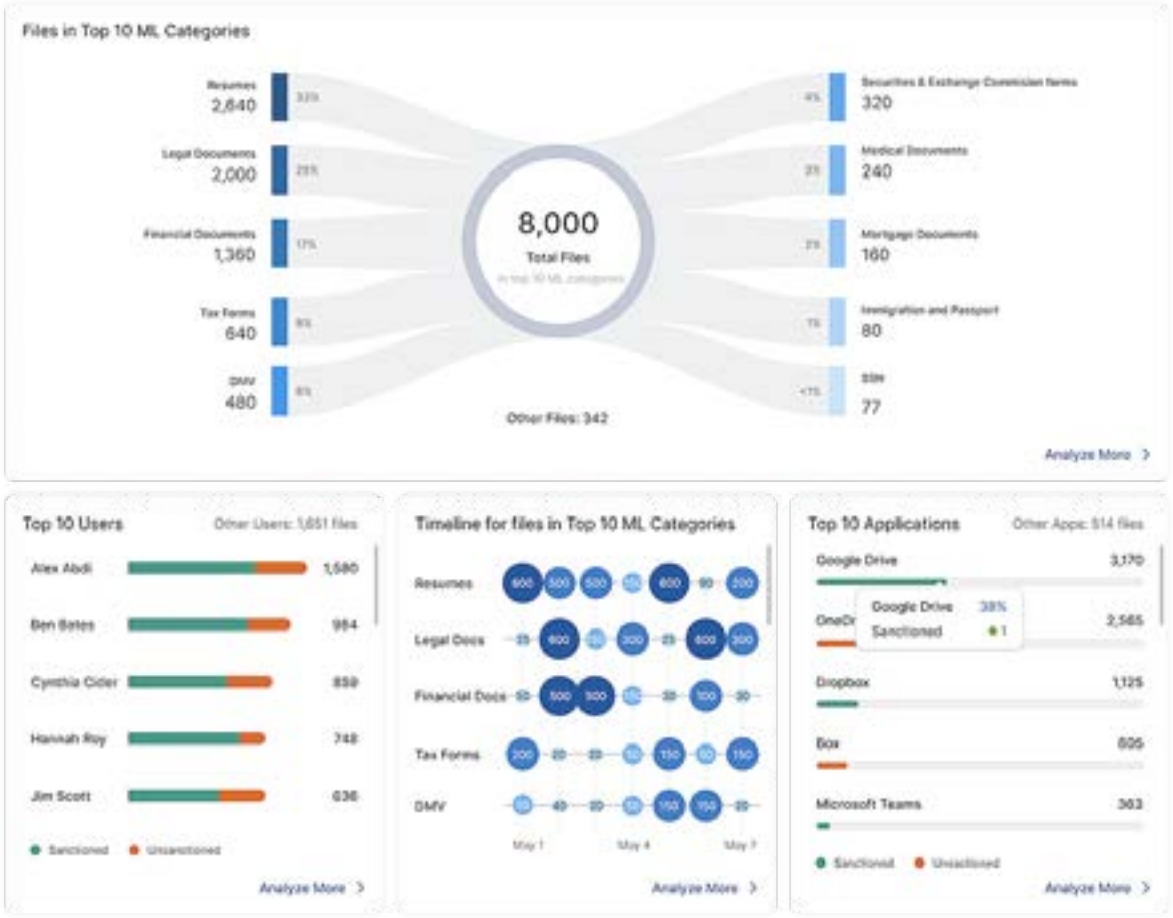
Descoberta automática de dados baseada em IA

Encontre e proteja dados instantaneamente com a descoberta de dados baseada em IA

A implementação e operacionalização de um programa de proteção de dados pode, por vezes, levar meses. Com a descoberta de dados inovadora da Zscaler, você pode compreender rapidamente os riscos e comportamentos associados aos seus dados.

Descoberta de dados baseada em IA:

- Descubra dados em terminais, em linha e nuvens públicas
- Entenda rapidamente os riscos de perda por usuários e aplicativos
- Alterne para a criação de políticas em poucos cliques



© 2024 Zscaler, Inc. Todos os direitos reservados.

Classificação avançada (EDM, IDM, OCR)

Classifique e proteja dados, formulários e imagens personalizados contra perda

A classificação de dados é a base de qualquer bom programa de DLP. Com a classificação avançada de dados, você pode proteger tipos especiais de dados sigilosos contra perda.

