The CASB Knows: Why cloud access security brokers are a must to protect your enterprise

Note: This is the first in a six-part series that will tackle some of the most important issues you need to consider in your cloud security policy and deployment of a cloud access security broker (CASB).

Like it or not, you're living in a cloud-centric world. The use of cloud-hosted applications, or apps, is growing as organizations and employees take advantage of the efficiencies they offer, such as cross-platform data access, multi-user collaboration and independence from local software installation. If you haven't embraced the cloud, it's time to do so. According to one study, as many as 88 percent of organizations now use public clouds, and 63 percent use private clouds. When clouds are done right, both IT departments and employees benefit.

When the cloud becomes a fog

With this kind of growth, it's not surprising that many of today's empowered, always-connected employees thrive on the cloud. To increase efficiency, they continuously seek out and use cloud apps in the course of their jobs. After all, this matches how they use computers and mobile devices in other contexts. The cloud is convenient and flexible—and it sounds wonderful from a "just get it done!" perspective. But it's not so great when you consider how little you, and your employees, may really know about the security of cloud-based apps, or how they're being used.

Some cloud-based apps may be legitimate and helpful—or at least harmless. Well-meaning employees may be using the best tools they know of. But the critical fact is that apps and services that your employees use outside the standard enterprise approval process—creating a parallel computing environment known as "shadow IT"—complicate life for system stakeholders like IT and security specialists.

You need to find out how shadow IT may be impacting your enterprise and how to rein it in. Where is data really moving? Does opening a connection to a new cloud service expose more data than it should? When you don't have visibility into cloud usage, it's hard to know its potential ramifications—good or bad—no matter how beneficial to the employee.

Paradoxically, the low cost and easy access of the cloud have placed cloud security issues at the top of virtually everyone's list of shadow IT challenges. You can't protect what you can't see, and that holds especially true with cloud security threats. If you do not have visibility into your employees' use of cloud-based apps, you can't take steps to protect the enterprise.

The challenge? Managing the use of cloud-based apps to benefit your employees—and your enterprise.

Why it's a tough job

Visibility is key, but cloud-based apps operate outside your network boundaries. Short of scrutinizing every network packet, you may be missing more than you see.

The proliferation of mobile devices that operate on—or outside of—your network makes policing app use trickier. You need to be able to identify employee app usage patterns and take steps to secure them.

Most employees have good intent; they just want to do their jobs as efficiently as possible. What many don't understand is that the path of least resistance may be jeopardizing enterprise security.

Dragging cloud-based software out of the IT shadows

You can take three easy steps to help ensure secure cloud use:

- **Detect**—Identify risky behavior, to understand the status quo
- **Connect—**Provide sanctioned paths to cloud-based software or usage roles
- **Protect—**Manage compliance, so employees have clear policies and secure access to the software they need

You're not alone

Luckily, there are ready-made cloud security solutions to the problem of un-managed or poorly managed cloud app access. CASBs such as IBM® Cloud Security Enforcer help document, control and safeguard the use of cloud-based software.

Deploying a CASB can give you critical insights into your organization's use of apps and services. Instead of just knowing (or not knowing!) that your employees are using cloud-based services, a CASB-equipped enterprise can see exactly what services are being used—sanctioned or unsanctioned. That's important not only for business planning, but for security and compliance efforts, too.

READ THE GARTNER REPORT: *HOW TO EVALUATE AND OPERATE A CLOUD ACCESS SECURITY BROKER.*