snare

CASESTUDY

HIGH FLYING PEACE OF MIND

HOW A MAJOR US AIRLINE FOUND PEACE OF MIND, DESPITE COMPLEX SIEM REQUIREMENTS

When your business is sending over 700 aircraft, on over 5,000 trips a day, in over 60 countries - you cannot afford to take unwarranted risks. So when a major international airline needed to change SIEM systems, only one company could get it done.

BACKGROUND

The airline industry is, by its very nature, volatile and exposed to economic downturns as people vacation less and businesses cut travel expenses. If market forces weren't enough to contend with, Mother Nature's untimely interventions all too frequently grounds and re-routes flights. While anyone who flies regularly can attest to how frustrating unexpected changes to travel plans can be, many of us don't take into account is how frustrating that is for airlines as well. Fortunately, rapid advancements in technology have helped airlines mitigate the impact of unforeseen circumstances. From new business models to the instantaneous communications and insights provided by the Internet, the airline industry has continued to leverage advancements in technology and communication to better serve stakeholders around the world. This digital revolution has provided new opportunities for airlines but progress is not without risks and going digital has exposed the industry to new threats, including those posed by potential hijackers sitting at home armed with nothing but their laptop.

THE FAA HELD MEETINGS WITH MAJOR US AIRLINES TO DISCUSS POSSIBLE BREACHES ON PLANES.

Our newfound global interconnectivity has given maliciously minded individuals and groups far more ways to wreak havoc for whatever nefarious purpose. These people are not theoretical threats either, in the summer of 2015 hackers successfully grounded 1,400 passengers in Europe.[1] It's not just ground computers that are exposed, either, the FAA held meetings with major US airlines to discuss possible breaches on the planes themselves. At the cruising altitude of a Boeing 747, 30,000 feet, mistakes can affect more than just the bottom line.[2] Passenger planes have been a boon to travel, allowing us to see faraway places and visit loved ones half a world away in a fraction of the time it took just 120 years ago. The whole industry is bent on keeping malevolence from turning our fastest mode of transportation into a weapon of destruction.

[1] Marsh, R. (2015, June 22).

[2] Vanian, J. (2015, June 29).

THE PROBLEM

When a major international airline needed to switch Security Information and Event Management ("SIEM") systems, they needed SIEM agents that could monitor and report logs between both the external and the new internal SIEM servers. A hefty chore that neither the existing SIEM solution nor the new one could handle. The airline also had network traffic concerns from event logging: *How do you filter the data to just the critical elements? What if you filter out something important?*

As the airline didn't want this period of transition to expose them to security threats, and they couldn't let the transition create a gap in their log monitoring. They needed a third-party solution.

Whenever organizational change is instituted, the process of change management can be a headache for all involved. No matter how organized or how diligent, things always seem to go awry at the most inopportune moment. So, the airline needed a solution that prevented threat exposure during their transition from one SIEM system to another.

THE SOLUTION

Most vendors require you to buy their SIEM servers if you wish to use their SIEM agents, and often the agents are an afterthought to the server. Meaning that the agents lack the desired functionality and usually don't work with third-party software.

This airline had a litany of criteria and was frustrated by how few of their requirements were met by any of the vendors they had investigated. However, there was one solution, Snare - a well-known and well-respected brand; that is used and trusted by governments and private enterprises around the world. Snare provides a complete SIEM solution, that can be 'mixed-and-matched' to optimize your existing platform. Snare is built to make life easier, not force you to redo your entire cybersecurity strategy. Thus, it was the only solution that could easily help this airline migrate from one system to the other.

MOST VENDORS DESIGN THEIR SIEM AGENTS AS AN AFTERTHOUGHT TO THEIR SIEM SERVER.

Snare Agents also provide a bevvy of functionality that made them more appealing than the agents of the airlines new SIEM system. While the airline was delighted that something out there could enable them to make a seamless transition between SIEMs, *what about their other criteria?*

Snare has granular objective based event filtering and truncation that minimizes network traffic requirements, a huge benefit for the airline. Snare also provides event log caching, which is

SNARE IS NOT JUST A STOP GAP BETWEEN THE OLD SIEM AND THE NEW, BUT A PERMANENT FIXTURE OF THEIR SIEM SOLUTION.

hugely beneficial in the event of a network or server disruption. The more the airline learned about Snare and the more they tested it out, they realized that they needed the Snare Agents as a permanent fixture in their SIEM solution.

As for the redundancies, the airline knows whenever massive change is instituted throughout an organization there is always the risk that things go awry in any number of ways. That is why this airline was excited that Snare provides plenty of failover and redundancy functionality as they transition. The Snare system met the airlines criteria and even had time-zone normalization to keep everything humming along smoothly.

In addition to their security requirements, the airline had several compliance requirements it was concerned with. Snare Enterprise complies with any number of standards. Upon learning that Snare also helped them meet the requirements of NISPOM, PCI, and SOX they decided that Snare would not just be a stop gap between the old SIEM and the new, but *a permanent fixture of their SIEM solution.*

This international airline learned why Snare is trusted globally, and you can too: Get your 30-day trial free now!

Sources:

Marsh, R. (2015, June 22). Hackers successfully ground 1,400 passengers. *CNN*. Retrieved from http://edition.cnn.com/2015/06/22/politics/lot-polish-airlines-hackers-ground-planes/.

Vanian, J. (2015, June 29). How the FAA and the airline industry hope to protect planes from hackers. *Fortune*. Retrieved from http://fortune.com/2015/06/29/faa-airlines-planes-hacked/.