5 Guiding Priciples to Start Protecting Your IP Effectively Implementing Zero Trust Architecture

Zero Trust is the new Buzz word in the cybersecurity arena. Ever since, *Forrester Analyst, Kindervag introduced* the term Zero Trust in his article **"Zero Trust Architecture"**, traditional security measures have become obsolete.

The concept of zero trust is a security framework that is based on an ***"I Trust No One" principle;*** it doesn't matter if the user is within or outside the organization. A user is not granted access unless he/she is authenticated and authorized first.

There are five guiding principles to begin before you start protecting your IP effectively by implementing a **Zero Trust Architecture.**

1

Principle 1 - Identify which portion of your IP is the most critical

It is important to know which systems contain data that is most critical and which databases have a specific combination of sensitive data that place them at higher risk. have a specific combination of sensitive data that place them at higher risk.

2

Principle 2 - Identify which application is affected

Once you have discovered which data is sensitive, it is now time to assess the risks. You need a robust risk assessment in place. Once you know where your highest vulnerabilities lie, you would be able to shape your security plan.

3

Principle 3 - Identify the user

The next principle is to identify the user. Authenticating users, knowing who they are, where they are, and how they are accessing your applications and networks is important to adopt Zero-Trust security.

4

Principle 4 - Identify if access is necessary

Organization should determine who needs access and ensure that they access the information to only what they need and not every other detail present in the system. This can be ensured by enforcing access control.

5

Principle 5 - Identify what happens to the data once it is accessed

Once a breach is noticed, it is important to quickly contain it. Investigate and assess the damage done. Once the damage is identified, notify the concerned users including third-party vendors.