Zero Trust in a nutshell

By Fudo Security

Trust is everything.

Organizations and businesses cannot live without it, and it is implicit in daily business activity. In the relationship between vendor and client, it should be sacrosanct, yet, more often than not, trust is abused, disregarded, and in many cases, lost.

The central assumption of Zero Trust Network Access is that users in the system begin their access journey with the lowest possible level of authorization and ensure that everything is verified at every step... This infographic will show that this type of approach gives organizations the best chance of winning the fight against attacks.

What exactly is Zero Trust?

Zero Trust is not just a simple solution or add on which can be integrated overnight.
It is a strategic initiative that helps mitigate and ultimately prevent data breaches by getting rid of the concept of trust from an organization's network architecture.

A common sentence that accompanies the concept is **"never trust, always verify".** One of the core principles of Zero Trust is the notion that

network segmentation is key, and therefore lateral movement within a network perimeter is not allowed.

The three pillars of a Zero Trust:

1. Making sure that all company resources are able to be accessed securely, irrespective of location.
2. Using and administering a least privilege strategy, as well as enforcing access control. Remembering that at the core of Zero Trust is the idea that every user is perceived as untrusted.
3. Auditing and monitoring all data traffic. The concept is based on the fact that even those within the perimeter may cause problems, such as insider misuse.

Some key facts

By 2022, 80% of new digital business applications opened up to ecosystem partners will be accessed through zero-trust network access (ZTNA) [1]

By 2023, 60% of enterprises will phase out most of their remote access virtual private networks (VPNs) in favor of **Zero Trust Network Access** [2]

Nearly 60% of attacks involve lateral movement [3]

77% of IT professionals believe that network segmentation can help prevent server compromise [4]

1 https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access
2 https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access
3 VMWare
4 https://www.sans.org/reading-room/whitepapers/networksecurity/paper/38030

How do you implement Zero Trust Network Access in a company?

This architecture is not associated with any specific technology. It can be used in both network administration and software development. We then assume that our system components should have limited access.

Suppose that one would like to apply Zero Trust architecture in their organization. In that case, one should assume that everything outside the company, and above all within the organization itself, is potentially vulnerable.

Therefore, the user with broad access should be avoided and any individual access to network resources must be verified. It would even be recommended to go one step further. **Not only to verify access to individual systems but also to individual actions performed on these systems.**

Zero Trust Network Access also assumes continuous verification. This means that all user actions should be recorded and analyzed – this will enable faster detection of attacks and mitigate their effects.

Zero Trust architecture is poised to be the future of the IT security industry. It will provide organizations with transparency regarding employee activities, accountability and even mitigate against costly errors.

Fudo PAM as a critical layer of ZTNA

1. Firstly, Fudo PAM's built-in multi-factor authentication schemes (MFA) takes the security model to a new level without the hassle of setting it up on several systems at once.
2. Secondly, the user does not have to know the server or web console password. However,the user is still able to access the service without any confusion hence another win for keeping true to the Zero Trust approach – everything is kept seamless for the user.

With the user sessions being recorded and analyzed in real-time with biometric-based AI, an advanced security orchestration is created based on session archiving and it constantly checks the user – once again, demonstrating a Zero Trust principle.
Furthermore, Fudo PAM's agentless approach makes all of this easy to set up and fast to deliver.

FUDO SECURITY
marketing@fudosecurity.com
fudosecurity.com