




BEST PRACTICE | IDENTITY AND ACCESS

Keys to the kingdom

Identity and access management is a core principle of ensuring a robust cybersecurity framework.

 Kirsten Doyle  Karolina Komendera

Any organisation that manages multiple users, all of whom need access to many types of data and applications, requires a robust set of solutions and standards to help implement access controls, to protect data from today's complex threats. Identity and access management (IAM) systems are designed to do exactly that.

According to Sana Rejibi, IAM consultant, BT, remote working and hybrid workforces are shining the spotlight on the need for these systems. Because work has moved from being centralised in an office location to taking place across myriad locations, this is placing greater demands on access management.

Gartner says organisations are finding themselves tasked with having to support multiple options for user and

device access as well as multiple generations of digital assets, all within a flexible modern identity infrastructure. "In the enterprise, identity governance and administration are essential to governing access to both on-premise and cloud resources," she says.

Another factor spurring on IAM adoption is the need for organisations to deliver a seamless user experience, adds Rejibi. This is particularly important as user and employee experience is now a business differentiator and essential to gaining competitive advantage.

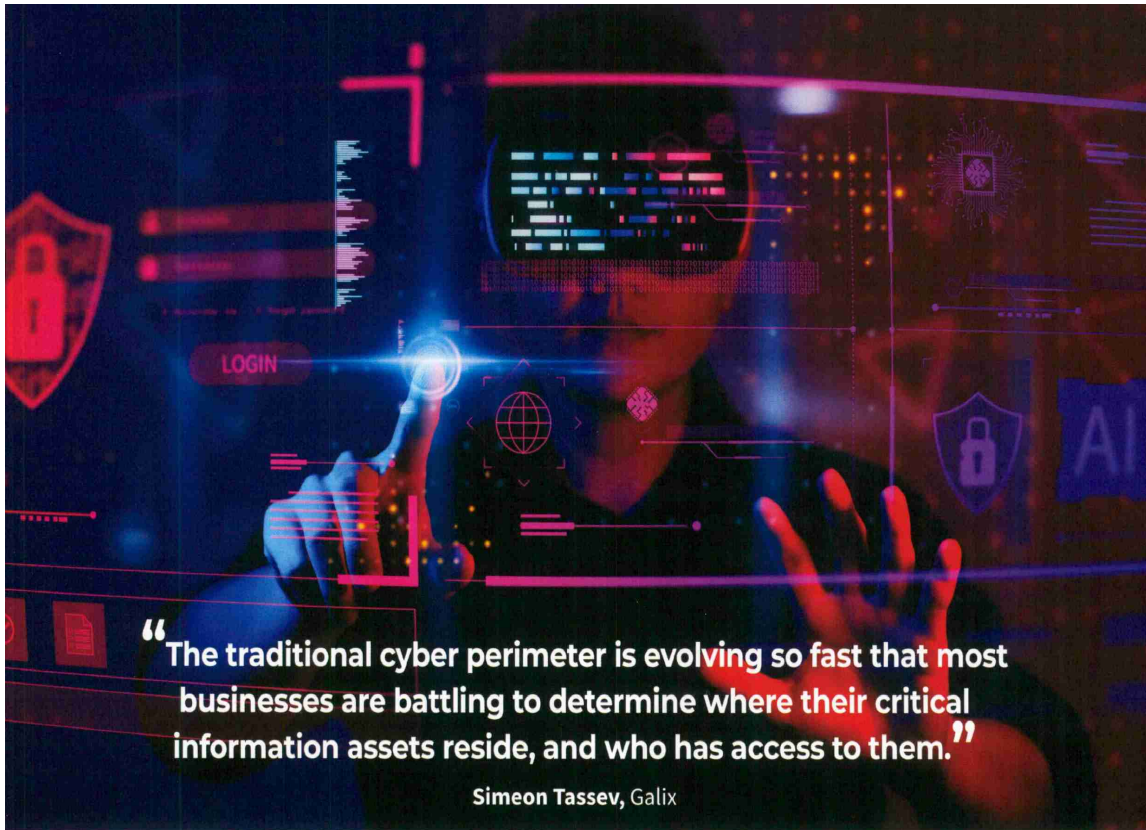
Simeon Tassev, MD and QSA, Galix, says businesses are faced with the challenge of providing their workforces with the right level of access to the right resources. "While employees are now used to being able to work from any place, and at any time, supporting user access from a wide range of locations on a slew of different

devices can not only introduce new risks, but added complexity.

"The old maxim is that companies can't protect what they don't know and what they can't see, and, unfortunately, the traditional cyber perimeter is evolving so fast that most businesses are battling to determine where their critical information assets reside, and who has access to them." In addition, he says, there are today's multicloud environments, the edge, IoT devices, an increasingly stringent regulatory environment, and an 'everything digital' world, and it's easy to see why getting a grip on IAM is one of the most complex and challenging issues enterprises must deal with.

"IAM has become an essential component of security and all principles of security, including the baseline principle of security – CIA (confidentiality, integrity, availability)," he adds.





Debilitating cases of ransomware and malicious software attacks are rising, with the potential to cost governments, public and private sector organisations dearly in capital, time and resources, says Jeremy Matthews, CEO, Panda Security Africa. “In addition to this, insider attacks are becoming more prevalent, with the potential to expose confidential client information and resources. Bring your own device and cloud reliance are driving the adoption of IAM, as it ensures that only authorised people use assigned resources, when required.”

