Três requisitos essenciais para a proteção de dados perfeita

Procurando um CASB melhor e um DLP mais robusto? Você precisa começar com a base certa.

Qualquer pessoa que trabalhe com TI ou segurança de rede dirá a mesma coisa: a proteção de dados costumava ser muito mais fácil quando todos os dados estavam no data center e os funcionários trabalhavam no escritório. Mas os tempos com certeza mudaram.

Agora, os seus dados saíram do data center e estão em todos os lugares, espalhados por centenas de aplicativos na nuvem. Seus funcionários estão adotando o trabalho remoto, fora da rede corporativa e longe dos seus controles de segurança. Como se não bastasse, a maior parte do tráfego de internet é criptografada e difícil de inspecionar, e é por isso que agentes maliciosos escondem suas ameaças lá. E seus funcionários estão usando redes inseguras ou dispositivos não gerenciados, oferecendo ainda mais oportunidades para expor seus dados.

Nesse admirável mundo novo, as organizações precisam de uma plataforma de proteção de dados criada desde o início com foco na nuvem e na mobilidade, e ela deve possuir os seguintes requisitos essenciais.

Você precisa saber

O nível da proteção de dados que um CASB e DLP proporcionam depende da arquitetura em que eles se encontram. É fundamental entender a receita para o sucesso.

Requisito essencial nº 1

Insista em uma arquitetura SASE criada para fins específicos

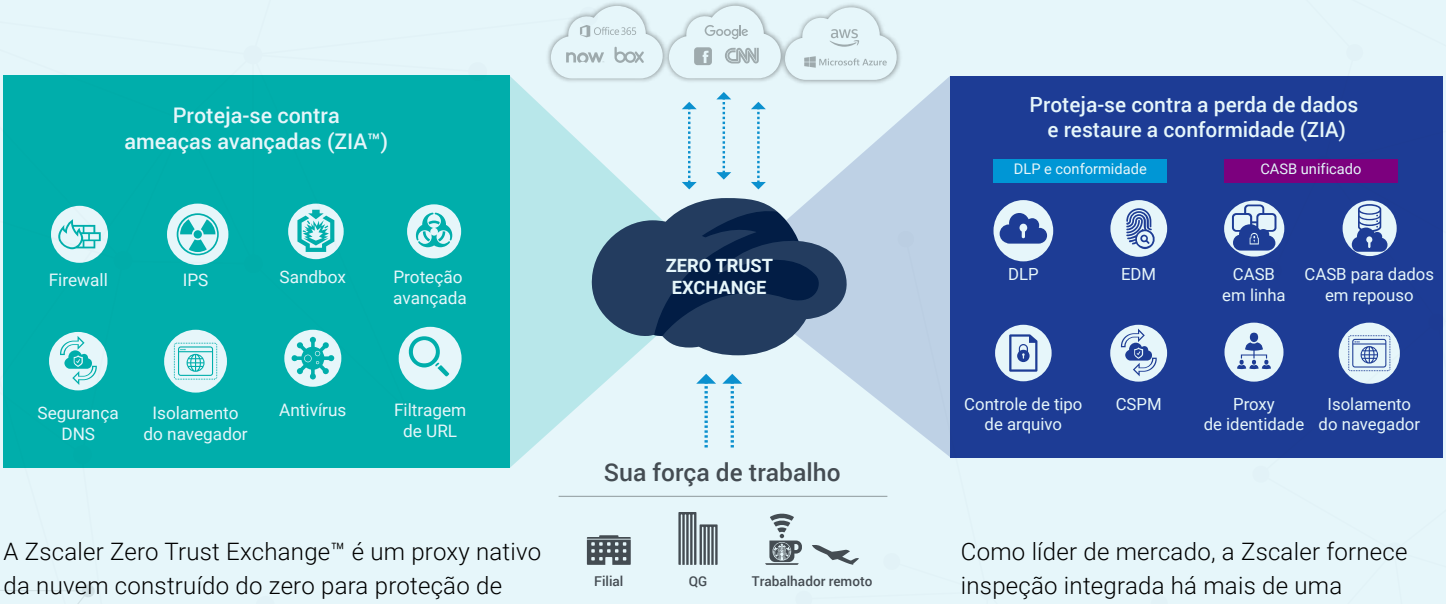
Com a nuvem e a mobilidade, os dispositivos de segurança não conseguem estar em todos os lugares. Quando os usuários saem da rede, você perde visibilidade e seus usuários e dados são expostos. Além disso, para oferecer recursos robustos de agente de segurança de acesso à rede (CASB) e proteção contra perda de dados (DLP), você precisa de inspeção de SSL completa. Devido às restrições de hardware, os dispositivos não conseguem fornecer isso.