Correspondência Exata de Dados (EDM)

Identifique e proteja dados personalizados da empresa. Exemplo: acionamento em números de cartão de crédito do cliente, não em todos os números de cartão de crédito (como uma compra na Amazon).

Correspondência de documentos indexados (IDM)

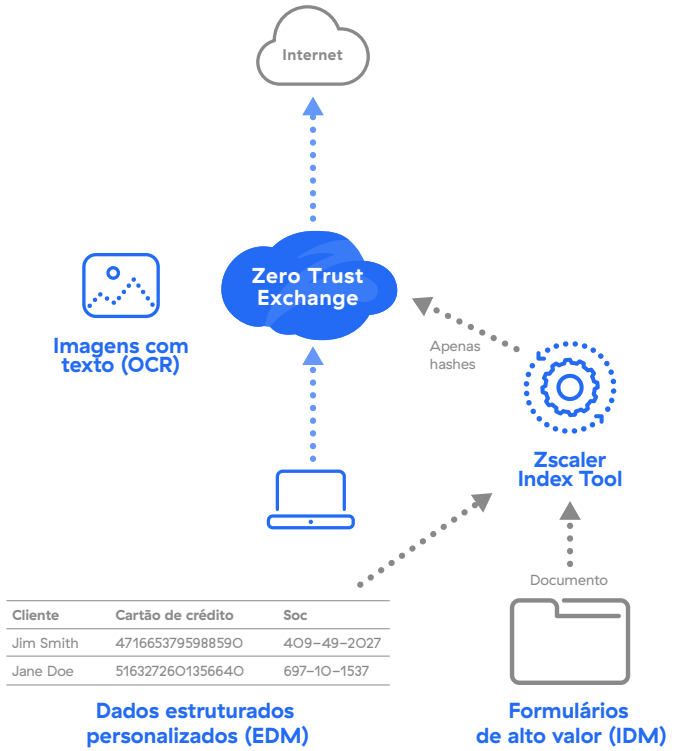
Identifique e proteja documentos e formulários personalizados. Exemplo: identifique um formulário em branco de imposto ou hipoteca e bloqueie qualquer outra cópia preenchida.

Reconhecimento óptico de caracteres (OCR)

Encontre e previna a perda de dados identificando texto dentro de imagens. Exemplo: monitore capturas de tela que possam conter conteúdo sigiloso.

Zscaler Indexing Tool

Ferramenta complementar de identificação para EDM e IDM. Cria hashes de dados de EDM e IDM e os carrega na nuvem da Zscaler para criação de políticas.



© 2024 Zscaler, Inc. Todos os direitos reservados.

Obtenha visibilidade e controle máximos sobre aplicativos de IA generativa

Controlar a perda de dados sigilosos para aplicativos de IA generativa é fundamental para permitir que esses aplicativos invisíveis aumentem a produtividade. A nova abordagem inovadora da Zscaler traz toda a proteção e visibilidade em um só lugar.

Os aplicativos de IA generativa têm o potencial de melhorar a produtividade em toda a sua organização, mas você precisa de visibilidade e controle completos sobre esses aplicativos para tomar melhores decisões de bloqueio.

A inovadora segurança de GenAI da Zscaler permite que as equipes de TI descubram todos os aplicativos de GenAI em toda a organização e oferece visibilidade sem precedentes, incluindo entradas de nível de prompt, para que possam tomar melhores decisões de bloqueio.

Benefícios

- Consulte os prompts de entrada enviados ao aplicativo de IA pelos usuários para obter visibilidade contextual completa
- Controles de política flexíveis na inspeção de DLP e no Cloud App Control
- Aplique acesso isolado e proteja dados no Zscaler Cloud Browser.

