SaaS Alerts
A Kaseya COMPANY

ArcLight Solutions

How SaaS Alerts helped ArcLight Solutions detect and stop a Chinese spy.

Location
Lincoln, Nebraska

Primary Markets
Manufacturing
Real estate
Private equity

MEET THE MSP

Frank Barrett, CTO of ArcLight Solutions, which serves SMBs with large-volume data centers.

Challenge

A small manufacturing company hired ArcLight to help with their ERP system. As part of the engagement, Barrett installed ArcLight's IT management software — which included remote monitoring and management (RMM) and, of course, SaaS Alerts — in the manufacturer's environment.

Immediately, SaaS Alerts found a red flag: The customer's Microsoft 365 files were being accessed by a location in China — a clear violation of the company's access policies.

Barrett dug in and discovered that the files had been copied to a public OneDrive folder by an employee at the company.
He immediately contacted the customer and asked if there was any reason for this person to circumvent company policies and log into Microsoft 365 from outside the U.S. Maybe they were attending a conference or working while on vacation?

The customer's answer was an unequivocal "no." In fact, they had long suspected that the person who made the files public was a Chinese spy.
"You don't hear that every day," said Barrett, a military veteran and former government IT worker.

Solution

Barrett immediately called SaaS Alerts, and our cybersecurity experts leapt into action. They quickly determined that the IP address accessing the Microsoft 365 files was a known Chinese government actor who had long been suspected of stealing proprietary manufacturing data from U.S. companies.

ArcLight's customer manufactures equipment used in utility networks. It became clear that a Chinese spy had infiltrated the customer's company to identify vulnerabilities in the U.S. electrical network.

Barrett could have used SaaS Alerts to automatically shut off the user's access. Instead, the manufacturer decided not to raise the bad actor's suspicions while they contacted the appropriate authorities. Within days, the unauthorized access from China stopped.

Results

Unlike SaaS Alerts, Barrett's previous SaaS monitoring tools didn't have a geolocation component. He would have likely missed the threat to his customer — and the country. Thanks to SaaS Alerts, Barrett now has extra peace of mind knowing ArcLight can improve their customers' security posture and help save the day if something goes wrong.

> **"The rise in ransomware, especially through social engineering on SaaS platforms, makes SaaS Alerts a mission-critical tool for our managed services business. Threat surfaces are being spread too thin to leave to chance. No matter how big or small, important or insignificant, you never know who is accessing your information."**
>
> *— Frank Barrett, ArcLight Solutions*