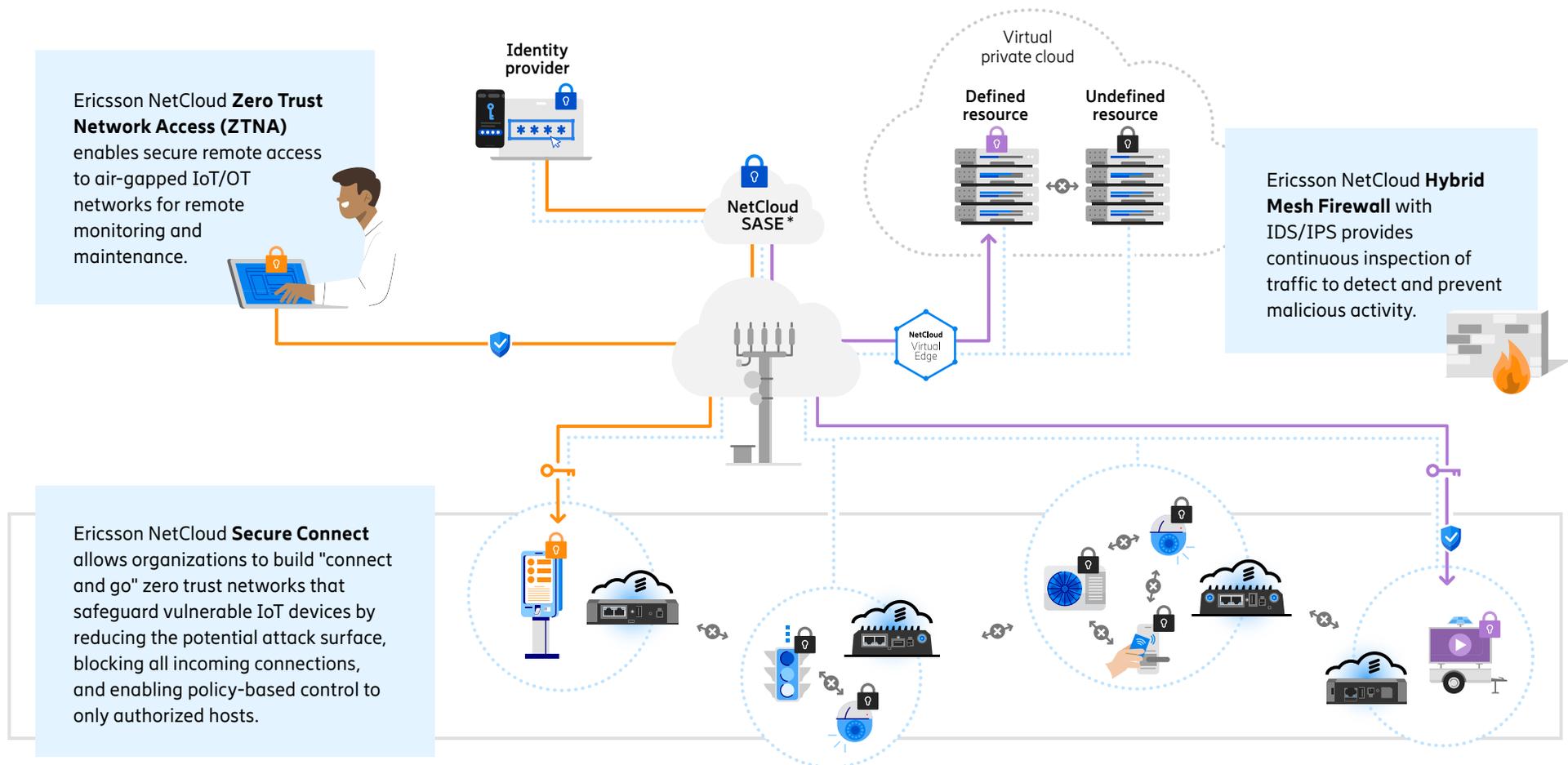# Zero trust security for cellular and hybrid IoT deployments

ERICSSON

IoT devices are inherently simple machines. They often lack onboard security or the ability to run an agent, which means these devices require protection from the network. By leveraging the right zero trust solution, IT teams and organizations can ensure IoT devices are secured in a simple, highly scalable way, enhancing their overall security posture.

Ericsson NetCloud **Zero Trust Network Access (ZTNA)** enables secure remote access to air-gapped IoT/OT networks for remote monitoring and maintenance.

Identity provider

Virtual private cloud

Defined resource　**Undefined resource**

NetCloud SASE*

NetCloud Virtual Edge

Ericsson NetCloud **Hybrid Mesh Firewall** with IDS/IPS provides continuous inspection of traffic to detect and prevent malicious activity.

Ericsson NetCloud **Secure Connect** allows organizations to build "connect and go" zero trust networks that safeguard vulnerable IoT devices by reducing the potential attack surface, blocking all incoming connections, and enabling policy-based control to only authorized hosts.

*Customer-hosted model also available

Learn more at cradlepoint.com