CLOUDFLARE

Cloudflare Zero Trust: A roadmap for high-risk organizations

Learn the steps, tools, and teams needed to transform your network and modernize your security for your organization.

Introduction

It is crucial for organizations of all sizes to prioritize cyber security, as a data breach or security incident can have significant consequences for operations, reputation, and safety of employees. For a range of vulnerable communities, including civil society organizations that promote democracy and accountability in the human rights space, journalism groups in authoritarian countries, nonprofits in community development, and local governments that manage elections, the security of information (both online and off) is a challenge that requires time, investment, and expertise.

We've seen these attacks first hand for organizations. For example, between July 1, 2022, and May 5, 2023, Cloudflare mitigated 20 billion attacks against organizations protected under Project Galileo. This is an average of nearly 67.7 million cyber attacks per day over the last 10 months.

By leveraging innovative security solutions like those offered by Cloudflare's Impact projects, smaller organizations can improve their security posture and protect themselves against increasingly sophisticated threats. In the past, advanced security tools and technologies were only available to large enterprises due to their high costs and complex implementation requirements. However, with the rise of cloud computing and software-as-a-service (SaaS) solutions, smaller organizations can now access enterprise-grade security tools and services to help keep their operations safe from powerful adversaries.

How to use this guide

Developing a comprehensive and implementable security plan is crucial in today's digital age, when the threat of cyber attacks and data breaches is growing. In this roadmap intended for civil society and at-risk organizations, we hope to demystify the work of Zero Trust security and offer easy to follow steps to boost your cyber security efforts in your organization. This roadmap includes a range of Cloudflare's security products with case studies, level of effort to implement, and the teams involved to make the complex world of cyber security more accessible and understandable to a wider audience.

This guide was built by Cloudflare security experts to provide guidance to smaller organizations that are beginning their journey with Cloudflare and looking to increase the security of their websites and internal teams. The timeline assumes that you are beginning your journey from scratch, and meant to be useful to a range of technical expertise levels.

This guide is structured into sections

- Level of effort
- Team(s) involved
- Products
- Summary of the products
- Steps to implement
- Resources available
- Links to resources on the product

At the end of the roadmap, you will find a recommended implementation timeline for your organization to get started on your Zero Trust journey.

Overview of Cloudflare Impact projects and services provided

Project Galileo

Project Galileo aims to provide protection and support to vulnerable targets on the Internet, specifically those in the realms of civil society, journalism, and human rights. Products include:

- Cloudflare's free Business-level services
    - Distributed denial-of-service (DDoS) protection
    - Domain name system (DNS)
    - Content Delivery Network (CDN)
    - End to end HTTPS encryption
    - Web Application Firewall (WAF)
    - Web analytics
    - 24/7/365 support via email and chat
    - Project Galileo Security Guide
- Zero Trust security
    - Cloudflare Access
    - Cloudflare Gateway
    - Cloudflare Area 1 Email Security
    - Cloudflare Remote Browser Isolation
    - Cloudflare Cloud Access Security Broker (CASB)
    - Cloudflare Data Loss Prevention (DLP)

Athenian Project

The Athenian Project aims to protect state and local election websites in the United States. The project aims to safeguard these critical websites from cyber attacks and ensure the integrity of the electoral process. Products include:

- Enterprise services
    - Distributed denial-of-service (DDoS) protection
    - Domain name system (DNS)
    - Content Delivery Network (CDN)
    - End to end HTTPS encryption
    - Web Application Firewall (WAF)
    - Web analytics
    - 24/7/365 support via email/chat with emergency support phone line
    - Athenian Project Security Guide

- Zero Trust security
    - Cloudflare Access
    - Cloudflare Gateway
    - Cloudflare Area 1 Email Security
    - Cloudflare Remote Browser Isolation
    - Cloudflare Cloud Access Security Broker (CASB)
    - Cloudflare Data Loss Prevention (DLP)

Cloudflare for Campaigns

Cloudflare for Campaigns is a suite of Cloudflare products focused on the needs of political campaigns and parties in the United States. Products include:

- Cloudflare's free Business-level services
    - Distributed denial-of-service (DDoS) protection
    - Domain name system (DNS)
    - Content Delivery Network (CDN)
    - End to end HTTPS encryption
    - Web Application Firewall (WAF)
    - Web analytics
    - 24/7/365 support via email and chat
    - Cloudflare for Campaigns Security Guide
- Rate Limiting
- Load Balancing
- Zero Trust Security
    - 100 Cloudflare Access seats
    - 100 Cloudflare Gateway seats

Project Pangea

Project Pangea is Cloudflare's effort to help bring underserved communities secure connectivity to the Internet through our global and interconnected network. Cloudflare is offering our suite of network services for free to eligible nonprofit community networks, local networks, or other networks primarily focused on providing Internet access to local underserved or developing areas. Products include:

- Cloudflare Network Interconnect
- Magic Transit
- Magic Firewall

Protect your organization’s internal teams with Zero Trust

What is Zero Trust?

Zero Trust security means that no one is trusted by default from inside or outside the network, and verification is required from everyone and everything trying to gain access to resources on a network. This allows organizations of any size to solve common security problems such as data loss, malware, and phishing.

The Zero Trust model is designed to address the shortcomings of traditional perimeter-based security models, which rely on the assumption that the internal network is safe, and that only external threats need to be defended against. The shift toward cloud hosting, remote work, and other modernization has created challenges with a traditional perimeter network architecture. The Zero Trust approach assumes that the internal network is already compromised or could be compromised at any time, and so all traffic must be scrutinized, regardless of its source.

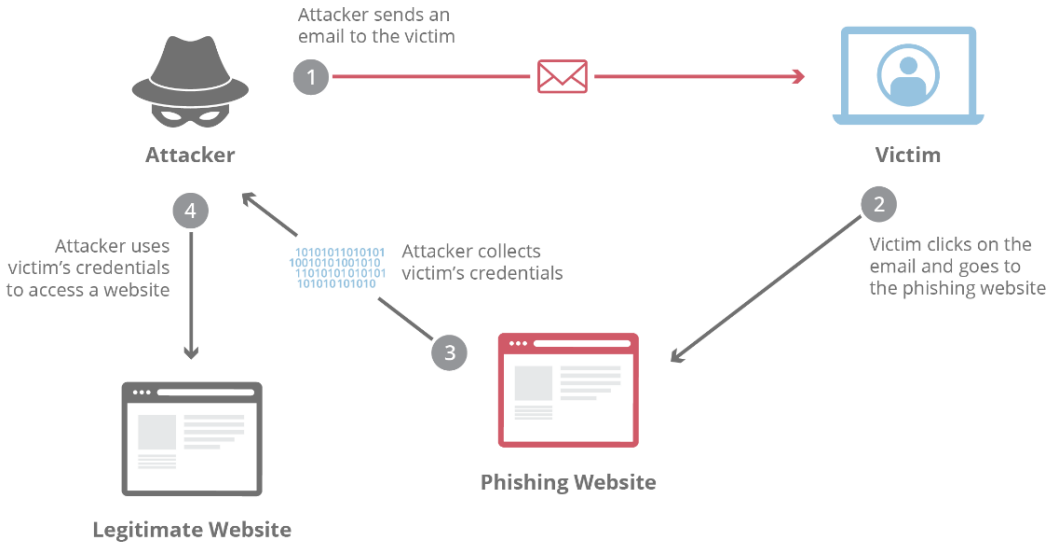
Key use cases for Zero Trust

Zero Trust is a security model and philosophy, rather than a specific set of tools or techniques. However, there are several attack vectors that Zero Trust seeks to mitigate. Here are some examples of attacks that Zero Trust can help defend against:

1. **Phishing:** One common attack method is to use social engineering tactics to trick users into divulging their credentials. Zero Trust can help protect against this by requiring multi-factor authentication for all users in your organization.

