

**Traditional Security**

Before Zero trust, IT security follow the traditional or perimeter security model which refers to the infrastructure where the external network needs a strict access control and the internal network simply trust all the users and provide access to all the resources. This is commonly known as the “Castle-and-moat” concept where it is hard to obtain access from outside the network, but everyone inside the network is trusted by default.

By this traditional approach, the attacker once gain access to the internal network can perform a lateral movement from one device to another easily compromising the security because internal network users are configured trusted because of their location and all services are accessible to them where there is “Trust” between the users and organization.

**Trust?**

In common words trust is the belief that somebody is good, honest, sincere. We know an employee who works on our organization for many years, we believe them and grant access blindly without knowing their intentions and mistakes they done in past. We implement trust on computer systems to make the computer to do our work. “Computer Security model based on human definition of trust is inherently flawed”.

**Zero Trust**

On basis of zero trust, an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter. Users, either they are on internal or external network are not trusted and granted access to all resources. They are given minimum access to those resources which are needed to do their task, commonly known as the Least privilege. This means giving users only as much access as they need.

By zero trust, users have access to the application or resources which they are verified. Verification is implemented by many methods but the major three methods are:

* **Identify:**

Under identify, Users need to identify themselves as the authorized person, authenticate themselves to prove that they are authorized personnel, and with the correct privilege they are authorized into the network.

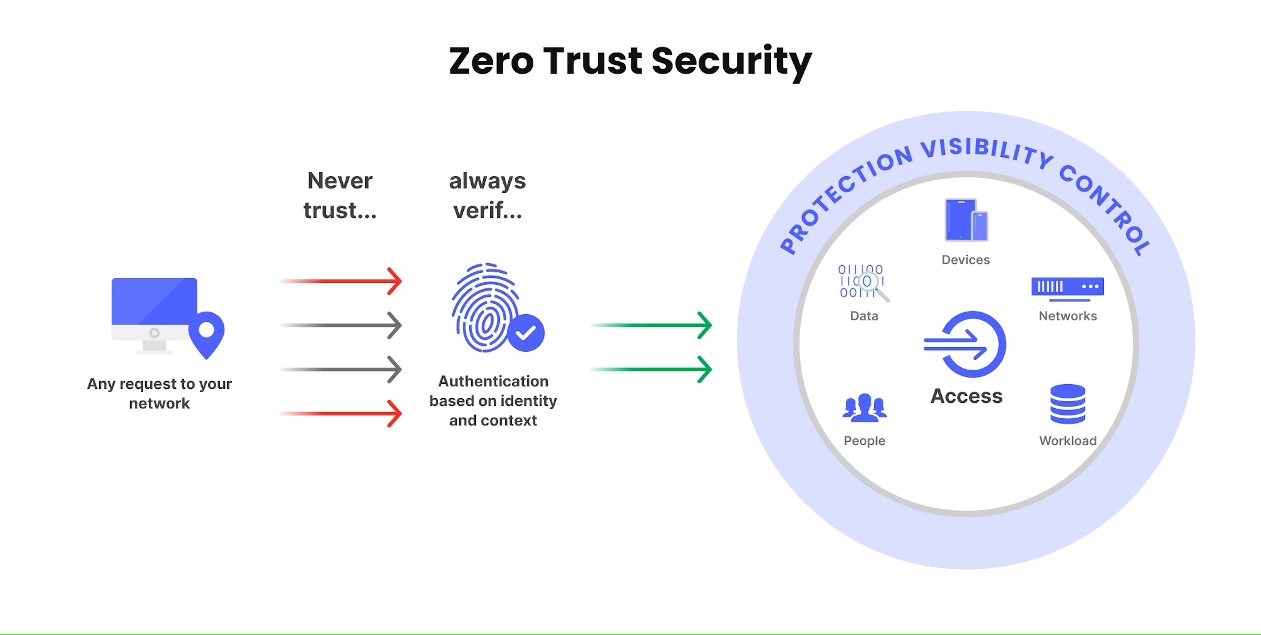
* **Context:**

How the users are trying to get into the network and by what means are determined. If the credentials are wrong, they cannot enter into the network by any cause. If verified what can the user do?

* **Security Posture:**

Security posture checks are very much important in the implementing of zero trust. How well is your machine and devices? Is the secure are not?

Answers to these questions are important to get into the network.



**Zero Trust Principle**

There are many principles which make the zero-trust model work but the major ones are:

* Never Trust, Always Verify

Without verifying the user don’t let them to access the application or the resources.

* Implement Least privilege

Give them minimum access so that they can be able to do their work properly.

* Assume Breach

Always be prepared for security breaches and keep on practicing on that avoids making big trouble when original breach happens.

