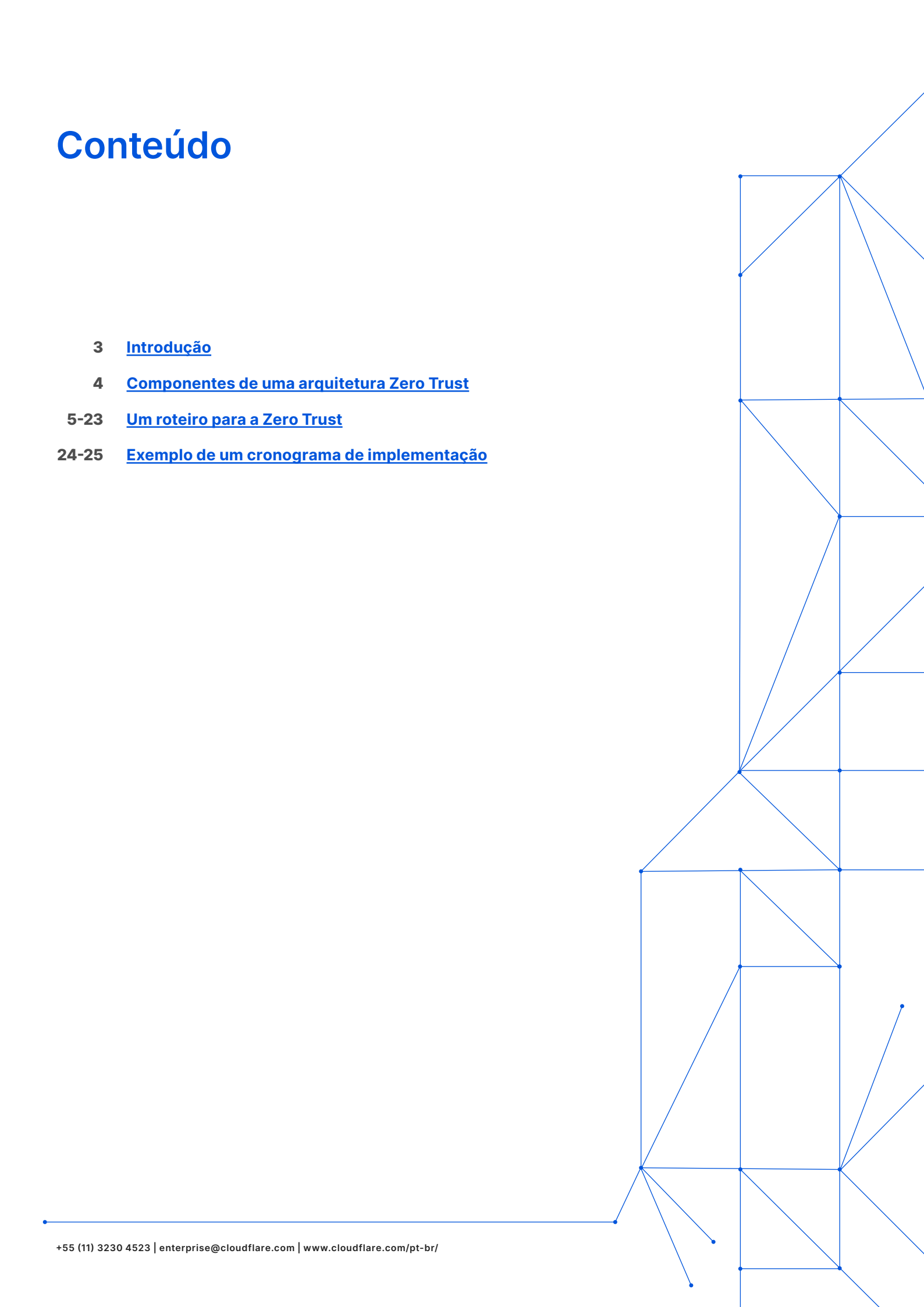
CLOUDFLARE

ARTIGO TÉCNICO

Roteiro da Arquitetura Zero Trust

Aprenda quais são as etapas, as ferramentas e as equipes necessárias para transformar sua rede e modernizar sua segurança

Conteúdo



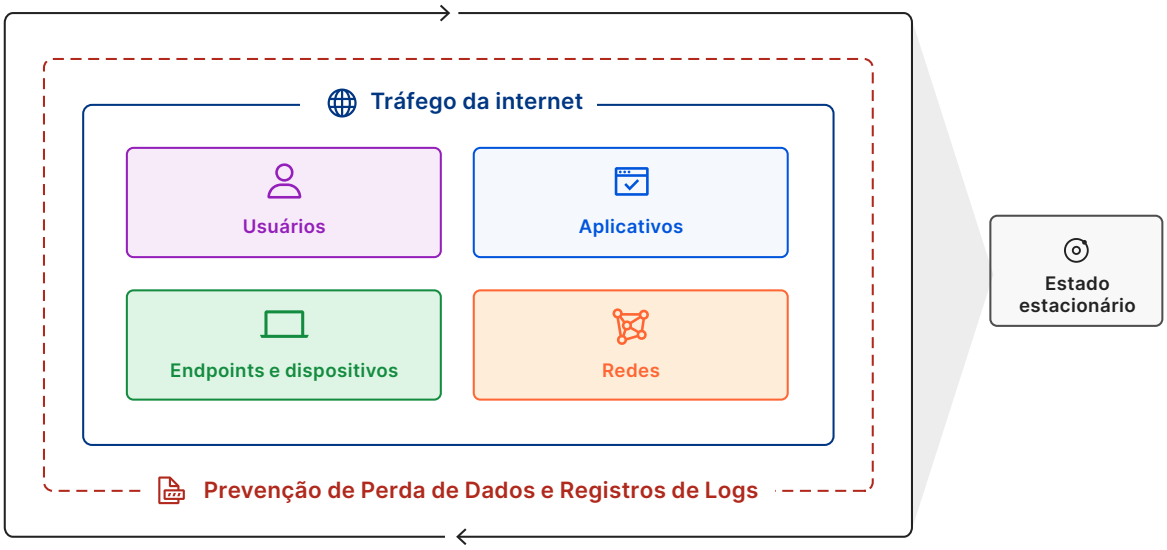
Introdução

A arquitetura de rede tradicional foi criada com base no conceito de um perímetro de rede dentro do qual, uma vez que a pessoa estivesse na rede, haveria um nível implícito de confiança. A migração em direção à hospedagem em nuvem, ao trabalho remoto e a outras modernizações criou desafios no que se refere ao perímetro de rede da arquitetura tradicional.

