

Case Study

COMPANY: INSURANCE COMPANY

INDUSTRY: INSURANCE

CHALLENGES

- LACK OF CONTINUOUS VISIBILITY INTO THEIR EXTERNAL PERIMETER
- DIFFICULTY TRACKING ASSETS ACROSS MULTIPLE CLOUD PROVIDERS (AWS, AZURE, GCP)
- INABILITY TO TRACK RESOURCES SPUN UP BY SUBSIDIARIES AND TEAMS
- NO SYSTEMATIC WAY TO DISCOVER AND MONITOR ALL POTENTIAL EXPOSURE POINTS

SOLUTION

ATTACK SURFACE MANAGEMENT (ASM)

“

This challenge became apparent during an initial demo with Searchlight, where a unique exposure was revealed that no other ASM tool had discovered.

This challenge became apparent during an initial demo with Searchlight, where a unique exposure was revealed that no other ASM tool had discovered. This issue involved an unauthorized asset exposing sensitive information, which if exploited, would have allowed an external party to gain full control over the resource.

The Information Security Manager explained, “We have a lot of subsidiaries that sit underneath our main grouping. So we've got the challenge of multiple cloud providers, firstly, but then also multiple teams in multiple organizations that can have different levels of access to be able to spin things up as and when needed.”

CLOSING THE DOOR TO THREAT ACTORS

This insurance company was seeking an Attack Surface Management (ASM) solution to gain continuous visibility across its external perimeter. They needed a way to understand the full extent of their rapidly evolving AWS, Azure, GCP environments, including newly created resources by teams across the business. Given how dynamic their attack surface is, the company wanted to be able to quickly discover unknown or improperly secured assets that could be exploited by attackers.

While the organization has previously attempted to manage its external attack surface manually, their offensive security team became frustrated with the lack of continuous, automated visibility and the inability to keep up with the rapid changes in their environment.

KEEPING UP WITH RAPID CLOUD INFRASTRUCTURE GROWTH

By working with Searchlight and adopting their Attack Surface Management tool, the insurance company has transformed the manual, labor-intensive process into an automated, continuous monitoring solution that keeps pace with their rapid cloud infrastructure growth.

This meant the organization could expand their monitoring by 400 per cent from 2,000 assets to over 10,000, all while having the confidence there wouldn't be any unknown or improperly secured assets that could open the door to threat actors.

Having this level of visibility matched the organization's risk-averse strategy by protecting its assets and liabilities, and the products they sell. Given the insurance sector's high bar for security, having full asset discovery and monitoring allows them to outpace attackers and avoid headline-making incidents.

RESPOND TO CRITICAL INCIDENTS QUICKER

According to the Information Security Officer, one of the main benefits of the tool is that it has accelerated how quickly they can detect and respond to critical incidents

"The platform has well and truly paid for itself in what it's found and how it's helped us respond to incidents," the Information Security Officer elaborated.

By integrating Searchlight's tool into their workflows, the organization has strengthened its ability to respond to critical exposures with speed and consistency. Automated, SLA driven alerts ensure the right teams are engaged the moment an issue is detected.

“

The platform has well and truly paid for itself in what it's found and how it's helped us respond to incidents.

The platform is now used across security operations, offensive security, application security, and incident response within the organization, giving each team the visibility and context they need to act decisively - delivering measurable ROI through faster response times and improved risk mitigation.