Visibilidade de IA generativa

Descoberta de IA oculta
Catálogo completo de todos os aplicativos de IA populares

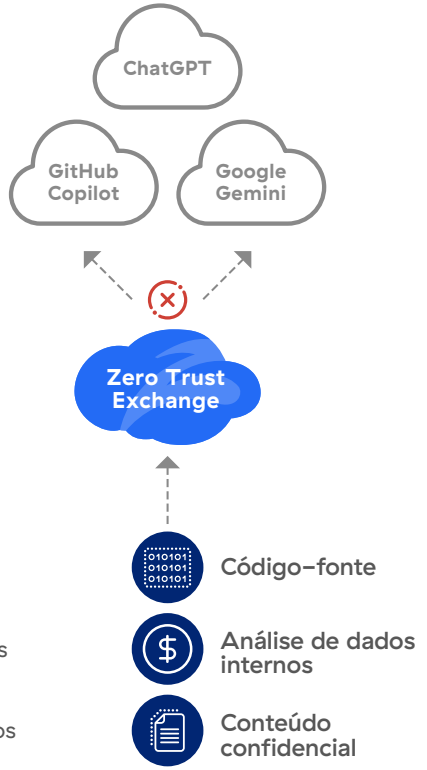
Visibilidade do prompt de entrada
Veja os prompts de entrada que os usuários estão enviando para os aplicativos de IA

Controles de aplicativos de IA generativa

Inspeção de DLP
Bloqueie dados sigilosos e conteúdo destinado a aplicativos de IA

Controle de aplicativos na nuvem
Controle o acesso a aplicativos de IA entre usuários, departamentos e locais

Isolamento do navegador
Confine os dados e o uso de aplicativos em um navegador de nuvem seguro



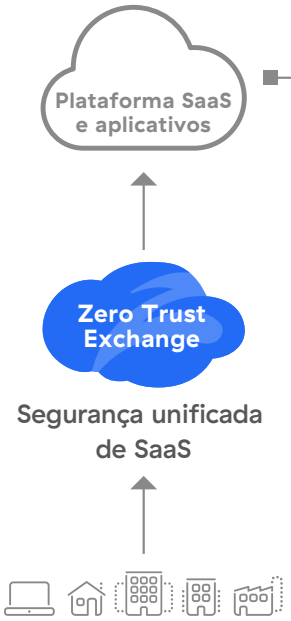
© 2024 Zscaler, Inc. Todos os direitos reservados.

Defenda sua plataforma SaaS com uma abordagem totalmente integrada

Proteger nuvens e dados SaaS requer muitas ferramentas. Unificar o SSPM com outras abordagens importantes de segurança de SaaS ajuda a simplificar drasticamente a forma como as equipes de TI protegem os dados e a postura de SaaS.

Muitas violações na nuvem são causadas por configurações incorretas perigosas ou aplicativos de terceiros conectados a plataformas SaaS. Compreender e controlar sua postura de SaaS é uma etapa importante para proteger as grandes quantidades de dados sigilosos nessas nuvens.

Com o gerenciamento da postura de segurança de SaaS (SSPM) da Zscaler, as organizações obtêm uma abordagem unificada para verificar e proteger plataformas SaaS como Office 365 ou Google. Obtenha visibilidade detalhada sobre configurações incorretas perigosas e integrações de aplicativos, com correção automática, orientação e controle sobre a revogação de aplicativos conectados arriscados.



Segurança unificada de SaaS
Tudo para proteger SaaS em um só lugar

Gerenciamento da postura de segurança de SaaS (SSPM)
Corrija configurações incorretas e desvios de configuração

Segurança da cadeia de suprimentos de SaaS
Desative integrações de terceiros arriscadas

API CASB
Evite o compartilhamento arriscado de dados sigilosos

Atividade do usuário
Monitore o acesso e os colaboradores de risco

Melhoria do contexto, da correlação e da redução de riscos

© 2024 Zscaler, Inc. Todos os direitos reservados.

Gerenciamento de postura da segurança de dados (DSPM)

Proteja nuvens e dados públicos com uma abordagem de proteção de dados totalmente integrada

As equipes de proteção de dados precisam de uma abordagem unificada para proteger os dados da nuvem pública. O DSPM da Zscaler integra-se perfeitamente aos programas de proteção de dados existentes.

Dados sigilosos armazenados em nuvens públicas como AWS e Azure podem ser muito dinâmicos. Desde privilégios e vulnerabilidades excessivos até dados ocultos, as equipes de TI precisam de uma maneira melhor de descobrir, classificar e proteger dados de nuvens públicas.

