



WHITEPAPER

# A Roadmap to Zero Trust Architecture

Learn the steps, tools, & teams needed to transform your network and modernize your security



# Content

- 3** [Introduction](#)
- 4** [Components of a Zero Trust Architecture](#)
- 5-23** [The Roadmap to Zero Trust](#)
- 24-25** [Example Implementation Timeline](#)

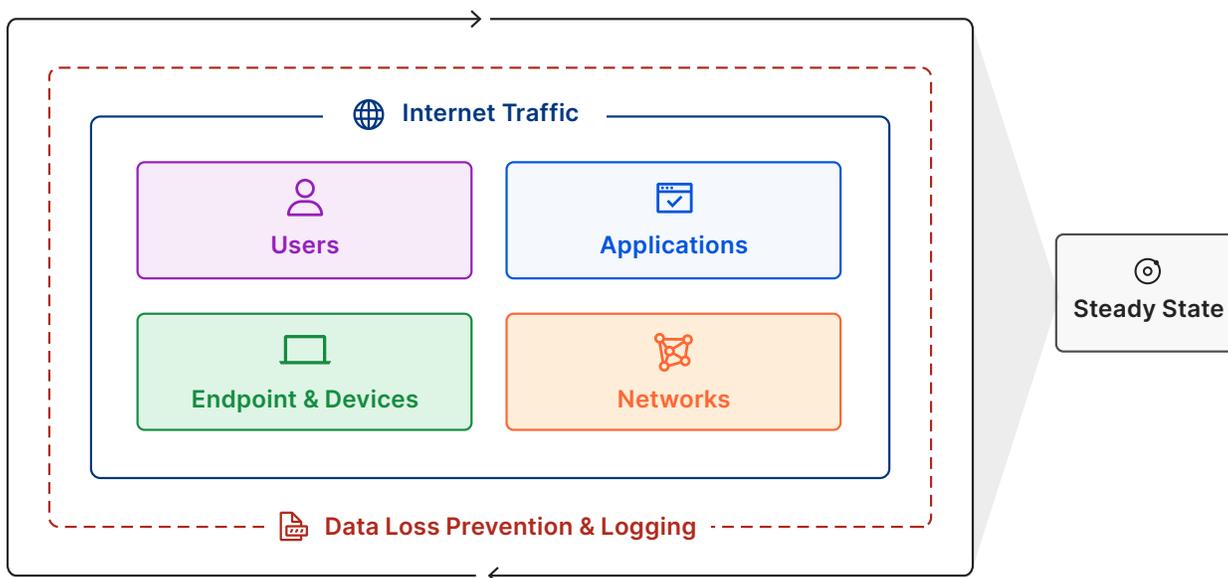
# Introduction

Traditional network architecture was built with the concept of a perimeter network where once someone was on the network, there was an implicit level of trust. The shift toward cloud hosting, remote work and other modernization has created challenges with a traditional perimeter network architecture.

These challenges can be addressed by implementing a Zero Trust Architecture, which ensures that all traffic in and out of a business is verified and authorized. Implementing a Zero Trust Architecture can be done in steps without disrupting employee productivity and connectivity.

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.



# Components of a Zero Trust Architecture

	Component	Goal	Level of Effort	Page
Phase 1	Internet traffic	Deploy global DNS filtering		<a href="#">9</a>
	Applications	Monitor inbound emails and filter out phishing attempts		<a href="#">13</a>
	DLP & logs	Identify misconfig and publicly shared data in SaaS tools		<a href="#">20</a>
Phase 2	Users	Establish corporate identity		<a href="#">5</a>
	Users	Enforce basic MFA for all applications		<a href="#">6</a>
	Applications	Enforce HTTPS and DNSsec		<a href="#">17</a>
	Internet traffic	Block or isolate threats behind SSL		<a href="#">9-10</a>
	Applications	ZT policy enforcement for publicly addressable apps		<a href="#">14-16</a>
	Applications	Protect applications from layer 7 attacks		<a href="#">16</a>
	Networks	Close all inbound ports open to the Internet for app delivery		<a href="#">12</a>
Phase 3	Applications	Inventory all corporate applications		<a href="#">13-14</a>
	Applications	ZT policy enforcement for SaaS applications		<a href="#">14-16</a>
	Networks	Segment user network access		<a href="#">11</a>
	Applications	ZTNA for critical privately addressable applications		<a href="#">14-16</a>
	Devices	Implement MDM/UEM to control corporate devices		<a href="#">7</a>
	DLP & logs	Define what data is sensitive and where it exists		<a href="#">18-19</a>
	Users	Send out hardware based authentication tokens		<a href="#">6</a>
	DLP & logs	Stay up to date on known threat actors		<a href="#">21</a>
Phase 4	Users	Enforce hardware token based MFA		<a href="#">6</a>
	Applications	ZT policy enforcement and network access for all applications		<a href="#">14-16</a>
	DLP & logs	Establish a SOC for log review, policy updates and mitigation		<a href="#">20</a>
	Devices	Implement endpoint protection		<a href="#">7</a>
	Devices	Inventory all corporate devices, APIs and services		<a href="#">8</a>
	Networks	Use broadband Internet for branch to branch connectivity		<a href="#">11-12</a>
	DLP & logs	Log and review employee activity on sensitive apps		<a href="#">18</a>
	DLP & logs	Stop sensitive data from leaving your applications		<a href="#">19</a>
	Steady state	DevOps approach for policy enforcement of new resources		<a href="#">22</a>
	Steady state	Implement auto-scaling for on-ramp resources		<a href="#">22-23</a>

