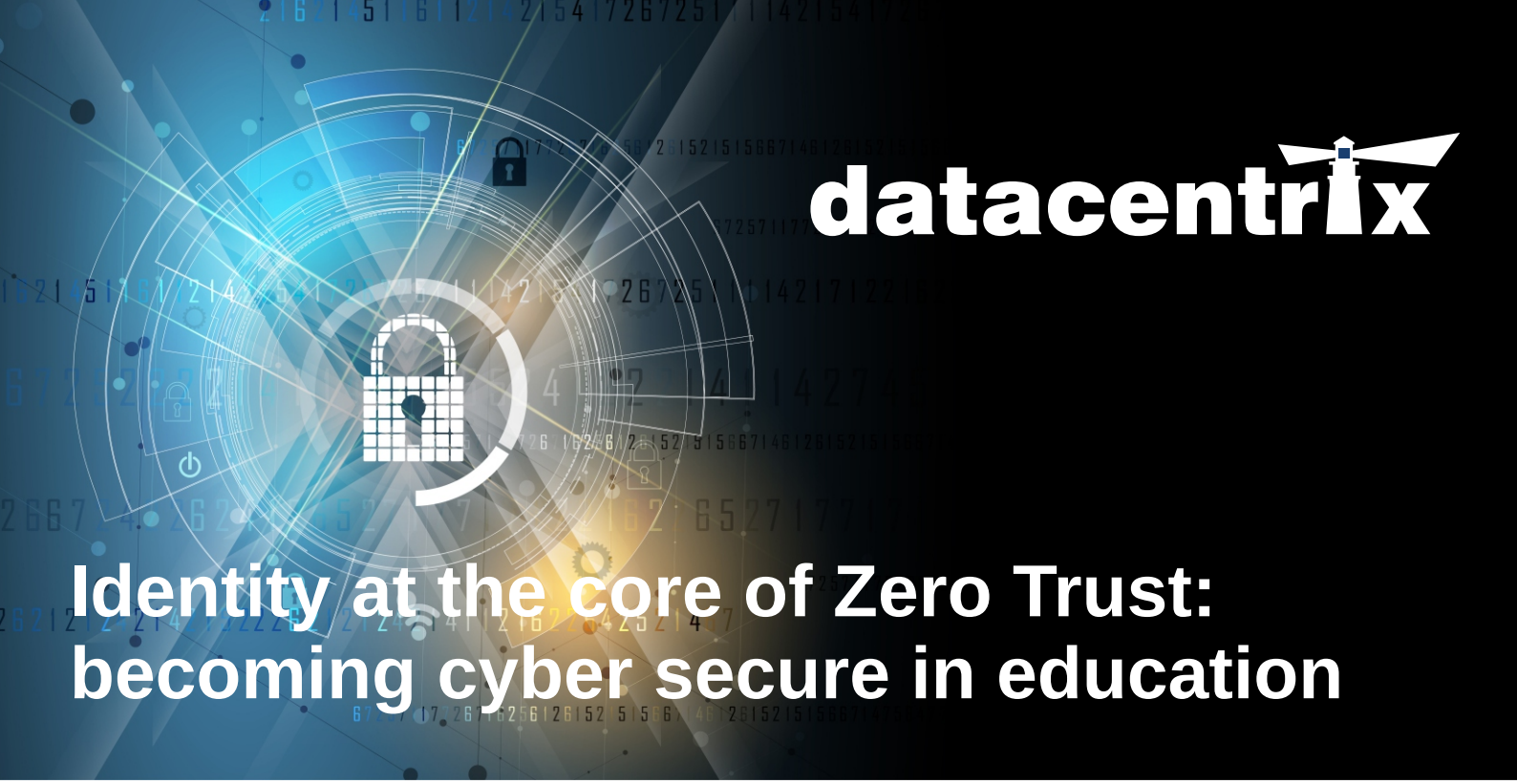

Identity at the core of Zero Trust: becoming cyber secure in education

In an age marked by an unprecedented surge in cyberthreats and data breaches, the importance of cybersecurity has reached new heights. Organisations worldwide are grappling with a mounting tide of cybercrime, with estimates from Cybersecurity Ventures projecting that cybercrime will cost the world a staggering $8 trillion in 2023; a number expected to soar to $10.5 trillion by 2025.

It's a daunting reality that no one can afford to ignore, regardless of their geographic location. The fact that businesses in Africa are not immune to this cybercrime deluge was a point under discussion at a recent joint Higher Education Information Technology South Africa (HEITSA) event with Datacentrix, a leading hybrid ICT systems integrator and managed services provider.

The organisation looked at the controls, processes, and technologies that African businesses can put in place to help mitigate this risk as we move into a new era, in particular exploring the Zero Trust model as a transformative approach.