Case study

Phishing attacks are one of the most simple and low-cost tactics for attacks to use to gain access to sensitive information to compromise individuals' devices and organization's internal applications.



In March 2020, Amnesty International reported that many human rights defenders and journalists in Uzbekistan were the target of a sophisticated phishing attack, and this follows a pattern of attacks that started in 2017. Attackers sent phishing emails pretending to be fake Google or Mail.ru addresses (a popular Russian email service) with a link that sent victims to websites that mirrored the original. They also made clones of legitimate websites to lure human rights defenders (HRDs) and steal credentials and eventually bypass the two-factor authentication that many of these victims had enabled.

2. **Malware:** Malware can be introduced through a variety of vectors, such as email attachments or malicious websites. Zero Trust can help protect against malware by requiring that all devices be verified and meet security requirements before being allowed onto the network.

Case study

In June 2020, Amnesty International reported on a coordinated spyware campaign that targeted at least nine HRDs, including activists, lawyers, and journalists in India. Between January and October 2019, these HRDs were targeted with a malicious link in emails that once clicked, would deploy spyware that would monitor communications on their Windows computers Many of these HRDs were calling for the release of many activists involved in the 2018 Dalit protests in Maharashtra Bhima Koregaon in India.

The spear phishing attack, which is designed to be highly targeted and personalized to an individual or organization, uses social engineering techniques to trick the victim into downloading malware or revealing sensitive information. The consequences of a successful spear phishing attack can be far-reaching, with the victim's computer or smartphone essentially becoming a wiretap that can be used to monitor every communication and interaction. This can have a chilling effect on their ability to communicate freely and collaborate with others, as they may begin to fear that any conversation could be monitored or intercepted.

3. **On-path attacks:** In an on-path attack, an attacker intercepts traffic between two parties, allowing them to eavesdrop or modify the communication. In this attack, the attacker positions themselves between the sender and the intended recipient, giving them the ability to eavesdrop on the communication and even manipulate the data being transmitted. Zero Trust can help prevent this by requiring secure connections, authentication of each user in the network, and a secure connection between the user and web services.

Case study

On-path attacks are a type of cyber attack in which an attacker intercepts and alters communications between two parties who believe they are communicating directly with each other. These attacks can be especially harmful to human rights organizations, which often handle sensitive information and rely on secure communication channels to protect the privacy and safety of their sources and partners.

In October 2019, Amnesty International reported on targeted attacks against two human rights defenders from Morocco. The attacks began at least in 2017 and involve sending malicious links via SMS messages to exploit the victims' mobile devices and install the spyware. In addition, they reported on-path attacks targeting the HRDs' mobile network to install the spyware. These attacks reflect a broader trend of reprisals by Moroccan authorities against HRDs and dissenting voices, undermining their freedom of expression, association, and peaceful assembly.

4. **Credential stuffing:** This attack involves using lists of stolen credentials to try to gain unauthorized access to accounts. Zero Trust can help protect against this by requiring every user to have multi-factor authentication and continuous authentication while using internal applications.

Case study

Credential stuffing is a type of cyber attack in which attackers use stolen usernames and passwords from one website or service to gain unauthorized access to another website or service, exploiting the fact that many people use the same login credentials across multiple accounts. Nonprofit organizations are not immune to credential stuffing attacks, which can result in stolen data, compromised accounts, and other serious consequences.

Basecamp, a project management service, experienced multiple credential stuffing attacks in 2019. The security team noticed a significant increase in login attempts and took measures to block suspicious IP addresses. They implemented CAPTCHA to mitigate the attacks, but 124 accounts were still accessed. Basecamp promptly logged out those users, reset their passwords, and sent them emails with instructions on reactivating their accounts.

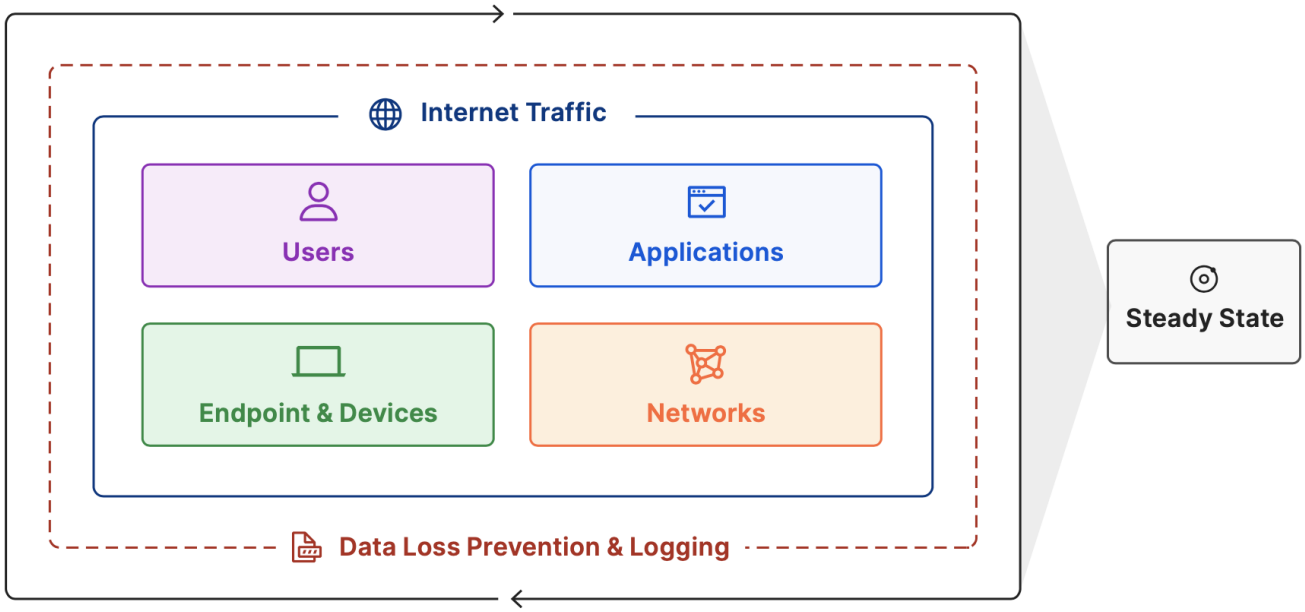
Overall, these attacks all share similar goals for adversaries: accessing sensitive internal information either for financial gain, strategic advantage, espionage or surveillance, ransom, or political leverage. The Zero Trust model is designed to be highly resilient to a wide range of attack vectors with a layered approach to help defend against even the most sophisticated attackers. For vulnerable communities, building trust and maintaining privacy are essential to encourage collaboration and protect the individuals who are often at risk due to their work in the human rights space.

