Cloud adoption, mobility and the consumerization of IT are transforming many business activities for enterprise employees, partners and customers. However, as we leverage these new capabilities, we face a highly fragmented IT environment that is quickly overtaking the comfortable security perimeter of firewalls and virtual private networks (VPNs) we so carefully constructed over the last decade. Protecting the cloud-based, mobile enterprise, therefore, requires a new approach where “identity is the new perimeter.”

To understand this new concept, first consider that every organization is adopting cloud computing in some way. Last year, IDC forecast that by 2015, about 24 percent of all new business software purchases will be of the service-enabled type. And as we know, many Software as a Service (SaaS) purchases are made by business users, completely bypassing IT and security organizations. Previously, this “shadow IT” environment was about a business user buying a server, getting an IP address and installing a stealth application. Now, a crafty marketing person needs only a credit card to start pushing corporate data to cloud storage!

And devices are proliferating. According to a February 2012 report by Forrester, 52 percent of all information workers now use three or more devices for work and many of these are not owned by the enterprise. Forrester further states that in four years, 350 million employees will use smartphones — 200 million of them not supplied by the business. Maintaining a high level of security is obviously difficult, given these statistics.

How should security professionals respond? We could ignore that business users are buying SaaS services since they don’t want to involve IT anyway, but that would also ignore the “shadow identity” of a cloud-based user account that is tied to corporate data. Every one of these accounts has an indirect, backdoor entry to the enterprise; but there’s a more direct threat, too. In most cases, users adopt the same account name and password on their personal devices as they do in the enterprise. That means that if the SaaS provider is compromised, the attacker is coming right through your front door and taking whatever they want.

And it’s not much better if a default personal account with the same password is used on other personal websites. This approach could allow attackers with credentials to come right through the SaaS provider and take your enterprise data. Neither option is acceptable.

JOHN HAWLEY is Senior Director of Business Strategy, Security, at CA Technologies.