Here is how we define different levels of effort required for each step:

- Small effort; this can be done by an individual or small team
- Medium effort; this will require a team and advanced preparation
- Large effort; this will require multiple teams and a project plan

# The Roadmap to Zero Trust

## Users

Users include employees, contractors and customers. 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.

### Establish a corporate Identity

<b>Level of effort</b>	 - Medium effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>• The team responsible for your identity provider (typically security or IT)</li> <li>• The admins who manage internal apps used by employees and partners</li> </ul>
<b>Product(s)</b>	<a href="#">Microsoft Azure AD</a> , <a href="#">Okta</a> , <a href="#">Ping Identity</a> <a href="#">PingOne</a> , <a href="#">OneLogin</a>
<b>Summary</b>	<p>A unified corporate identity is required to accurately authenticate and authorize user access to corporate applications. A consistent corporate Identity will make granular policy enforcement for your applications more seamless.</p> <p><b>Additional points to consider:</b></p> <ul style="list-style-type: none"> <li>• Is your company active in M&amp;A? How will you consolidate identity stores?</li> <li>• Do you have any non-web based authentication protocols in use (e.g. active directory, ntml, kerberos)</li> </ul>
<b>Steps</b>	<ol style="list-style-type: none"> <li>1. Add all corporate users to the identity provider             <ol style="list-style-type: none"> <li>a. These values can often be synchronized from an HR system like Workday, ADP, etc</li> </ol> </li> <li>2. Verify that each user’s information is correct</li> <li>3. Send new users registration information to set up login credentials</li> </ol>

### Enforce multi-factor authentication for all applications

<p><b>Level of effort</b></p>	<ul style="list-style-type: none"> <li>■ - <b>Small effort</b> (if applying basic MFA)</li> <li>■■ - <b>Medium effort</b> (if using hard keys)</li> </ul>
<p><b>Team(s) involved</b></p>	<ul style="list-style-type: none"> <li>• The team responsible for your identity provider (typically security or IT)</li> <li>• The admins who manage internal apps used by employees and partners</li> </ul>
<p><b>Product(s)</b></p>	<p><b>Identity providers:</b> <a href="#">Microsoft Azure AD</a>, <a href="#">Okta</a>, <a href="#">Ping Identity PingOne</a>, <a href="#">OneLogin</a></p> <p><b>Application Reverse Proxies:</b> <a href="#">Microsoft Azure AD App Proxy</a>, <a href="#">Akamai EAA</a>, <a href="#">Cloudflare Access</a>, <a href="#">Netskope Private Access</a>, <a href="#">Zscaler Private Access (ZPA)</a></p> <p><b>Hard Keys:</b> <a href="#">Yubico</a></p>
<p><b>Summary</b></p>	<p>Multi-Factor Authentication (MFA) is the best protection against stolen user credentials via phishing or data leaks. Most MFA can be enabled directly in an IdP.</p> <p>For applications not directly integrated with your IdP consider using an Application Reverse Proxy in front of the application to enforce MFA.</p>
<p><b>Steps</b></p>	<ol style="list-style-type: none"> <li>1. Alert internal users to upcoming MFA enforcement. Provide options to sign up for SMS or App-based authenticators</li> <li>2. Enable MFA in your IdP</li> <li>3. Enable Application Reverse Proxy in front of applications not integrated with your IdP</li> <li>4. (Bonus) Distribute Hardware keys to employees via Mail or In Person distribution</li> <li>5. (Bonus) Enforce Hardware key only MFA for your most sensitive applications</li> </ol>

## □ Endpoints & Devices

Endpoints and Devices include any device, API or software service within an organization or that have access to organizational data. 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

<b>Level of effort</b>	■■ - Medium effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>IT Team</li> </ul>
<b>Product(s)</b>	Mac: <a href="#">Jamf</a> , <a href="#">Kandji</a> Windows: <a href="#">Microsoft Intune</a>
<b>Summary</b>	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.
<b>Steps</b>	See MDM Vendor site for specific details.

