The rise of zero-trust cyber security; unlocking the full potential of zero-trust for UK organisations and their people

Simon Moyes
Technical Services Director

Simon investigates the importance of implementing a zero-trust security model, the potential impact on people and how truly transformative zero-trust enables organisations to leave their legacy infrastructure behind.

Against a backdrop of rapid digital transformation in the post-Covid era and with increasing battles against threat factors to businesses; zero-trust policies have emerged as the ideal framework for securing enterprise users, workloads, and devices in the cloud-centric world.

A recent independent industry survey revealed that just 7% of IT professionals believe that security is at the forefront of their organisation's strategic thinking – highlighting a great need for businesses to ensure that they implement zero-trust architecture.

As businesses grapple with providing a new workplace experience and digitised infrastructure, they are relying on a range of emerging technologies such as IoT, 5G and even AI to support them, and as innovative and cutting edge as they are, businesses must broaden the lens through which they see zero-trust and digital transformation.

It is imperative for leaders focused on business growth and stability to view digital transformation as not only about migrating apps to the cloud, but to ensure that its network and security infrastructure is transformed in order to realise the full potential of digitisation – positively impacting upon the organisation and its people.

Implementing zero-trust and its challenges

Taking a zero-trust, guilty-until-proven-innocent approach sees organisations assume that active threats exist both inside and outside a network's perimeter, with on-site and remote users alike required to meet stringent authentication and authorisation requirements, before gaining access to a given resource.

Implementing a zero-trust model requires careful planning, delivery and management.

Organisations should work closely with security experts to ensure that the systems and networks are fully protected against cyber threats. And given that in 2022 UK organisations experienced an average of 788 weekly cyber attacks, it is clear why this is an essential business practice.

However, a security approach based on the principle that no network element can be trusted does present some challenges. Zero-trust requires a fundamental mindset shift for an organisation's IT function and people, as the traditional security model is focused on the perimeter alone, whereas zero-trust security is focused on the data – meaning a shift in the way organisations think about IT security and the infrastructure that supports it.

Delivering this can require investment in resources and expertise in order to address implementation complexities. This may see the need for additional investment in security technologies, such as multi-factor authentication and network segmentation – increasing costs for organisations.

It can also have a significant impact on people and culture, which must be considered to minimise the impact.

Cultural considerations

Zero-trust can impact organisational culture as it changes the user experience, creating potentially stressful situations, as people may need to go through multiple authentication steps to access the required resources.

The practice can also generate false positives, where legitimate user requests are denied or flagged as suspicious. This can potentially disrupt business operations and create frustration among users.

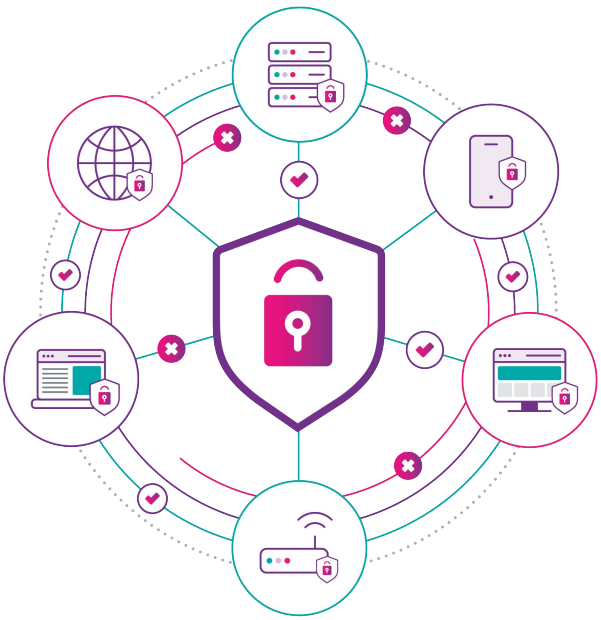
All of which impacts both productivity and user satisfaction – creating a negative user experience – potentially damaging organisational culture.

However, implementing a zero-trust security model can help build trust between an organisation and its people.

Based on the principle of least privilege, zero-trust with users granted access to only the resources they need to perform their job functions, this can help organisations limit the amount of sensitive data and systems that employees have access to, which in turn can reduce the risk of data breaches and other security incidents.

It can also provide employees with greater visibility and control over their own data and systems, which can boost trust and confidence.

Organisations adopting a zero-trust approach can build a culture of trust and accountability, empowering people to play an active role in protecting their own data and systems.



The hybrid balancing act

Balancing the need for flexibility and security when managing an anywhere, anytime working practice requires a balanced and comprehensive approach. Incorporating the establishment of clear security policies, using secure communication tools, implementing access controls, providing training and support – balancing security with usability, and taking people with you on the journey.

A zero-trust approach protects against any security gaps appearing from remote working and helps to deliver tangible business benefits, including:

- **Supporting digital transformation:** zero-trust models empower people to deliver their roles with confidence and agility. Accessing all the systems they need, whilst getting 'hands-on' with the technology, increasing their IT literacy and confidence.
- **Strengthening recruitment and retention:** embracing flexibility is an essential ingredient when looking to attract and retain people - according to IWG's HR Leaders & Hybrid Working Report, 95% of HR leaders believe that a hybrid working model can be used as an effective recruitment tool.
- **Increasing productivity:** zero-trust enables password-less authentication and single sign-on, whilst eliminating VPN clients and reducing license costs - improving the user experience by tackling inconsistent access experiences and enabling staff to work from home, enrolling new devices from anywhere safely.

Unlocking zero-trust's true potential

In a world with increasing threat factors operating, the traditional perimeter-based security model simply doesn't cut it anymore. A zero-trust approach gives organisations a canvas to redesign organisational infrastructure requirements.

But it goes much deeper than this, it provides an opportunity for organisations to harness zero-trust to become a key driver, enabling leaders not only to offer the hybrid work model people are demanding but also to become fully digitised organisations – reaping the benefits this entails.

Implementing a zero-trust model can have a profound organisational impact, as it helps to educate people to be more mindful and security conscious, as well as creating new business models where technology enables innovation, change and growth.

But it is essential that businesses create the culture and environment to take their people on the journey with them.

Ultimately helping organisations to forge a safe and seamless path to digital transformation, enabling them to leave their legacy infrastructure behind.

With the landscape of cyber security ever-changing, it is no longer a matter of "if" you get attacked, but "when". Adopting a zero-trust approach to your cyber security methods can help you stay one step ahead of any threats you're presented with.

If you are ready to talk about creating or refining your zero-trust cyber security strategy, reach out to our team of security experts today.

CAE
TECHNOLOGY ON POINT