

'Zero Trust' authentication is still evolving and developing new strengths by going another step further in authenticating the computer device the user is accessing. The use of bring your own device (BYOD) has been responsible for a lot of cyber and data breaches over the years and so by identifying the machine the user is accessing delivers another layer of security.

Zero Trust environments warrant having individual machine and or device identities to verify which is being used by which employee. Having a firewall is all well and good but now that most firms have multiple machines in and outside their office walls, especially as so many employees are working from home today, this is now not enough.

Creating a stronger sense of security that is real and active promotes greater productivity as well as delivering a deep and lasting security taken from a zero trust platform. In an increasingly mobile and digital world where almost everything is transmitted digitally and more often than not, from outside the comparative safety of the office network and cloud systems, zero trust protocols need now to persist.

Placing emphasis on the user as the driver for who accesses the firm's systems, moves the right of access to the individual credentials of the employee and the machine or device they are using. This delivers frictionless access to what the employee needs, wherever and at whatever time on the office Cloud service and or local databases to perform their job more productively.



On a Zero Trust platform everyone is treated the same – with suspicion. Until a user can prove who they are through a software defined perimeter (SDP), access will not be granted. A Zero Trust platform can be applied to the Cloud, Webservers, mobile phones, travelling sales reps and homeworkers with each required to confirm:

1. their identity – authentication
2. they are on a sufficiently secure connection
3. they are authorised to access the resources they need
4. which device they want access from
5. where they are – on a business network or café wi-fi

By treating employees with respect and confidence the zero trust regime gets on with doing its job of ensuring users prove themselves worthy of access, to deliver stricter cyber and data security for the firm and all its employees.

For further information about zero trust platforms

Phone: 01342 301325

Email: thebureau@the-bureau.co.uk