Uma plataforma SASE na nuvem especialmente desenvolvida é o primeiro requisito necessário para fornecer conexões de alta performance e sempre ativas, não importando a localização do usuário. A SASE unifica todos os serviços de CASB, DLP e segurança em uma plataforma na nuvem distribuída globalmente para que você tenha menos complexidade, melhor proteção de dados e uma experiência de usuário mais rápida.

Você precisa saber

Não é fácil construir uma arquitetura integrada de proteção de dados de nível corporativo que seja dimensionável em SSL. Confie o seu tráfego apenas a um fornecedor altamente experiente, com histórico comprovado e SLAs de nível corporativo.

A maneira Zscaler™



A Zscaler Zero Trust Exchange™ é um proxy nativo da nuvem construído do zero para proteção de dados e inspeção de SSL em larga escala através de 150 data centers. Cada usuário obtém uma conexão rápida e segura. E nossa capacidade ilimitada de SSL significa que você consegue proteger os seus dados em cada conexão de usuário, seja dentro ou fora da rede.

Como líder de mercado, a Zscaler fornece inspeção integrada há mais de uma década. E o melhor de tudo: como DLP, CASB e outros serviços de segurança são integrados, você obtém políticas simplificadas e uma abordagem unificada para proteção contra perda de dados e ameaças.

Requisito essencial nº 2

A melhor proteção de dados requer o melhor contexto

Você precisa de contexto para classificar adequadamente os dados, mas é a qualidade do contexto que o ajuda a tomar decisões melhores e mais bem informadas.

Antigamente, era fácil — os usuários acessavam o e-mail por um servidor de Exchange ou havia apenas alguns servidores de arquivos. Tudo que você precisava para tomar decisões bem informadas estava lá e era de fácil acesso.

Agora, seus dados se movem entre centenas de canais, de aplicativos na nuvem a nuvens públicas e plataformas de compartilhamento de arquivos. E todo o contexto que você precisa nesses canais fica oculto pela criptografia SSL.

Você precisa saber

O contexto é a força vital do CASB e do DLP. Busque a plataforma com o mecanismo de classificação mais robusto, que descubra mais atributos em cada transação na nuvem, dentro ou fora da rede, e dentro do SSL.

A maneira Zscaler

Quando o assunto é contexto, a Zscaler é inigualável.

Nossa Zero Trust Exchange e o nosso aplicativo Client Connector ajudam a fornecer proteção de dados sempre ativa em cada conexão, dentro ou fora da rede. Eles também oferecem visibilidade de TODO o seu tráfego SSL, fornecendo uma enorme quantidade de contexto às empresas.

E, ao aproveitar os dicionários personalizados e do setor, da Zscaler, e utilizar técnicas avançadas, como a impressão digital Exact Data Match (EDM), é possível classificar os dados rapidamente em formatos comuns do setor (PCI, HIPAA) bem como definições personalizadas.

Contexto de um firewall ou proxy	**IP de origem** 172.16.1.12 | **IP de destino** 64.81.2.24 | **Porta de destino** TCP/443 **Protocolo** SSL | **Protocolo** HTTPS	As abordagens integradas tradicionais não fornecem visibilidade suficiente sobre o contexto.
Contexto adicional obtido com a descriptografia SSL completa	**Usuário** JohnDoe | **grupo** prodmgmt | **Localização da** sede **função do aplicativo** upload | **aplicativo** jumpshare | **Tipo de arquivo** PowerPoint **categoria do URL** compartilhamento de arquivo | **Conteúdo** confidencial	Quando você descriptografa todo SSL sem limites, você obtém o contexto necessário para tomar decisões de proteção melhores.

Requisito essencial nº 3

Exija uma plataforma unificada que proteja todos os canais

Proteger seus dados contra vazamentos e exfiltrações exige que a segurança esteja onde seus dados estiverem. Se você não controla cada canal, seus dados estão vulneráveis e expostos à ameaças potenciais.

Além disso, se você não consegue unificar todas as proteções de CASB e DLP em uma plataforma, o processo se torna muito complexo. Sem a visão de uma plataforma única, você termina com uma política desarticulada, falhas de segurança e uma maior tendência a cometer erros graves de configuração.