Esses desafios podem ser abordados por meio da implementação de uma Arquitetura Zero Trust, que garante que todo o tráfego de entrada e saída de uma empresa seja verificado e autorizado. A implementação de uma Arquitetura Zero Trust pode ser feita em etapas, sem perturbar a conectividade e a produtividade dos funcionários.

Este guia foi desenvolvido por especialistas em segurança para fornecer uma arquitetura Zero Trust independente de fornecedor e um exemplo de cronograma de implementação. O cronograma pressupõe que uma organização está iniciando sua jornada Zero Trust a partir do zero, mas pretende ser útil para todas as organizações.

Existem sete componentes principais da segurança organizacional que precisam ser levados em conta quando se trata de implementar uma Arquitetura Zero Trust abrangente.
A ordem de implementação que você adotar não precisa ser a mesma que está listada nas seções de componentes e arquitetura de referência a seguir.



Componentes de uma arquitetura Zero Trust

	Componente	Objetivo	Nível de esforço	Página
Fase 1	Tráfego de internet	Implementar filtragem de DNS global	▮	9
	Aplicativos	Monitorar a entrada de e-mails e filtrar as tentativas de phishing	▮	13
	DLP e registros	Identificar configurações erradas e dados compartilhados publicamente nas ferramentas de SaaS	▮	20
Fase 2	Usuários	Estabelecer uma identidade corporativa	▮▮	5
	Usuários	Implementar uma MFA básica para todos os aplicativos	▮	6
	Aplicativos	Implementar HTTPS e DNSSEC	▮	17
	Tráfego de internet	Bloquear ou isolar as ameaças por trás do SSL	▮▮	9-10
	Aplicativos	Implementação de políticas ZT para aplicativos endereçáveis publicamente	▮	14-16
	Aplicativos	Proteger aplicativos contra ataques na camada 7	▮	16
	Redes	Fechar todas as portas de entrada abertas para a internet para entrega de aplicativos	▮	12
Fase 3	Aplicativos	Inventariar todos os aplicativos corporativos	▮▮	13-14
	Aplicativos	Implementação de políticas ZT para aplicativos SaaS	▮▮	14-16
	Redes	Segmentar o acesso de usuários à rede	▮▮▮	11
	Aplicativos	ZTNA para aplicativos críticos endereçáveis de forma privada	▮	14-16
	Dispositivos	Implementar MDM/UEM para controlar dispositivos corporativos	▮▮	7
	DLP e registros	Definir quais dados são confidenciais e onde eles existem	▮▮	18-19
	Usuários	Enviar tokens de autenticação baseados em hardware	▮▮	6
	DLP e registros	Manter-se atualizado com relação a agentes de ameaças conhecidos	▮	21
Fase 4	Usuários	Implementar uma MFA baseada em tokens de hardware	▮▮	6
	Aplicativos	Implementação de políticas e acesso à rede ZT para todos os aplicativos	▮▮▮	14-16
	DLP e registros	Estabelecer um SOC para análise de registros, atualizações de política e mitigação	▮▮	20
	Dispositivos	Implementar a proteção de endpoints	▮▮	7
	Dispositivos	Inventariar todos os dispositivos, APIs e serviços corporativos	▮	8
	Redes	Usar a internet banda larga para conexão entre filiais	▮▮▮	11-12
	DLP e registros	Registrar e analisar a atividade de funcionários em aplicativos confidenciais	▮▮	18
	DLP e registros	Impedir que dados confidenciais saiam dos seus aplicativos	▮▮▮	19
	Estado estacionário	A abordagem do DevOps para a implementação de políticas de novos recursos	▮▮	22
	Estado estacionário	Implementar a escala automática para recursos de acesso à rede	▮▮▮	22-23

Veja como definimos os diferentes níveis de esforço necessários para cada etapa:

- ▮ - **Pouco esforço:** algo que pode ser feito por uma só pessoa ou uma equipe pequena
- ▮▮ - **Médio esforço:** algo que requer uma equipe e preparação antecipada
- ▮▮▮ - **Grande esforço:** algo que requer diversas equipes e um plano de projeto

Um roteiro para a Zero Trust

Usuários

Os usuários incluem funcionários, prestadores de serviços e clientes. Para implementar a Zero Trust, uma organização precisa, primeiro, adquirir uma noção precisa de quem deve, de fato, ser digno de confiança e com referência a quê — algo que costumamos chamar de Identidade. A seguir, é preciso estabelecer uma forma de autenticar com segurança a identidade de seus usuários.

