How Platform Thinking Can Supercharge Identity & Access Management

By George Symons, Vice President of Strategy for Cloud, Infrastructure and Security, Persistent Systems

The move to the cloud – be it applications, data, or IT systems – mirrors a consequent shift in users operating outside the office. With the prevalence of hybrid working environments, employees, guest users, or third-party entities seek to access applications and data from outside the enterprise's IT boundaries. As this expands the network and the devices deployed to carry out business-critical activities, it enables bad actors another vector to put their foot through the door.

Traditional security practices focused on securing the perimeter can no longer account for this shift. They worked on securing the enterprise data center and providing blanket access to anyone inside the network. This hub-and-spoke model of the traditional security practices cannot manage the security and connectivity requirements of a digital enterprise that works on dynamic access requests, many of which emanate from users and devices outside the enterprise for applications it cannot fully control. Whether attacks from outside the firewall or by users inside, there needs to be protection from bad actors moving laterally inside the data center (or cloud), gaining access to more applications and data once they are within the perimeter.

Enterprises feel the need to shift focus away from the perimeter to user identities and access privileges. This approach is called Zero Trust, and it denies access by default, requiring users to validate their identities within context when requesting access – no matter their location.

Zero Trust builds on the foundation laid by Identity and Access Management (IAM), which will be followed by Secure Service Edge (SSE) solutions to invoke trusted communications along with other technologies. This practice helps enterprises move security protocols to the identity, not the network, by attaching access controls and role-based policies to the user. However, as with any shift, operationalizing and ensuring the currency of an IAM system requires management buy-ins, breaking through cross-functional silos to embed security deeper into business functions, and bringing context to access policies across applications.

IAM investments cannot be successful if enterprises approach it in isolation within either security or operations. Because it pushes enterprises to align the application landscape with evolving security needs and ongoing personnel changes within the organization, it must be orchestrated via a platform with automation.

Here are three reasons why approaching IAM as a platform helps:

- **Automated Access Controls**: As users continue to access applications via locations, devices, and networks from within and outside the enterprise, it becomes necessary to define, keep current, and enforce contextual and role-based access policies. This requires proactive intervention during employee onboarding, offboarding, or lateral shifts within the organization. Privileged access is a case in point, which needs to be time-based and role-defined for it to work effectively and prevent broad access if these credentials are compromised. Most enterprises rely on processes across multiple business functions that are difficult to enforce and often negatively impact employee experience. Automating these access controls by integration with systems such as HR, ITSM, and others eliminates the manual processes for updating user identity, organizational role, and access requirements to streamline the process. Generative AI can come in handy in defining access rules based on role and organization by utilizing conversational prompts and parsing through corporate policy documents on previously defined access policies. A platform-led IAM system can help security teams map user profiles with applications to orchestrate access only to those validated for access to certain applications.

- **Sanitized Application Access**: Applications can only be properly secured if they are appropriately integrated with the IAM systems to leverage the current information on users' access rights for that particular application. Enterprises struggle to maintain the status of applications integrated with the IAM system in a central database, which becomes even more complicated as applications grow in numbers and across organizations within a company. A platform approach can bring the much-needed alignment in application access and verified business users. This provides the updated status of application onboarding to security teams, business unit management, and executives. With applications onboarded, incidents of unauthorized data access are better contained, and the ability to measure the status of these integrations with IAM systems helps meet regulatory requirements in the EU and the US.

- **Orchestrated Identity Proofing**: Based on business criticality, applications may make use of different forms of IAM controls, such as IGA or SSO. Enterprises will also deploy security mechanisms such as passwords, multi-factor authentication, or biometrics. With visibility into user identities, locations, devices, and the type of applications being accessed, an IAM platform can be leveraged by application owners to integrate applications and identify proofing mechanisms as per the business use case, ensuring streamlined enforcement of access policies without compromising on employee experience.

Toward a Future-Ready Cybersecurity Posture

Stolen identities comprise the highest number of enterprise security breaches, mostly due to employees doing something they should not or unwittingly falling prey to bad actors. IAM compels enterprises to rethink their security models. It is the first step toward achieving a future-ready cybersecurity posture, safeguarding enterprise data and applications by tying access to user identities, especially in a distributed IT environment for an increasingly mobile workforce.

About the Author

George Symons is VP of Strategy for the Cloud, Infrastructure and Security practice at Persistent Systems. He came to Persistent through the acquisition of Sureline Systems, a supplier of cloud migration and disaster recovery software where he served as the COO. George has worked with both software and hardware vendors throughout his career and he has a proven track record of driving growth. He has held executive roles in product management, engineering, marketing, strategy and overall executive management in both small organizations and large public companies. In the past 20 years the organizations he has worked for have focused on enterprise IT solutions around infrastructure, storage, and security. Key roles include CTO for information management at EMC; CTO for Legato Systems; CEO roles at 3 startups in backup recovery, storage and hyperconverged systems; COO at Xiotech; CSO at Nexsan; as well as various product management and product marketing roles at Sun Microsystems.

George Symons can be reached online at LinkedIn and at our company website https://www.persistent.com/