CLOUD ACCESS SECURITY BROKERS

PROTECTING YOUR DATA

TODAY'S CORPORATE ENVIRONMENTS INCLUDE A RANGE OF technologies that are fundamentally changing the pace and flow of global commerce. In this new era of readily available cloud-based apps and services, there's renewed focus on the value of data as the lifeblood of business. Ensuring adequate protection of that data can mean the difference between the success and failure of a company, whether it's a small or midsize business or a large enterprise.

THE ISSUE OF SECURITY has long been at the forefront of deploying the cloud for business purposes. Early on, concerns revolved around the integrity and ability of vendors to adequately secure their cloud infrastructures. As cloud adoption has grown exponentially, security concerns have shifted to the actual data itself—ensuring protection of information both in transit as well as at rest. Corporations of all sizes are quickly realizing that they're responsible both for their own data security and for enforcing access control policies on end users.

As they move toward increased cloud adoption and greater digital enablement, C-suite executives and IT professionals have identified Cloud Access Security Brokers (CASBs) as offering crucial resource protection. CASBs provide security tools that act as intermediaries between end users and cloud applications. They have the ability to see all traffic to and from cloud applications, and to inspect and secure data both on the move and at rest. Gartner Research has predicted that CASB technology will be an essential component of all software-as-a-service (SaaS) deployments. In fact, it says, "85% of large enterprises will use a cloud access security broker solution for their cloud services" by 2020, which is up from less than 5% in 2015.

All Things CASB

Digital commerce, comprising devices, services, and end users with digital identities, represents the wave of the future. As we create and use more data, companies of any size can rely on CASBs for comprehensive security to cover their cloud activity. Key areas covered by that security include:

SHADOW IT: These are corporate end users who deploy their own cloud apps and services without company oversight or following IT policy. To counter the trend, CASBs audit company networks to identify the use of SaaS applications and to protect against unforeseen data loss.

ACCESS CONTROL: CASB technology employs end-user identity and context to strictly enforce access to sanctioned applications.

ENCRYPTION: To maintain data privacy and regulatory compliance, CASBs can provide a common point of data encryption. Information management is thus maintained by the organization instead of the SaaS provider.

DATA LOSS PREVENTION (DLP): Increased visibility provided by a CASB enables it to verify the context of cloud access by any end user and provide the means for forensics and auditing through reports and activity logs.

USER ANALYTICS: Establishing user behavior and baselines enables CASBs to detect external threats by analyzing anomalous behavior.

"The information security industry continues to evolve at a rapid pace due to the ever-evolving threat landscape across all industries," says Linda Gray Martin, Director & General Manager, RSA Conference. "Gathering the greatest minds in the industry to collaborate and challenge each other is a vital component to effectively fight cyber threats and defend critical data and infrastructure in this digital age. RSA Conference not only continues to evolve each year with the industry but also brings together thought leaders, industry influencers, and security professionals to share best practices on how to secure enterprise assets and consumer livelihoods."

One industry leader, ManagedMethods, is helping organizations see how their users are storing, sharing, and accessing cloud data. Cloud Access Monitor is a flexible, easy-to-deploy, and integrated solution that will comprehensively cover cloud security, from monitoring SaaS business apps to detecting Shadow IT activity. "Our strategy of leveraging a company's existing investments in security technology has opened the door for us to deliver unparalleled protection to our customers," according to Charlie Sander, Chairman and CEO of ManagedMethods.

Rethinking Network Security

Eight years ago, Zscaler recognized that fundamental changes taking place in the way people work would have an indelible impact on IT security. Employees were accessing an increasing array of cloud applications and data using devices neither sanctioned nor controlled by IT. The typical corporate network was simply not designed to support the volume of Internet-bound traffic—and the resulting security risks—brought about by the cloud.

"Network security as we've known it is dead. We need to look at it differently," says Jay Chaudhry, CEO and founder of Zscaler. He adds, "The current hub-and-spoke architecture that defines perimeter-based security was effective when the data center was the destination, but today's workforce consists of an increasingly digital and widely dispersed user base. To meet the new demand, one has to treat the Internet as the new corporate network and secure employees based on their identity rather than location." The Zscaler cloud security platform is built on a global network of more than 100 data centers and protects 15 million users across 185 countries.

As the demand for SaaS applications continues unabated, organizations—regardless of their size—need to develop effective protection. CASB offers a new class of cloud intermediaries that make it possible to ensure high levels of security policy enforcement.

CHRIS CLOR/GETTY IMAGES

GETTY IMAGES

SPONSORED CONTENT