Estabelecer uma identidade corporativa

Nível de esforço	**- Médio esforço**
Equipe(s) envolvida(s)	• Equipe responsável pelo seu provedor de identidade (tipicamente de segurança ou de TI) • Os administradores que gerenciam aplicativos internos usados por funcionários e parceiros
Produto(s)	Microsoft Azure AD, Okta, PingOne da Ping Identity, OneLogin
Resumo	Uma identidade corporativa unificada é necessária para autenticar e autorizar com precisão o acesso de usuários aos aplicativos corporativos. Uma Identidade corporativa consistente fará com que a implementação granular de políticas em seus aplicativos enfrente menos obstáculos. **Pontos adicionais a se considerar:** • Sua empresa está ativa em F&A? O que você fará para consolidar armazenamentos de identidade? • Você tem protocolos de autenticação não baseados na web sendo usados (por exemplo, Active Directory, NTLM, Kerberos)?
Etapas	1. Adicionar todos os usuários corporativos ao provedor de identidade a. Esses valores podem com frequência ser sincronizados a partir de um sistema de RH, como o Workday, o ADP etc. 2. Verificar se as informações de cada usuário estão corretas 3. Enviar as informações de cadastro de novos usuários para configurar credenciais de login

Implementar a autenticação multifator para todos os aplicativos

Nível de esforço	 - **Pouco esforço** (se estiver aplicando MFA básica)  - **Médio esforço** (se estiver usando Hard Keys)
Equipe(s) envolvida(s)	• Equipe responsável pelo seu provedor de identidade (tipicamente de segurança ou de TI) • Os administradores que gerenciam aplicativos internos usados por funcionários e parceiros
Produto(s)	**Provedores de identidade:** Microsoft Azure AD, Okta, PingOne da Ping Identity, OneLogin **Proxies Reversos de Aplicativos:** Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA) **Hard Keys:** Yubico
Resumo	A Autenticação Multifator (MFA) é a melhor proteção contra credenciais do usuário roubadas por meio de phishing ou vazamento de dados. A maioria das MFAs pode ser habilitada diretamente em um IdP. Para implementar a MFA nos aplicativos não integrados diretamente com seu IdP, pense em usar um Proxy Reverso de Aplicativo na frente do aplicativo.
Etapas	1. Alertar os usuários internos quanto à futura implementação da MFA; fornecer opções de cadastramento para receber autenticadores por SMS ou baseados em aplicativos. 2. Habilitar a MFA no seu IdP 3. Habilitar um Proxy Reverso de Aplicativo na frente dos aplicativos não integrados diretamente com seu IdP 4. (Bônus) Distribuir chaves de hardware para os funcionários por correio ou entrega em mãos 5. (Bônus) Implementar MFA somente com chaves de hardware para seus aplicativos mais confidenciais

Endpoints e dispositivos

Endpoints e dispositivos incluem qualquer dispositivo, API ou serviço de software dentro de uma organização ou que tenham acesso aos dados da organização. Em primeiro lugar, as organizações precisam entender todo o seu conjunto de dispositivos, APIs e serviços. A seguir, as políticas de Zero Trust podem ser implementadas com base no contexto do dispositivo, API ou serviço.

Implementar o gerenciamento de dispositivos móveis

Nível de esforço	**- Médio esforço**
Equipe(s) envolvida(s)	• Equipe de TI
Produto(s)	**Mac:** Jamf, Kandji **Windows:** Microsoft Intune
Resumo	A maior parte das arquiteturas Zero Trust requer que um software seja instalado em pelo menos um subconjunto de computadores de usuários. O Gerenciamento de Dispositivos Móveis (MDM) é usado pela maioria das organizações para gerenciar o software e a configuração em todo o seu inventário de dispositivos de usuários.
Etapas	Consulte o site do fornecedor de MDM para obter os detalhes específicos.

Implementar a proteção de endpoints

Nível de esforço	**- Médio esforço**
Equipe(s) envolvida(s)	• Equipe de segurança • Equipe de TI
Produto(s)	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender
Resumo	O software de proteção de endpoints é instalado no computador de um usuário e faz a varredura de ameaças conhecidas que afetam os dispositivos. O software de proteção de endpoints também pode ser usado para implementar a conformidade das atualizações e patches do sistema operacional. O sinal do seu software de proteção de endpoints pode e deve ser usado nas políticas de controle de acesso do seu aplicativo.
Etapas	1. Instalar o software de proteção de endpoints nos computadores dos usuários usando o MDM 2. Habilitar a proteção contra ameaças e o controle de conformidade na plataforma de proteção de endpoints

Inventariar dispositivos, APIs e serviços

Nível de esforço	**- Pouco esforço**
Equipe(s) envolvida(s)	• Equipe de segurança • Equipe de TI
Produto(s)	**Inventário de dispositivos:** VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender, Oomnitza **Inventário de APIs/Serviços:** Conector de aplicativos da Cloudflare, Zscaler Private Access (ZPA)
Resumo	Os softwares de proteção de endpoints e de gerenciamento de ativos podem ser usados para rastrear todos os dispositivos que foram distribuídos para os usuários. Deve ser mantida uma lista precisa dos dispositivos para rastrear quais dispositivos são válidos e devem ter acesso a aplicativos específicos. As APIs e serviços também devem ser detectados e mantidos em um inventário. A varredura de rede pode ser aproveitada para identificar as APIs e serviços de software vistos recentemente que possam se comunicar pela internet ou pela rede externa.
Etapas	1. Instalar o software de proteção de endpoints nos computadores dos usuários usando o MDM 2. Instalar o scanner de APIs/Serviços na sua rede

Tráfego da internet

O tráfego da internet inclui todo o tráfego de usuários cujo destino são sites fora do controle de uma organização. Isso pode variar desde tarefas relacionadas a negócios até o uso pessoal de um site. Todo o tráfego de saída é suscetível a malware e sites maliciosos. Uma organização precisa estabelecer visibilidade e controle sobre o tráfego de usuários destinado à internet.

Bloquear solicitações de DNS para ameaças conhecidas ou destinos arriscados

Nível de esforço	- **Pouco esforço**
Equipe(s) envolvida(s)	• Equipe de TI com acesso a um roteador ou à configuração de um computador • Equipe de segurança
Produto(s)	**Filtragem de DNS:** Cisco Umbrella DNS, Gateway da Cloudflare, DNSFilter, Zscaler Shift
Resumo	A filtragem de DNS pode ser aplicada por meio da configuração do roteador ou diretamente no computador do usuário. Trata-se de uma das maneiras mais rápidas de proteger usuários contra sites sabidamente maliciosos.
Etapas	**Filtragem de DNS:** Atualizar a configuração da resolução de DNS no Wi-Fi do seu escritório para que aponte para o serviço de resolução de DNS apropriado. Isso pode ser usado para bloquear sites sabidamente maliciosos.

