CASE STUDY

Media Provider Enhances Cloud Security

This premier developer of entertainment software is renowned for creating some of the industry's most critically acclaimed games. Their track record includes over a dozen #1 games and multiple Game of the Year awards. The company's online gaming service is one of the largest in the world, with millions of active players.

Customers have high expectations of games from this label, so the company has begun hosting new games on infrastructure from a large public cloud provider. The flexibility of the cloud lets them quickly scale to meet the demand for highly anticipated new games. At the same time, they must rethink how they will manage security and optimize performance in an environment where they do not have access to packet-level data.

Maintaining Security in the Public Cloud

Hosting multi-player games in the public cloud exposes the company to web attacks, data theft, and fraud on a daily basis. Robust security solutions are needed to keep an attack from disrupting the online game experience, corrupting individual player histories, or stealing sensitive customer data.

In addition to a using a Web application firewall, the security team relied on intrusion detection systems (IDS) and forensics tools to identify anomalies in user behavior. Attacks are increasingly multi-level and the advanced algorithms of these solutions are used to detect complex threat signatures. The challenge was getting access to the packet-level data the solutions required. The public cloud provider offered a proprietary monitoring solution, but the security team did not believe it offered enough protection for the launch of a highly-anticipated new game. Working with their local cloud integrator, the company deployed Keysight's cloud visibility solution to provide copies of cloud traffic data to their security solutions. A key advantage was being able to manipulate the data sent to each solution from a central location. This minimized the need for manual configuration and reduced the risk of error. And with application layer visibility, they could track user access and activity to detect security exposure such as changes to configuration files and stop attacks that may be in process.

"Now that traffic in the public cloud can be inspected, we are more confident of being able to identify attacks and implement a recovery plan to protect our assets." — Senior Director of IT Security

Company:

- Provider of media and entertainment software

Key issues:

- Online gaming constantly exposed to attacks and malware
- Need way to identify malicious traffic and reduce impact to users and gaming experience

Challenge:

- Intrusion detection solutions require packet-level data that is not accessible from public cloud providers

Solution:

- Keysight CloudLens platform for data visibility

Results:

- Ability to see data inside every cloud deployed
- Automatic deployment and scalability of visibility sensors

Increased protection from attacks that impact game experience or expose customer data

KEYSIGHT TECHNOLOGIES

Visibility Deployed Automatically

Because packet access was critical to the detection and forensics, the company wanted to make sure configuration errors were minimized. They were reassured to know that Keysight CloudLens is a fully distributed, container-based solution and is deployed automatically inside each new public cloud instance that is spun up.

- No additional infrastructure is needed, and no manual configuration is required.
- Visibility is automatically installed in each cloud instance and is consistent every time, eliminating configuration errors.
- Pre-validation between CloudLens and security solutions means copies of packet data immediately begin flowing to the IDS and forensics tools.
- Full inspection of cloud traffic begins at the same time cloud is deployed.

Unlimited, Cost-Effective Scalability

The team considered another visibility solution, but found it was not fully distributed and relied on a centralized visibility engine to collect and filter cloud traffic. At some point, when traffic volume exceeds capacity, a centralized infrastructure will need to be upgraded. With more workloads moving to the cloud, the company's infrastructure budget was shrinking, and the team was concerned about the cost of such an upgrade. They appreciated the fact that Keysight CloudLens collects and filters data right inside each cloud instance, so it can scale without limit, right along with their clouds.

Another advantage is that CloudLens visibility is available as a cloud-based service, so the company can pay for it as a monthly operating expense, instead of as a capital expenditure, to match the way they pay for their cloud infrastructure.

Conclusion

This digital media provider successfully deployed a visibility platform to see inside their public cloud instances and access the packet-level data they needed to improve their security posture. Their security solutions now get complete access to data and metadata in the cloud, so the cloud is no longer a blind spot in their network. With this information, the IDS and forensics tools can pinpoint attacks more quickly and initiate recovery before vulnerabilities can be exploited. The security team can resolve alerts more efficiently and the network team does not have to manually configure visibility with each cloud deployment.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES