Critical Infrastructure Defense Project

CLOUDFLARE | CROWDSTRIKE | PingIdentity

Introduction

In response to the Russian invasion of Ukraine, national security experts have highlighted the increased risk of cyber attacks and have urged organizations to adopt a heightened cybersecurity posture. All organizations should be prepared for increasingly frequent and sophisticated attacks with goals that include stealing data, compromising applications, and shutting down networks and devices.

To address this threat, leading Zero Trust cyber security providers have partnered to launch the Critical Infrastructure Defense Project. Our goal is to quickly improve the cyber readiness of US critical infrastructure–hospitals, energy utilities and water utilities–by providing free services and support.

The combination of cyber security capabilities offered by the project enables a robust Zero Trust defense-in-depth approach that can be implemented quickly.

Although the Critical Infrastructure Defense Project is designed for high impact US providers like hospitals, water utilities and power utilities, all organizations need a defense-in-depth strategy to protect their teams and critical infrastructure and can benefit from the Critical Infrastructure Defense checklist.

The Critical Infrastructure Defense Project

The Critical Infrastructure Defense Project provides a comprehensive and easy-to-follow roadmap to implement the tools needed by teams of any size to defend themselves from attack.

The security features available to organizations through the Critical Infrastructure Defense provide a defense-in-depth approach to securing teams that are at risk of attack. Each component secures a distinct risk surface area and works together to provide organizations with comprehensive defense against attack.

1 Secure DNS Filtering
2 Single Sign-on
3 Multi-factor Authentication
4 Endpoint Protection
5 Secure Web Gateway
6 Zero Trust Access Control
7 Email Protection
8 DNS Infrastructure
9 WAF and DDoS Mitigation
10 Risk Monitoring and Management

Program

Checklist
The program includes a checklist with phased milestones that make your team safer with every step. All products are designed to be deployed in hours, not days, but the timeline suggested gives organizations a template based on team member availability.

Cost and Eligibility
The supporting partners are making these services available at no cost for the next four months to organizations in the at-risk industries of healthcare and water and power utilities.

Onboarding
Cloudflare, CrowdStrike and Ping Identity will each provide 1-1 guided onboarding to organizations supported by the Critical Infrastructure Defense Project.

Checklist

Timeline	Goal	Defend against	Relevant Products
Next hour	Deploy global DNS filtering	Phishing, malware	Cloudflare 1.1.1.2
Next 24 hours	Deploy targeted DNS filtering and logging	Phishing, malware	Cloudflare Gateway DNS Filter
	Harden authoritative DNS infrastructure	DDoS of applications due to DNS outage	Cloudflare DNS Cloudflare DNS Firewall
	Protect public applications from attack	OWASP Top Ten, DDoS, account takeover, zero-day vulnerabilities	Cloudflare WAF Cloudflare DDoS Mitigation
	Deploy consistent and secure sign-on for every user to all apps	Credential stuffing, password reuse	PingOne SSO
	Gain an extra level of assurance about user identities	Phishing, account takeover	PingOne MFA
Next week	Require SSO and MFA on all applications and network connections	Spearphishing, lateral movement	Cloudflare Access
	Protect infrastructure from attack	Network-level DDoS and recon	Cloudflare Magic Transit Cloudflare Magic Firewall
	Inspect traffic for hidden threats	Malware, ransomware	Cloudflare Gateway SWG
	Scan email for threats	Ransomware, phishing	Cloudflare Email security
	Monitor scripts and other dependencies for malicious changes	Exfiltration of sensitive user data, including login credentials	Cloudflare Page Shield
	Review security settings for misconfigurations	Weak authentication, insecure encryption and DNS config	Cloudflare Security Center

Timeline	Goal	Defend against	Relevant Products
Next week	Deploy sensors across network endpoints and cloud workloads	Malware	CrowdStrike Falcon Endpoint Protection Pro
	Enable monitoring and tracking of adversaries	Adversaries across the deep and dark web	CrowdStrike Falcon X Recon
	Employ advanced risk signals during authentication	Suspicious sign-on activity, phishing, account takeover	PingOne Risk
	Enable a single place to create secure flows for security services	Deploy security services across user journeys	PingOne DaVinci
Next month	Isolate risky traffic	Malicious code, phishing	Cloudflare Browser Isolation
	Secure your domain registration	Domain takeover	Cloudflare Registrar

Step-by-step guide

1 Next hour

Deploy global DNS filtering

Time required	10 minutes
Team(s)	The IT team responsible for managing your corporate and guest Internet access
Product(s)	Cloudflare 1.1.1.2
Summary	Attackers plant links in websites, text messages, and emails that lure users to malicious hostnames to phish credentials or download malware. Every device in your network starts every connection to a hostname with a DNS query. A DNS filter checks the hostname requested against a list of known dangerous destinations and, if the hostname matches, stops the user from inadvertently reaching the destination.
Steps	1. Modify the DNS resolvers of the routers in your network and, if using MDM, of your roaming devices to point to 1.1.1.2

2 Next 24 hours

Deploy targeted DNS filtering and logging

Time required	30 minutes
Team(s)	The IT team responsible for managing your corporate and guest Internet access
Product(s)	Cloudflare Gateway DNS Filtering
Summary	Cloudflare's 1.1.1.2 service provides a set of default DNS filtering rules to secure against common attacks. Some teams and industries need more specific rules and control over the rulesets and logs. Your team can deploy a version of Cloudflare's DNS filtering, using Cloudflare Gateway, to:
Steps	1. Use a template rule to create a standard DNS filtering policy. 2. Modify the DNS resolvers of the routers in your network and, if using MDM, of your roaming devices. 3. *Optional:* export DNS queries to storage for forensic analysis.

Harden authoritative DNS infrastructure

Time required	8 hours
Team(s)	IT team responsible for authoritative DNS
Product(s)	Cloudflare Authoritative DNS
Summary	Websites and apps rely on successful resolution of hostnames against your authoritative DNS servers to function. When these DNS servers are attacked they can become slow to respond or unavailable, which can make apps inaccessible.
Steps	1. Migrate authoritative DNS to anycast-based provider that's hardened against DDoS attacks (if not already running on one). 2. Alternatively, deploy DNS Firewall when unable to change authoritative provider.

Protect public applications from attack

Time required	2 hours
Team(s)	The admins who manage public-facing apps
Product(s)	Cloudflare WAF and DDoS Mitigation
Summary	Your public-facing apps, like marketing sites or customer portals, can be vulnerable to attacks that make the websites inaccessible or compromise end user data. Web Application Firewall (WAF) and Distributed Denial of Service (DDoS) solutions can protect your applications from attack while ensuring your audience can continue to reach them for critical updates or information.
Steps	1. Define a template policy to filter web attacks. 2. Change the authoritative nameservers of your application(s).

Deploy Single Sign-on

Time required	1 hour (may vary depending on number of apps)
Team(s)	• The security team responsible for your identity provider • The admins who manage internal apps used by employees and partners
Product(s)	PingOne SSO
Summary	Having disparate ways to access applications increases your attack surface, making you more vulnerable to poor security hygiene like common passwords or password reuse. Even if you hide your apps behind a virtual private network (VPN), bad actors can attempt to reach your private network and move laterally to reach your internal resources. Single sign-on (SSO) solutions control user authentication centrally and allow for quick revocation of passwords. The PingOne Cloud Platform makes it easy to deploy SSO for every application, even if applications are custom, non-standards-based apps.
Steps	1. Configure SSO provider with existing applications 2. Define policies to determine who has access to which applications

Deploy Multi-factor Authentication

Time required	2 hours
Team(s)	• The security team responsible for your identity provider • The admins who manage internal apps used by employees and partners
Product(s)	PingOne MFA
Summary	Whether from successful phishing attempts, password reuse, or purchased credential lists, bad actors may have legitimate credentials to access your systems. In these scenarios, multi-factor authentication (MFA) can protect your organization by requiring users to authenticate with a second factor—like an SMS code, physical key, or push notification from an MFA application—in addition to their password.
Steps	1. Configure MFA and choose available methods 2. Modify SSO policies to add MFA where appropriate