Bloquear ou isolar as ameaças por trás de SSL/TLS

Nível de esforço	- **Médio esforço**
Equipe(s) envolvida(s)	• Equipe de TI com acesso a um roteador ou à configuração de um computador • Equipe de segurança
Produto(s)	**Descriptografia TLS:** Gateway da Cloudflare, Next Gen SWG da Netskope, Zscaler Internet Access (ZIA) **Isolamento do Navegador:** Isolamento do Navegador da Cloudflare, Isolamento do Navegador em Nuvem da Zscaler

Bloquear ou isolar as ameaças por trás de SSL/TLS (continuação)

Resumo	Algumas ameaças estão ocultas por trás do SSL e não podem ser bloqueadas apenas por meio da inspeção de HTTPS. Para proteger ainda mais os usuários, a descriptografia TLS deve ser aproveitada para também proteger os usuários contra as ameaças por trás do SSL.

Etapas	**Descriptografia TLS:**
	1. Garantir que o software cliente correto seja instalado no computador de um usuário
	  a. Verificar a presença de qualquer VPN ou outro software que possam interferir com o tráfego de saída da internet no dispositivo
	2. Configurar o certificado raiz no dispositivo para descriptografia TLS
	3. Habilitar políticas em torno de quando evitar a descriptografia do tráfego de usuário
	  a. Isso deve ser feito para os sites que utilizam pinning de certificado
	  b. Algumas empresas também ignoram a descriptografia para o tráfego pessoal dos usuários (por exemplo, operações bancárias, redes sociais etc.)
	
	Isolamento do navegador:
	1. O isolamento do navegador pode ser implantado por meio do software cliente no dispositivo ou por meio de um link de isolamento. Ambas as abordagens devem ser levadas em conta.

Redes

As redes incluem todas as redes públicas, privadas e virtuais dentro de uma organização. Em primeiro lugar, as organizações precisam entender seu conjunto de redes existentes e segmentá-las de forma a impedir o movimento lateral. A seguir, podem ser criadas políticas Zero Trust que controlem de forma granular quais segmentos de uma rede os usuários, endpoints e dispositivos podem acessar.

Segmentar o acesso de usuários à rede

Nível de esforço	 **- Grande esforço**
Equipe(s) envolvida(s)	• Equipe de segurança • Equipe de TI
Produto(s)	**Acesso à Rede Zero Trust (ZTNA):** Zero Trust da Cloudflare (Access e Gateway usados em conjunto), Netskope Private Access, Zscaler Private Access (ZPA)
Resumo	De modo geral, os usuários podem acessar uma rede privada em sua totalidade usando uma VPN ou enquanto estiverem na rede do escritório. Uma estrutura Zero Trust requer que os usuários tenham acesso apenas aos segmentos específicos da rede necessários para que executem determinada tarefa. As soluções de Rede Zero Trust permitem que os usuários acessem uma rede local remotamente, mas com políticas granulares baseadas no usuário, no dispositivo e em outros fatores.
Etapas	1. Tornar a rede privada disponível para o ZTNA a. Tipicamente, um conector de aplicativo, GRE ou Túnel IPsec 2. Instalar o cliente ZTNA nos dispositivos do usuário usando MDM 3. Configurar políticas que segmentem o acesso do usuário ao longo da rede privada

Usar a internet banda larga para conexão entre filiais

Nível de esforço	 **- Grande esforço**
Equipe(s) envolvida(s)	• Equipe de engenharia de rede • Equipe de TI
Produto(s)	Magic WAN da Cloudflare, Cato Networks, Aryaka FlexCore

Usar a internet banda larga para conexão entre filiais (continuação)

Resumo	A conectividade entre os locais de uma rede privada (por exemplo, data centers e filiais) geralmente tem sido estabelecida com o uso de linhas de Comutação de Rótulos Multiprotocolo (MPLS) ou outras formas de links privados oferecidos por provedores de telecomunicações. Esses links MPLS costumam ser caros e, à medida que a alta qualidade se torna uma commodity na internet, as organizações passam a poder fornecer o mesmo nível de acesso seguro roteando o tráfego pela internet por meio de túneis seguros, a uma fração do custo.
Etapas	1. Escolher dois locais conectados por MPLS para começar. Esses locais irão precisar de alguma de forma de conectividade com a internet 2. Estabelecer um par de GRE Anycast redundante ou túneis IPsec por meio dos seus circuitos de internet para a rede de borda do seu provedor de WAN em nuvem 3. Verificar a integridade e a conectividade entre esses túneis. Testar o desempenho (produtividade, latência, perda de pacotes, jitter) de cargas de trabalho de tráfego o mais semelhantes possível ao tráfego de produção 4. Mudar as políticas de roteamento de modo a migrar o tráfego de produção de MPLS para os túneis de internet 5. Repetir no próximo local conectado por MPLS 6. Desativar os circuitos MPLS

Fechar todas as portas de entrada abertas para a internet para entrega de aplicativos

Nível de esforço	**- Pouco esforço**
Equipe(s) envolvida(s)	• Equipe de engenharia de rede
Produto(s)	**Proxies Reversos Zero Trust:** Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access (ZPA)
Resumo	Portas de entrada de rede abertas podem ser encontradas com o uso de tecnologia de varredura e constituem um vetor de ataque comum. Os Proxies Reversos Zero Trust permitem que você exponha um aplicativo web com segurança, sem abrir nenhuma porta de entrada. O registro de DNS do aplicativo é o único registro publicamente visível do aplicativo. E o registro de DNS é protegido por políticas Zero Trust. Como uma camada adicional de segurança, o DNS interno/privado pode ser melhor aproveitado com o uso de um serviço de Acesso à Rede Zero Trust (mais detalhes abaixo).
Etapas	1. Instalar o conector do aplicativo de Proxy Reverso — tipicamente um daemon ou máquina virtual em algum lugar da mesma rede 2. Conectar o Aplicativo de Proxy Reverso ao conector do aplicativo 3. Feche todas as portas de entrada na rede privada com uma regra de firewall

Aplicativos

Os aplicativos incluem quaisquer recursos nos quais dados da organização estejam presentes ou processos comerciais sejam executados. Em primeiro lugar, as organizações precisam entender quais aplicativos existem e, em seguida, estabelecer políticas Zero Trust para cada aplicativo ou, em alguns casos, bloquear aplicativos não aprovados.

