Observability Case Study: Interview with the CTO of a Travel and Hospitality Agency in the U.S.

ASSOCIATED WITH THE WHITE PAPER:

Network Intelligence and Insights: Driving Performance, Protection, and Productivity in Observability

AUTHORS:

Christopher Kissel

Mark Leary

Business Scenario

This travel and hospitality agency in the United States was heavily affected by the COVID-19 pandemic in 2020 and going into 2021. The company looked at its hand and decided that it would use the slowdown to bolster its digital transformation (DX) initiatives. The DX timetables for completion went from a five-year project to 18 months.

Critically, the number one initiative for the company was to develop an all-cloud architecture. At first, this seems counter-intuitive. Many travel/hospitality companies have legacy mainframe computers hosted in private datacenters. To this day, mainframes have great capacity with the ability to instantaneously update records for keystroke errors and have several failover procedures. However, when interviewed, the CTO spoke enthusiastically about the combination and possibilities of using Google Cloud Platform (GCP) with Kubernetes. In Kubernetes, there is a feature called Horizontal Pod Autoscaler (HPA). This Kubernetes cluster manager basically looks for CPU usage and allocates more capacity to keep the current levels of utilization. The solution seems to be more elegant than the traditional paradigm of provisioning servers for load balancing. **Read on...**

How Network and Security Operations (NOC/SOC) Are Managed

The CTO is responsible for all product engineering, data engineering, infrastructure operations and machine learning. The IT infrastructure is still somewhat siloed in that the company has a security engineering team, a SecOps team, and an infrastructure engineering team, and underneath infrastructure engineering it has network engineering and observability departments.

The CTO estimates that the transition to an all-cloud architecture is about 90% complete. According to the CTO, the network engineering team was given the advanced work in developing cloud architectures. The CTO is satisfied that while the telemetry and tools that are used by networking and security teams are slightly different, they ultimately provide a holistic view of the network and enable a unified workflow. Every two weeks, the CTO puts the company through its paces as it performs chaos testing to ensure that platforms can handle a maximum workload.

Where Observability Fits In

In this case, observability existed as an important consideration when transitioning to the all-cloud environment. The CTO described Kubernetes as a Ferrari—a high performance machine that requires a lot of tuning and maintenance to work as expected. Kubernetes combines auto scaling with networking and, the CTO cautions, *"with DNS, if you do not get all three of those components running the right way, it can go horribly wrong."*

The biggest concern that the CTO has is vulnerabilities coming in from the supply chain. The travel/hospitality company has a tool that can scan its entire container environment and find third-party vulnerabilities. Another tool can see if there are any rogue containers that are unaccounted for and running on the network.

Even as the company is transitioning into GCP environments, the need for observability exists. The company does not do microsegmentation by logical business groups, but it monitors by front-end/back-end processes, and within zones. The challenge is that the adversary is fluid. If an identity is compromised, there are no additional controls that can find the adversary. An observability platform will monitor Port anomalies and anomalies based on user behavioral analytics (UBA), in GCP or in heterogeneous networks.

Opportunities to Enhance Operations with a Greater Commitment to Observability

Redundancy is useful. The metadata from GCP and what remains in the on-premises environment should still be cross-correlated. Interestingly, the company uses an identity and access management (IAM) vendor to authenticate its employees and its customers. The company has two-factor authentication for customers logging onto the website.

One objective the CTO was persistent in achieving was perfect compliance with NIST frameworks. NIST SP 800-53 is a list of controls that is operational, technical, and managerial. Like the MITRE framework for vulnerability scoring, the NIST controls aim to mitigate confidentiality, integrity, and availability stemming from vulnerabilities. Toward compliance, the NIST 800-207 network compliance standard is, *"the enterprise must be able to view all network traffic,"* and an observability tool satisfies this requirement.

Relying upon what can natively be accomplished within GCP isn't enough. Do keep in mind that any internet session requires an initial association between a request for access and the formal acceptance that the session should begin. With a clever adversary, port spoofing becomes problematic. Assuming that the adversary is in the network and can access the NetStat/S registry, the adversary can initiate a port spoofing session that appears to be encrypted transmission but is in fact an obfuscated SSH session.

Observability is inextricably tied to network performance monitoring. Part of an observability platform is monitoring for CPU availability for security tools and applications. Security becomes compromised when CPUs are at capacity and application performance degrades or is dropped at CPU capacity. Native support for multi-honing is an important feature that can be offered in an observability platform. A host configuration is created that provides multiple options for remote workers or other types of devices to access the internet (as well as east-west traffic optimization).

Part of the reason to move toward a cloud environment is the ability to facilitate DevOps. The principles of observability can be applied to Kubernetes, Dockers, or cloud instances like EC2.

Observability still acts as the final arbiter of device discovery. Devices fall off of the network due to power surges or software updates or any number of mundane but common network events. Observability can track entities and applications without an agent and can do so in hybrid or heterogeneous networks.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

@idc @idc idc.com

Privacy Policy | CCPA