3 Next week

Require SSO and MFA on all applications and network connections

Time required	4 hours
Team(s)	• The security team responsible for your identity provider. • The admins who manage internal apps used by employees and partners.
Product(s)	Cloudflare Access
Summary	Attackers can steal passwords or reuse common passwords to access the applications you host for team members. If you hide those apps behind a virtual private network (VPN), bad actors can attempt to reach your private network and move laterally to reach your internal resources. Multifactor authentication (MFA) requires users to authenticate with a second factor in addition to their password, like an SMS code or physical key. Single sign-on (SSO) solutions control user passwords centrally and allow for quick revocation. Deploying MFA and SSO requirements on legacy applications can be difficult or impossible. However, you can use Cloudflare's Zero Trust reverse proxy, Cloudflare Access, to shield applications and require MFA and other attributes on every request or connection -- regardless of native support in the app itself.
Steps	1. Integrate your identity provider. 2. Define a policy to determine who can reach your applications. 3. Connect your applications with a secure, outbound-only tunnel that forces all traffic through the Zero Trust reverse proxy.

Protect infrastructure from attack

Time required	12 hours
Team(s)	Network administrators
Product(s)	Cloudflare Magic Transit
Summary	Web applications tend to be more shielded than the networks and IP addresses maintained by most teams. Bad actors exploit that difference by overwhelming networks with DDoS attacks, disabling critical infrastructure. Distributed Denial of Service (DDoS) solutions can also protect your networks from disruption by mitigating attacks before they overwhelm your infrastructure.
Steps	1. Delegate IP range to DDoS solution. 2. Connect your network through GRE tunnels, IPsec tunnels, or physical interconnects. 3. Restrict ingress traffic ("allow list") to DDoS provider IP ranges.

Inspect traffic for hidden threats

Time required	8 hours
Team(s)	IT teams responsible for managing corporate devices
Product(s)	Cloudflare Secure Web Gateway
Summary	DNS filtering stops users from reaching known malicious destinations, but bad actors can hide attacks inside of the traffic of otherwise healthy websites. These attacks can download malware and ransomware on devices, which can spread to your organization. A Secure Web Gateway (SWG) receives all of the traffic leaving devices before it heads to the Internet. The SWG inspects the traffic to determine if the destination is malicious at a more granular level, searches for malware in traffic being returned to your devices, and scans for files leaving the devices unintentionally.
Steps	1. Deploy a lightweight agent and certificate to your corporate devices. 2. Use a template security policy to inspect traffic for threats and malware. 3. Proxy traffic leaving devices through the SWG.

Scan email for threats

Time required	10 hours
Team(s)	IT team managing your email provider
Product(s)	Cloudflare Email Security
Summary	Email inboxes represent an open door to attackers and is the first line of attack. Default spam filters miss sophisticated attacks, especially those purporting to be from authority figures. Email security solutions scan email before it arrives in your inbox to detect advanced threats.
Steps	1. Modify the MX records of the domain used for your corporate email.

Monitor scripts and other dependencies for malicious changes

Time required	4 hours
Team(s)	IT team responsible for managing websites
Product(s)	Cloudflare Page Shield
Summary	Websites typically rely on third-party JavaScript to operate. When changes to these JS dependencies are malicious, sensitive data can be exfiltrated from users including credentials (usernames and passwords), and other sensitive data. When credentials are stolen they can be used to pivot. Cloudflare Page Shield is a monitoring solution that utilizes reports from browsers (Content Security Policy) can detect when scripts are changed or added and evaluate those scripts for malicious intent.
Steps	1. Serve web traffic from behind a reverse proxy. 2. Insert CSP response headers to receive script executions. 3. Use automated tool to collect and monitor changes for malicious intent.