Monitorar os aplicativos de e-mail e filtrar as tentativas de phishing

Nível de esforço	**- Pouco esforço**
Equipe(s) envolvida(s)	• Equipe responsável pela configuração do seu provedor de e-mail (tipicamente de TI)
Produto(s)	**Segurança de e-mails em nuvem:** Segurança de e-mails Area 1 da Cloudflare, Mimecast, TitanHQ **Isolamento do Navegador:** Isolamento do Navegador da Cloudflare, Isolamento do Navegador em Nuvem da Zscaler
Resumo	O e-mail é um dos poucos canais de comunicação por meio do qual os invasores têm um livre acesso aos seus funcionários. A implementação de um gateway seguro de e-mail é um etapa crucial para garantir que e-mails maliciosos ou não confiáveis nunca alcancem seus funcionários. Além disso, as equipes de segurança devem pensar na opção de colocar em quarentena em um navegador isolado os links que não são suspeitos o suficiente para serem totalmente bloqueados.
Etapas	1. Configurar os registros MX do seu domínio para que apontem para um serviço de gateway seguro de e-mail 2. Monitorar falsos positivos nas primeiras semanas 3. (Bônus) implementar uma abordagem de isolamento do navegador baseada em links para os links de e-mails no limite da suspeição.

Inventariar todos os aplicativos corporativos

Nível de esforço	**- Médio esforço**
Equipe(s) envolvida(s)	• Equipe de segurança
Produto(s)	**Gateway seguro da web e CASBs com descoberta de TI invisível:** Gateway da Cloudflare, Microsoft Defender para Aplicativos em Nuvem, Next Gen SWG da Netskope, Zscaler Internet Access (ZIA)

Inventariar todos os aplicativos corporativos (continuação)

Resumo	É crucial que a equipe de segurança entenda o inventário completo de aplicativos usados em toda a empresa. As equipes de segurança com frequência irão descobrir aplicativos desconhecidos ou não permitidos sendo usados em toda a empresa, geralmente conhecidos como "TI Invisível". Um Gateway seguro da web com descriptografia TLS pode ser usado para identificar aplicativos. O Gateway seguro da web também pode ser usado para bloquear aplicativos ou locatários de aplicativos não aprovados (por exemplo, contas pessoais do Dropbox).
Etapas	1. Habilitar varreduras da TI invisível no Gateway seguro da web 2. Garantir que um cliente de Gateway seguro da web seja instalado nos dispositivos de usuários 3. Permitir 2 a 3 semanas de tráfego de usuários 4. Avaliar a lista de aplicativos identificados 5. Todos os aplicativos não aprovados devem ser bloqueados pelas políticas de Gateway seguro da web 6. Os aplicativos aprovados devem ser protegidos por políticas Zero Trust

Implementação de políticas Zero Trust para aplicativos

Nível de esforço	**- Pouco esforço** (para os aplicativos mais críticos) **- Grande esforço** (para todos os aplicativos)
Equipe(s) envolvida(s)	• Equipe de segurança • Equipe de desenvolvimento de aplicativos • Equipe de TI
Produto(s)	**Proxies Reversos Zero Trust:** Azure App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA) **Acesso à Rede Zero Trust (ZTNA):** Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA) **CASB:** CASB da Cloudflare, CASB da Netskope, CASB da Zscaler **Isolamento do Navegador Remoto:** Isolamento do Navegador da Cloudflare, Isolamento do Navegador em Nuvem da Zscaler

Implementação de políticas Zero Trust para aplicativos (continuação)

Resumo	Os aplicativos precisam estar protegidos com políticas Zero Trust que levem em conta a identidade, o dispositivo e o contexto de rede de um usuário antes de autenticar e autorizar o acesso. Os aplicativos devem ter políticas granulares que implementem o menor privilégio, especialmente no caso de aplicativos que contenham dados confidenciais. Existem três tipos principais de aplicativos e o modelo de segurança Zero Trust varia de acordo com cada tipo. Os principais tipos de aplicativos são: 1. Aplicativos privados auto-hospedados (endereçáveis apenas na rede corporativa) 2. Aplicativos públicos auto-hospedados (endereçáveis pela internet) 3. Aplicativos SaaS **Observação:** se o contexto ou status de conformidade de um dispositivo estiverem sujeitos a uma política de segurança obrigatória, de modo geral será necessário um software cliente no dispositivo.
Etapas	**Aplicativos privados auto-hospedados** 1. Construir um túnel criptografado entre o aplicativo e a camada da política Zero Trust. De modo geral trata-se de um "conector de aplicativo", GRE ou túnel IPsec 2. Disponibilizar o resolvedor de DNS privado para os usuários do cliente de dispositivo ZTNA 3. Criar políticas baseadas no contexto do usuário, dispositivo e rede para estabelecer quem pode acessar o aplicativo **Aplicativos públicos auto-hospedados** 1. Migrar o DNS autoritativo ou um registro CNAME para o Proxy Reverso de Aplicativo 2. Garantir que todas as portas de entrada estejam fechadas na rede do aplicativo 3. Criar políticas baseadas no contexto do usuário, dispositivo e rede para estabelecer quem pode acessar o aplicativo **Aplicativos SaaS** Existem algumas opções diferentes para implementar políticas Zero Trust nos aplicativos SaaS **Proxy de identidade** A Cloudflare, a Netskope e a Zscaler fornecem Proxies de Identidade que permitem a mesma implementação de política como um aplicativo de proxy reverso auto-hospedado. Isso requer que o Proxy de Identidade seja configurado como o provedor de SSO do aplicativo SaaS 1. Remover a integração de SSO existente do aplicativo Saas, caso esteja presente 2. Integrar o Proxy de Identidade com o aplicativo SaaS 3. Garantir que os atributos SAML corretos sejam enviados para serem criados e atualizados pelo usuário 4. Criar políticas baseadas no contexto do usuário, dispositivo e rede