### Implement endpoint protection

<b>Level of effort</b>	■■ - Medium effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>Security team</li> <li>IT Team</li> </ul>
<b>Product(s)</b>	<a href="#">VMWare Carbon Black</a> , <a href="#">CrowdStrike</a> , <a href="#">SentinelOne</a> , <a href="#">Windows Defender</a>
<b>Summary</b>	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.
<b>Steps</b>	<ol style="list-style-type: none"> <li>1. Install the Endpoint Protection Software on users’ machines using MDM</li> <li>2. Enable threat protection and compliance control in the Endpoint Protection platform</li> </ol>

## Inventory devices, APIs and services

<b>Level of effort</b>	■ - Small effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>• Security team</li> <li>• IT Team</li> </ul>
<b>Product(s)</b>	<p><b>Device Inventory:</b> <a href="#">VMWare Carbon Black</a>, <a href="#">CrowdStrike</a>, <a href="#">SentinelOne</a>, <a href="#">Windows Defender</a>, <a href="#">Oomnitza</a></p> <p><b>API/Service inventory:</b> <a href="#">Cloudflare application connector</a>, <a href="#">Zscaler Private Access (ZPA)</a></p>
<b>Summary</b>	<p>Endpoint protection software and asset management software can be used to track all devices that have been distributed to users. An accurate list of devices should be maintained to track which devices are valid and should have access to specific applications.</p> <p>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.</p>
<b>Steps</b>	<ol style="list-style-type: none"> <li>1. Install the Endpoint Protection Software on users' machines using MDM</li> <li>2. Install the API/Service scanner within your network</li> </ol>

## Internet Traffic

Internet Traffic includes all user traffic destined for websites outside of an organization’s control. This can range from business 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

<b>Level of effort</b>	 - Small effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>IT team with access to either router or machine configuration</li> <li>Security team</li> </ul>
<b>Product(s)</b>	<b>DNS Filtering:</b> <a href="#">Cisco Umbrella DNS</a> , <a href="#">Cloudflare Gateway</a> , <a href="#">DNSFilter</a> , <a href="#">Zscaler Shift</a>
<b>Summary</b>	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.
<b>Steps</b>	<b>DNS Filtering:</b> 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.

### Block or isolate threats behind SSL/TLS

<b>Level of effort</b>	 - Medium effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>IT team with access to either router or machine configuration</li> <li>Security team</li> </ul>
<b>Product(s)</b>	<p><b>TLS Decryption:</b> <a href="#">Cloudflare Gateway</a>, <a href="#">Netskope Next Gen SWG</a>, <a href="#">Zscaler Internet Access (ZIA)</a></p> <p><b>Browser Isolation:</b> <a href="#">Cloudflare Browser Isolation</a>, <a href="#">Zscaler Cloud Browser Isolation</a></p>

**Block or isolate threats behind SSL/TLS (continued)**

<b>Summary</b>	Some threats are hidden behind SSL and cannot be blocked through only HTTPS inspection. To further protect users, TLS decryption should be leveraged to further protect users from threats behind SSL.
<b>Steps</b>	<p><b>TLS decryption:</b></p> <ol style="list-style-type: none"><li>1. Ensure the correct client software is installed on a user machine<ol style="list-style-type: none"><li>a. Check for any VPN or other software that might interfere with the outbound web traffic on the device</li></ol></li><li>2. Configure the root certificate on the device for TLS decryption</li><li>3. Enable policies of when to avoid decrypting user traffic<ol style="list-style-type: none"><li>a. This should be done for sites that use certificate pinning</li><li>b. Some companies also bypass decryption for user's personal traffic (e.g banking, social media, etc)</li></ol></li></ol> <p><b>Browser Isolation:</b></p> <ol style="list-style-type: none"><li>1. Browser isolation can be deployed via the on-device client software or via an isolation link. Both approaches should be considered.</li></ol>

## Networks

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, endpoint and devices can access.

### Segment user network access

<b>Level of effort</b>	 - Large effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>• Security team</li> <li>• IT Team</li> </ul>
<b>Product(s)</b>	<b>Zero Trust Network Access (ZTNA):</b> <a href="#">Cloudflare Zero Trust (Access and Gateway used together)</a> , <a href="#">Netskope Private Access</a> , <a href="#">Zscaler Private Access (ZPA)</a>
<b>Summary</b>	Users can generally access an entire private network 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 but, with granular policies based on user, device and other factors.
<b>Steps</b>	<ol style="list-style-type: none"> <li>1. Make the private network available to the ZTNA             <ol style="list-style-type: none"> <li>a. Typically an application connector, GRE or IPSec Tunnel</li> </ol> </li> <li>2. Install the ZTNA client on user devices using MDM</li> <li>3. Set policies to segment user access across the private network</li> </ol>

