The CASB knows: What’s lurking in the IT shadows

This is part three in a six-part series.

Shadow IT is the use of technology, systems or solutions that have not been approved for use by an organization’s own IT staff—you may know it as “stealth IT” or “rogue IT.” And it’s everywhere, thanks to bring-your-own-device policies, empowered employees and easy-to-find cloud-based software. According to a Softchoice survey, 31% of millennials have downloaded cloud apps on their company’s network without telling the IT department.

On one hand, that’s because cloud apps are easy to find, download and use—and employees looking for the best tools to get their own jobs done are taking the initiative. But on the other? Sidestepping IT departments’ security concerns comes with serious risks, because cloud apps aren’t all legitimate, and even legitimate ones can come with security flaws. Telling the good from the bad isn’t a task best left to end users. In fact, ESET research shows that users downloaded 200,000 imposter apps in just a single month.

Keep the baby, toss the bathwater

Keep in mind that employees are looking for the most efficient way to get their job done—their intent is not to put the company at risk. If they are using shadow IT, it may be because they don’t have approved tools available to them, or the approved tools aren’t getting the job done. Intentions aside, when employees introduce unvetted cloud apps into the enterprise, there are some serious implications in three big areas:

- **Data security:** Most obviously, downloading unapproved applications may expose the organization to data loss (or loss of data integrity), because an application is itself sending data off-site, or because it’s part of a social engineering scheme. Widespread but poor password practices—like re-using passwords across sites and systems or employing weak passwords—mean that an innocently exposed password could open the door to corporate systems.

- **Privacy and data ownership:** Who owns the data exposed to a cloud application—the end user? The enterprise or the cloud service provider? The answer isn’t always clear cut or obvious. In many cases, the agreement with the cloud service provider means that *they* are the owner of the data. That means a third party may open and mine your data for interesting information—or even aggregate and resell it.

Shadow IT on your network can expose data that deserves special protection—which can mean not just data loss but legal liability (for failing to meet security mandates) as well as reputational damage.

- **Compliance:** How and where the data is stored matters. Government and industry standards mean that data must be retained for the proper amount of time—if a third party keeps data for too short or too long a time, it could violate those standards. Without knowing what users are doing (and where data is going), the organization may be exposed to needless risks.

Can you bring cloud applications back into the light?

Employees need the best tools for their jobs, and cloud applications are among the efficient tools they'll employ. You can't expect to put the cloud-application genie back in the bottle—but you can put the genie to work for you.

So don't punish employees for legitimately seeking out new software—instead, adopt a secure cloud policy. Employ tools that let you draw insight about what kind of cloud-based apps your users are already using, both to identity ones that should be approved and managed, and to steer them away from risky ones.

With cloud-application visibility, you can also find places where data that's flowing between your organization and an unapproved app could be routed instead to benefit the whole organization, and discover which applications that *are* approved aren't doing as good a job as they should—or are unknown to users.

(Note: You can read more in the second installment of this series about deploying a Cloud Security Access Broker (CASB) such as IBM Cloud Security Enforcer to detect unauthorized applications, connect users to approved cloud software, and protect both users and data from data breaches.)

If you use a ready-made solution—a CASB—to survey the real-world use of cloud applications in your enterprise, you can expose the data flows that are currently in the shadows, and educate users about the security problems of clandestine software on your organization's network. You can even analyze the data to find whether you could be getting a better ROI by managing your cloud-application provisioning contracts.

The CASB knows what's lurking in the IT shadow—and you can, too.

READ OUR PAPER: THE CASB KNOWS: HOW GOOD INTENTIONED EMPLOYEES PUT YOUR ENTERPRISE AT RISK.