How to get started with Cloudflare Zero Trust

This guide was built by security experts to provide a vendor-agnostic Zero Trust architecture and example implementation timeline. The timeline assumes that an organization is beginning their Zero Trust journey from scratch, but is meant to be useful for all organizations.

There are seven major components to organizational security that need to be considered when it comes to implementing a comprehensive Zero Trust architecture. Your implementation order does not need to match how they are listed in the component and reference architecture sections below.

1. User
2. Endpoint & Devices
3. Application
4. Networks
5. Data Loss Prevention & Logging
6. Steady State



The roadmap to Zero Trust

1. Users

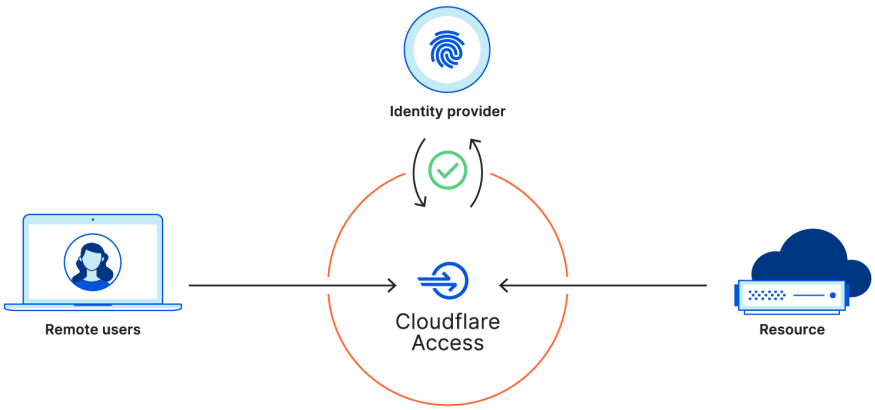
Users include employees, volunteers, and contractors. To implement Zero Trust, an organization must first have an accurate picture of who should actually be trusted, and with what — otherwise known as "identity." Then it must establish a way to securely authenticate the identity of its users. For your organization, a user may be a volunteer, a journalist accessing internal applications such as applications with sensitive source information, or election officials who manage a database with personal voter information.

Establish a corporate identity[1]

Level of effort	🔧🔧 - Medium effort
Team(s) involved	• The team responsible for your identity provider[2] (typically security or IT) • The admins who manage internal applications used by your employees, partners, or volunteers
Product(s)	Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin
Summary	A unified corporate identity is required to accurately authenticate and authorize user access to your organization's applications. A corporate identity is used to establish trust between different components of a Zero Trust network, such as users, devices, applications, and services. For example, when a user tries to access a resource in the network, the resource may check the user's corporate identity to determine whether the user is authorized to access the resource, and whether the user's device meets the security requirements of the network.
Steps	1. Add all corporate users to the identity provider. a. These values can often be synchronized from an HR system like Workday, ADP, etc. 2. Verify that each user's information is correct. 3. Send new users registration information to set up login credentials.
Resources available	Microsoft Azure AD: Microsoft provides grants and discounts for eligible nonprofit organizations, including cloud services like Microsoft 365, Azure and Dynamics 365, Surface hardware, on-premise software, and digital skilling Okta for Nonprofits: Okta offers IdP servers at a discounted rate to nonprofit organizations, making it an affordable solution for organizations with limited budgets OneLogin: This company provides discounts for nonprofit organizations
Cloudflare tools available for your organization	Organizations can integrate their chosen identity solution with Cloudflare Access, which is included in all of the Cloudflare limpact projects. Learn more at https://www.cloudflare.com/impact-portal.

[1] How an organization presents itself to the public (including both internal and external audiences).
[2] An identity provider (IdP) stores and manages users' digital identities. An IdP may check user identities via username-password combinations and other factors, or it may simply provide a list of user identities that another service provider (like an SSO) checks.

Enforce multi-factor authentication for all applications

Level of effort	🔧 - Small effort (if applying basic MFA) 🔧🔧 - Medium effort (if using hard keys)
Team(s) involved	• The team responsible for your identity provider (typically security or IT) • The admins who manage internal applications used by your employees, partners, or volunteers
Product(s)	Identity providers: Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin Application reverse proxies: Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA) Hard keys: Yubico
Summary	Multi-factor authentication (MFA) is the best protection against stolen user credentials via phishing or data leaks. Common authentication factors include passwords, biometrics (such as fingerprint or facial recognition), and physical tokens (such as smart cards or USB keys). Most MFA can be enabled directly in an identity provider (IdP). For example, your organization has an application that your volunteers use to track volunteer service events. When the user signs in to the application that requires multi-factor authentication, they enter their username and password, and the application sends a one-time passcode (OTP) to the user's registered mobile phone (if using MFA via SMS). The user retrieves the OTP from their phone and enters it into the login page. The application verifies the OTP and grants the user access to their account.  In this example, the use of MFA provides an additional layer of security to protect the user's account from unauthorized access. Even if someone obtains the user's username and password, they would still need access to the user's mobile device to retrieve the OTP and complete the authentication process.
Steps	1. Alert internal users to upcoming MFA enforcement. 2. Provide options to sign up for SMS or app-based authenticators. 3. Enable MFA in your IdP.

	4. Enable application reverse proxy in front of applications not integrated with your IdP. 5. (Bonus) Distribute hardware keys to employees via mail or in person. 6. (Bonus) Enforce hardware key–only MFA for your most sensitive applications.
Cloudflare tools available for your organization	Cloudflare Access is part of the Zero Trust package provided to organizations protected under Cloudflare's Impact projects. Learn more at https://www.cloudflare.com/impact-portal.
Resources on how to use Cloudflare Access	How to get started with Cloudflare Access: ● 30-minute demo of Cloudflare Access ● Securing your SaaS application ● Securing your self-hosted application Developer resources: ● Get started with Cloudflare Access

2. Endpoints and devices

Endpoints[3] and devices include any device, API, or software service within an organization or that have access to internal organizational data. Securing your endpoints and devices is important to protect against malware, prevent unauthorized access, and improve productivity.

Organizations must first understand their full set of devices, APIs, and services. Then Zero Trust policies can be implemented based on the context of the device, API, and service.

Implement mobile device management

Level of effort	🔧🔧 - Medium effort
Team(s) involved	• IT team
Product(s)	Mac: Jamf, Kandji Windows: Microsoft Intune
Summary	A majority of Zero Trust architecture requires software to be installed on at least a subset of user machines. Mobile device management (MDM) is how most organizations manage the software and configuration across their inventory of user devices.
Steps	See mobile device management vendor sites for specific details.
Resources available	Microsoft Intune provided non-profit discounts.

