SASE: Deliver Cloudflare anywhere with ZPE Systems' Services Delivery Platform

Summary

Cloudflare One provides Secure Access Service Edge (SASE) and Zero Trust Network Access (ZTNA). This industry-leading solution is trusted worldwide to provide enterprises with secure connectivity for their distributed workforces. The challenge is that many devices and solutions lack native support for the service. This leaves critical systems — from work-at-home networks, to healthcare machines, industrial control systems, and PoS systems — suffering from unreliable connectivity and poor security.

ZPE Systems' Services Delivery Platform solves this challenge by extending Cloudflare One across environments. ZPE's Nodegrid devices interface with a wide range of physical and virtual solutions, serving as the SASE on-ramp anywhere they are deployed. This brings reliable connectivity to locations small and large, while unifying the security posture with enterprise-wide ZTNA functionality. Cloudflare One hosted on the Services Delivery Platform makes SASE easy to deploy anytime, anywhere.

Cloudflare Overview

Cloudflare is well known as a global network built for the cloud. Cloudflare operates one of the largest networks in the world, serving an average of 45 million HTTP requests per second and powering internet requests for millions of websites. The company has data centers and PoPs in almost every country and a dedicated backbone network that spans the globe. Customer security is a cornerstone for Cloudflare.

Cloudflare One is the company's SASE/ZTNA offering, which offers fast, reliable, and secure connectivity for distributed workforces. This solution allows IT administrators to easily build, enforce, and monitor security policies across enrolled devices. Enterprises use Cloudflare One to deliver Cloudflare's expertise in security and visibility to their global fleet.

Problem – Many devices remain outside of Zero Trust

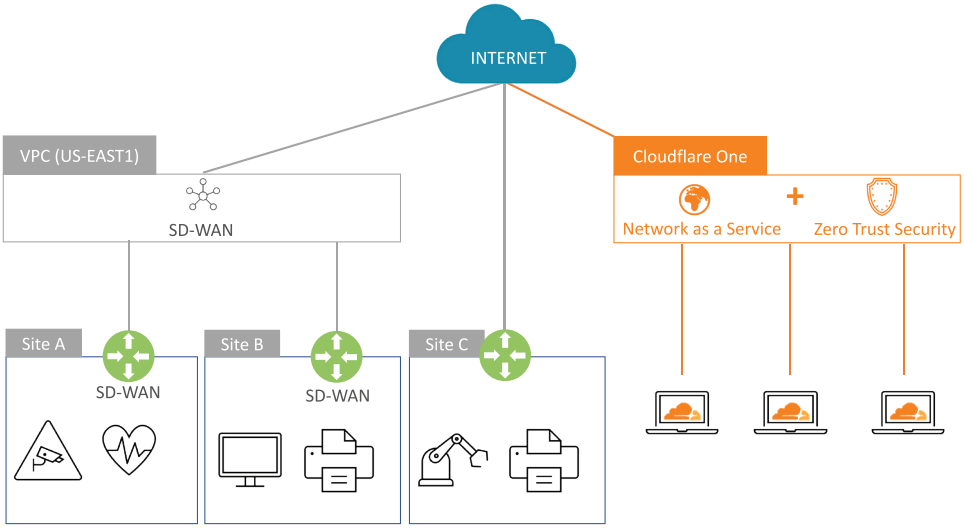
Achieving Zero Trust Security means segmenting the network and applying specific security policies to devices and users. This allows for enforcement of MFA, for example, when a user attempts to access company resources from their home network. The Zero Trust model aims to limit lateral movement and contain the damage in the event that an attack is successful.

The problem is, administrators trying to integrate SASE/ZTNA are forced to leave many areas of their networks outside of the Zero Trust umbrella. This is because most SD-WAN and branch gateway solutions are unable to host the required SASE agents. This not only fractures the enterprise's security posture, but also increases the operational overhead as IT teams are forced to monitor and maintain many distributed solutions.