Implementação de políticas Zero Trust para aplicativos (continuação)

Etapas	**Gateway seguro da web e Login único** A outra abordagem é usar um provedor de login único existente para controlar quais usuários podem ou não acessar o aplicativo SaaS. A seguir, um Gateway seguro da web com um endereço de IP dedicado pode ser usado para garantir que apenas usuários de dispositivos gerenciados com inspeção de tráfego possam acessar o aplicativo SaaS. 1. Adicionar o aplicativo SaaS ao provedor de SSO 2. Criar políticas que imponham quais usuários estão autorizados 3. Adicionar o endereço de IP da instância de Gateway seguro da web à Lista de IPs Permitidos do aplicativo SaaS (a maioria dos aplicativos SaaS fornece compatibilidade com listas de IPs permitidos em suas configurações básicas de segurança) 4. Criar políticas de Gateway seguro da web que controlem quais usuários podem acessar o aplicativo SaaS

Proteger os aplicativos contra ataques na Camada 7 (DDoS, injeção, bots etc.)

Nível de esforço	**- Pouco esforço**
Equipe(s) envolvida(s)	• Equipe de segurança • Equipe de desenvolvimento de aplicativos
Produto(s)	Akamai, AWS, Azure, Cloudflare, GCP
Resumo	Todos os aplicativos auto-hospedados são suscetíveis a ataques na Camada 7, que incluem ataques DDoS, de injeção de código, de bots e outros mais. As equipes de segurança devem aplicar um firewall de aplicativos web e proteção contra DDoS na frente de todos os aplicativos auto-hospedados, endereçáveis privada ou publicamente.
Etapas	1. Adicionar todos os registro de DNS autoritativo do aplicativo público 2. Habilitar o Firewall de aplicativos web e proteção contra DDoS

Implementar HTTPS e DNSSEC

Nível de esforço	**- Pouco esforço**
Equipe(s) envolvida(s)	• Equipe de segurança • Equipe de desenvolvimento de aplicativos
Produto(s)	Akamai, AWS, Azure, Cloudflare, GCP
Resumo	Todos os aplicativos web auto-hospedados devem aproveitar o HTTPS e o DNSSEC. Isso evita todas as possibilidades de farejamento de pacotes ou sequestro de domínios.
Etapas	1. Adicionar todos os registro de DNS autoritativo do aplicativo público 2. Configurar o HTTPS como rigoroso e habilitar o DNSSEC

Prevenção de Perda de Dados e Registros de Logs

Após ter estabelecido todos os elementos Zero Trust da sua arquitetura até este ponto, sua arquitetura estará gerando grandes volumes de dados relativos ao que está acontecendo dentro da sua rede. Neste ponto, chegou o momento de implementar a Prevenção de Perda de Dados e Registros de Logs, um conjunto de processos e ferramentas focados em manter os dados confidenciais dentro de uma empresa e alertar quanto a quaisquer possíveis oportunidades de vazamento de dados. Em primeiro lugar, as organizações precisam entender onde estão seus dados confidenciais. A seguir, podem estabelecer controles Zero Trust para impedir que os dados confidenciais sejam acessados e exfiltrados.

Estabelecer um processo para registrar e analisar o tráfego nos aplicativos confidenciais

Nível de esforço	**- Médio esforço**
Equipe(s) envolvida(s)	• Equipe de segurança
Produto(s)	**Gateway seguro da web (SWG):** Cisco Umbrella, Gateway da Cloudflare, Next Gen SWG da Netskope, Zscaler Internet Access (ZIA) **Monitoramento de Eventos e Incidentes de Segurança (SIEM):** DataDog, Splunk, SolarWinds
Resumo	As soluções de Gateway seguro da web têm funcionalidades que transmitem logs de tráfego de usuários para uma ferramenta de SIEM. A equipe de segurança deve tornar rotina o exercício de avaliar os logs de tráfego destinados a aplicativos confidenciais. Alertas específicos para tráfego anômalo ou malicioso podem ser configurados no SIEM e ajustados ao longo do tempo.
Etapas	1. Garantir que todo o tráfego de usuários destinado a aplicativos confidenciais faça proxy usando um SWG 2. Habilitar uma funcionalidade de envio ou extração de logs entre o seu SWG e o seu SIEM 3. Configurar um intervalo específico para a equipe de segurança avaliar os logs de tráfego 4. Configurar alertas no SIEM baseados nos achados ao longo do tempo

Definir quais dados são confidenciais e onde eles existem

Nível de esforço	**- Médio esforço**
Equipe(s) envolvida(s)	• Equipe de segurança • Equipe jurídica/de conformidade
Produto(s)	**Monitoramento de Eventos e Incidentes de Segurança (SIEM):** DataDog, Splunk, SolarWinds

Definir quais dados são confidenciais e onde eles existem (continuação)

Resumo	Os dados confidenciais apresentam ampla variação, dependendo do setor. As empresas de tecnologia estão preocupadas em proteger o código-fonte, enquanto os provedores de atendimento médico mantém um foco intenso na conformidade com a HIPAA. É importante estabelecer o significado de "dados confidenciais" para a sua empresa e saber onde estão presentes. Uma definição precisa e um inventário dos dados confidenciais irão fundamentar a implementação de ferramentas de Prevenção de Perda de Dados.
Etapas	1. Avaliar os logs de tráfego nas ferramentas de SIEM ou diretamente em um Gateway seguro da web para identificar quais aplicativos e armazenamentos de dados devem ser visados 2. Fazer um inventário dos dados confidenciais existentes