Enhanced security

Approaches to authentication have evolved in that using a single-factor authentication, such as a password, to protect from cyberattacks is no longer sufficient in today's hyperconnected world, adds Rejibi. Cybercriminals are exploiting weak, stolen, or compromised credentials to take on the identity of certain individuals, and hunting for privileged accounts and credentials that can help gain them access to an organisation's most critical infra-

structure and sensitive data. “A more modern approach is to rely on multi-factor authentication (MFA), which entails using an extra method of identification in addition to a username and password when logging into an account. This enhanced method of security ensures that the person requesting access is the right person by requiring additional verification information,” she says.

MFA provides security to protect users' identities, assets, accounts and information, adds Matthews. “Its benefits can be appreciated in sectors such as banking – powerful systems protect sensitive data and the financial assets of their users. MFA ensures that only authenticated users have access to specific resources.”

Over and above a security tool, IAM is also a business enabler. Rejibi says security is essential to cloud adoption and digital transformation. The latter is reliant upon being able to securely connect with people, applications, and devices.

“IAM is a business enabler in the sense that as a core security solution, it's now essential


that organisations adopt IAM. Without it, there is a high risk that they will leave themselves open to cybersecurity threats,” says Matthews. “IAM, paired with MFA, should be used to protect companies' remote networks, as well as email and administrative access. This also allows the visibility of all endpoints and will significantly minimise the threat of a breach, especially when combined with mature patching requirements, employee training and increased awareness. If implemented correctly, IAM drives business productivity and the uninterrupted functioning of digital systems. Employees can work effectively, whether in the office or remotely, through centralised management and by connecting systems to customers, contractors and suppliers, increasing efficiency and lowering costs.”

Some new frameworks are focusing more around security on the edge by identifying who needs access based on various factors such as identity, location, or devices they are connecting from. These factors could be part of a user's identity, comments Tashev.

More frameworks have emerged in recent years, one of which is secure access service edge (SASE), which was identified and coined by Gartner. SASE works on a process that every access that an individual requires will be provided based on their identity and not where they are from. "This is the framework that every organisation is moving towards, in order to enable the workforce to do their jobs no matter what device they're using or where they're connecting from," says Tassev.

Safe collaboration

In terms of where IAM fits in with the overall security posture, Matthews says it has evolved into a vital area of any organisation's overall security strategy. Services like WatchGuard Authpoint MFA, offer a strong identity framework and enable organisational productivity and the uninterrupted functioning of digital systems. In today's business climate, employees and management teams require rapid and easy access to data and IT resources. An organisation's security strategy should incorporate IAM with MFA and encourage the safe collaboration between employees, while enabling them to work and safely share information across the organisation. IAM lays the foundation for the secure sharing of identity information across applications and tools without compromising security. This will ultimately improve productivity, research and development and the longevity of an organisation.

Says Tassev: "It's difficult to have a security strategy without identifying the users, whether that's an individual or a service account. These accounts would be automated to deal with a specific aspect of the organisation's data, such as backing up the system. In the remote working world, IAM is important to the cybersecurity strategy as it ensures that an identity is only given access to what they need and nothing else. This decreases the chances of a cybersecurity threat, or an individual accidentally deleting data they shouldn't. IAM and its many layers of authentication, enables full accountability." 



IAM AND ZERO TRUST

Identity is one of the fundamental factors at the core of a successful zero trust model. The guiding principle of zero trust is the assumption that a dynamic network is operating within a continuously hostile environment and building a security strategy around that.

BT's Sana Rejibi says one approach to leveraging zero trust entails securing cloud and datacentre servers using zero trust segmentation to co-ordinate traffic authorisations. With this, servers only accept traffic that is sent by authorised users, which is where user identification comes in.

"By making user identity the first requirement to access systems, and only opening ports in the environment when they're required, organisations can limit their exposure to risk," she says.

IAM is a viable alternative to the traditional perimeter-based approach to security that relies primarily on firewalls, as it focuses on who can access what – and on ensuring that only the right person can access the information they're verified for.

Additionally, it's widely known that the weakest link in the security chain is people, as they can and do make cybersecurity mistakes.

The more a business grows and needs to bring more people into the organisation, the greater the risk of human error or fraudulent activity causing a breach of the defences.

"Successful IAM is a viable way to address this, through for example only giving people access to the information they need and segmenting access to the system based on identity," she says.

"Zero trust requires that an individual proves who they are and why they need certain access to certain information before access is provided," says Simeon Tassev, Galix.

This approach requires the individual to have the mechanisms of confirming their identity and validating who they are.

"Examples of the mechanisms would be the multi-factor authentication (MFA), where an individual needs to confirm either through biometric mechanisms, SMSes or one-time pins. This is in addition to the individual's username and password being a factor."

By combining zero trust and IAM, organisations can have a strong security policy and productive end-user experience, says Panda Security's Jeremy Matthews.

Traditionally, organisations have opted for perimeter-based security, based on the assumption that all resources behind the perimeter were protected.

"Zero trust effectively integrates within an IAM strategy, enabling frictionless access with MFA," he says.

It employs the principle of least privilege and just-in-time access so that users are only granted access to essential resources to narrow the risk if resources are compromised.

"A company's IT team is also able to contextualise change requests in a given network and maintain an audit trail," Matthews says.

However, to maintain the successful implementation of zero trust architecture, strict security and access policies must be in place.