IAM at the heart of the zero trust approach

Atos

The rapid rise of cyberattacks of all kinds, particularly ransomware, is pushing companies to expand their defense perimeter by applying a zero-trust approach. But how does it work? And more importantly, how can its effectiveness be calibrated?

Often, an organization's first instinct is to implement zero trust at the network level by reinforcing access to company resources, particularly via VPN for remote workers. However, in the event of an intrusion on the company network, access to information depends entirely on user access rights. It is therefore necessary to manage these access rights to ensure minimal user privileges.

This is where the role of identity and access management (IAM) takes center stage.

IAM: The cornerstone of zero trust

The constantly **increasing number of applications** in use, especially SaaS applications in the cloud, leads to an increase in the number of identities for the company and for each user.
This translates into the at many more access doors for hackers. All these identities, regardless of their location, must follow the same security policy and the same constraints as the main identity of the user in the company. Here again, IAM plays a key role in the zero trust policy being implemented — helping maintain control over user identities and guaranteeing the minimum access rights for each resource accessed, whether internal or external.

On the other hand, a large proportion of intrusions employ user identifiers, often taking advantage of **weak passwords.** Tightening an organization's password policy may lead to a less-than-optimal user experience and can become counterproductive. The answer to that is to move to stronger authentication methods that are more acceptable to users. Because users now log-in from various locations and devices, these authentication methods must adapt to the criticality of applications and data — as well as to the user's login context. This calls for an integrated IAM solution, where identity governance and access (IGA) functions are connected to authentication and access control functions, possibly in a dynamic way.

Depending on an organization's business and need, information systems are now available to the **outside world,** enabling partners and even customers to access certain applications. Inevitably, this widens the attack surface for hackers, making it extremely important to extend the zero-trust approach to this new set of users and integrate them into the IAM solution. You need to be able to manage and control their access rights, even if you delegate the administration of these identities to third parties or to the users themselves.

Managing identity as the new benchmark in zero trust

Identity federation forms an integral part of IAM, making it possible to limit the proliferation of user identities, especially in SaaS applications. In doing so, the company retains sovereignty over user authentications, as well as control of access rights to applications. It is an application of the zero-trust approach by limiting the trust given to applications and the functionalities they provide, without entrusting them with the primary functions of authentication and authorization.

User lifecycle management, enforcement of a comprehensive security policy, approval of rights by key individuals, and automatic provisioning of accounts and access rights ensure that only authorized individuals have access to applications and data with minimal rights. This shows how central IAM is to a zero trust approach. Adding identity federation and multi-factor authentication (MFA) greatly reduces attack surfaces while providing a better user experience.

For applications outside of identity federation, adding a single sign-on (SSO) brick (either desktop or web-based) strengthens security by increasing the complexity of passwords that are no longer known to users. Of course, it is necessary to use MFA for the primary authentication. This is another way to decrease the attack surface and extend the zero trust approach while making life easier for users.

Numbers matter: The role of governance and analytics

Just like in any security strategy, governance is an integral element in the zero trust approach, as is IAM. Dashboards and alerts from both identity management and authentication and access control bricks enable proper execution of the policy and the detection of deviant behavior — like multiple requests for specific application rights not allocated by the role-based access control (RBAC) model. Processes such as the re-certification of rights, roles and accounts also contribute to governance, thereby reinforcing the zero trust approach by regularly questioning and verifying the rights acquired by users.

All IAM components generate audit information that can be processed for risk analysis purposes or to identify the cause of an intrusion — such as a fraudulent assignment of a right to a user.

Going further, IAM can participate in the dynamic side of the zero-trust approach by using artificial intelligence to analyze events coming from IAM, and taking decisions such as deactivating an account, disconnecting a user, or increasing the level of user authentication required in response to an anomaly. This is exactly the prescriptive approach employed by our Evidian IAM software suite.

IAM: An integral lever in an enriched zero trust policy

Making information systems accessible to the outside world and the extensive (and necessary) use of cloud can expose organizations to different types of threats. Identities, application accounts and the associated rights are at the heart of hacker attacks, so they must be managed and fiercely protected as key elements of a zero-trust approach. Complemented by strong authentication and reinforced access control for all types of internal or external users, IAM enriches the zero trust policy by applying it right down to the application level.

About the author

Yann Morvan

Evidian Product Line & Presales Director, Atos

Yann Morvan has 25+ years of experience in the Identity and Access Management domain and in other cybersecurity technologies.

Holding many different positions in consulting and presales in major software editors including Sun and Oracle, he is now leading the product management and presales teams at Evidian.

He is a member of the Atos expert community.

About Atos

Atos is a global leader in digital transformation with 112,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together

CT-221121-JR-BR-ZERO TRUST APPROACH-DARK MODE