CASE STUDY

Engineering Services in Public Cloud Get Security Upgrade

KEYSIGHT

Organization

- Government agency

Challenges

- Validate security in the cloud
- Enable threat hunting in public cloud infrastructure

Solutions

- Keysight CloudLens visibility to application-layer data
- Keysight BreakingPoint simulations

Results

- Forensics solution reduces security risk by 50%
- Manual effort to test security reduced by one third
- Time required to detect and contain DDoS attacks reduced by 50%

Challenge

A government agency that provides engineering services for constructing physical infrastructure migrated their key applications and services to a public cloud infrastructure as part of a cloud first mandate intended to reduce spending on IT infrastructure and maintenance. As part of the migration, the agency wanted to deploy a robust security architecture.

Public cloud is a good fit for agency's work

Government agencies in many countries are recognizing the maturity of the public cloud and adopting it to reduce infrastructure costs and introduce new services more quickly. The agency was rolling out new structural engineering and construction management applications that would allow them to more easily coordinate their work with other entities and complete projects with greater speed, efficiency, and accuracy. Public cloud infrastructure was chosen for its ability to scale easily as projects expand and be dismantled when projects are complete.

The agency's adoption of the public cloud aligns to a new federal strategy on digital transformation. This strategy requires all new services be architected specifically for the cloud, encourages using the public cloud as the default platform, and advocates for taking full advantage of cloud automation practices.

> “Cloud security fears are often overstated as specific to cloud, when the risks apply equally to cloud providers or inhouse architectures.”
>
> **Chief of Information Security, Federal Engineering Agency**

Security in the Cloud is a Shared Responsibility

The agency’s chief of information security (CISO) was not overly concerned about the move to the public cloud but was concerned with the general prevalence of cyberattacks and security incidents. The potential risk of outages in critical public resources such as water treatment plants, energy production facilities, and transportation infrastructure can affect national security. This meant that traffic flowing to, from, and between their cloud instances would need to be closely monitored for red flags that could indicate an intrusion or data breach.

Security Forensics Requires Network Packets

Although the public cloud can be an essential tool for helping federal agencies increase operating speed and efficiency, agencies must still pay close attention to incident detection and response—particularly as cybercrime grows more sophisticated. The security team evaluated several forensics solutions that use correlation analysis to uncover the source of breaches and attacks. They realized the solutions required packet-level data, which was not available from their public cloud providers. To solve this problem, the team turned to Keysight CloudLens, a visibility solution for accessing packet-level data in cloud environments.

The team appreciated that Keysight CloudLens works with all major public and private cloud platforms, so they are not locked into any single vendor. Also, because CloudLens is container-based, it scales automatically every time a new cloud instance is generated, so there are no blind spots where malware can hide.

An unexpected benefit of deploying Keysight CloudLens was the agency’s ability to reduce consumption of cloud-based security solutions. Keysight CloudLens is able to sort and segment network packets based on application and context information, which reduces the volume of relevant traffic delivered to each security solution. With less traffic to process, the agency estimates they will save $41,000 each month (or nearly half a million dollars a year) on cloud-based threat detection and security services.

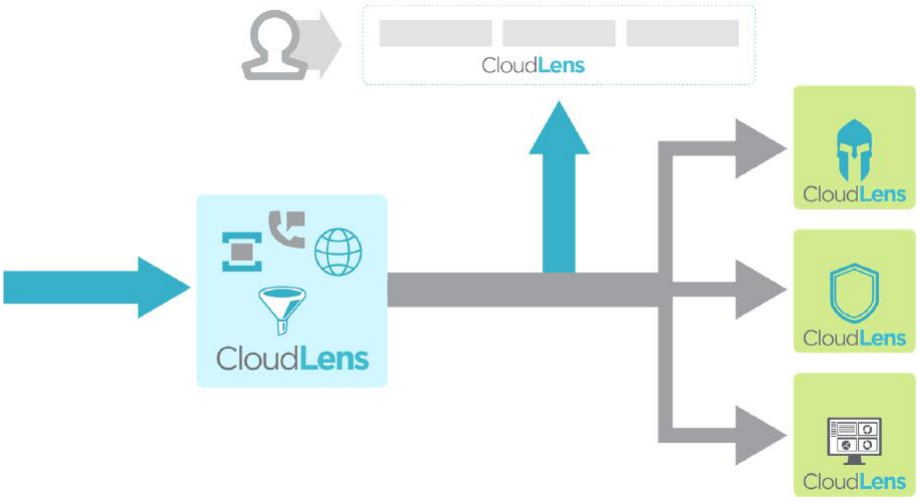

Figure 1. Function of Keysight CloudLens

Security Validation Is Essential

As application development has become more agile and continuous, federal agencies are required to perform quarterly drills to validate the continued effectiveness of security systems, processes, and personnel. To reduce the manual effort involved in executing these drills, the agency implemented the Keysight BreakingPoint test platform with security intelligence provided by the Keysight Application and Threat Intelligence (ATI) Research Center.

Using advanced surveillance techniques and methodologies, the ATI team aggregates and confirms all newly discovered attacks and malware into a threat intelligence database that is updated hourly. Keysight BreakingPoint uses this intelligence to model security breaches and threat vectors in extremely realistic test simulations. The agency can measure their response to a simulated attack and make adjustments as needed. The CISO estimates the manual effort involved in these tests is a third of what it was before implementation of BreakingPoint.

> “With forensics in place, we believe our total security exposure is reduced by 50 percent. Packets contain information that even a cybercriminal cannot manipulate. Our forensics analysis can reveal incredible detail about any malware in our network.”
>
> **Senior Security Analyst, Federal Engineering Agency**

Cyber Training for DDoS Response Team

The simulation capability of Keysight BreakingPoint Cloud is also helpful in training the agency's DDoS response team, which is responsible for ensuring a fast and effective response to an attack if one should make it through the company's defenses. Through repeated simulations, the team was able to improve the speed of detection and containment by nearly 50 percent, reducing the risk that an attack would harm the agency's work or limit public access.

Conclusion

The federal government agency is deploying new services on public cloud platforms with confidence. They are able to access all the packets moving through their clouds, eliminating blind spots that can harbor security attacks. Their security forensics solutions help them detect multi-stage attacks that can hide from firewalls and malware detection tools. Visibility to packet level data gives them valuable insight they can use to improve the speed of detection and incident remediation to limit damage. Continuous validation of security infrastructure helps them ensure their solutions are still configured properly and working effectively.