SaaS Alerts™
Cover Your SaaS

MSP
ArcLight Solutions

CASE STUDY

How SaaS Alerts Helped ArcLight Solutions Detect and Stop a Chinese Spy

ABOUT ARCLIGHT SOLUTIONS

ArcLight Solutions is a managed service provider (MSP) for small to medium-sized businesses (SMBs) with large-volume data centers—primarily in the manufacturing, real estate, and private equity sectors. ArcLight's mission is to provide customers with strategic IT solutions that increase revenue, create efficiencies, and optimize resources while mitigating risk.

OVERVIEW

It's not every day that a small MSP in Lincoln, Nebraska gets pulled into a case of international espionage. But that's exactly where Frank Barrett, CTO of ArcLight Solutions, found himself while onboarding a prospective client.

The small manufacturing company contacted ArcLight to help with their ERP system. As part of the initial engagement, Barrett installed ArcLight's IT management software in the manufacturer's environment. The software stack included remote monitoring and management (RMM) and, of course, security tools to give Barrett's team visibility into critical business systems, including SaaS Alerts.

Immediately, a red flag popped up on Barrett's SaaS Alerts dashboard. Looking at a geographic map of Windows 365 login requests, Barrett discovered that the company's information was being accessed by someone in China.

Barrett checked the company's access policies and couldn't find any legitimate business reason for the access requests. Further investigation found that all the requests were made under a single username, and that user had set up a OneDrive folder that was publicly available to anyone who knew where to look.

Still, Barrett needed to be sure. He contacted the client, briefed them on the situation, and asked if there was any reason for the user to log in to the company's Windows 365 account from outside the U.S. Perhaps he or she was traveling to a conference or was working while on vacation?

Phone :
+1 (910) 887-3352

Email :
sales@saasalerts.com

Web :
www.saasalerts.com

A SWIFT RESPONSE

The answer from the client was an unequivocal "no." There was no reason for the user or anyone else to access the company's data from anywhere outside of the U.S. or the U.K. In fact, the client admitted that the user had long been suspected of being a Chinese spy.

"You don't hear that every day," Barrett, a military veteran and former government IT worker, recalled. "That sticks in your head, for sure."

Barrett immediately called SaaS Alerts and brought our cybersecurity experts into the conversation. After a brief investigation, it was determined that the suspicious IP addresses accessing the files through Windows 365 were known Chinese government actors who have long been suspected of stealing proprietary manufacturing data from U.S.-based companies. Given that ArcLight's client manufacturers equipment used in utility networks, it was clear that a nation state had placed an asset on the inside of the small manufacturing company to help identify vulnerabilities in the United States' electrical network.

At this point, Barrett could have used SaaS Alerts to automatically shut off the user's access. However, the manufacturer elected to maintain normalcy and contact the appropriate authorities. Within days, Barrett noticed that the unauthorized access from China had stopped, and felt it best not to ask further questions.

SUMMARY OF THE ATTACK

Suspicious Activity

Barrett received a notification from SaaS Alerts that a user was logging in to Windows 365 from a location in China—a clear violation of the customer's access policies.

Threat Validated

Upon further investigation, Barrett found that an internal user had set up a publicly available OneDrive folder that was being accessed by unknown actors in China.

Threat Neutralized

Armed with this evidence, the customer notified the authorities of the insider threat. Not only did the suspicious activity come to a stop, but sensitive data was kept out of the hands of potential bad actors.

"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

THE RIGHT TOOLS

Barrett says that it's likely he wouldn't have detected the insider threat without SaaS Alerts. His previous SaaS monitoring tools didn't have a geo-location component, and the logins from China would have appeared to have been from the employee in Wisconsin.

SaaS Alerts gives Barrett that extra peace of mind that a potential customer's environment is secure before he starts a new engagement. For just a few dollars per endpoint, ArcLight can improve the client's security posture, establish a baseline, streamline the engagement, and provide critical insurance in case something is found or goes wrong.