### Use broadband Internet for branch to branch connectivity

<b>Level of effort</b>	 - Large effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>• Network engineering team</li> <li>• IT Team</li> </ul>
<b>Product(s)</b>	<a href="#">Cloudflare Magic WAN</a> , <a href="#">Cato Networks</a> , <a href="#">Aryaka FlexCore</a>

**Use broadband Internet for branch to branch connectivity (continued)**

<p><b>Summary</b></p>	<p>Connectivity between private network locations (eg. data centers and branches) has generally been established using Multi-Protocol 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.</p>
<p><b>Steps</b></p>	<ol style="list-style-type: none"> <li>1. Choose two MPLS-connected locations to start with. These locations will need some form of Internet connectivity.</li> <li>2. Establish a pair of redundant Anycast GRE or IPsec tunnels over your Internet circuits to your cloud WAN provider’s edge network.</li> <li>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.</li> <li>4. Change routing policies to migrate production traffic from MPLS to Internet tunnels</li> <li>5. Repeat at next MPLS-connected location</li> <li>6. Decommission MPLS circuits</li> </ol>

**Close all inbound ports open to the Internet for application delivery**

<p><b>Level of effort</b></p>	<p>■ - Small effort</p>
<p><b>Team(s) involved</b></p>	<ul style="list-style-type: none"> <li>• Network engineering team</li> </ul>
<p><b>Product(s)</b></p>	<p><b>Zero Trust Reverse Proxies:</b> <a href="#">Akamai EAA</a>, <a href="#">Cloudflare Access</a>, <a href="#">Netskope</a>, <a href="#">Zscaler Private Access (ZPA)</a></p>
<p><b>Summary</b></p>	<p>Open inbound network ports can be found using scanning technology and are a common attack vector. 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 (more details below).</p>
<p><b>Steps</b></p>	<ol style="list-style-type: none"> <li>1. Install Reverse Proxy application connector — typically a daemon or virtual machine somewhere in the same network</li> <li>2. Connect the Reverse Proxy Application to the application connector</li> <li>3. Close all inbound port on the private network with a firewall rule</li> </ol>

## Applications

Applications include any resource where organizational data exists or business 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

<b>Level of effort</b>	 - Small effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>The team responsible for your email provider configuration (typically IT)</li> </ul>
<b>Product(s)</b>	<p><b>Cloud Email Security:</b> <a href="#">Cloudflare Area 1 Email Security</a>, <a href="#">Mimecast</a>, <a href="#">TitanHQ</a></p> <p><b>Browser Isolation:</b> <a href="#">Cloudflare Browser Isolation</a>, <a href="#">Zscaler Cloud Browser Isolation</a></p>
<b>Summary</b>	<p>Email is one of the few communications channels that 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. Additionally, security teams should consider an option to quarantine links in an isolated browser that are not suspicious enough to completely block.</p>
<b>Steps</b>	<ol style="list-style-type: none"> <li>Configure your domain's MX records to point to the secure email gateway service</li> <li>Monitor for false positives in the first few weeks</li> <li>(Bonus) implement a link based browser isolation approach for borderline suspicious email links.</li> </ol>

### Inventory all corporate applications

<b>Level of effort</b>	 - Medium effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>Security Team</li> </ul>
<b>Product(s)</b>	<p><b>Secure Web Gateway and CASBs with Shadow IT discovery:</b> <a href="#">Cloudflare Gateway</a>, <a href="#">Microsoft Defender for Cloud Apps</a>, <a href="#">Netskope Next Gen SWG</a>, <a href="#">Zscaler Internet Access (ZIA)</a></p>

### Inventory all corporate applications (continued)

<p><b>Summary</b></p>	<p>It is critical for a security team to understand their full inventory of applications used across the business. Often 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).</p>
<p><b>Steps</b></p>	<ol style="list-style-type: none"> <li>1. Enable Shadow IT scanning in the Secure Web Gateway</li> <li>2. Ensure the Secure Web Gateway client is installed on user devices</li> <li>3. Allow 2-3 weeks of traffic from users</li> <li>4. Review the list of identified applications</li> <li>5. Any unapproved applications should be blocked with Secure Web Gateway policies</li> <li>6. Approved applications should be protected with Zero Trust policies</li> </ol>