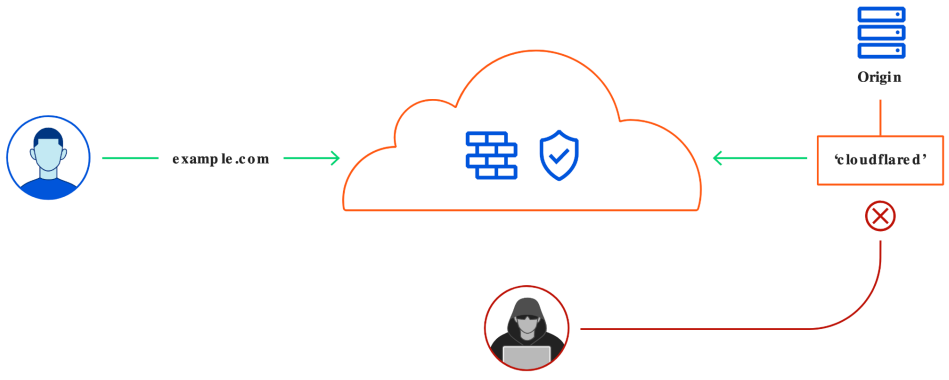
Implement endpoint protection

Level of effort	🔧🔧 - Medium effort
Team(s) involved	• Security team • IT team
Product(s)	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender
Summary	Endpoint protection software is installed on a user's machine and scans for known threats that affect devices. Endpoint protection software can also be used to enforce compliance of OS patches and updates. The signal from your endpoint protection software can and should be used in your application access control policies.
Steps	1. Install the endpoint protection software on users' machines using MDM. 2. Enable threat protection and compliance control in the endpoint protection platform.

[3] In the context of zero trust security, an endpoint is any device or user-facing component that connects to an organization's network, such as a laptop, desktop computer, mobile device, or server. Endpoints can be physical or virtual, and they can run on a variety of operating systems and platforms.

Cloudflare tools available for your organization	We do not offer any products for this under Cloudflare Impact projects at this time.

Inventory devices, APIs, and services

Level of effort	🔧 - Small effort
Team(s) involved	• Security team • IT team
Product(s)	Device inventory: VMWare Carbon Black, Crowdstrike, Omnitza, SentinelOne API/service inventory: Cloudflare application connector (Cloudflare Tunnel), Zscaler Private Access (ZPA)
Summary	Endpoint protection software and asset management software can be used to track all devices that have been distributed to your users. An accurate list of devices should be maintained to track which devices are valid and should have access to specific applications. APIs and services should also be detected and maintained in an inventory. Network scanning can be leveraged to identify newly seen APIs and software services that can communicate over an internal or external network. Cloudflare Tunnel provides you with a secure way to connect your resources to Cloudflare without a publicly routable IP address. With Tunnel, you do not send traffic to an external IP — instead, a lightweight daemon in your infrastructure (cloudflared) creates outbound-only connections to Cloudflare's global network. Cloudflare Tunnel can connect HTTP web servers, SSH servers, remote desktops, and other protocols safely to Cloudflare. This way, your origins can serve traffic through Cloudflare without being vulnerable to attacks that bypass Cloudflare. 
Steps	1. Install the endpoint protection software on users' machines using MDM. 2. Install the API/service scanner within your network.

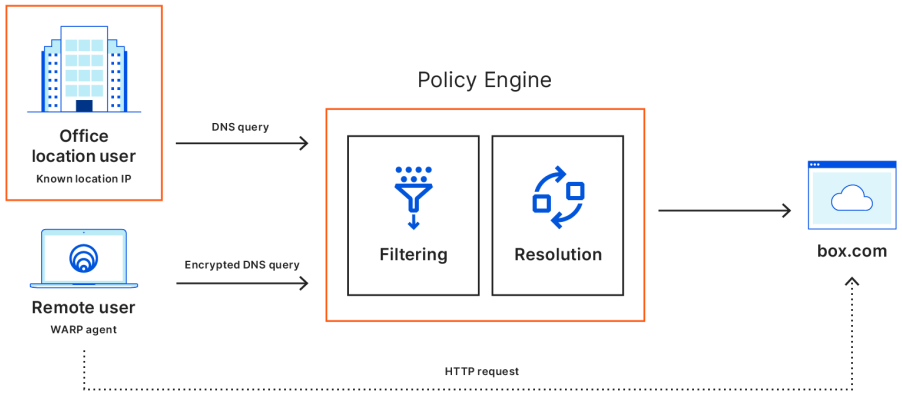
Cloudflare tools available for your organization	Cloudflare Tunnel is part of the Zero Trust package provided to organizations protected under Cloudflare's Impact projects. Learn more at https://www.cloudflare.com/impact-portal
Resources on how to use Cloudflare Tunnel	• Useful terms when getting started with Cloudflare Tunnel • How to set up your first tunnel

3. Internet Traffic

Internet traffic includes all user traffic destined for websites outside of an organization's control. This can range from work-related tasks to personal website usage.

All outbound traffic is susceptible to malware and malicious sites. An organization must establish visibility and control over user traffic destined for the Internet.

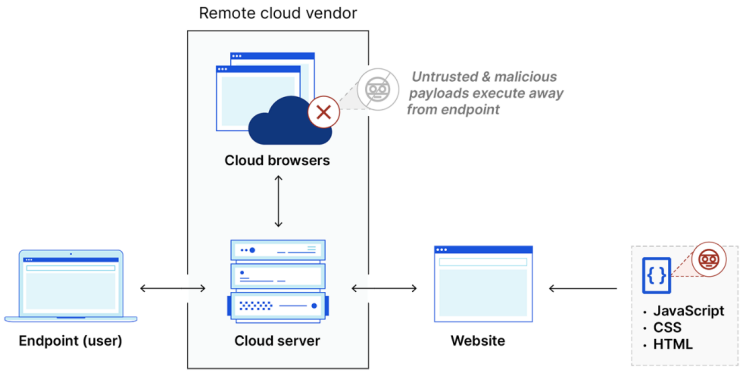
Block DNS requests to known threats or risky destinations

Level of effort	🔧 - Small effort
Team(s) involved	• IT team with access to either router or machine configuration • Security team
Product(s)	DNS Filtering: Cisco Umbrella DNS, Cloudflare Gateway, DNSFilter, Zscaler Shift
Summary	DNS filtering can be applied via router configuration or directly on a user machine. It is one of the fastest ways to protect users from known malicious websites. DNS filtering is a technique used to block or allow access to certain websites or domains based on their domain name server (DNS) information. It involves intercepting DNS requests and using filtering rules to determine whether a request should be allowed or blocked. DNS filtering can be used to restrict access to certain websites or categories of websites that are deemed inappropriate or potentially harmful, such as phishing sites and malware-infected domains. 
Steps	DNS filtering: 1. Update DNS resolution configuration on your office WiFi to point to the appropriate DNS resolution service. This can be used to block known malicious sites.
Cloudflare tools available for your organization	Cloudflare Gateway is part of the Zero Trust package provided to organizations protected under Cloudflare's Impact projects. Learn more at https://www.cloudflare.com/impact-portal
Resources on how to use	• 30-minute Cloudflare Gateway demo • Get started with Cloudflare Gateway for your nonprofit organization • Zero Trust live demo

Cloudflare Gateway	

Block or isolate threats behind SSL/TLS

Level of effort	🔧🔧 - Medium effort
Team(s) involved	• IT team with access to either router or machine configuration • Security team
Product(s)	TLS decryption: Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) Browser isolation: Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
Summary	Some threats are hidden behind SSL and cannot be blocked through only HTTPS inspection. For example, attackers can use SSL to encrypt malware downloads, making it difficult for security tools to detect and block them. Once the malware is downloaded onto a victim's device, it can be used to steal sensitive information or cause other types of damage. To detect and block cyber threats hidden by SSL, organizations can implement SSL inspection or SSL decryption. This involves intercepting SSL traffic, decrypting it, and inspecting it for potential threats before re-encrypting and forwarding it to its intended destination.
Steps	TLS decryption: 1. Ensure the correct client software is installed on a user machine. a. Check for any VPN or other software that might interfere with the outbound web traffic on the device. 2. Configure the root certificate on the device for TLS decryption. 3. Enable policies of when to avoid decrypting user traffic. a. This should be done for sites that use certificate pinning. b. Some organizations also bypass decryption for user's personal traffic (e.g. banking, social media). Browser isolation: Browser isolation can be deployed via the on-device client software or via an isolation link. Both approaches should be considered. Cloudflare Browser Isolation is a security service that isolates web browsing activity in a virtual environment in the cloud, keeping end-user devices and networks safe from web-based threats. It works by executing web sessions in a secure, isolated virtual environment in the cloud, separate from the user's local machine.