Review security settings for misconfigurations

Time required	2 hours
Team(s)	Security team
Product(s)	Cloudflare Security Center
Summary	Securing an entire organization, across several tools and features, can be difficult to manage and audit. Cloudflare Security Center automatically reviews your existing security configuration, across all Cloudflare tools, and detects potential issues and recommends new settings on a real-time basis.
Steps	1. Login to your Cloudflare dashboard. 2. Navigate to the Cloudflare Security Center. 3. Review potential issues and proposed remediations in priority order.

Deploy sensors across network endpoints and cloud workloads

Time required	1 hour (depending on number of sensors deployed)
Team(s)	IT Operations or Security Operations
Product(s)	CrowdStrike Falcon Endpoint Protection
Summary	Activate your CrowdStrike Falcon Endpoint Protection Pro trial and start sensor deployment(s) to detect and block threats
Steps	1. Check your email for the initial account activation one-time setup link 2. Setup your account password 3. Establish a method for 2-factor authentication 4. Download and install the Falcon sensor 5. Confirm the sensor is running 6. Verify sensor visibility in the cloud

Enable monitoring and tracking of adversaries

Time required	20 minutes
Team(s)	IT Operations or Security Operations
Product(s)	Falcon X Recon
Summary	Enable monitoring of your organization from hidden risks across the Internet by registering your organization with Falcon X Recon and configure notifications
Steps	1. Register your organization 2. Set alert priority 3. Customize notifications and alerts 4. Access and view results

Add Risk Signals for More Intelligent SSO and MFA

Time required	2 hours
Team(s)	• The security team responsible for your identity provider • The admins who manage internal apps used by employees and partners
Product(s)	PingOne Risk
Summary	Detect sophisticated attacks by assessing risk level associated with authentication events. Risk scoring ensures you only require MFA in risky scenarios.
Steps	1. Define the risk signals you want to evaluate and your risk-score threshold 2. Configure SSO and MFA policies to react appropriately to high, medium, and low-risk scenarios

Establish a Zero Trust Foundation with Orchestration

Time required	2 to 4 hours
Team(s)	• The security team responsible for your identity provider • Other security teams • The admins who manage internal apps used by employees and partners
Product(s)	PingOne DaVinci
Summary	Identity and access management—including SSO, MFA, and risk signals—is an important line of defense that protects your organization, but there is more to Zero Trust. Establishing a true Zero Trust foundation includes many other capabilities that you'll want to implement, maintain, and optimize over time. Adding a foundation of orchestration gives you a drag-and-drop interface to create user flows and connect security services from any vendor to create the most secure, convenient experiences for your users and protect your organization from attackers. It even provides analytics that let you A/B test and optimize your user journeys and security. And it's all done with a visual, no-code canvas.
Steps	1. Select pre-configured connectors to the security services you'd like to include 2. Drag and drop your user journey and security services into a flow

4 Next month

Isolate risky traffic

Time required	2 hours
Team(s)	Security team responsible for SWG policies
Product(s)	Cloudflare Browser Isolation
Summary	Attackers can compromise websites and exploit vulnerabilities in the browser to launch attacks that infect your devices. Browser isolation runs the browser session off of the device, in a secure cloud deployment, and only sends vector renderings to the device itself. No code is ever delivered or executed. You can choose to only isolate unknown or high-risk websites to reduce false positive blocks but prevent sophisticated attacks.
Steps	1. Build a new rule in your existing SWG deployment to isolate all unknown, new or risky destinations on the Internet. 2. Extend that rule to block text input to those destinations.

Secure your domain registration

Time required	2 hours
Team(s)	IT admin responsible for the domains you own
Product(s)	Cloudflare Registrar
Summary	The domains used by your organization power systems that include your website, your public-facing applications, and your email. If attackers compromise your domain registration, they can take down your services and impersonate your email. Domain registration can be better secured through a registrar which supports MFA and advanced domain registration locks to prevent domain takeover.
Steps	1. Obtain an authentication code from your current registrar. 2. Migrate to Cloudflare's domain registrar. 3. Apply domain registration control locks.