Gap – 50% of IT can't run the Cloudflare One agent

Cloudflare One works well if the end device can install the Cloudflare One agent. However, more than 50% of network-connected devices aren't laptops or mobile devices, consisting of appliances like printers, sensors, cameras, and building management systems that are unable to run agents.

This is the gap that administrators face when integrating Cloudflare One into their environments: How can IT secure an entire site, including headless IoT/OT devices, using Cloudlfare One?



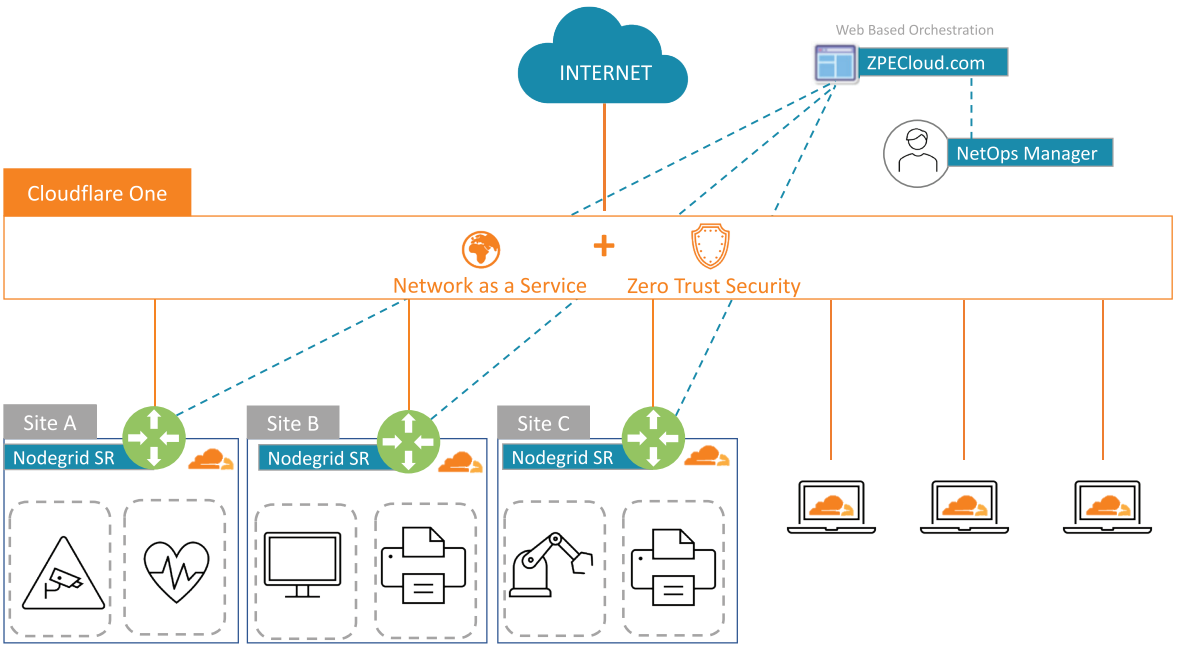
For example, printers, healthcare imaging devices, and building management systems unable to run the appropriate agent do not fall under the Zero Trust umbrella. Therefore, access to these devices can't be controlled, leaving them exposed to third-party or internal attackers. These systems force enterprises to break the Zero Trust model by defining exceptions and neglecting to integrate devices altogether.

SD-WAN gateways and branch/edge routers can't solve the problem, since the required agents can not be installed or configured appropriately on these appliances.

ZPE Systems' Services Delivery Platform Extends Cloudflare One to Every Network and Device

As a trusted Cloudflare partner, ZPE Systems provides the on-ramp to Cloudflare One SASE with the Services Delivery Platform. This allows enterprises to extend Cloudflare One to devices that can not natively run its agent. This joint solution is designed to enable easy SASE deployments and deliver ZTNA functionality across environments.