	 When a user clicks on a link or visits a website, the website content is rendered in a remote browser in the cloud, and only safe and sanitized visual data is sent to the user's local browser for display. This way, any malicious content, such as malware or phishing attempts, is prevented from reaching the user's device or network.
Cloudflare tools available for your organization	Cloudflare Gateway (section above) and Browser Isolation are part of the Zero Trust package provided to organizations protected under Cloudflare's Impact projects. Learn more at https://www.cloudflare.com/impact-portal
Resources on how to use Cloudflare Gateway and Cloudflare Browser Isolation	• 30-minute Cloudflare Gateway demo • Get started with Cloudflare Gateway for your nonprofit organization • Zero Trust live demo • Product demo of Browser Isolation • Set up Browser Isolation

4. Network

Networks include all public, private, and virtual networks within an organization. Organizations must first understand their existing set of networks and segment them to prevent lateral movement. Then, Zero Trust policies can be created that granularly control which segments of a network that users, endpoints, and devices can access.

Segment user network access

Level of effort	🔧🔧🔧 - Large effort
Team(s) involved	• Security team • IT team
Product(s)	Zero Trust Network Access (ZTNA): Cloudflare Zero Trust (Access and Gateway used together), Netskope Private Access, Zscaler Private Access (ZPA)
Summary	Users can generally access an entire private network[4] using a VPN or while in the office network. A Zero Trust framework requires that users only have access to specific segments of the network required to complete a given task. Zero Trust network solutions allow users to access a local network remotely with granular policies based on user, device, and other factors. Traditionally, organizations would create private networks, such as VPNs, to allow remote access to their internal network resources. However, in the Zero Trust model, remote access to the internal network is not automatically trusted and requires authentication and authorization before access is granted.
Steps	1. Make the private network available to the ZTNA. a. Typically, an application connector, GRE, or IPSec Tunnel. 2. Install the ZTNA client on user devices using MDM. 3. Set policies to segment user access across the private network.
Cloudflare tools available for your organization	Cloudflare Access and Gateway (sections above) arepart of the Zero Trust package provided to organizations protected under Cloudflare's Impact projects. Learn more at https://www.cloudflare.com/impact-portal
Resources on how to use Cloudflare Access and Cloudflare Gateway	• Integrating Cloudflare Access and Gateway • Case Study with Cloudflare

Use broadband Internet for branch to branch connectivity

Level of effort	🔧🔧🔧 - Large effort

[4] In ZT security, a private network refers to a network that is not automatically trusted and requires verification and authorization of all network traffic, regardless of whether it is from inside or outside the network.

Team(s) involved	• Network engineering team • IT team
Product(s)	Cloudflare Magic WAN, Cato Networks, Aryaka FlexCore
Summary	Connectivity between private network locations (e.g. data centers and branches) has generally been established using multiprotocol label switching (MPLS) lines or other forms of private links offered by telecom providers. These MPLS links are typically expensive, and as commodity Internet has become higher quality, organizations can provide the same level of secure access by routing traffic over the Internet via secure tunnels at a fraction of the cost.
Steps	1. Choose two MPLS-connected locations to start with. These locations will need some form of Internet connectivity. 2. Establish a pair of redundant Anycast GRE or IPsec tunnels over your Internet circuits to your cloud WAN provider's edge network. 3. Verify health and connectivity between those tunnels. Test performance (throughput, latency, packet loss, jitter) of traffic workloads as similar as possible to production traffic. 4. Change routing policies to migrate production traffic from MPLS to Internet tunnels. 5. Repeat at next MPLS-connected location. 6. Decommission MPLS circuits.
Cloudflare tools available for your organization	At this time, we do not provide Cloudflare Magic WAN under our Impact Projects.

Close all inbound ports open to the Internet for application delivery

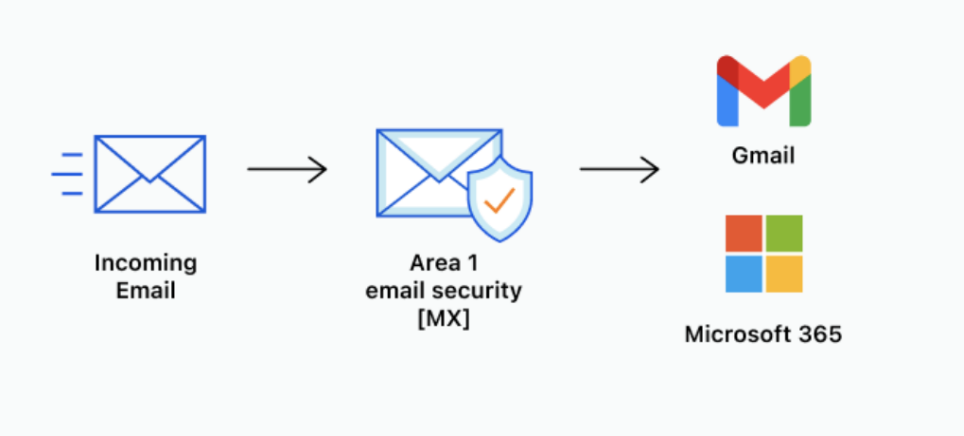
Level of effort	🔧 - Small effort
Team(s) involved	• Network engineering team
Product(s)	Zero Trust Reverse Proxies: Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access (ZPA)
Summary	Open inbound network ports can be found using scanning technology and are a common attack vector. Open inbound network ports refer to network ports on a device or system that are configured to allow incoming network traffic from external sources. A network port is a communication endpoint that is identified by a unique number, and open ports are those that are available for communication. Open inbound network ports can be a potential security risk, as they allow external sources to initiate communication with a device or system. It is important to properly configure firewall rules and access controls to ensure that only authorized traffic is allowed through open inbound ports. Zero Trust reverse proxies allow you to securely expose a web application without opening any inbound ports. The DNS record of the application is the only publicly visible record of the application. And the DNS record is

	protected with Zero Trust policies. As an added layer of security, internal/private DNS can be leveraged using a Zero Trust Network Access service.
Steps	1. Install reverse proxy application connector — typically a daemon or virtual machine somewhere in the same network. 2. Connect the reverse proxy application to the application connector. 3. Close all inbound port on the private network with a firewall rule.
Cloudflare tools available for your organization	Cloudflare Access is part of the Zero Trust package provided to organizations protected under Cloudflare's Impact projects. Learn more at https://www.cloudflare.com/impact-portal
Resources on how to use Cloudflare Access	How to get started with Cloudflare Access: ● 30-minute demo of Cloudflare Access ● Securing your SaaS application for your nonprofit ● Securing your self-hosted application for your nonprofit Developer resources: ● Get started with Cloudflare Access

5. Applications

Applications include any resource where organizational data exists or organizational processes are performed. Organizations must first understand the applications that exist and then establish Zero Trust policies for each application or, in some cases, block unapproved applications.

