DeviceAssure

ZERO TRUST EXPLAINED – BUT WHAT ABOUT BYOD?

With the rise of "Zero Trust" implementation into IT networks we take a look at its definition, why it's on the rise, key benefits, basic components and a key risk that can be solved with effective real-time device authentication.

What Is Zero Trust?

The term "Zero Trust" was coined by Forrester Research Inc. in 2010. The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, notes that "Zero Trust refers to an evolving set of network security paradigms that narrows defenses from wide network perimeters to individuals or small groups of resources." In other words, and to oversimplify, the Zero Trust concept shifts access controls from the network perimeter to individual users and devices.

Why The Rise In Zero Trust?

The increasing number and cost of data breaches are adding pressure on businesses to take necessary actions to mitigate risk. In 2018, a typical data breach cost a company $3.86M – this is up 6.4% on 2017.

Gartner notes that the old security mindset of "inside means trusted" and "outside means untrusted" is broken in the modern world of digital business. The assumption that everything behind a firewall is safe means that malicious actors that gain access can cause significant damage within a network.

With Zero Trust, however, damage via lateral movement is restricted. Additionally, less modern enterprise...

...security systems can be seen to restrict growing business trends such as the rise in remote working and the bring your own device (BYOD) movement.

An increasing number of businesses want to enable their employees to easily and quickly access required business resources from their own devices at any time, in any location. Enabling this in older security systems can be cumbersome and, when implemented, the user experience can be less than ideal.

Key Benefits Of Zero Trust

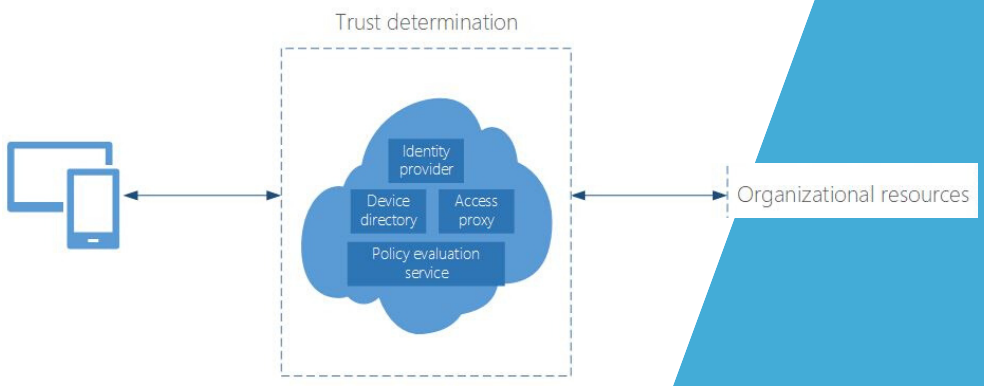
Akamai (a leading content delivery network services provider for media and software delivery, and cloud security solutions), highlights the following 6 business and security benefits of Zero Trust:

1. Protect your customers' data and your business
2. Reduce time to breach detection and gain visibility into your enterprise traffic
3. Reduce the complexity of the security stack
4. Solve the security skills shortage
5. Deliver both security and an excellent end-user experience
6. Facilitate the move to the cloud

Get further details on Akamai's 6 business and security benefits of Zero Trust on their website, here.

Basic Components Of A Zero Trust Network Model

In his presentation at RSAConference2019 titled "No More Firewalls! How Zero Trust Networks are Reshaping Cyber Security", Matt Soseman (Security Architect, Microsoft) described the basic components of a Zero Trust network model using the following diagram:



Source: Microsoft via RSAConference2019 – YouTube.com.

As can be seen above, devices can access certain organizational resources when trust has been established. Trust is dynamic and is determined via different components including an identity provider, access proxy, policy evaluation service and device directory.

Example Of A Zero Trust Model:

Google's BeyondCorp initiative implements a Zero Trust security model. Now open to the wider market, BeyondCorp was originally used by Google to enable their employees and contractors to work from anywhere, from any network, without the use of a VPN. Google has documented and published BeyondCorp research, from concept through to implementation – these papers describing their new approach to enterprise security can be accessed, here.

– BYOD Limitation

Gartner, in their Market Guide for Zero Trust Network Access, recommends that security and risk management leaders responsible for secure network access should "support unmanaged devices for employees". However, as noted in the paper A New Approach to Enterprise Security, "BeyondCorp uses the concept of a 'managed device,' which is a device that is procured and actively managed by the enterprise. Only managed devices can access corporate applications. A device tracking and procurement process revolving around a device inventory database is one...

...cornerstone of this model."

A focus on Managed Devices ignores the BYOD trend and can lead to an assumption that any already procured device is authentic. The provenance of the devices themselves don't appear to have had much consideration in many Zero Trust solutions.

Counterfeit Devices, BYOD And Zero Trust

Counterfeit devices can come with pre-installed malware, fake security and compromised operating systems while still appearing as genuine – learn more about the anatomy of a counterfeit phone, here.

DeviceAtlas, a sister product offering of DeviceAssure, predicts a growth in counterfeit devices in 2020 and beyond. DeviceAtlas noted that "a study by the OECD and the EUIPO, published March 2019, highlighted a growing trend in the trade of counterfeit and pirated goods. Counterfeit devices, according to an EUIPO-ITU study published in 2017, represent close to **13% of mobile phones sold** globally."

The increasing number of inauthentic devices combined with the growing BYOD trend could mean that many Zero Trust based enterprise security models can be compromised from the outset. This might be why BeyondCorp and many Zero Trust network solution providers focus on Managed Devices and do not address BYOD.

Enabling BYOD Within Your Zero Trust Model With Device Authentication

The negative impact caused by inauthentic devices on Zero Trust networks, in theory, should be less compared to more outdated network security architectures. However, with the rise of BYOD combined with the ever-increasing number of apparently genuine inauthentic devices appearing on the market, enterprise security systems (even those with Zero Trust models) are at a growing risk from IT security-oblivious, bargain hunting employees.

With the advent of BYOD, the challenge for security and IT personnel as well as Mobile Device Management and Enterprise Mobility Management organizations, is to ensure that devices used by employees are secure and pose no risk to the enterprise security. To help mitigate risk while facilitating BYOD, it is increasingly important to authenticate devices in real-time.

DeviceAssure offers a transparent way to validate the authenticity of devices used on enterprise networks and services to mitigate security risks from rogue devices – learn more about how we can enable you to accurately identify counterfeit devices in real-time, here.

DeviceAssure