Sedgwick confirms cyber incident affecting its major federal contractor subsidiary

By Jonathan Greig

Published: 2026-01-02 · Archived: 2026-04-05 14:16:27 UTC

Claims administration company Sedgwick confirmed that its government-focused subsidiary is dealing with a cybersecurity incident.

On New Year's Eve, the TridentLocker ransomware gang claimed it attacked Sedgwick Government Solutions and stole 3.4 gigabytes of data.

A Sedgwick spokesperson confirmed the company is currently addressing a security incident at the subsidiary, which provides claims and risk management services to federal agencies like the Department of Homeland Security (DHS), Immigration and Customs Enforcement, Customs and Border Protection, Citizenship and Immigration Services, the Department of Labor, and the Cybersecurity and Infrastructure Security Agency (CISA).

"Following the detection of the incident, we initiated our incident response protocols and engaged external cybersecurity experts through outside counsel to assist with our investigation of the affected isolated file transfer system," the spokesperson said.

"Importantly, Sedgwick Government Solutions is segmented from the rest of our business, and no wider Sedgwick systems or data were affected. Further, there is no evidence of access to claims management servers nor any impact on Sedgwick Government Solutions ability to continue serving its clients."

The company has notified law enforcement and is in contact with its customers about the incident.

CISA and DHS did not respond to requests for comment. The company also provides services to municipal agencies in all 50 states as well as the Smithsonian Institution and the Port Authority of New York and New Jersey.

TridentLocker is a new ransomware gang that emerged in November, cybersecurity experts said. The group previously took credit for an attack on the Belgian postal and package delivery service bpost, which confirmed that it recently suffered from a data breach.

The group has listed a total of 12 victims on its leak site since its emergence.

Ransomware gangs have repeatedly targeted federal government contractors like Sedgwick. More than 10 million people had information leaked after the prominent government contractor Conduent was attacked one year ago.

Intelligence Cloud.

Learn more.
