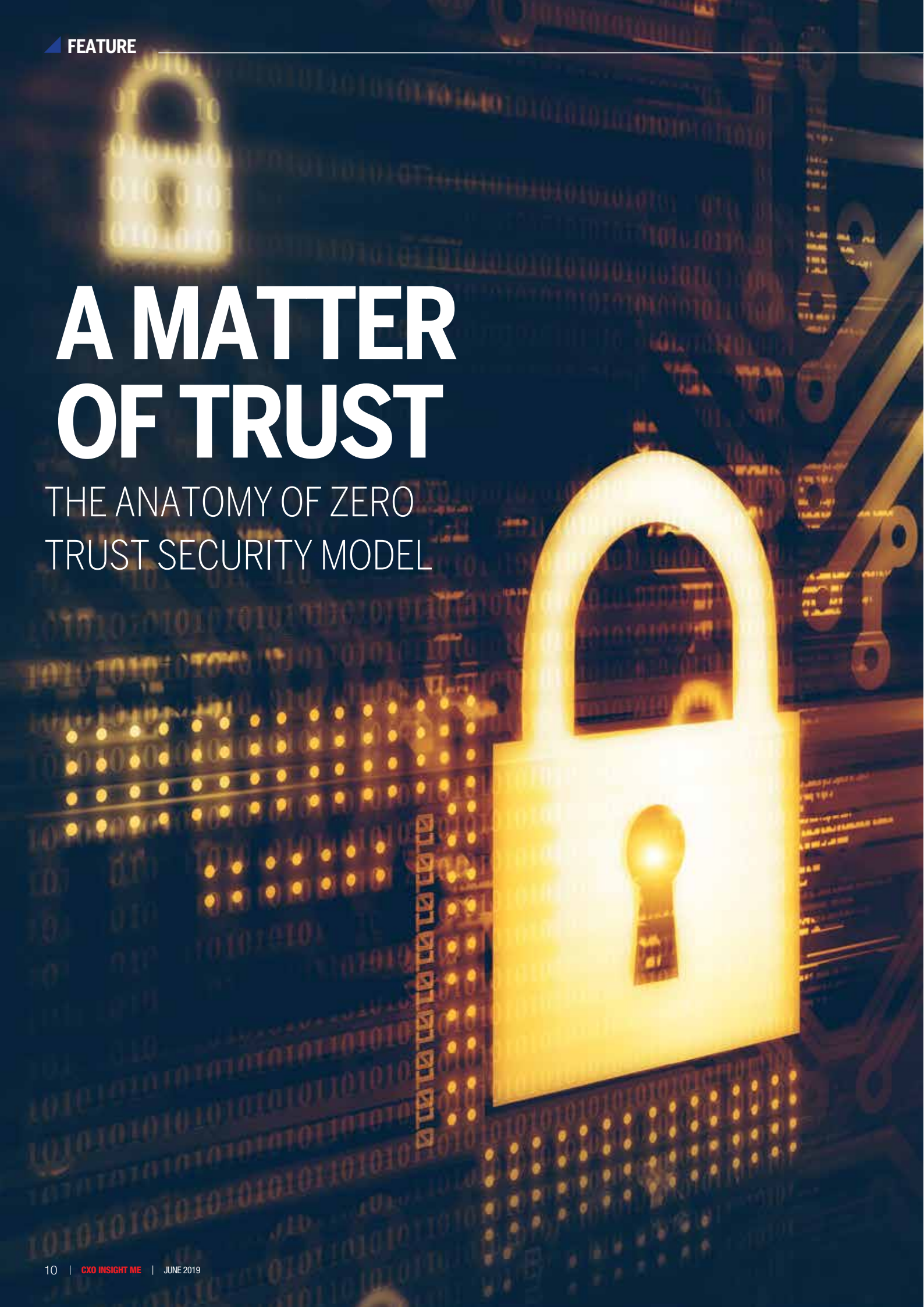

A MATTER OF TRUST

THE ANATOMY OF ZERO TRUST SECURITY MODEL

Zero trust is the next big thing in security. The concept was introduced by Forrester almost a decade ago as an alternative architectural approach to security based on microsegmentation and microperimeters to counter escalating risks. The core principle at the heart of zero trust model is security by design, and command and control over who has access to the network and data. It changes the paradigm from 'trust but verify' to 'never trust but always verify' with a data-centric approach to security.

With the ever-changing threat landscape and increasing sophistication, security leaders are now forced to rethink their traditional approach to security and adopt a zero trust security model to protect enterprise systems and data.

Why zero trust?

"Organisations need a zero trust security model because when it comes to networks, trust is nothing more than a vulnerability to be exploited. Many people harbour the false notion that there are trusted networks and untrusted networks: They believe that if they are on a "trusted network," they are safe from harm. This is a naïve and leads to a failure to adopt adequate protection: most attacks and exploits occur as a result of this trust model," says Tarek Abbas, Director, Systems Engineering, Emerging Markets, Palo Alto Networks.