Monitor email applications and filter out phishing attempts

Level of effort	🔧 - Small effort
Team(s) involved	• The team responsible for your email provider configuration (typically IT)
Product(s)	Cloud Email Security: Cloudflare Area 1 Email Security, Mimecast, TitanHQ Browser Isolation: Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
Summary	Email is one of the few communications channels for which attackers have unfettered access to your employees. Deploying a secure email gateway is a critical step to ensure that malicious or untrusted emails do not reach your employees. Common email security threats that organizations and individuals should be aware of include: • Phishing • Malware attachments • Spoofing • Email interception • Emails scams Additionally, security teams should consider an option to quarantine links in an isolated browser that are not suspicious enough to completely block.  Cloudflare Area 1 Email Security is a cloud-based email security solution that helps organizations protect their email systems from advanced phishing attacks, business email compromise (BEC), malware, and other email-based threats. The solution uses advanced machine learning and artificial intelligence algorithms to analyze and classify incoming emails, identifying and blocking any messages that contain suspicious content or attachments.

	Cloudflare Area 1 Email Security is designed to integrate with existing email systems, including Microsoft Office 365 and Google Workspace, and can be deployed quickly and easily without the need for additional hardware or software.
Steps	1. Configure your domain's MX records to point to the secure email gateway service. 2. Monitor for false positives in the first few weeks. 3. (Bonus) Implement a link-based browser isolation approach for borderline suspicious email links.
Cloudflare tools available for your organization	Cloudflare Area 1 Email Security is part of the Zero Trust package provided to organizations protected under Cloudflare's Impact projects. Learn more at https://www.cloudflare.com/impact-portal
Resources on how to use Cloudflare Area 1 Email Security	• Area 1 Email Security Overview • Integrate Cloudflare Area 1 with Access for SaaS

Inventory all corporate applications

Level of effort	🔧🔧 - Medium effort
Team(s) involved	• Security team
Product(s)	Secure Web Gateway and CASBs with Shadow IT discovery: Cloudflare Gateway, Microsoft Defender for Cloud Apps, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
Summary	It is critical for a security team to understand their full inventory of applications used across the business. Also referred to as "shadow IT," security teams will often discover unsanctioned or unknown applications being used across the business. A secure web gateway with TLS decryption can be used to identify applications. The secure web gateway can also be used to block unapproved applications or tenants of applications (e.g. personal Dropbox accounts). Cloudflare CASB (Cloud Access Security Broker) is a cloud-based security solution that provides visibility and control over an organization's cloud-based applications and services. CASBs are designed to address security concerns associated with the use of cloud-based services, such as unauthorized access, data leakage, and compliance violations.
Steps	1. Enable Shadow IT scanning in the secure web gateway. 2. Ensure the secure web gateway client is installed on user devices. 3. Allow 2-3 weeks of traffic from users. 4. Review the list of identified applications. 5. Block any unapproved applications with secure web gateway policies. 6. Protect approved applications with Zero Trust policies.
Cloudflare tools available for your organization	Cloudflare Gateway (section above) and CASB (Cloud Access Security Broker) are part of the Zero Trust package provided to organizations protected under Cloudflare's Impact projects. Learn more at https://www.cloudflare.com/impact-portal
Resources on how to use Cloudflare Gateway and CASB	• 30-minute Cloudflare Gateway demo • Get started with Cloudflare Gateway for your nonprofit organization • Zero Trust live demo • What is CASB? • CASB Integrations

Zero Trust policy enforcement for applications

Level of effort	🔧 - Small effort (for most critical applications) 🔧🔧🔧 - Large effort (for all applications)

Team(s) involved	• Security team • Application development team • IT team
Product(s)	Zero Trust reverse proxies: Azure App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA) Zero Trust Network Access (ZTNA): Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA) CASB: Cloudflare CASB, Netskope CASB, Zscaler CASB Remote browser isolation: Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
Summary	Applications must be protected with Zero Trust policies that consider a user identity, device, and network context before authenticating and authorizing access. Applications should have granular policies that enforce least privilege, especially for applications that contain sensitive data. There are three major application types, and the Zero Trust security model varies for each type. The major application types are: 1. Private self-hosted applications (addressable only on the corporate network) 2. Public self-hosted applications (addressable over the Internet) 3. SaaS applications
Steps	Private self-hosted applications: 1. Build an encrypted tunnel between the application and Zero Trust policy layer. Typically this will be an “application connector,” GRE, or IPSec tunnel. 2. Make the private DNS resolver available for users of the ZTNA device client. 3. Build policies based on user, device, and network context to establish who can access the application. Public self-hosted applications: 1. Move the authoritative DNS or a CNAME record to the application reverse proxy. 2. Ensure all inbound ports for closed for the application’s network. 3. Build policies based on user, device, and network context to establish who can access the application. SaaS applications: There are a few different options to enforce Zero Trust policies for SaaS applications. **Identity proxy** Cloudflare, Netskope, and Zscaler provide identity proxies that allow the same policy enforcement as a reverse proxy self-hosted application. This does require that the identity proxy is set up as the single sign-on (SSO) provider of the SaaS application. 1. Remove the existing SSO integration to the SaaS app, if present. 2. Integrate the identity proxy with the SaaS application.

	3. Ensure the correct SAML attributes are sent for user creation and updates. 4. Create policies based on the user, device, and network context. **Secure web gateway and single sign-n** The other approach is to use an existing single sign-on provider to control which users can and cannot access the SaaS application. Then the secure web gateway, with a dedicated IP address, can be used to ensure that only users from managed devices with traffic inspection can access the SaaS application. 1. Add the SaaS application to the SSO provider. 2. Create policies to enforce which users are authorized. 3. Add the IP address of the secure web gateway instance to the SaaS application's IP Allow List (most SaaS apps support IP allowlists in their base security settings). 4. Create secure web gateway policies that control which users can access the SaaS application.
Cloudflare tools available for your organization	Cloudflare Access (section above), CASB (Cloud Access Security Broker), and Browser Isolation are part of the Zero Trust package provided to organizations protected under Cloudflare's Impact projects. Learn more at https://www.cloudflare.com/impact-portal
Resources on how to use Access, CASB and Browser Isolation	• 30-minute demo of Cloudflare Access • Securing your SaaS application for your nonprofit • Securing your self-hosted application for your nonprofit • What is CASB? • CASB Integrations • Product demo of Browser Isolation • Set up Browser Isolation

Protect applications from Layer 7 attacks (DDoS, injection, bots, etc.)

Level of effort	🔧 - Small effort
Team(s) involved	• Security team • Application development team
Product(s)	Akamai, AWS, Azure, Cloudflare, GCP
Summary	Any self-hosted application is susceptible to Layer 7 attacks, including DDoS, code injection, bots, and more. Security teams should deploy a Web Application Firewall and DDoS protection in front of all self-hosted applications, privately and publicly addressable.
Steps	1. Add any public application's authoritative DNS record. 2. Enable the Web Application Firewall and DDoS protection.
Cloudflare tools available for your organization	Cloudflare's Impact projects include free Business-level services, including DDoS mitigation, SSL encryption, Content Delivery Network, Web Application Firewall (WAF), and more.

