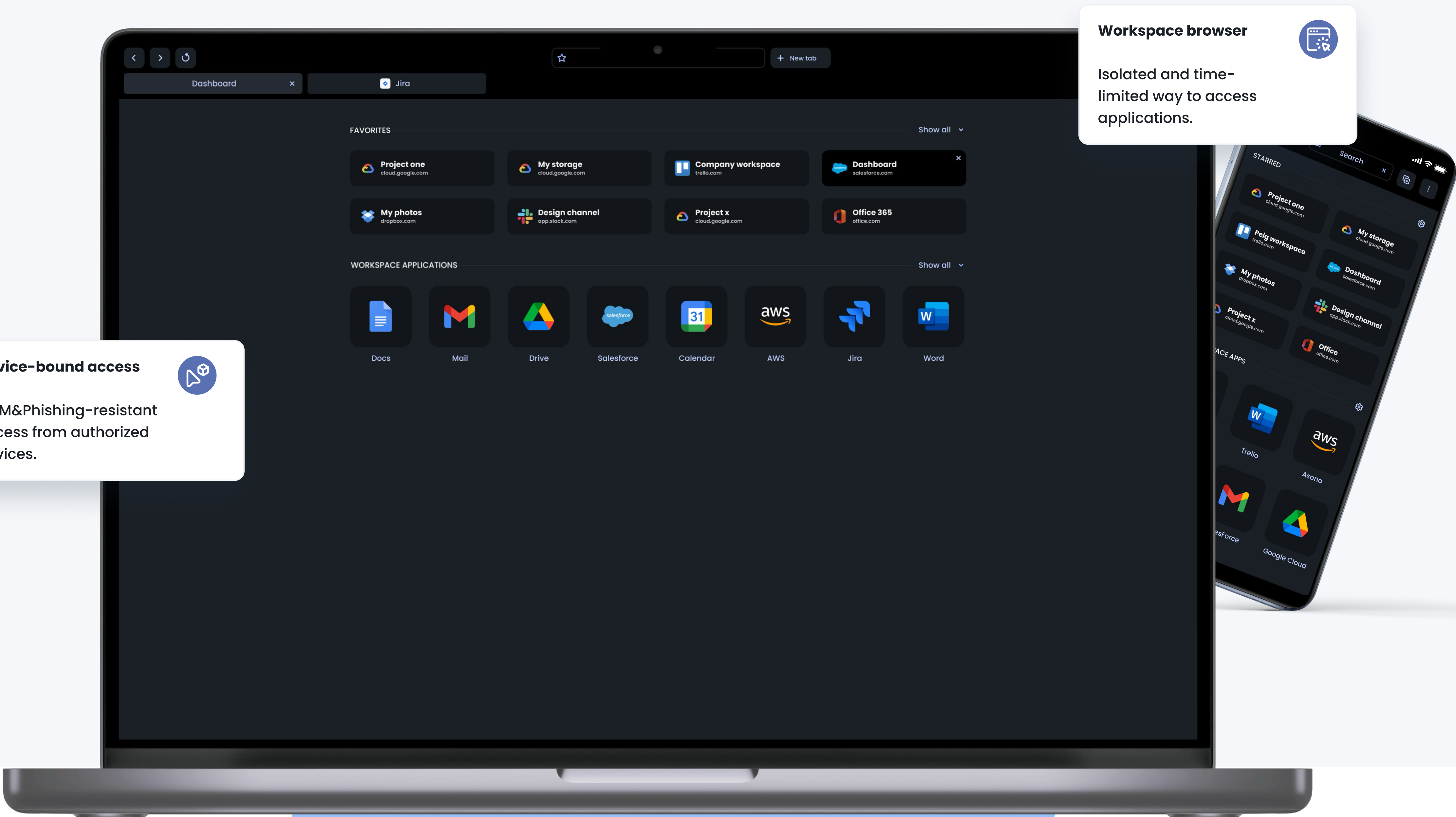


Device-Bound & Passwordless Access Security

Access security is normally about how to add layers to improve password security. It's time to change this. Our **workspace browser** introduces a **device-bound security** model that ensures applications are only accessible from authorized devices—mitigating remote threats by design.



Why Peig Workspace?

Control users & devices

From a single **dashboard**, control who is in your organization, what **applications** they have access to, and from which **devices** they can access them.