The concept of zero trust is as profound in cybersecurity as the sweeping transformation generated by the arrival of cloud, mobility, agility, and availability, according to Kamel Heus, Regional Director, Northern, Southern Europe, Middle East and Africa, Centrify. "Zero trust security assumes that the threat actor may be already within an organisation and is posing as an employee of the organisation. Or, alternatively has assumed the credentials of an employee of the organisation. The concept of zero trust seeks to limit the opportunity of such an internal threat actor to use the assumed

Kamel Heus, Regional Director, Northern, Southern Europe, Middle East and Africa, Centrify

Maher Jadallah, Regional Director - Middle East, Tenable

employee credentials and breach other parts of the organisation," he says.

Maher Jadallah, Regional Director - Middle East, Tenable, says implementing a zero-trust model is all about control. It requires a complete picture of the environment - covering what network assets exist and where data resides, with the right level of control to provision access. Typical solutions include a robust admin access management solution, firewalls, micro-segmentation capabilities, controls on endpoints and servers, vulnerability management, etc., to ensure that all access requests are legitimate and the security posture of devices complies with existing protocols.

Nicolai Solling, CTO of Help AG, agrees that zero trust is more relevant today than it has ever been, and this is largely on account of malware and insider threats. "The issue with the threats today is that they are exploiting the elevated rights and capabilities of systems and users to spread laterally to systems with higher criticality. The obvious example is a user receiving an e-mail with a phishing element which infects the user's machine, and the absence of zero-trust allows infection of further connected systems where rights exist. This is also sometimes referred to as lateral movement. By implementing a zero-trust approach, you greatly reduce the attack surface on your systems and hence limit the possibility of lateral movement of attacks."

Though the concept might sound relatively simple, and draws on a range of existing technologies, implementing a zero trust model can be a daunting challenge for many. Industry experts point out zero trust is a journey, not a destination.

"Zero trust can be challenging to implement because it doesn't involve just one element or product but covers many functionalities within your ICT environment. It requires architecting and enhancing your infrastructure and applications with the intent of being able to control – not just the network, but also endpoints, access, user rights and privileges which are all extremely important areas to focus on," says Solling.

Abbas from Palo Alto Networks says Implementing zero trust is, to a large extent, about changing the mindset that companies have towards cyber security and modifying the way people – whether that's staff or customers – access your network. Firms need to ensure that all data and resources are accessed securely, based on user and location. They must identify the traffic and data flow and have visibility to the application, the user and the flows. Understanding

Mathivanan Venkatachalam, vice president, ManageEngine

Nicolai Solling, CTO of Help AG

Tarek Abbas, Director, Systems Engineering, Emerging Markets, Palo Alto Networks

who the users are, what applications they are using and the appropriate connection method is key to determining and enforcing a policy that ensures secure access to your data, he adds.

Mathivanan Venkatachalam,VP, ManageEngine, recommends that businesses implement zero trust model gradually, as opposed to embracing a particular product as an immediate solution. "Though there will likely be a boon to cybersecurity while establishing this zero trust model, there are also challenges businesses need to endure while going through the implementation process. First, the existing mindset of IT security professionals can be a challenge to overcome, as they generally expect threats to come from outside the network; now, IT personnel need to analyse entities not only from the outside but also from the inside of the network. Second, the incompatibility of legacy systems with zero trust security procedures will likely prove to be a challenge as well. Third, there will be a hit on employee productivity, as zero trust model implementation will delay the normal workflow for employees by requesting their identity every time they try to establish contact with the network."

Jadallah says before moving anything to a zero trust model you need basic foundational controls. This requires

> **"THOUGH THE CONCEPT MIGHT SOUND RELATIVELY SIMPLE, AND DRAWS ON A RANGE OF EXISTING TECHNOLOGIES, IMPLEMENTING A ZERO TRUST MODEL CAN BE A DAUNTING CHALLENGE FOR MANY. INDUSTRY EXPERTS POINT OUT ZERO TRUST IS A JOURNEY, NOT A DESTINATION."**

understanding of what you have, how it's accessed, and by whom. Without this basic understanding, it's impossible to implement zero trust successfully.

The best time to align the move to zero trust is as part of current digital transformation projects. As you move to the cloud, for example. When you have a Greenfield site, it's far easier to implement a zero trust model rather than trying to stick it over the top of an aging environment, he says.

What are some of the common pitfalls to avoid when you move to a Zero trust security model?

"The pitfalls to avoid are mainly around the human aspect: making sure that all departments and employees in an organisation are on board with the security procedures and understand why they need to participate in additional layers of authentication and why procedures are so important to follow. Implementing a zero trust approach requires good communication across the organisation," says Abbas.

Solling from Help AG notes that there are, of course, many technical pitfalls you can fall into – but at the end of the day this boils down to product selection and implementation, And just as with your car, if you choose the wrong brand or service it at the wrong mechanic, you will burn your fingers.

"However, at the root of most of the pitfalls is the fact that zero trust is very often positioned as a product while it is actually an approach or design paradigm. Once you understand this and break it down to a prioritised approach, the issue becomes much more manageable. If you try to do everything in one go, you will ultimately set yourself up for failure," he adds.