### Zero Trust policy enforcement for applications

<p><b>Level of effort</b></p>	<p>  - Small effort (for most critical applications)   - Large effort (for all applications)         </p>
<p><b>Team(s) involved</b></p>	<ul style="list-style-type: none"> <li>• Security team</li> <li>• Application development team</li> <li>• IT team</li> </ul>
<p><b>Product(s)</b></p>	<p><b>Zero Trust Reverse Proxies:</b> <a href="#">Azure App Proxy</a>, <a href="#">Cloudflare Access</a>, <a href="#">Netskope Private Access</a>, <a href="#">Zscaler Private Access (ZPA)</a></p> <p><b>Zero Trust Network Access (ZTNA):</b> <a href="#">Cloudflare Access</a>, <a href="#">Netskope Private Access</a>, <a href="#">Zscaler Internet Access (ZIA)</a></p> <p><b>CASB:</b> <a href="#">Cloudflare CASB</a>, <a href="#">Netskope CASB</a>, <a href="#">Zscaler CASB</a></p> <p><b>Remote Browser Isolation:</b> <a href="#">Cloudflare Browser Isolation</a>, <a href="#">Zscaler Cloud Browser Isolation</a></p>

**Zero Trust policy enforcement for applications (continued)**

<p><b>Summary</b></p>	<p>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:</p> <ol style="list-style-type: none"> <li>1. Private self-hosted applications (addressable only on the corporate network)</li> <li>2. Public self-hosted applications (addressable over the Internet)</li> <li>3. SaaS applications</li> </ol> <p><b>Note:</b> If device context or compliance status is a required security policy then typically on-device client software is required.</p>
<p><b>Steps</b></p>	<p><b>Private Self-Hosted Applications</b></p> <ol style="list-style-type: none"> <li>1. Build an encrypted tunnel between the application and Zero Trust policy layer. Typically this will be an “application connector”, GRE or IPSec tunnel</li> <li>2. Make the private DNS resolver available for users of the ZTNA device client</li> <li>3. Build policies based on user, device and network context to establish who can access the application</li> </ol> <p><b>Public Self-Hosted Applications</b></p> <ol style="list-style-type: none"> <li>1. Move the authoritative DNS or a CNAME record to the Application Reverse Proxy</li> <li>2. Ensure all inbound ports for closed for the application’s network</li> <li>3. Build policies based on user, device and network context to establish who can access the application</li> </ol> <p><b>SaaS Applications</b></p> <p>There are a few different options to enforce Zero Trust policies for SaaS applications</p> <p><b>Identity Proxy</b></p> <p>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 SSO provider of the SaaS application</p> <ol style="list-style-type: none"> <li>1. Remove the existing SSO integration to the SaaS app, if present</li> <li>2. Integrate the Identity proxy with the SaaS application</li> <li>3. Ensure the correct SAML attributes are sent for user creation and updates</li> <li>4. Create policies based on the user, device and network context</li> </ol>

**Zero Trust policy enforcement for applications (continued)**

<b>Steps</b>	<p><b>Secure Web Gateway and Single Sign On</b></p> <p>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.</p> <ol style="list-style-type: none"> <li>1. Add the SaaS application to the SSO provider</li> <li>2. Create policies to enforce which users are authorized</li> <li>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)</li> <li>4. Create Secure Web Gateway policies that control which users can access the SaaS application</li> </ol>
--------------	---

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

<b>Level of effort</b>	<p> - Small effort</p>
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>• Security team</li> <li>• Application development team</li> </ul>
<b>Product(s)</b>	<p><a href="#">Akamai</a>, <a href="#">AWS</a>, <a href="#">Azure</a>, <a href="#">Cloudflare</a>, <a href="#">GCP</a></p>
<b>Summary</b>	<p>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.</p>
<b>Steps</b>	<ol style="list-style-type: none"> <li>1. Add any public application's authoritative DNS record</li> <li>2. Enable the Web Application Firewall and DDoS protection</li> </ol>

## Enforce HTTPS and DNSsec

<b>Level of effort</b>	■ - Small effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"><li>• Security team</li><li>• Application development team</li></ul>
<b>Product(s)</b>	<a href="#">Akamai</a> , <a href="#">AWS</a> , <a href="#">Azure</a> , <a href="#">Cloudflare</a> , <a href="#">GCP</a>
<b>Summary</b>	Any self-hosted web application should leverage HTTPS and DNSSec. This prevents any potential for packet sniffing or domain hijacking.
<b>Steps</b>	<ol style="list-style-type: none"><li>1. Add any public application's authoritative DNS record</li><li>2. Set HTTPS to strict and enable DNSSEC</li></ol>

## Data Loss Prevention & 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. These are 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

<b>Level of effort</b>	■■ - Medium effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>Security team</li> </ul>
<b>Product(s)</b>	<p><b>Secure Web Gateway (SWG):</b> <a href="#">Cisco Umbrella</a>, <a href="#">Cloudflare Gateway</a>, <a href="#">Netskope Next Gen SWG</a>, <a href="#">Zscaler Internet Access (ZIA)</a></p> <p><b>Security Incident and Event Monitoring (SIEM):</b> <a href="#">DataDog</a>, <a href="#">Splunk</a>, <a href="#">SolarWinds</a></p>
<b>Summary</b>	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 tuned over time in the SIEM.
<b>Steps</b>	<ol style="list-style-type: none"> <li>1. Ensure all user traffic destined to sensitive applications is proxied using the SWG</li> <li>2. Enable the log push or pull functionality between your SWG and SIEM</li> <li>3. Set a specific interval for the security team to review traffic logs</li> <li>4. Configure alerts in the SIEM based on findings over time</li> </ol>