The evolution of Zero Trust

“Zero Trust has evolved into a comprehensive framework, with identity as its central pillar,” explained Francois Jacobs, Business Unit Manager at Datacentrix. “That is, knowing who someone is, where they are coming from, and how they are attempting to access data. Within the context of higher education and other sectors, the management of identities can present unique challenges and opportunities.”

The concept of Zero Trust originated in 2004 when the notion of 'access control' was introduced. This initial approach focused on device health and the origins of network traffic to segregate and grant access. However, it was a very network-focused approach, he stated. “It wasn't until around 2010 that the model expanded to encompass identity and data, moving beyond the network as the sole vector of trust.”

By 2014, the first real vendor solutions emerged, encompassing the core pillars of Zero Trust: identity, network and device, and data. Major companies like Google and Microsoft played pivotal roles in shaping the Zero Trust landscape. In the late 2020s, assessment models and practical guidelines – such as ZTX, the Zero Trust security framework from Forrester – further fuelled Zero Trust adoption.

> Zero Trust has evolved into a comprehensive framework, with identity as its central pillar. That is, knowing who someone is, where they are coming from, and how they are attempting to access data. Within the context of higher education and other sectors, the management of identities can present unique challenges and opportunities.

“These steps provided the guidance that businesses needed on how to practically implement Zero Trust, as well as empowering the vendors in building the tools for organisations to use,” Jacobs continued, adding that the last big push for Zero Trust adoption was during the COVID period, driven by remote and hybrid working.

Zero Trust, as we know it today

According to Jacobs, many of these key Zero Trust principles have their foundations in identity. “However, in today's context, considering the concept of assumed breach and trusting no-one until they have verified themselves in some authoritative way, it must be extended to include other important areas.”

> The landscape of cybersecurity is rapidly evolving, and Zero Trust has emerged as a powerful model to protect against the rising tide of cyber threats. It places identity at its core, necessitating robust identity verification, strong authentication, access controls, and governance practices.

Thus, Zero Trust, as we know it today, revolves around five core pillars:

- **Identity**: Knowing an individual's identity beyond a shadow of a doubt is the first pillar. This encompasses authentication and authorisation practices that apply token-based or multi-factor authentication methods.
- **Telemetry and analysis**: It is crucial to understand where an individual is coming from, the type of device they're using, the data they are trying to access, and the workload they are attempting to access. This provides the foundation for trust decisions.
- **Data access**: Zero Trust requires a comprehensive view of who is trying to access data and under what conditions. This ensures that data remains protected against unauthorised access.
- **Automation and orchestration**: These technologies enable real-time or near-real-time trust decisions and actions, ensuring that the security posture remains robust, and adequate action can be taken when needed.
- **Governance**: Maintaining detailed records of who had access to what resources, and for what reasons, is essential for Zero Trust.

Francois Jacobs, Business Unit Manager at Datacentrix

Challenges and opportunities in higher education

Implementing Zero Trust in higher education can present unique challenges, but can also be fruitful in many ways, said Jacobs. “Firstly, the scale and diversity of identities within higher education can be complex when compared to enterprises in other sectors, where you would typically find full-time employees and contractors, as well as long-term vendors and so on. Higher education institutions have a diverse array of identities, including students, faculty, administrators, and even visiting professors and examiners. Managing the lifecycles and verifying the identities of individuals that don't exist in strong, authoritative sources of identity can be a significant challenge.”

Adoption resistance with regards to new technologies can be another hurdle, particularly in a setting where connectivity issues and remote learning can be commonplace.

“We also see, quite often, that legacy platforms are still in use within these environments, which may not support these newer methods of authentication and analysis and identity management systems, or the required telemetry to support the Zero Trust framework.”

On the flip side, the shift towards cloud-based learning platforms and hybrid education has provided a unique opportunity for the adoption of Zero Trust within higher education, as it allows for better validation and verification of users, like those visiting professors, who fall outside the network perimeter.

The landscape of cybersecurity is rapidly evolving, and Zero Trust has emerged as a powerful model to protect against the rising tide of cyber threats. It places identity at its core, necessitating robust identity verification, strong authentication, access controls, and governance practices. In higher education, where diverse identities and hybrid learning have become the norm, the adoption of Zero Trust presents both challenges and opportunities.

The fundamental shift in perspective is clear, added Jacobs, namely that trust can no longer rely solely on network parameters or application-centric thinking. “The Zero Trust framework provides a comprehensive approach that empowers organisations, including those in higher education, to manage access through a lens of trust that extends to identity, context, and data.”

For more information on Datacentrix’s Managed Security solutions, please visit: www.datacentrix.co.za/security-services.html