TRUST NO ONE:

The re-emergence of Zero Trust

FUDO SECURITY

Trust is everything.

Any organization or business 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.

Once there is a data breach, misconfiguration, or a hack, be it intentional or by accident, the consequences to the relationship between customer and vendor are shattered. Once the damage has been done, the result can come in the form of painful financial loss or a permanent stain to brand reputation.

Once the damage has been done, the result can come in the form of painful financial loss or a permanent stain to brand reputation.

DID YOU KNOW...

The term Zero Trust was first coined by John Kindervag in 2010. Kindervag was VP and principal analyst at Forrester Research. Now a decade later, the term has seen a resurgence in the cyber and Infosecurity community as a way of addressing the need for better security.

With the average cost of a data breach numbering **$3.86 million** according to the most recent study by IBM and the Ponemon Institute[1], there is increasing pressure to stop sophisticated attacks and prevent breaches. **So how does the world move forward and address this serious security gap?**

[1] www.ibm.com/security/digital-assets/cost-data-breach-report/#/

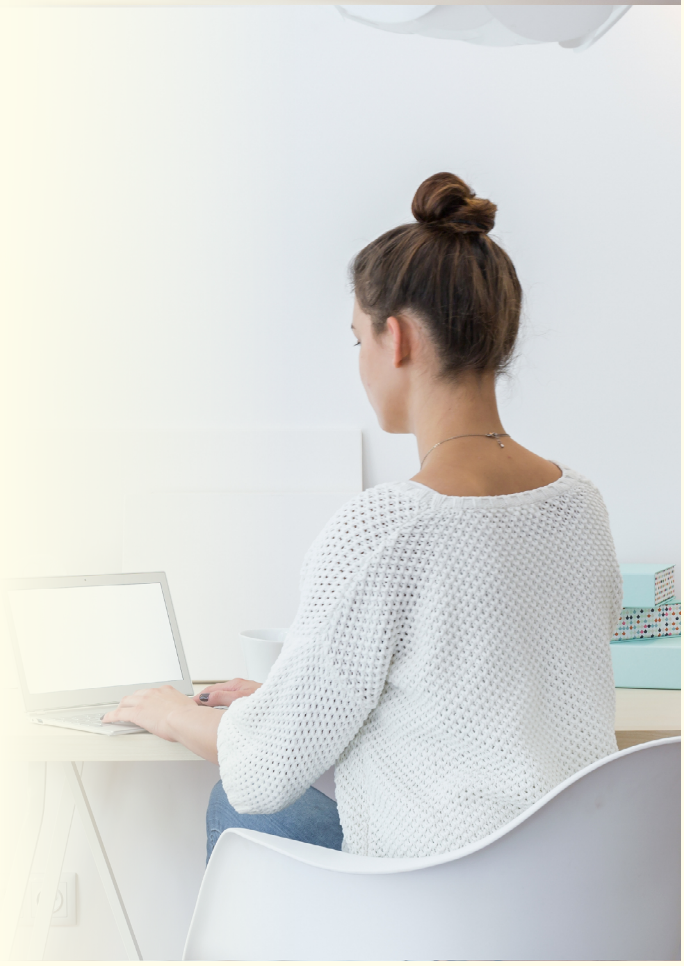
The focus is not on some new form of technology but in fact, something that has been around for several years.

What 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.

> **“Never trust, always verify.**



Up until recently the modus operandi for many organizations was that once within a network perimeter, a user could be trusted. This is the key differentiation for Zero Trust, as it foresees access for users only on the basis of least privilege. In essence, one only is given as much access to what someone needs to complete their task, nothing more, nothing less.

In essence, a thorough Zero Trust strategy is built on three main pillars:

Making sure that all company resources are able to be accessed securely, irrespective of location.

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.

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.

Fudo PAM can add valuable procedures and relieves administrators of the hassle of configuring accesses individually, even in an Active Directory environment. With Fudo PAM's User Access Gateway, one can leverage a single sign-on approach to multiple servers and systems, including web-based management consoles.

There are a few powerful points about Fudo PAM worth mentioning.

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.

Secondly, **the user does not have to know the server's or web console's 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.**

There may already be several layers of security in place, and many organizations may dismiss Zero Trust as just another marketing buzzword from the infosec industry.

> **...Fudo PAM's agentless approach makes all of this easy to set up and fast to deliver.**

So why does Zero Trust matter so much?

There are a number of reasons, though the most powerful will be of course this staggering statistic:

Cybercrime will cost the world a whopping $ 10 trillion by 2025[2].

Anything that we can do to improve how we work, and optimize the way we perceive access security will go a long way to bring this number down.

It is the right time for Zero Trust, given the additional strains put on companies and individuals during the pandemic, the crisis now needs an answer.

It certainly cannot be implemented overnight, and Zero Trust is as much a strategic decision as a technical one. Fudo PAM serves an integral part in the entire Zero Trust journey, it is part of many other components and pieces that an organization must adopt to have a comprehensive Zero Trust architecture in place.

Though with the success of introducing and utilizing Zero Trust in your network, it will enable a seamless transition to better security for everyone.

Sascha Fahrbach

Fudo Evangelist and digital influencer.

He engages himself globally to spread cybersecurity awareness and the importance of PAM solutions to all organizations. He hosts various digital events for Fudo Security for a global audience. He's a media facilitator, hosts Fudo's podcasts, conducts interviews and runs dynamic security webinars. He's also a regular guest at a Central European TV broadcaster.

[2] cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

fudosecurity.com

Zero Trust Network Access

Deployable in a single day.

☎ US: +1 (408) 320 0980
EMEA: +48 22 100 67 00
DACH: +49 911 - 30 91 80

sales@fudosecurity.com

FUDO SECURITY