S&P Global
Market Intelligence **Business Impact Brief**

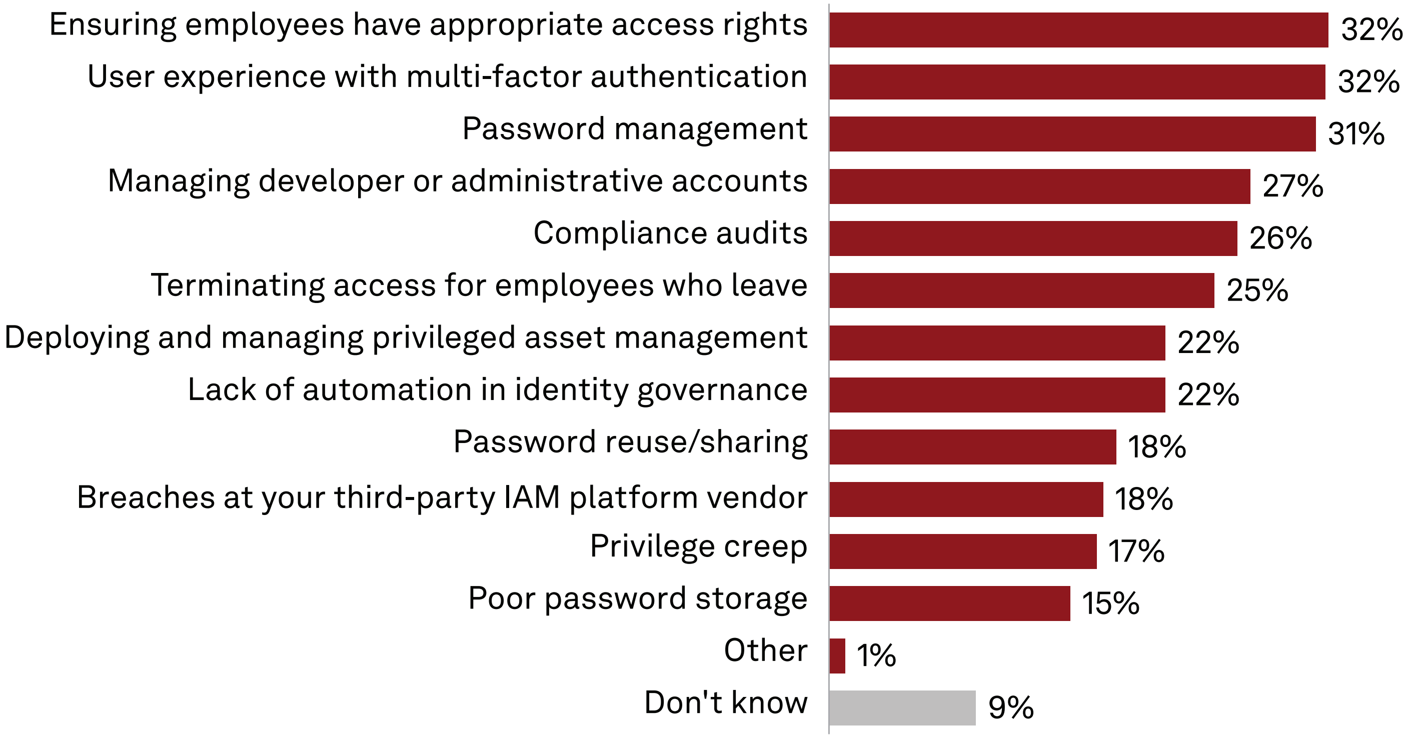
PAM for SMBs: The Democratization of PAM

The Take

As the threat landscape evolves and attack surfaces expand, privileged access management (PAM) is becoming increasingly critical. Most successful breaches involve stolen or compromised credentials and the escalation of privileges via lateral movement, something that PAM offerings are ideally suited to protect against. However, PAM products have historically been highly complex, expensive to purchase, costly to deploy and maintain, and extremely difficult to use, often requiring substantial dedicated staff to operate.

For these and other reasons, enterprise PAM deployments lag behind other security tools by a wide margin. Survey data from 451 Research's Voice of the Enterprise (VotE) service shows just 43% of enterprise respondents have deployed PAM, compared to other leading security technologies, such as network security, email security, endpoint security and SIEM tools, which are all above 75% deployment. PAM deployments are particularly vexing for small and medium-sized businesses (SMBs), which typically don't have the same level of financial and technical resources and staff as larger firms. Additionally, deploying and managing PAM is a top identity management pain point, along with user experience, password management and managing access rights.

MFA, UX and PAM are key identity management pain points



Q. What are your organization's key pain points when it comes to identity management or governance? Please select all that apply.
Base: All respondents (n=479)
Source: 451 Research's Voice of the Enterprise: Information Security, Identity Management 2022

Business impact

The concept of a "privileged user" is too narrow. PAM was originally designed to be used by a small set of IT staff (such as database, network and systems administrators and network engineers, etc.) who are accessing back-end IT systems.

Traditional PAM protects on-premises infrastructure. For most of the past two decades, PAM has been focused on managing access to a limited set of resources, typically UNIX, Linux and Windows servers, relational databases, IT and network infrastructure, etc.

PAM for the few. As noted earlier, PAM deployments have lagged other security tools, and those deployments were mainly by large enterprises — adoption levels are presumably much lower for SMBs.

PAM is one part of a larger identity and access management (IAM) puzzle. Organizations of all sizes are exposed to a variety of attacks and breaches, and thus, all organizations need a full IAM stack, regardless of their size, in order to eliminate PAM silos.

Looking ahead

With the shift to cloud-native computing, the PAM market will continue to evolve — across several dimensions — to what can be referred to as "cloud-native PAM." For starters, cloud-native PAM must address what we have termed the "democratization of PAM." In addition to the standard database administrators and IT admins, PAM needs to support a much wider range of users, including data scientists, marketing and sales teams, research and development staff, executive leadership and others who have access to digital intellectual property and other highly sensitive company data.

As cloud-native PAM adapts to a "shift left" world, it needs to address a much wider range of resources — IaaS, PaaS, containers, Kubernetes and serverless functions, infrastructure as code, etc. A modern PAM portfolio also needs to embrace new technology approaches that span all PAM use cases, not just vaulting and standing credentials and privileges, with support for greater use of ephemeral privileges and just-In-time access. Ease of use and simplicity will be critical, with the ability to provide simple, rapid deployment and an easy migration path to the cloud. Making PAM uncomplicated to consume, as well as cost-effective and easy to roll out, will help bring PAM to the masses that need it most — SMBs and the midmarket.