The solution components include ZPE's Nodegrid devices and ZPE Cloud. At each location, enterprises can install a Nodegrid device, which can directly run the Cloudflare One agent. IT teams can then use ZPE Cloud as their central control point, capable of deploying the Cloudflare One agent to their global fleet of Nodegrid devices.

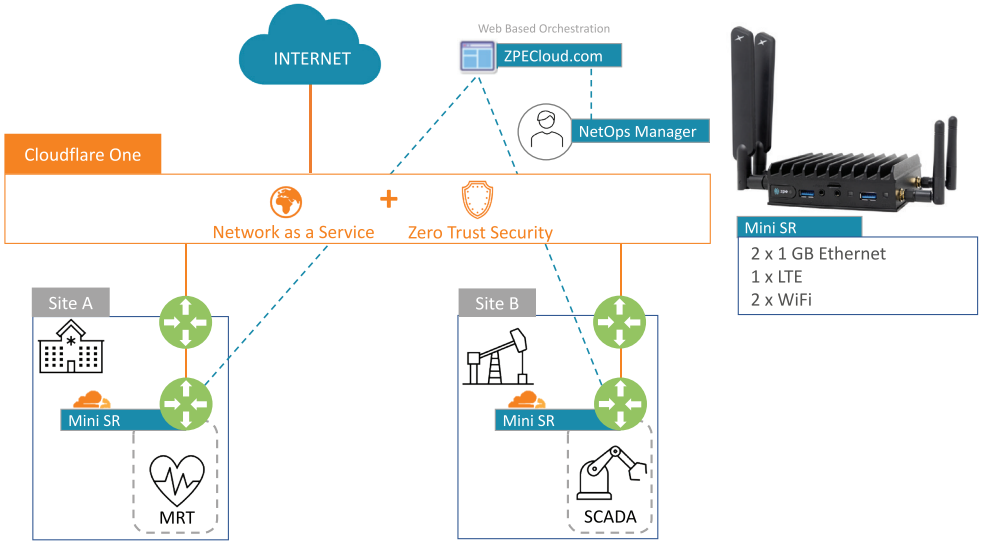


The Nodegrid device family provides a wide range of LAN and WAN connectivity, which ensures that end devices and users are always able to connect to Cloudflare services. All Nodegrid devices enforce security from the hardware level up, with full data encryption at rest, securing of secrets in TPM 2.0, and validation of a signed Nodegrid OS. Only trusted hardware and software can run on each appliance. Nodegrid devices also provide a wide range of environmental support for deploying and extending Cloudflare One to any location.

Because the Cloudflare One agent can be easily deployed from ZPE Cloud, enterprises gain the flexibility to adapt this joint solution to any use case.

Protecting critical systems

Building management, industrial control, and medical systems



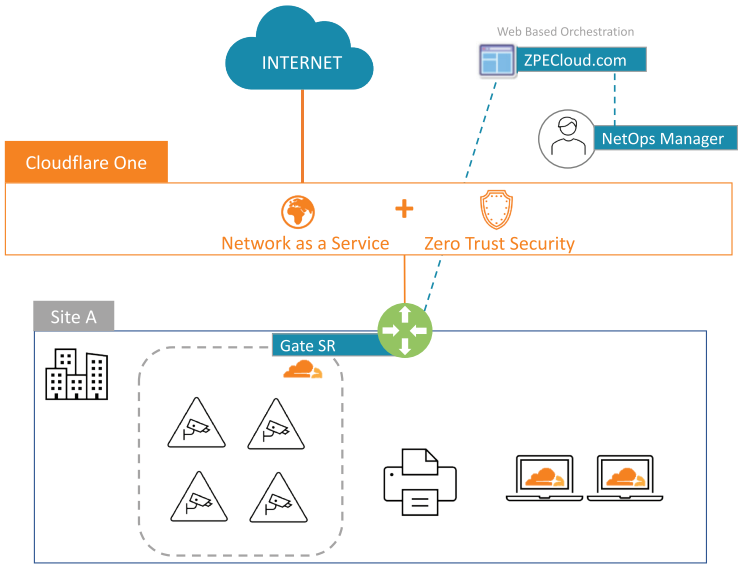
Mini SR
2 x 1 GB Ethernet
1 x LTE
2 x WiFi

Security of critical systems is often a challenge for organizations. Control software often has a long lifetime, but the required support tools become outdated and insecure. For example, many control systems still run on outdated versions of Windows, which require insecure RDP connections.