Você precisa saber

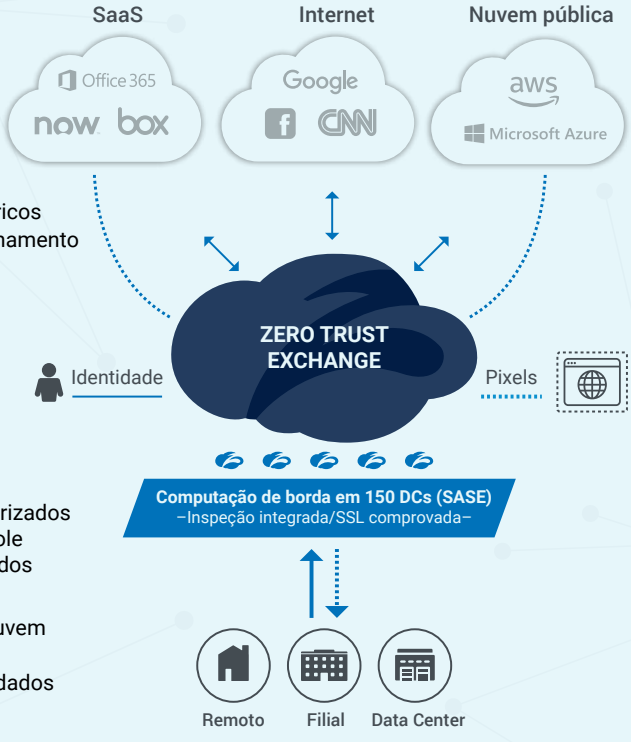
Para todos os principais canais de dados — em trânsito, em repouso, terminais e provedores na nuvem — uma plataforma unificada vai melhorar dramaticamente a força de suas políticas e simplificar seus fluxos de trabalho.

A maneira Zscaler

Como todos os serviços na nuvem da Zscaler são integrados à uma arquitetura de nuvem especialmente desenvolvida, todos os serviços trabalham em harmonia para unificar políticas e facilitar a proteção dos canais de dados na nuvem.

Dados em repouso
Controle de exposição de usuários e ameaças no Microsoft 365 e SaaS

- DLP
- Prevenção contra ameaças
- Verificação de dados históricos
- Exposição sobre compartilhamento



Provedores
Corrija configurações incorretas em nuvens públicas e SaaS (CSPM)

Dados em trânsito
Controle aplicativos não autorizados e ocultos, classifique e controle dados do setor e personalizados

- Controle de tipo de arquivo
- Controle de aplicativo na nuvem
- Cloud DLP
- Correspondência exata de dados
- Inspeção do Microsoft 365

Terminais
Restrinja o acesso de dispositivos próprios e não gerenciados e controle vazamentos de dados

- Proxy de identidade
- Isolamento do navegador

Veja como funciona:

Dados em trânsito: a inspeção integrada de nível corporativo é essencial para fornecer proteção de dados em tempo real. Com a nuvem integrada especialmente desenvolvida da Zscaler, é possível seguir todos os usuários fora da rede e em SSL. Classifique e bloqueie dados críticos rapidamente, não importa para onde estejam indo, e bloqueie aplicativos na nuvem não autorizados.

Dados em repouso: à medida que seus usuários adotam aplicativos na nuvem, é necessário confirmar se eles estão tomando as decisões certas. Com o CASB fora de banda da Zscaler, você pode controlar facilmente o compartilhamento impróprio de arquivos nos aplicativos do Microsoft 365, como SharePoint e OneDrive, bem como analisar repositórios de arquivos em busca de problemas de DLP e malware.

Terminais: esse canal trata de se certificar que apenas as pessoas certas tenham acesso aos seus dados. Com o controle de acesso para dispositivos pessoais, é possível fazer uma rápida pesquisa SAML/SSO e bloquear o acesso não autorizado a recursos do Microsoft 365. Além disso, o Zscaler Cloud Browser Isolation ajuda a evitar vazamentos em dispositivos não gerenciados (BYOD), uma vez que renderiza os dados nos terminais apenas como pixels. Isso significa que um prestador de serviço poderá ver e interagir com os dados, mas não poderá salvar, baixar e nem copiar e colar esses dados. Isso garante que nada permaneça no dispositivo ao final da sessão.

Provedores: A configuração acidental incorreta de aplicativos na nuvem é uma das causas mais comuns de exposição dos dados, custando tempo e dinheiro às empresas. O Zscaler Cloud Security Posture Management (CSPM) automaticamente identifica e corrige configurações incorretas de aplicativos SaaS, IaaS e PaaS, para que o risco de perder dados seja reduzido e você possa manter a conformidade.

Resumo

A nuvem e a mobilidade mudaram a maneira como as empresas fazem negócios e como os funcionários trabalham. Os dados são tratados de forma diferente agora, então precisam de uma proteção diferente. Os dispositivos de segurança não oferecem mais proteção adequada para os dados no mundo atual. Você precisa de uma plataforma de segurança criada na nuvem — com uma base SASE — que proteja os seus dados onde quer que eles estejam. Você precisa da Zscaler.

Veja o nosso CASB/DLP integrado em ação
youtube.com/watch?v=R88TlNEMgGE

Veja o nosso CASB fora de banda em ação
youtube.com/watch?v=1KtoW-IXgMs

Entre em contato conosco ou agende uma demonstração personalizada
zscaler.com/company/contact

Sobre a Zscaler
A Zscaler acelera a transformação digital com sua Zero Trust Exchange, uma plataforma baseada em SASE que oferece conexões rápidas e seguras entre usuários, dispositivos e aplicativos em qualquer rede.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com