bitglass

case study

Freight Giant Uncovers Breach with Next-Gen CASB

A multi-national transportation company turned to Bitglass for their annual audit. The auditors wanted to catalog Shadow IT cloud apps on their network for their annual compliance report. Bitglass was able to do that and a whole lot more.

Auditors at this firm contacted Bitglass and simply uploaded two weeks of firewall logs, approximately 2M log lines per day. Bitglass did the rest.

The Bitglass Breach Discovery Engine identified four high-risk cloud apps widely used on the network. The top- ranked high-risk apps were YouTube, MSN, Facebook, Dropbox and Evernote. The company had previously blocked Gmail and Yahoo due to security concerns.

These cloud apps were a compliance risk and merited mention in the annual audit. But there was worse. The Bitglass Breach Discovery Engine uncovered a TOR (The Onion Router) node operating within the corporate network. In repressive societies, TOR plays a valuable role in enabling the uncensored flow of information. In free societies, TOR is used almost entirely for criminal enterprise—porn, drugs and data exfiltration. Bitglass found sustained traffic to about 200 nodes in the TOR network during the two-week span. Bitglass alerted the audit and security teams at the customer.

Remediation was swift. Using pinpoint diagnostics from the Bitglass Breach Discovery report, the customer was able to track down the breached device. The customer also upgraded to next-gen firewalls to improve visibility.

Once a hacker gets inside the network, even the latest firewalls can do nothing. New risks and new hacks daily cause breaches. And the average breach lasts almost eight months. Bitglass' Breach Discovery Engine tracks the latest risks to uncover breaches early so you can limit the damage.

"A routine end-of-year audit at this multi- national uncovered a major data breach"

—CISO, Freight Giant