### Define what data is sensitive and where it exists

<b>Level of effort</b>	■■ - Medium effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>Security team</li> <li>Compliance/Legal team</li> </ul>
<b>Product(s)</b>	<p><b>Security Incident and Event Monitoring (SIEM):</b> <a href="#">DataDog</a>, <a href="#">Splunk</a>, <a href="#">SolarWinds</a></p>

### Define what data is sensitive and where it exists (continued)

<p><b>Summary</b></p>	<p>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 is for your company and where it lives.</p> <p>An accurate definition and inventory of sensitive data will inform the implementation of Data Loss Prevention tools.</p>
<p><b>Steps</b></p>	<ol style="list-style-type: none"> <li>1. Review traffic logs in the SIEM tools or directly in a Secure Web Gateway to identify target applications and data stores</li> <li>2. Take an inventory of existing sensitive data</li> </ol>

### Prevent sensitive data from leaving your applications

<p><b>Level of effort</b></p>	<p>■■■ - Large effort</p>
<p><b>Team(s) involved</b></p>	<ul style="list-style-type: none"> <li>• Security team</li> <li>• IT Team</li> <li>• Compliance/Legal team</li> </ul>
<p><b>Product(s)</b></p>	<p><b>In-line Data Loss Prevention (DLP):</b> <a href="#">Cisco Umbrella</a>, <a href="#">Cloudflare Gateway</a>, <a href="#">Netskope Next Gen SWG</a>, <a href="#">Zscaler Internet Access (ZIA)</a></p>
<p><b>Summary</b></p>	<p>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, etc) 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.</p>
<p><b>Steps</b></p>	<ol style="list-style-type: none"> <li>1. Install the client software from the DLP provider</li> <li>2. Ensure there is no existing VPN or other tool that will disrupt connectivity</li> <li>3. Ensure TLS decryption is enabled and a root certificate is present on each user machine</li> <li>4. Enable DLP controls</li> <li>5. Monitor for DLP block events and verify if it is valid or a false positive</li> </ol>

### Identify misconfigurations and publicly shared data in SaaS tools

<b>Level of effort</b>	■ - Small effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>Security team</li> </ul>
<b>Product(s)</b>	API based Cloud Access Security Broker (CASB): <a href="#">Cloudflare CASB</a> , <a href="#">DoControl</a> , <a href="#">Netskope</a> , <a href="#">Zscaler CSPM</a>
<b>Summary</b>	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.
<b>Steps</b>	<ol style="list-style-type: none"> <li>1. Connect each SaaS application via the provider’s API integration instructions</li> <li>2. Run scans for each SaaS application</li> <li>3. Review the scan results and begin remediation in each SaaS application where appropriate</li> </ol>

### Establish a Security Operations Center (SOC) for log review, policy updates and mitigation

<b>Level of effort</b>	■■ - Medium effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>Security team</li> </ul>
<b>Product(s)</b>	None
<b>Summary</b>	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.
<b>Steps</b>	<ol style="list-style-type: none"> <li>1. Review logs in SIEM or directly in security product</li> <li>2. Identify any alerts or anomalous activity</li> <li>3. Update Zero Trust policies across each tool based on findings</li> </ol>

**Stay up to date on known threat actors**

<b>Level of effort</b>	■ - Small effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"><li>• Security team</li></ul>
<b>Product(s)</b>	Threat intelligence providers: <a href="#">Cloudflare Radar</a> , <a href="#">CISA</a> , <a href="#">OWASP</a>
<b>Summary</b>	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.
<b>Steps</b>	<ol style="list-style-type: none"><li>1. Connect threat feed into Secure Web Gateway</li><li>2. Enable threat protection in DNS and HTTP filtering</li></ol>

## ⦿ 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

<b>Level of effort</b>	■■■ - Large effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>• Security team</li> <li>• Application development team</li> </ul>
<b>Product(s)</b>	Infrastructure automation: <a href="#">Ansible</a> , <a href="#">Puppet</a> , <a href="#">Terraform</a>
<b>Summary</b>	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.
<b>Steps</b>	<ol style="list-style-type: none"> <li>1. Define a standard policy for new applications</li> <li>2. Add tests in the application deployment process that require Zero Trust Reverse Proxy protection</li> </ol>

