CLOUDFLARE

SOLUTION BRIEF

Three high-value steps to defend any critical infrastructure network

Critical infrastructure communities know the peril they face. Foreign state actors and cyber criminals are waging aggressive and persistent attacks on them, often using artificial intelligence (AI)-enabled tools and tactics to gain easier entry to their networks.

Meanwhile, their attack surfaces are growing larger and more difficult to defend. Attack surfaces are expanding as operators continue merging operational technology (OT) and information technology (IT) systems to embrace the benefits of Internet of Things (IoT) devices and products.

There is a clear imperative to modernize security — but how?

Critical infrastructure organizations need to protect the IT side of their networks from cyber threats that could affect the OT side.

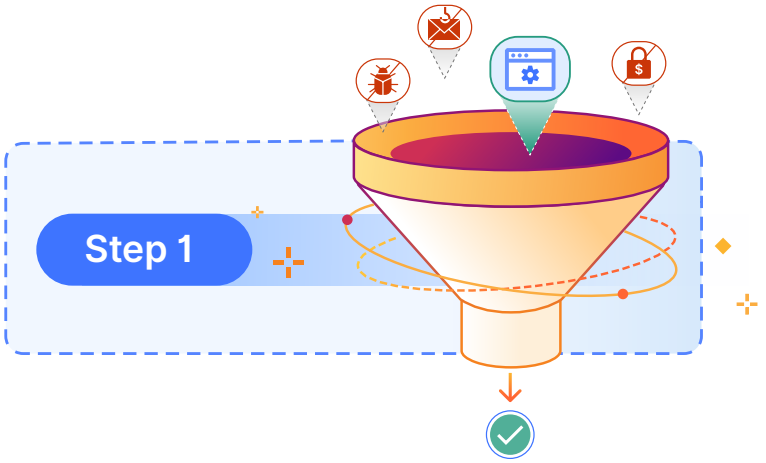
While this much is clear, the path forward is not. That is not due to a shortage of guidance — infrastructure operators have been inundated with guidance. Their questions are: What to do first? And what is the quickest, most direct way forward to address their biggest gaps and vulnerabilities?

These challenges require solutions that go beyond patchwork defenses and do not rely on traditional perimeter-based defenses. What is needed is an integrated Zero Trust architecture that can adapt dynamically to changing risks — without slowing down mission-critical operations.

The good news is that reaching that goal of that integrated Zero Trust architecture can be done incrementally, step by step.

Confidently start your cyber modernization journey with these three steps

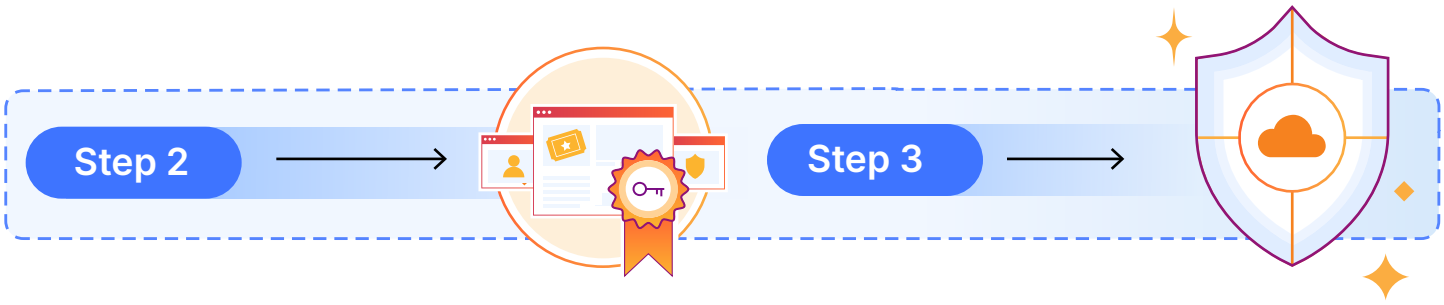
The path to addressing today and tomorrow's cyber threats will look different for every organization. Public utilities, manufacturing plants, ports, hospitals, and transportation networks will all have distinct journeys. But there are three high-value steps that every critical infrastructure organization can take to strengthen their cybersecurity postures:



Get phishing attacks under control and filter out malicious content immediately.

More than 90% of all successful cyber attacks begin with phishing. Phishing emails trick employees into downloading malware or ransomware, or clicking links that lead to credential theft and network compromise. Stopping these attacks early by deploying these three solutions can help shield you from the largest category of serious threats:

- **Cloudflare Email Security** stops phishing and ransomware threats before they land in users' inboxes.
- **Cloudflare Gateway** blocks access to malicious sites, even if users click on a dangerous link.
- **Cloudflare Browser Isolation** prevents harmful content from reaching and compromising endpoint devices.



Meet the minimum cyber protections recommended for critical infrastructure sectors.

The Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) developed key goals to help all critical infrastructure sectors achieve a critical baseline of cyber resilience. They align with the NIST Cybersecurity Framework (CSF) that organizes its recommendations in six simple functions: govern, identify, protect, detect, respond, and recover.

Cloudflare solutions address and speed the implementation of recommended cyber controls, including:

Identify

- Manage asset inventory
- Mitigate known vulnerabilities

Protect

- Separate privileged and user accounts
- Employ phishing-resistant multi-factor authentication (MFA)
- Implement strong and agile encryption
- Strengthen email security

Detect

- Catch relevant threats

Respond

- Conduct incident reporting

These recommendations help prioritize the right investments that achieve the most immediate and highest-impact security outcomes.

Adopt the NIST CSF to manage your cyber risk.

A minimum baseline is just that — the bare minimum. But for critical infrastructure organizations, the real goal is managing cyber risk efficiently and effectively. The NIST CSF has long been the gold standard for this, and Cloudflare's platform maps directly to the CSF's core functions so you can see exactly where Cloudflare solutions can help. For more information on this, please see Cloudflare for NIST CSF.

A more modern, secure cyber posture is within reach

With Cloudflare solutions, critical infrastructure organizations:

- Immediately reduce risk by protecting against phishing attacks, malicious links, and harmful content.
- Progress faster toward the cyber essentials that every critical infrastructure organization must achieve.
- Manage cyber risk with discipline by accelerating NIST CSF adoption and maintaining progress.
- Achieve measurable efficiency, productivity, and return on investment.

Relentless cyber attacks on critical infrastructure, combined with geopolitical instability, increases the urgency for our nation's critical infrastructure organizations to act now. It requires more than just stronger locks — it demands smarter architecture and an achievable way to get there. Cloudflare gives public utilities, manufacturing plants, ports, hospitals, transportation networks, and other critical infrastructure organizations the solutions they need to defend what matters most.

To learn more about how Cloudflare can help modernize your organization's networks, go to cloudflare.com/public-sector/.

REV:BDES-7778.2025JUL07