**Monitoring**

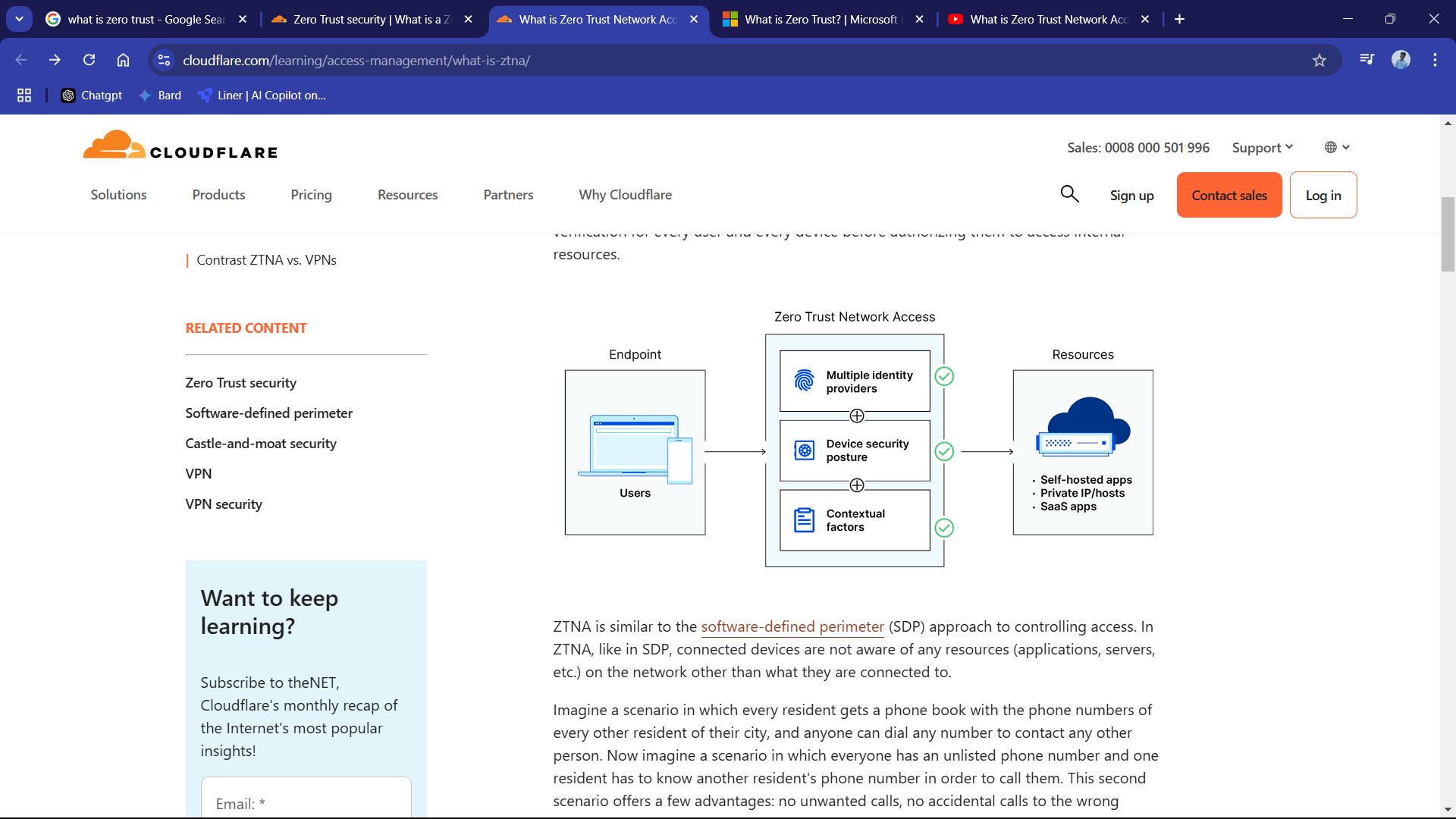
The important thing to know that zero trust never stops on just verification, once a user has been granted access, zero trust requires continuous monitoring and validation. Any changes to the identity, context or the security posture will be revaluated and revokes as necessary.

Zero trust security is a model and a mindset about how to approach network security however it is not a technology.

Zero trust Network access is a technology by which the principle of zero trust can be used to secure access to applications and resources.

**Zero trust network access**

Zero Trust Network Access (ZTNA) is the technology that makes it possible to implement a zero-trust model.



Initially ZTNS wants the user to authenticate themselves to be the authorized person (passwords, MFA).

Then the system verifies the device for specification, if the device is secure and getting the required security report from the device, then the system verifies if the user has permission to access the specific application or resource by comparing the user’s identity and device info with set policies.

Finally, the connection is established for that specific service or resource which the user authenticates for, the connection is isolated so that the other resources are not accessible by the specific user.

Throughout the session ZTNA monitors the user’s action. If something is malicious then the permissions are revoked and they need to go on for requesting again.

**Advantages**

* Enhanced Security
* Limited exposure
* Better Insider threat protection
* Supports remote work
* Reduced lateral movement