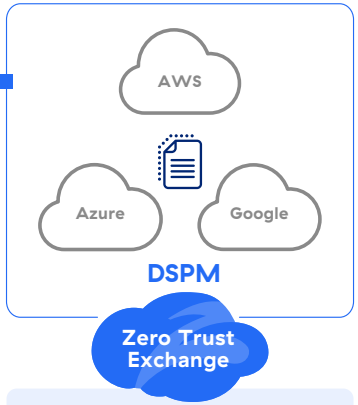
O Zscaler DSPM descobre rapidamente dados sigilosos, entende os riscos e controla o acesso e a postura. O melhor de tudo é que o DSPM integrado da Zscaler aproveita o mesmo mecanismo de DLP de todos os outros canais (terminais, rede, SaaS), portanto, os alertas são consistentes, não importa para onde seus dados sejam transferidos.

Benefícios

- Encontre rapidamente dados sigilosos com a descoberta automática baseada em IA
- Correlacione configurações incorretas, exposições e vulnerabilidades para obter maior compreensão do risco de dados na nuvem
- Estenda os dicionários de DLP existentes para dados de nuvem pública para obter melhor visibilidade e contexto
- Elimine riscos rapidamente com orientação prática sobre correções

Proteja os dados e a postura da nuvem
Localize e proteja os dados e compreenda totalmente os riscos de exposição

1. **Mapeie armazenamentos de dados**
   Mapeie buckets, VMs e bancos de dados com descoberta automática de dados
2. **Priorize os riscos**
   Entenda as configurações incorretas e o risco de exposição dos dados
3. **Corrija riscos**
   Tome medidas com a orientação e as políticas de remediação



DLP centralizado:
defina uma vez, implante em todos os lugares

© 2024 Zscaler, Inc. Todos os direitos reservados.

Dados seguros de aplicativos web e acesso para dispositivos pessoais

Parceiros, prestadores de serviços ou funcionários às vezes exigem acesso aos seus dados enquanto usam dispositivos pessoais. Como manter o controle sobre esses dados quando esses dispositivos não são gerenciados?

Com o Zscaler User Portal 2.0 e o Cloud Browser, as organizações podem oferecer suporte a dispositivos não gerenciados com segurança. Veja como:

Como o User Portal 2.0 protege o acesso e os dados:

- Os usuários, sem requisitos de agente de terminais, autenticam-se no portal para obter uma visualização do painel de aplicativos web autorizados (SaaS ou privados).
- Os usuários acessam o aplicativo dentro de um navegador contido/isolado. Os dados são então transmitidos com segurança para o terminal como pixels.
- Os aplicativos são totalmente interativos, mas as ações de cortar, colar, baixar e imprimir são bloqueadas, e as capturas de tela têm marca d'água.

Benefícios para dispositivos pessoais:

Proteção contra ameaças e de dados
Inspecione todo o tráfego em linha, garantindo o mesmo nível de segurança dos dispositivos gerenciados.

Isolamento de dados e arquivos
Visualize documentos ou compartilhe arquivos (entre aplicativos), sem download ou recursos de área de transferência no terminal.

Políticas de DLP integradas
Aproveite as políticas de negócios para garantir proteção consistente e alertas de dados sigilosos.

© 2024 Zscaler, Inc. Todos os direitos reservados.

Automação do fluxo de trabalho

Gerencie melhor os incidentes de perda de dados com a Workflow Automation

Para levar seu programa de proteção de dados para o próximo nível, você precisa de uma ferramenta poderosa de gerenciamento de incidentes que simplifique as operações e ofereça treinamento de usuários.

Muitos programas de proteção enfrentam dificuldades devido a incidentes e ferramentas desconexas. Além disso, os usuários nunca aprendem quais comportamentos de risco eles cometeram ao manipular os dados incorretamente.

A Zscaler Workflow Automation oferece uma ferramenta dedicada para administradores de DLP para turbinar o gerenciamento de incidentes.

Com toda a análise forense em um só lugar, os administradores podem compreender rapidamente comportamentos de risco, atribuir incidentes a usuários para fins de justificativa e implementar rapidamente ações de políticas para solucionar incidentes.