### Implement auto-scaling for on-ramp resources

<b>Level of effort</b>	■■■ - Large effort
<b>Team(s) involved</b>	<ul style="list-style-type: none"> <li>• Security team</li> <li>• Application development team</li> </ul>
<b>Product(s)</b>	<p>Load balancers: <a href="#">Akamai</a>, <a href="#">Cloudflare</a></p> <p>Infrastructure automation: <a href="#">Ansible</a>, <a href="#">Puppet</a>, <a href="#">Terraform</a></p>

**Implement auto-scaling for on-ramp resources (continued)**

<b>Summary</b>	<p>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.</p> <p>Infrastructure automation tools can be used to spin up new resources if specific traffic thresholds are crossed.</p>
<b>Steps</b>	<ol style="list-style-type: none"><li>1. Configure a load balancer in front of Zero Trust Reverse Proxy Application connector</li><li>2. Enable load balancing rules based on traffic volumes and/or geo-location of users.</li><li>3. Implement infrastructure automation policies that will provision new virtual machines if sufficient load is generated for a specific set of applications</li></ol>

# Example Implementation Timeline

Every Zero Trust Architecture deployment is unique but there are a common set of steps that most projects follow. This is a recommended timeline for a business getting started on a Zero Trust Architecture implementation.

Timeline	Goal	Relevant Products
Phase 1	<input type="checkbox"/> Deploy global DNS filtering	<a href="#">Cisco Umbrella DNS</a> , <a href="#">Cloudflare Gateway</a> , <a href="#">DNSFilter</a> , <a href="#">Zscaler Shift</a>
	<input type="checkbox"/> Monitor inbound emails and filter out phishing attempts	<b>Cloud Email Security:</b> <a href="#">Cloudflare Area 1 Email Security</a> , <a href="#">Mimecast</a> , <a href="#">TitanHQ</a> <b>Browser Isolation:</b> <a href="#">Cloudflare Browser Isolation</a> , <a href="#">Zscaler Cloud Browser Isolation</a>
	<input type="checkbox"/> Identify misconfig and publicly shared data in SaaS tools	<a href="#">Cloudflare CASB</a> , <a href="#">DoControl</a> , <a href="#">Netskope</a> , <a href="#">Zscaler CSPM</a>
Phase 2	<input type="checkbox"/> Establish corporate identity	<a href="#">Microsoft Azure AD</a> , <a href="#">Okta</a> , <a href="#">Ping Identity PingOne</a> , <a href="#">OneLogin</a>
	<input type="checkbox"/> Enforce basic MFA for all applications	<b>Identity providers:</b> <a href="#">Microsoft Azure AD</a> , <a href="#">Okta</a> , <a href="#">Ping Identity PingOne</a> , <a href="#">OneLogin</a> <b>Application Reverse Proxies:</b> <a href="#">Microsoft Azure AD App Proxy</a> , <a href="#">Akamai EAA</a> , <a href="#">Cloudflare Access</a> , <a href="#">Netskope Private Access</a> , <a href="#">Zscaler Private Access (ZPA)</a>
	<input type="checkbox"/> Enforce HTTPS and DNSsec	<a href="#">Akamai</a> , <a href="#">AWS</a> , <a href="#">Azure</a> , <a href="#">Cloudflare</a> , <a href="#">GCP</a>
	<input type="checkbox"/> Block or isolate threats behind SSL	<b>TLS Decryption:</b> <a href="#">Cloudflare Gateway</a> , <a href="#">Netskope Next Gen SWG</a> , <a href="#">Zscaler Internet Access (ZIA)</a> <b>Browser Isolation:</b> <a href="#">Cloudflare Browser Isolation</a> , <a href="#">Zscaler Cloud Browser Isolation</a>
	<input type="checkbox"/> ZT policy enforcement for publicly addressable apps	<b>Zero Trust Reverse Proxies:</b> <a href="#">Azure App Proxy</a> , <a href="#">Cloudflare Access</a> , <a href="#">Netskope Private Access</a> , <a href="#">Zscaler Private Access (ZPA)</a>
	<input type="checkbox"/> Protect applications from layer 7 attacks	<a href="#">Akamai</a> , <a href="#">AWS</a> , <a href="#">Azure</a> , <a href="#">Cloudflare</a> , <a href="#">GCP</a>
	<input type="checkbox"/> Close all inbound ports open to the Internet for app delivery	<a href="#">Akamai EAA</a> , <a href="#">Cloudflare Access</a> , <a href="#">Netskope</a> , <a href="#">Zscaler Private Access (ZPA)</a>
Phase 3	<input type="checkbox"/> Inventory all corporate applications	<b>Secure Web Gateway and CASBs with Shadow IT discovery:</b> <a href="#">Cloudflare Gateway</a> , <a href="#">Microsoft Defender for Cloud Apps</a> , <a href="#">Netskope Next Gen SWG</a> , <a href="#">Zscaler Internet Access (ZIA)</a>
	<input type="checkbox"/> ZT policy enforcement for SaaS applications	<b>Zero Trust Network Access (ZTNA):</b> <a href="#">Cloudflare Access</a> , <a href="#">Netskope Private Access</a> , <a href="#">Zscaler Internet Access (ZIA)</a> <b>CASB:</b> <a href="#">Cloudflare CASB</a> , <a href="#">Netskope CASB</a> , <a href="#">Zscaler CASB</a>