Resources on how to use Cloudflare Layer 7 Application products	• Full website security product video demos for your nonprofit • Cloudflare DDoS protection Developer documents • Cloudflare Web Application Firewall Developer documents • Cloudflare SSL/TLS Developer documents

Enforce HTTPS and DNSSEC

Level of effort	🔧 - Small effort
Team(s) involved	• Security team • Application development team
Product(s)	Akamai, AWS, Azure, Cloudflare, GCP
Summary	Any self-hosted web application should leverage HTTPS and DNSSEC. This prevents any potential for packet sniffing or domain hijacking. DNSSEC creates a secure domain name system by adding cryptographic signatures to existing DNS records. These digital signatures are stored in DNS name servers alongside common record types like A, AAAA, MX, CNAME, etc. By checking its associated signature, you can verify that a requested DNS record comes from its authoritative name server and wasn't altered en route, as opposed to a fake record injected in an on-path attack.
Steps	1. Add any public application's authoritative DNS record. 2. Set HTTPS to strict and enable DNSSEC.
Cloudflare tools available for your organization	Enforce HTTPS Connections and DNSSEC are included in all Cloudflare plans.
Resources on how to use Cloudflare Layer 7 products	• Full website security product video demos for your nonprofit • Cloudflare SSL/TLS Developer documents • Overview of DNSSEC

6. Data loss prevention and logging

Once you have established all the Zero Trust elements of your architecture to this point, your architecture will be generating large volumes of data on what's happening inside your network. At this point, it's time to implement data loss prevention and logging. This is a set of processes and tools that focus on keeping sensitive data inside of a business and flagging any potential opportunities for data leakage. Organizations must first understand where their sensitive data exists. Then they can establish Zero Trust controls to block sensitive data being accessed and exfiltrated.

Establish a process to log and review traffic on sensitive applications

Level of effort	🔧🔧 - Medium effort
Team(s) involved	• Security team
Product(s)	Secure web gateway (SWG): Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) Security Incident and event monitoring (SIEM): DataDog, Splunk, SolarWinds
Summary	Secure web gateway solutions have functionality to pass user traffic logs to a SIEM tool. A security team should make it a regular exercise to review traffic logs destined for sensitive applications. Specific alerts for anomalous or malicious traffic can be set up and fine-tuned over time in the SIEM.
Steps	1. Ensure all user traffic destined to sensitive applications is proxied using the SWG. 2. Enable the logpush or pull functionality between your SWG and SIEM. 3. Set a specific interval for the security team to review traffic logs. 4. Configure alerts in the SIEM based on findings over time.
Cloudflare tools available for your organization	Cloudflare Gateway (section above) is part of the Zero Trust package provided to organizations protected under Cloudflare's Impact projects. Learn more at https://www.cloudflare.com/impact-portal
Resources on how to use Cloudflare Gateway	• 30-minute Cloudflare Gateway demo • Get started with Cloudflare Gateway for your nonprofit organization • Zero Trust live demo

Define what data is sensitive and where it exists

Level of effort	🔧🔧 - Medium effort
Team(s) involved	• Security team • Compliance/legal team
Product(s)	Security incident and event monitoring (SIEM): DataDog, Splunk, SolarWinds
Summary	Sensitive data varies widely depending on industry. Technology companies are concerned about protecting source code while medical providers are heavily focused on HIPAA compliance. It is important to establish what sensitive data your company has and where it lives.

	An accurate definition and inventory of sensitive data will inform the implementation of data loss prevention tools.
Steps	1. Review traffic logs in the SIEM tools or directly in a secure web gateway to identify target applications and data stores. 2. Take an inventory of existing sensitive data.
Cloudflare tools available for your organization	We do not offer any products for this at Cloudflare at this time.

Prevent sensitive data from leaving your applications

Level of effort	🔧🔧🔧 - Large effort
Team(s) involved	• Security team • IT team • Compliance/Legal team
Product(s)	In-line data loss prevention (DLP): Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
Summary	In-line DLP solutions inspect user traffic and file uploads/downloads for sensitive data. The sensitive data is available in well-known predefined lists (e.g. PII, SSNs, credit cards) or specific patterns can be manually configured by an administrator. DLP controls should be enabled for sensitive applications and can be expanded for all user traffic.
Steps	1. Install the client software from the DLP provider. 2. Ensure there is no existing VPN or other tool that will disrupt connectivity. 3. Ensure TLS decryption is enabled and a root certificate is present on each user machine. 4. Enable DLP controls. 5. Monitor for DLP block events and verify if it is valid or a false positive.
Cloudflare tools available for your organization	Cloudflare Gateway (section above) is part of the Zero Trust package provided to organizations protected under Cloudflare's Impact projects. Learn more at https://www.cloudflare.com/impact-portal
Resources on how to use Cloudflare Gateway	• 30-minute Cloudflare Gateway demo • Get started with Cloudflare Gateway for your nonprofit organization • Zero Trust live demo

Identify misconfigurations and publicly shared data in SaaS tools

Level of effort	🔧 - Small effort
Team(s) involved	• Security team
Product(s)	API-based Cloud Access Security Broker (CASB): Cloudflare CASB, DoControl, Netskope, Zscaler CSPM

Summary	CASBs integrate with major SaaS applications via an API integration. The CASB will then scan the SaaS application for known security misconfiguration and data that has been publicly shared. A security team should establish a regular cadence to review CASB findings.
Steps	1. Connect each SaaS application via the provider's API integration instructions. 2. Run scans for each SaaS application. 3. Review the scan results and begin remediation in each SaaS application where appropriate.
Cloudflare tools available for your organization	Cloudflare CASB (Cloud Access Security Broker) is part of the Zero Trust package provided to organizations protected under Cloudflare's Impact projects. Learn more at https://www.cloudflare.com/impact-portal
Resources on how to use Cloudflare CASB	• What is CASB? • CASB Integrations

Establish a security operations center (SOC) for log review, policy updates, and mitigation

Level of effort	🔧🔧- Medium effort
Team(s) involved	• Security team
Product(s)	None
Summary	A SOC is a critical function within a security team in a Zero Trust framework. It should focus on reviewing log information and security alerts and adjusting Zero Trust policies across all core security products.
Steps	1. Review logs in SIEM or directly in security product. 2. Identify any alerts or anomalous activity. 3. Update Zero Trust policies across each tool based on findings.

Stay up to date on known threat actors

Level of effort	🔧- Small effort
Team(s) involved	• Security team
Product(s)	Threat intelligence providers: Cloudflare Radar, CISA, OWASP
Summary	There are multiple providers focused on compiling a list of known threat actors and malicious websites. These threat feeds can be automatically loaded into a secure web gateway to protect users from attacks. Cloudflare Radar is a public service that focuses on providing insights and intelligence about Internet traffic, security threats, and performance metrics. It aims to help organizations gain a deeper understanding of their Internet properties and make informed decisions to enhance their online presence and protect against various threats.
Steps	1. Connect threat feed into secure web gateway (see Gateway section).