To protect these systems, IT teams deploy the Nodegrid Mini SR device running Cloudflare One. This ensures all traffic is routed through Cloudflare One, where the access and control policies are monitored and enforced.

Protecting device groups

Security cameras, IoT sensors, PoS, and more



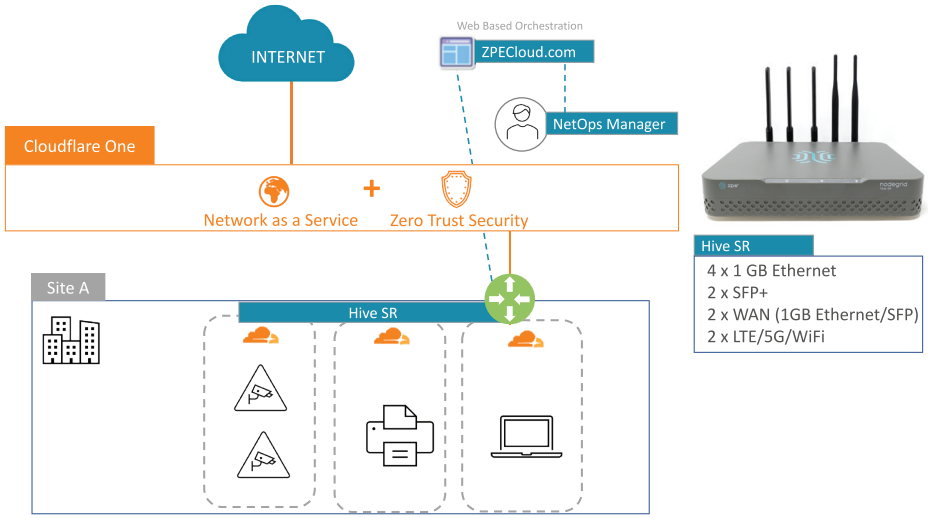
Gate SR
9 x 1 GB Ethernet
2 x SFP+
4 x PoE
2 x LTE/5G/WiFi

Devices are often grouped together, especially when they provide similar functionality and have the same security policies. Examples include security cameras and Point-of-Sale solutions at a branch location.

In these situations, devices can be separated on the network layer by using VLANs or connecting directly to a Nodegrid switch interface. A single Cloudflare One agent will be deployed for a dedicated VLAN or a group of connected devices. This gives administrators an easy way to apply a single ruleset to a specific device group.

Protecting different device groups

Small offices with cameras, printers, local storage, and more



Most enterprises have small branch offices or edge locations that must be managed. A wide range of device types are typically deployed at these locations, each requiring a different security profile. By directly connecting these devices to a Nodegrid appliance — or by separating them through VLANs and the deployment of multiple agents onto a single Nodegrid appliance — IT teams can easily associate each device to a specific security profile, and separate and enforce each device or device group's security policy.

Deliver Cloudflare One anytime, anywhere with the Services Delivery Platform

ZPE Systems' Services Delivery Platform provides a scalable and secure SASE on-ramp solution for devices that can not natively run Cloudflare One. Because Nodegrid devices come in many sizes, customers can on-ramp SASE/ZTNA in any environment, and remotely manage their global fleet via ZPE Cloud. They can maintain their Zero Trust Security approach while keeping operational costs down.

Protect your distributed IT environments with ZPE Systems and Cloudflare. Set up your personalized demo or POC at zpesystems.com/contact