Phase 4	<input type="checkbox"/>	Segment user network access	Zero Trust Network Access (ZTNA): <a href="#">Cloudflare Zero Trust (Access and Gateway used together)</a> , <a href="#">Netskope Private Access</a> , <a href="#">Zscaler Private Access (ZPA)</a>
	<input type="checkbox"/>	ZTNA for critical privately addressable applications	<a href="#">Cloudflare Access</a> , <a href="#">Netskope Private Access</a> , <a href="#">Zscaler Internet Access (ZIA)</a>
	<input type="checkbox"/>	Implement MDM/UEM to control corporate devices	Mac: <a href="#">Jamf</a> , <a href="#">Kandji</a> Windows: <a href="#">Microsoft Intune</a>
	<input type="checkbox"/>	Define what data is sensitive and where it exists	<a href="#">DataDog</a> , <a href="#">Splunk</a> , <a href="#">SolarWinds</a>
	<input type="checkbox"/>	Send out hardware based authentication tokens	Hard Keys: <a href="#">Yubico</a>
	<input type="checkbox"/>	Stay up to date on known threat actors	<a href="#">Cloudflare Radar</a> , <a href="#">CISA</a> , <a href="#">OWASP</a>
	<input type="checkbox"/>	Enforce hardware token based MFA	Hard Keys: <a href="#">Yubico</a>
	<input type="checkbox"/>	ZT policy enforcement and network access for all applications	<a href="#">Cloudflare Access</a> , <a href="#">Netskope Private Access</a> , <a href="#">Zscaler Internet Access (ZIA)</a>
	<input type="checkbox"/>	Establish a SOC for log review, policy updates and mitigation	N/A
	<input type="checkbox"/>	Implement endpoint protection	<a href="#">VMWare Carbon Black</a> , <a href="#">CrowdStrike</a> , <a href="#">SentinelOne</a> , <a href="#">Windows Defender</a>
	<input type="checkbox"/>	Inventory all corporate devices, APIs and services	Device Inventory: <a href="#">VMWare Carbon Black</a> , <a href="#">CrowdStrike</a> , <a href="#">SentinelOne</a> , <a href="#">Windows Defender</a> , <a href="#">Omnitza</a> API/Service inventory: <a href="#">Cloudflare application connector</a> , <a href="#">Zscaler Private Access (ZPA)</a>
	<input type="checkbox"/>	Use broadband Internet for branch to branch connectivity	<a href="#">Cloudflare Magic WAN</a> , <a href="#">Cato Networks</a> , <a href="#">Aryaka FlexCore</a>
	<input type="checkbox"/>	Establish a process to log and review employee activity on sensitive applications	Secure Web Gateway (SWG): <a href="#">Cisco Umbrella</a> , <a href="#">Cloudflare Gateway</a> , <a href="#">Netskope Next Gen SWG</a> , <a href="#">Zscaler Internet Access (ZIA)</a> Security Incident and Event Monitoring (SIEM): <a href="#">DataDog</a> , <a href="#">Splunk</a> , <a href="#">SolarWinds</a>
<input type="checkbox"/>	Stop sensitive data from leaving your applications (e.g. PII, Credit Cards, SSNs, etc)	<a href="#">Cisco Umbrella</a> , <a href="#">Cloudflare Gateway</a> , <a href="#">Netskope Next Gen SWG</a> , <a href="#">Zscaler Internet Access (ZIA)</a>	
<input type="checkbox"/>	Employ a DevOps approach to ensure policy enforcement for all new resources	<a href="#">Ansible</a> , <a href="#">Puppet</a> , <a href="#">Terraform</a>	
<input type="checkbox"/>	Implement auto-scaling for on-ramp resources	Load balancers: <a href="#">Akamai</a> , <a href="#">Cloudflare</a> Infrastructure automation: <a href="#">Ansible</a> , <a href="#">Puppet</a> , <a href="#">Terraform</a>	



© 2022 Cloudflare Inc. All rights reserved. The Cloudflare logo is a trademark of Cloudflare. All other company and product names may be trademarks of the respective companies with which they are associated.

1 888 99 FLARE | [enterprise@cloudflare.com](mailto:enterprise@cloudflare.com) | [www.cloudflare.com](http://www.cloudflare.com)