	2. Enable threat protection in DNS and HTTP filtering (see Gateway section).
Cloudflare tools available for your organization	Cloudflare Radar is a public tool available at https://radar.cloudflare.com.
Resources on how to use Cloudflare Radar	• Project Galileo 7th Anniversary Radar Dashboard (2021) • Project Galileo 8th Anniversary Radar Dashboard (2022) • Athenian Project Radar Dashboard (2020)

7. Steady state

Once you have built out your Zero Trust architecture for all the other elements of your organization, there are a set of actions you can take to move your organization to a Zero Trust steady state, ensuring consistency with the architecture moving forward.

Employ a DevOps approach to ensure consistent policy enforcement for all new resources

Level of effort	🔧🔧🔧 - Large effort
Team(s) involved	• Security team • Application development team
Product(s)	Infrastructure automation: Ansible, Puppet, Terraform
Summary	Infrastructure automation tools allow developers to automatically deploy Zero Trust security as part of their application development pipeline. Establish internal testing that will trigger if an application is deployed with Zero Trust Reverse Proxy protection.
Steps	1. Define a standard policy for new applications. 2. Add tests in the application deployment process that require Zero Trust reverse proxy protection.
Cloudflare tools available for your organization	Configure Cloudflare using HashiCorp's "Infrastructure as Code" tool, Terraform. With Cloudflare's Terraform provider, you can manage the Cloudflare global network using the same familiar tools you use to automate the rest of your infrastructure.

Implement auto-scaling for on-ramp resources

Level of effort	🔧🔧🔧 - Large effort
Team(s) involved	• Security team • Application development team
Product(s)	Load balancers: Akamai, Cloudflare Infrastructure automation: Ansible, Puppet, Terraform
Summary	Load balancers can be effective tools to ensure individual application infrastructure is never overloaded, as well as providing a level of redundancy if one application server began to fail. Infrastructure automation tools can be used to spin up new resources if specific traffic thresholds are crossed.
Steps	1. Configure a load balancer in front of Zero Trust reverse proxy application connector. 2. Enable load balancing rules based on traffic volumes and/or geolocation of users. 3. Implement infrastructure automation policies that will provision new virtual machines if sufficient load is generated for a specific set of applications.

Cloudflare tools available for your organization	Load Balancing can be requested under Cloudflare Impact projects, and may be granted depending on the use case. Learn more at https://www.cloudflare.com/impact-portal
Resources on how to use Cloudflare Layer 7 Application products	• How to use Cloudflare Load Balancing

Example implementation timeline

Every Zero Trust deployment path is unique but there are a common set of steps that most projects follow. This is a recommended timeline for your organization to get started on a path to Zero Trust.

Timeline	Goal	Relevant Products	Provided under Cloudflare's Impact Projects
Phase 1	☐ Deploy global DNS filtering	Cisco Umbrella DNS, Cloudflare Gateway, DNSFilter, Zscaler Shift	Cloudflare Gateway
	☐ Monitor inbound emails and filter out phishing attempts	**Security Email Gateways:** Cloudflare Area 1 Email Security, Mimecast, TitanHQ **Browser Isolation:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation	Cloudflare Area 1 Email Security Cloudflare Browser Isolation
	☐ Identify misconfigurations and publicly shared data in SaaS tools	Cloudflare CASB, Netskope, Zscaler CSPM	Cloudflare CASB
Phase 2	☐ Establish corporate identity	Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin	At this time, we do not provide these products at Cloudflare.
	☐ Enforce MFA for all application	**Identity providers:** Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin, Duo **Application Reverse Proxies:** Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA)	Cloudflare Access
	☐ Enforce HTTPS and DNSsec	Akamai, AWS, Azure, Cloudflare, GCP	Cloudflare Web security services
	☐ Block or isolate threats behind SSL	**TLS Decryption:** Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Browser Isolation:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation	Cloudflare Gateway Cloudflare Browser Isolation,
	☐ Zero Trust policy enforcement for publicly addressable applications	**Zero Trust Reverse Proxies:** Microsoft Azure AD App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA)	Cloudflare Access

	☐ Protect applications from Layer 7 attacks (DDoS, Injection, Bots, etc.)	Akamai, AWS, Azure, Cloudflare, GCP	Cloudflare web security services
	☐ Close all inbound ports open to the Internet for application delivery	Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access (ZPA)	Cloudflare Access
Phase 3	☐ Inventory all corporate applications	**Secure Web Gateway and CASB with Shadow IT discovery:** Cloudflare Gateway, Microsoft Defender for Cloud Apps, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)	Cloudflare Gateway
	☐ Zero Trust policy enforcement for SaaS applications	**Zero Trust Network Access (ZTNA):** Cloudflare Access, Netskope, Zscaler Private Access (ZPA) **CASB:** Cloudflare CASB, Netskope CASB, Zscaler CASB	Cloudflare Access Cloudflare CASB
	☐ Segment user network access	Cloudflare Zero Trust (Access and Gateway), Netskope Private Access, Zscaler Private Access (ZPA)	Cloudflare Zero Trust (Access and Gateway
	☐ Zero Trust Network Access for critical privately addressable applications	Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA)	Cloudflare Access
	☐ Implement MDM/UEM to control corporate devices	**Mac:** Jamf, Kandji **Windows:** Microsoft Intune	At this time, we do not provide these products at Cloudflare.
	☐ Define what data is sensitive and where it exists	DataDog, Splunk, SolarWinds	At this time, we do not provide these products at Cloudflare.
	☐ Send out hardware-based authentication tokens	**Hard Keys:** Yubico	At this time, we do not provide these products at Cloudflare.
	☐ Stay up to date on known threat actors	Cloudflare Radar, CISA, OWASP	Cloudflare Radar
Phase 4	☐ Enforce hardware token-based MFA	**Hard Keys:** Yubico	At this time, we do not provide these products at Cloudflare.

	🔲 Zero Trust policy enforcement and network access for *all* applications	Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA)	Cloudflare Access
	🔲 Establish a SOC for log review, policy updates, and mitigation	N/A	
	🔲 Implement endpoint protection	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender	
	🔲 Inventory all corporate devices, APIs, and services	**Device Inventory:** VMWare Carbon Black, Crowdstrike, Omnitza, SentinelOne **API/Service inventory:** Cloudflare application connector, Zscaler Private Access (ZPA)	Cloudflare application connector (Tunnels)
	🔲 Use broadband Internet for branch to branch connectivity	Cloudflare Magic WAN, Cato Networks, Aryaka FlexCore	We do not provide Cloudflare Magic WAN under our Impact projects at this time.
	🔲 Establish a process to log and review employee activity on sensitive applications	**Secure Web Gateway (SWG):** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Security Incident and Event Monitoring (SIEM):** DataDog, Splunk, SolarWinds	Cloudflare Gateway
	🔲 Stop sensitive data from leaving your applications (e.g. PII, credit cards, SSNs)	Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)	Cloudflare Gateway
	🔲 Employ a DevOps approach to ensure policy enforcement for all new resources	Ansible, Puppet, Terraform	
	🔲 Implement auto-scaling for on-ramp resources	**Load balancers:** Akamai, Cloudflare **Infrastructure automation:** Ansible, Puppet, Terraform	Cloudflare web security services