Como a Workflow Automation ajuda seu programa de proteção de dados

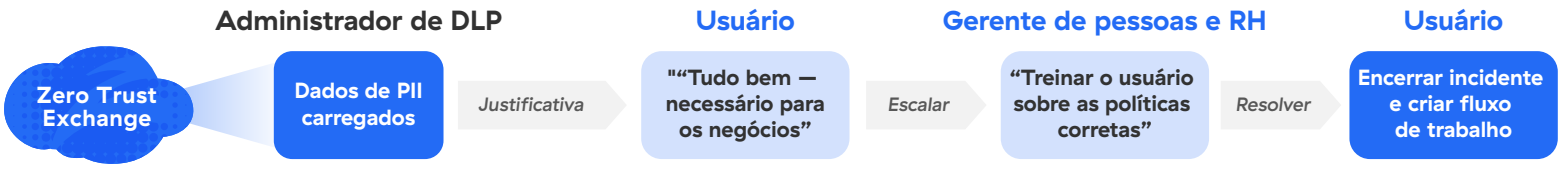
Gerenciamento mais rápido de incidentes
Economize tempo com uma plataforma desenvolvida especificamente para gerenciamento de incidentes de perda de dados

Rotinas automatizadas
Simplifique as operações diárias usando fluxos de trabalho para automatizar tarefas repetitivas e escalonamentos

Treinamento de usuários
Justifique incidentes com usuários via Slack, Teams ou e-mail, e instrua-os sobre as práticas recomendadas de proteção de dados

Totalmente integrada
Evite falhas comuns no programa de proteção, fornecendo um sistema abrangente de tratamento de incidentes

Fluxos de trabalho poderosos
Gerencie incidentes, instrua usuários e automatize fluxos de trabalho



© 2024 Zscaler, Inc. Todos os direitos reservados.

Resumo

Proteção máxima, esforço mínimo

A proteção de dados da Zscaler segue seus usuários e os aplicativos que eles acessam para proteger seus dados na nuvem e no mundo móvel. A Zscaler Zero Trust Exchange™ é uma plataforma desenvolvida para fins específicos que oferece a proteção e a visibilidade que você precisa para simplificar a conformidade e tornar a proteção de dados fácil.

A Zero Trust Exchange:

- **Fornece proteção idêntica** para que você possa disponibilizar uma política de proteção de dados consistente para todos os usuários, independentemente de sua conexão ou localização.
- **Inspeciona todo o seu tráfego em TLS/SSL** para eliminar os pontos cegos, tudo respaldado pelos melhores SLAs do setor.
- **Simplifica a conformidade** para que você possa encontrar e controlar dados de PCI, PII e PHI com facilidade, ao mesmo tempo em que melhora sua capacidade de manter os requisitos de conformidade.
- **Elimina a complexidade** com uma plataforma unificada que permite proteger todos os seus canais de dados na nuvem: dados em trânsito, em repouso e entre terminais e nuvens.

© 2024 Zscaler, Inc. Todos os direitos reservados.

Obtenha proteção de dados desenvolvida para um mundo móvel e orientado para a nuvem

Seus dados não ficam mais no data center. Estão em qualquer lugar e acessíveis aos funcionários que trabalham fora do escritório e praticamente em qualquer lugar. Suas abordagens de segurança existentes não podem proteger os dados em um mundo móvel e na nuvem. Com os serviços de proteção de dados da Zscaler, você pode fornecer proteção idêntica para seus dados críticos, independentemente de onde os usuários se conectam ou onde os aplicativos estão hospedados. **Deixe-nos mostrar como.**

Veja histórias de sucesso de clientes sobre Zscaler Data Protection >

Obter e-book

Saiba mais sobre a plataforma Zcaler Data Protection >

Visite-nos on-line

zscaler™ | Experience your world, secured.™

Sobre a Zscaler
A Zscaler (NASDAQ: ZS) acelera a transformação digital para que seus clientes possam ter mais agilidade, eficiência, resiliência e segurança. A solução Zscaler Zero Trust Exchange protege milhares de clientes contra ataques cibernéticos e perda de dados, conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange baseada em SSE é a maior plataforma integrada de segurança na nuvem do mundo. Saiba mais em **zscaler.com/br** ou siga-nos no Twitter **@zscaler**.

© 2024 Zscaler, Inc. Todos os direitos reservados. Zscaler™, Zero Trust Exchange™ e outras marcas registradas listadas em **zscaler.com/br/legal/trademarks** são (i) marcas registradas ou marcas de serviço ou (ii) marcas comerciais ou marcas de serviço da Zscaler, Inc. nos Estados Unidos e/ou em outros países. Quaisquer outras marcas registradas são de propriedade de seus respectivos detentores.

+1 408.533.0288 Zscaler, Inc. (Sede) • 120 Holger Way • San Jose, CA 95134 zscaler.com/br