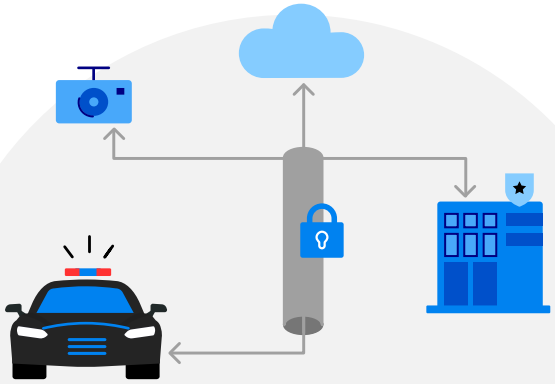
Zero trust security across the attack surface

ERICSSON

The ever-expanding enterprise network attack surface has ushered in the zero trust era. Zero trust security solutions aim to minimize the spread of breaches by condensing that attack surface — all based on the elimination of default access. Zero trust strategies range from VPN alternatives to secure remote access for employees and third parties to protecting users from malware and phishing attacks.



Scalable VPN alternative

Replace your aging VPN with a zero trust solution that limits lateral movement for a more secure connection between IoT devices, vehicles, sites, and headquarters — explicitly defined by policy, not by default. Zero trust enables simpler setup and management while eliminating east-west default access in the case of a breach.

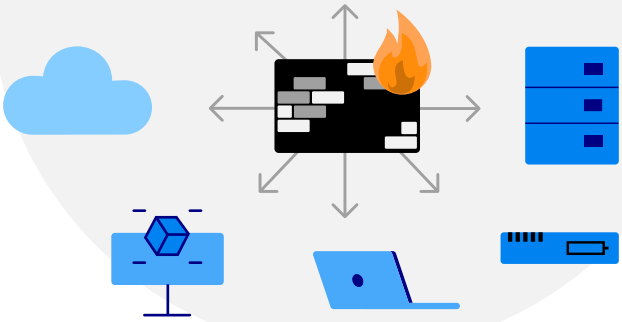
ZTNA for secure remote access

Use zero trust network access (ZTNA) to give employees (with a client) and third-party contractors (clientless) right-sized access to the right applications — anywhere.

Zero trust network

Simplified, unified firewall management

A hybrid mesh firewall delivers next-generation web filtering and IDS/IPS features while supporting firewalls in multiple form factors, including virtual machines and firewall as a service (FWaaS). It's a modern, scalable way to manage multiple firewall types through a single platform with a single policy engine.



Protection from malware and phishing attacks

A multipronged defense leverages hybrid mesh firewall, secure web gateway, and remote browser isolation (RBI) for strong protection of users accessing the web. RBI confines potential web attacks in remote cloud containers and delivers a safe rendering of the requested website to the user. Further, websites launched from URLs in phishing emails are presented in "read-only" mode, blocking users from entering their IDs and passwords and preventing credential theft.

Learn more at cradlepoint.com