FROM ZERO TO HERO: MAKING ZERO TRUST HAPPEN

How confident are you that your mainframe systems and data are as protected and secure as they should be?

I saw recently that the global zero trust security market is predicted to grow from USD19.6 billion in 2020 to USD51.6 billion by 2026, with the data security segment now leading the market. There's a reason for that growth.

Zero trust is not an individual tool or a single platform. It's a strategy, a security framework founded on the notion of "never trust, always verify" – or in simpler terms, "don't trust anyone". Nor is there an end point (pun intended) with the zero trust model. It's an ongoing journey, a state of being that needs refreshing, updating, and nurturing. When you consider the enduring popularity and pervasiveness of the mainframe – its role as the system of record and mighty transactional "beast of burden" – it does seem that applying a zero trust approach in this world is long overdue.

In the latest BMC Annual Mainframe Survey, Security and Compliance were identified as the top mainframe priorities by most survey respondents. In fact, 'Security' over-took 'Cost Optimization' as the leading priority for the first time in the survey's 15-year history. It's very encouraging. And zero trust is the future we should be working towards, from access rights, password policies and insecure applications to overprivileged users, the threat of unencrypted communications and more.

One of the basic issues is that READ access is so often the norm. In reality, default access should be NONE. I believe it's simple commonsense that you shouldn't automatically trust *anyone and anything*, inside or outside your perimeters. The most appropriate course of action is to *verify everyone and everything*. For some years, I've been advocating the principle of least privilege (PoLP). Least privilege is simply about restricting access and permission rights for users, accounts and processes to only those resources that are absolutely necessary to carry out routine, authorized

tasks. While that might be a significant change in mindset for some, the equation for me is a simple one:

Authenticating everybody + least privilege for all your data access, systems and applications = Zero Trust Security for your mainframe shop.

Organizations should also be looking to improve their threat detection and response capabilities. Ask yourself the question, is an approach that utilizes endpoint detection and response (EDR) and managed detection and response (MDR) still enough in the "new normal" landscape of mass home and remote working? As we all know, the coronavirus pandemic and shift to home working has exposed the vulnerability of companies, individuals and nations to rising levels of cybercrime.

Extended Detection and Response (XDR) cyber security technology is coming to the fore. In a zero trust world, XDR might as well mean "anywhere, everyone and everything detection response". The point is that every system, every user, every drift "from the normal" in behavior counts. The actionable threat intelligence provided through XDR capabilities could mean the difference between assured security levels or damaging hacks and data breaches.

While security should never sleep, the reality is that there simply are not enough talented and skilled mainframe security experts on the planet to constantly monitor all of our systems all of the time. That's why harnessing automation, AI and machine learning through XDR is so important. Mainframe modernization work including AI and machine learning will mean you can pick up on anomalies and exceptions extremely quickly - because you've been tracking, learning from, and so better *understanding* previously undetected patterns.

What else? Oh yes, passwords. Don't get me started on passwords. If you want to know more, you can have a read of my short paper on password insecurity, stolen credentials, data breaches and multi-factor authentication (MFA), The Problem With Passwords.

It's clear we need to continue pushing back against the complacency that still exists, and the mistaken belief that the mainframe is inherently secure "out of the box". The zero trust model is the best way to properly protect our systems and data. It's no longer enough to slavishly follow what *James Stanger of the* Computing Technology Industry Association (*CompTIA) describes as* "traditional measures based on a firewall-first, signature-based, trusted-partner mindset." He described that old-school approach as Cowboy IT: "underutilization of modern tools, over-reliance on old ones and a lack of proper monitoring." I couldn't agree more.

We need to better protect ourselves and the tools are already out there, as I've often said; it's the mindset that is perhaps lacking. And it's not as if there aren't external experts you can call on for advice and guidance, either. We're here to help. A a good starting point can be external pen testing to see just how secure you are, ideally followed by a more in-depth security assessment. The only thing you have to lose is… a leaky and potentially dangerous security posture. If you are completely secure and have nothing to worry about, it would be great to have that verified too. But can you be sure?

Zero trust is not only an excellent collaborative goal to build towards, founded on better analytics, automation and adaptiveness - it's increasingly the only game in town when it comes to security.