Evitar que os dados confidenciais saiam dos seus aplicativos

Nível de esforço	**- Grande esforço**
Equipe(s) envolvida(s)	• Equipe de segurança • Equipe de TI • Equipe jurídica/de conformidade
Produto(s)	**Prevenção de Perda de Dados (DLP) integrada:** Cisco Umbrella, Gateway da Cloudflare, Next Gen SWG da Netskope, Zscaler Internet Access (ZIA)
Resumo	As soluções de DLP integradas inspecionam o tráfego dos usuários e os uploads/downloads para detectar dados confidenciais. Os dados confidenciais ficam disponíveis em listas predefinidas bem conhecidas (por exemplo, PII, CPF, Cartões de Crédito etc.) ou em padrões específicos que podem ser configurados manualmente por um administrador. Os controles de DLP devem ser habilitados para os aplicativos confidenciais e podem ser ampliados de modo a englobar todo o tráfego de usuários.
Etapas	1. Instalar o software cliente do provedor de DLP 2. Garantir que não exista nenhuma VPN ou outra ferramenta que possa perturbar a conectividade 3. Garantir que a descriptografia TLS esteja habilitada e um certificado raiz esteja presente no computador de cada usuário 4. Habilitar os controles de DLP 5. Monitorar os eventos de bloqueio de DLP e verificar se são válidos ou falsos positivos

Identificar configurações erradas e dados compartilhados publicamente nas ferramentas de SaaS

Nível de esforço	**- Pouco esforço**
Equipe(s) envolvida(s)	• Equipe de segurança
Produto(s)	**Agente de Segurança de Acesso à Nuvem (CASB) baseado em API:** CASB da Cloudflare, DoControl, Netskope, CSPM da Zscaler
Resumo	Os CASBs se integram com os principais aplicativos SaaS por meio de uma integração por API. Em seguida, o CASB irá fazer uma varredura do aplicativo SaaS para detectar configurações erradas conhecidas e dados que foram compartilhados publicamente. Uma equipe de segurança deve estabelecer um ritmo regular para avaliar os achados do CASB.
Etapas	1. Conectar cada aplicativo SaaS por meio das instruções de integração de API do provedor 2. Fazer varreduras em cada aplicativo SaaS 3. Avaliar os resultados das varreduras e dar início às correções de cada aplicativo SaaS sempre que for apropriado

Estabelecer um Centro de Operações de Segurança (SOC) para avaliar registros, atualizar políticas e para fins de mitigação

Nível de esforço	**- Médio esforço**
Equipe(s) envolvida(s)	• Equipe de segurança
Produto(s)	**Nenhum**
Resumo	Um SOC é uma função crítica dentro de uma equipe de segurança em uma estrutura Zero Trust e deve se concentrar na avaliação das informações dos registros e dos alertas de segurança e em ajustar as políticas Zero Trust em todos os produtos básicos de segurança.
Etapas	1. Avaliar os registros no SIEM ou diretamente no produto de segurança 2. Identificar quaisquer alertas ou atividades anômalas 3. Atualizar as políticas Zero Trust de cada ferramenta com base nos achados

Manter-se atualizado com relação a agentes de ameaças conhecidos

Nível de esforço	**- Pouco esforço**
Equipe(s) envolvida(s)	• Equipe de segurança
Produto(s)	**Fornecedores de inteligência de segurança:** Radar da Cloudflare, CISA, OWASP
Resumo	Existem vários fornecedores cujo foco é compilar uma lista de agentes de ameaças e sites maliciosos conhecidos. Esses feeds de ameaças podem ser carregados automaticamente no Gateway seguro da web para proteger os usuários contra ataques.
Etapas	1. Conectar o feed de ameaças no Gateway seguro da web 2. Habilitar a proteção contra ameaças na filtragem de DNS e HTTP

Estado estacionário

Após ter construído nossa arquitetura Zero Trust para todos os outros elementos da sua organização, temos uma série de medidas que você pode adotar para migrar sua organização para um estado estacionário Zero Trust, garantindo consistência à arquitetura desse ponto em diante.

Implantar uma abordagem de DevOps para garantir uma implementação consistente de políticas para todos os novos recursos

Nível de esforço	**- Grande esforço**
Equipe(s) envolvida(s)	• Equipe de segurança • Equipe de desenvolvimento de aplicativos
Produto(s)	**Automação de infraestrutura:** Ansible, Puppet, Terraform
Resumo	As ferramentas de automação de infraestrutura permitem que os desenvolvedores implantem a segurança Zero Trust automaticamente como parte do seu pipeline de desenvolvimento de aplicativos. Estabelecer testes internos que serão acionados se um aplicativo for implantado com proteção de Proxy Reverso Zero Trust.
Etapas	1. Definir uma política padrão para novos aplicativos 2. Adicionar testes ao processo de implementação de aplicativos que requerem proteção de Proxy Reverso Zero Trust

Implementar a escala automática para recursos de acesso à rede

Nível de esforço	**- Grande esforço**
Equipe(s) envolvida(s)	• Equipe de segurança • Equipe de desenvolvimento de aplicativos
Produto(s)	**Balanceadores de carga:** Akamai, Cloudflare **Automação de infraestrutura:** Ansible, Puppet, Terraform

Implementar a escala automática para recursos de acesso à rede (continuação)

Resumo	Os balanceadores de carga podem ser ferramentas eficazes para garantir que a infraestrutura de aplicativos nunca fique sobrecarregada, além de fornecer um nível de redundância caso um servidor de aplicativos comece a falhar. As ferramentas de automação de infraestrutura podem ser usadas para programar novos recursos caso limites de tráfego específicos sejam ultrapassados.
Etapas	1. Configurar um balanceador de carga na frente do conector do Aplicativo de Proxy Reverso Zero Trust 2. Habilitar regras de balanceamento de carga baseadas nos volumes de tráfego e/ou na localização geográfica dos usuários. 3. Implementar políticas de automação de infraestrutura que irão provisionar novas máquinas virtuais caso uma carga suficiente seja gerada para um conjunto de aplicativos específico

Exemplo de um cronograma de implementação

Toda implantação de Arquitetura Zero Trust é única, mas a maioria dos projetos segue um conjunto de etapas comum. Este é um cronograma recomendado para que uma empresa comece sua implementação de uma arquitetura Zero Trust.

