Preventing data loss in the cloud

Case Study

Ascensus helps more than 15 million people save for what matters—retirement, education, and healthcare. Through co-branded, private-labeled, and other governmental partnerships, our technology, market insights, and business knowledge enhance the growth and success of our partners, their clients, and savers. Ascensus is a leading recordkeeping services provider, third-party administrator, and government savings facilitator in the United States.

How can a financial services company optimize security across thousands of cloud-based apps?

For two decades, Ascensus has been expanding both organically and through acquisition. "We've grown from being a centralized company with several hundred employees to having diverse business units with 10 times the staff," says Clayton Krueger, Business Information Security Officer. "Our technology landscape is complex and requires strict security protocols."

Today, Ascensus employees use more than 2,000 different cloud applications. "Some are used more than others," Krueger says, "but there are hundreds of apps out there that employees use regularly."

Addressing that sprawl became paramount when Ascensus transitioned to Microsoft 365. "That was the moment we could no longer consider SaaS applications to be an exception," Krueger says. Ascensus' on-premises data loss prevention (DLP) would not be able to securely cover the transition, so Ascensus proactively searched for another solution to ensure that users could still access essential applications after transitioning to M365.

"We couldn't just put the security hammer down and tell business users that applications they want are off-limits," Krueger emphasizes. "That would be a career-limiting approach. What we needed was information about how employees were using cloud solutions so that we could prioritize our efforts and, essentially, pick our battles."

"If you don't even know all the cloud solutions you need to protect, much less how they're being used, then how can you know you're applying best-in-class controls to everything that's important? That's the Netskope value proposition."

– Clayton Krueger, Business Information Security Officer, Ascensus

ASCENSUS®

Profile

Industry	Region	Employees	Assets Under Administration
Financial Services	United States	5.5K	$745 Billion

Click here to visit the Ascensus website

Challenges

- Understand security risk across diverse cloud infrastructure
- Prioritize security efforts based on risk to the business

Solutions

- Netskope CASB provides visibility to usage for cloud solutions
- CASB blocks outbound transfer of some sensitive data
- Other outbound data triggers alert and warning to end user
- Netskope SWG filters all web traffic, enhancing DLP

Results

- Converged management minimizes ongoing staff time required
- Each solution deployed within one hour

Leveraging CASB visibility to optimize cloud security

After six months of deploying another CASB, the solution still had coverage gaps. "We did a proof-of-concept with the Netskope CASB, and it worked out of the gate," Krueger says. We installed and configured it during a one hour-long call with Netskope. The next day, we started seeing what cloud applications our users were accessing."

Krueger's team initially configured the CASB to only uncover and monitor cloud activity. The tool began mining log files of the company's cloud solutions, tracking app use and frequency by person. Krueger's team established DLP rules for movement of sensitive data out of the corporate network. Now the CASB notes any upload of regulated data to the cloud.

"Netskope CASB helps us understand our usage and where we face the greatest security risk, which is crucial given the complexities in our different operational areas," Krueger says. "We can put together a shortlist of our biggest risks. Then we can spin up a response in our 'cloud sanctioning' process."

The team is using Netskope CASB to evaluate prospective cloud applications, as well. "We'll open up Netskope and look at an app an end user is interested in," Krueger says. "If the analysis indicates that security would be problematic, we might ask the business whether they've considered another tool that is similar but would pose less risk."

> "My team has become a business enabler. When you look at old-school content filtering, security [is] binary. The Netskope solution enables us to have more nuance around the rules. We can protect our data and applications without ever just telling users 'no.'"
>
> – Clayton Krueger, Business Information Security Officer, Ascensus

"Most platforms include some security, but we may have 12 other areas where we want protection, like access management or encryption of data," Krueger continues. "On all these platforms, customers make a lot of configuration decisions. We leverage the CASB's data on usage to ensure apps conform to our security rules and expectations."

"Netskope CASB is a very advanced tool," he adds. "The more you dig into it, the more ways you find to use it."

Building DLP for all Ascensus web traffic

The CASB proved so effective that Krueger's team considered the Netskope Next Gen Secure Web Gateway (SWG) as well. "We literally got on the phone with Netskope and deployed," Krueger reports. "It took us five minutes to set up a rule, and it worked exactly as we expected. It's doing a great job of content filtering, and we appreciate the converged management between the Netskope solutions.

"Having a singular view of cloud security enables us to take a more holistic DLP approach," he adds. "We can straight-up block outbound data: Suppose the relationship owner says Social Security numbers should never be sent to a particular app. If a user tries to send Social Security numbers, the CASB will block that action." An alternative response is to generate a security alert for Krueger's team to investigate, and to simultaneously present the end user with a message describing how their actions violate corporate policy.

Krueger expects to continue adding Netskope solutions to Ascensus' environment. "We are comfortable looking into the future with Netskope," he says. "We have a very strong partnership."

Krueger is confident that Ascensus takes proactive measures in securing its "cloud crown jewels." Better yet, he says, "my team has become a business enabler vs. business restrictor. Users expect to be allowed to access the online systems they need. When you look at old-school content filtering, security has to be very binary—actions are either allowed or not, across the board. The Netskope solution enables us to have more nuance around the rules. This means we can protect our data and applications without ever just telling users 'no.'"