Device-bound security

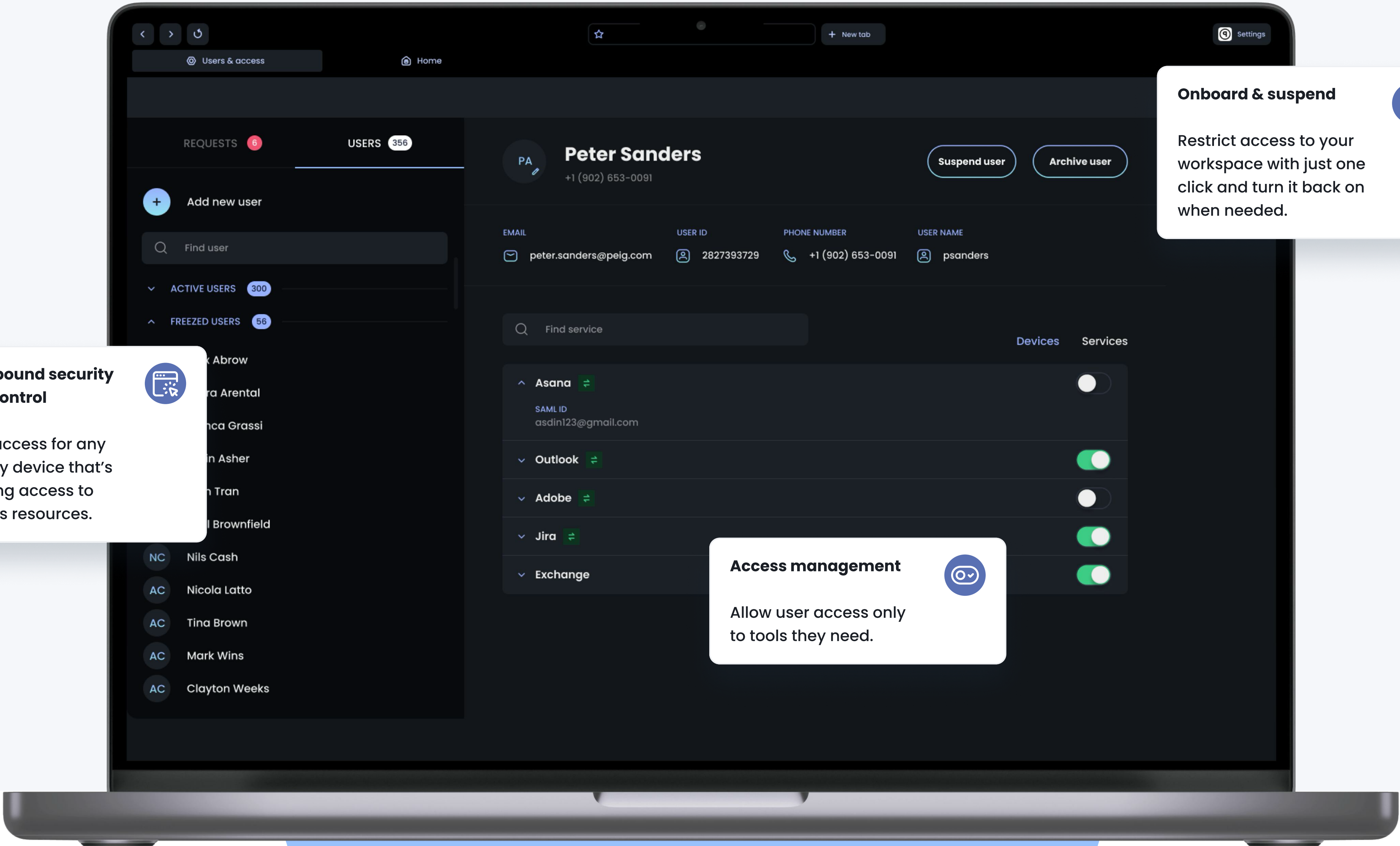
Each access request is **bound to an authorized device** so that adversaries can't access from remote locations, or infiltrate network traffic to steal access credentials or tokens.

Container on BYOD

The **workspace browser** provides **time-limited** access to web resources from **authorized devices** only. Thus making it a secure way to access applications from unmanaged devices.

Total Control over Device-Bound User Access

Enforce consistent, **strong access security across all applications** by authorising both users and their devices—ideal for **BYOD** environments. Admins and managers maintain full control over each workspace browser instance to tailor protections to their needs.



Your new secure workspace

Connect your public & on-prem applications with standard-based no-code configuration interfaces.



Securing workspace access means controlling who gets in—exactly where your data and assets live. With Peig, you can protect both mission-critical systems and peripheral tools that often introduce unnecessary risk.