Cronograma		Objetivo	Produtos relevantes
Fase 1	☐	**Implementar filtragem de DNS global**	Cisco Umbrella DNS, Gateway da Cloudflare, DNSFilter, Zscaler Shift
	☐	**Monitorar a entrada de e-mails e filtrar as tentativas de phishing**	**Segurança de e-mails em nuvem:** Segurança de e-mails Area 1 da Cloudflare, Mimecast, TitanHQ **Isolamento do Navegador:** Isolamento do Navegador da Cloudflare, Isolamento do Navegador em Nuvem da Zscaler
	☐	**Identificar configurações erradas e dados compartilhados publicamente nas ferramentas de SaaS**	CASB da Cloudflare, DoControl, Netskope, CSPM da Zscaler
Fase 2	☐	**Estabelecer uma identidade corporativa**	Microsoft Azure AD, Okta, PingOne da Ping Identity, OneLogin
	☐	**Implementar uma MFA básica para todos os aplicativos**	**Provedores de identidade:** Microsoft Azure AD, Okta, PingOne da Ping Identity, OneLogin **Proxies Reversos de Aplicativos:** Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA)
	☐	**Implementar HTTPS e DNSSEC**	Akamai, AWS, Azure, Cloudflare, GCP
	☐	**Bloquear ou isolar as ameaças por trás do SSL**	**Descriptografia TLS:** Gateway da Cloudflare, Next Gen SWG da Netskope, Zscaler Internet Access (ZIA) **Isolamento do Navegador:** Isolamento do Navegador da Cloudflare, Isolamento do Navegador em Nuvem da Zscaler
	☐	**Implementação de políticas ZT para aplicativos endereçáveis publicamente**	**Proxies Reversos Zero Trust:** Azure App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA)
	☐	**Proteger aplicativos contra ataques na camada 7**	Akamai, AWS, Azure, Cloudflare, GCP
	☐	**Fechar todas as portas de entrada abertas para a internet para entrega de aplicativos**	Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access (ZPA)
Fase 3	☐	**Inventariar todos os aplicativos corporativos**	**Gateway seguro da web e CASBs com descoberta de TI invisível:** Gateway da Cloudflare, Microsoft Defender para Aplicativos em Nuvem, Next Gen SWG da Netskope, Zscaler Internet Access (ZIA)
	☐	**Implementação de políticas ZT para aplicativos SaaS**	**Acesso à Rede Zero Trust (ZTNA):** Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA) **CASB:** CASB da Cloudflare, CASB da Netskope, CASB da Zscaler

	☐ **Segmentar o acesso de usuários à rede**	**Acesso à Rede Zero Trust (ZTNA):** Zero Trust da Cloudflare (Access e Gateway usados em conjunto), Netskope Private Access, Zscaler Private Access (ZPA)
	☐ **ZTNA para aplicativos críticos endereçáveis de forma privada**	Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA)
	☐ **Implementar MDM/UEM para controlar dispositivos corporativos**	**Mac:** Jamf, Kandji **Windows:** Microsoft Intune
	☐ **Definir quais dados são confidenciais e onde eles existem**	DataDog, Splunk, SolarWinds
	☐ **Enviar tokens de autenticação baseados em hardware**	**Hard Keys:** Yubico
	☐ **Manter-se atualizado com relação a agentes de ameaças conhecidos**	Radar da Cloudflare, CISA, OWASP
Fase 4	☐ **Implementar uma MFA baseada em tokens de hardware**	**Hard Keys:** Yubico
	☐ **Implementação de políticas e acesso à rede ZT para todos os aplicativos**	Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA)
	☐ **Estabelecer um SOC para análise de registros, atualizações de política e mitigação**	N/A
	☐ **Implementar a proteção de endpoints**	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender
	☐ **Inventariar todos os dispositivos, APIs e serviços corporativos**	**Inventário de dispositivos:** VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender, Oomnitza **Inventário de APIs/Serviços:** Conector de aplicativos da Cloudflare, Zscaler Private Access (ZPA)
	☐ **Usar a internet banda larga para conexão entre filiais**	Magic WAN da Cloudflare, Cato Networks, Aryaka FlexCore
	☐ **Estabelecer um processo para registrar e analisar a atividade de funcionários nos aplicativos confidenciais**	**Gateway seguro da web (SWG):** Cisco Umbrella, Gateway da Cloudflare, Next Gen SWG da Netskope, Zscaler Internet Access (ZIA) **Monitoramento de Eventos e Incidentes de Segurança (SIEM):** DataDog, Splunk, SolarWinds
	☐ **Impedir que dados confidenciais saiam dos seus aplicativos (por exemplo, PII, Cartões de Crédito, CPF etc.)**	Cisco Umbrella, Gateway da Cloudflare, Next Gen SWG da Netskope, Zscaler Internet Access (ZIA)
	☐ **Implantar uma abordagem de DevOps para garantir a implementação de políticas para todos os novos recursos**	Ansible, Puppet, Terraform
	☐ **Implementar a escala automática para recursos de acesso à rede**	Balanceadores de carga: Akamai, Cloudflare Automação de infraestrutura: Ansible, Puppet, Terraform

+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

REV:BDES-3584.2022AUG09