AT&T Business

The New Normal

Unique Challenges When Monitoring Hybrid Cloud Environments

The Evolving Cybersecurity Landscape

Every day, the cybersecurity landscape is expanding around us. Each new device connected to the network presents a new attack surface for those with malicious intent. With so many companies migrating to the cloud, the security landscape is only becoming more complex. In recent studies[1], 91% of modern enterprises have already begun scaling to the cloud. However, 60% of those organizations will likely never transition their entire IT services to the cloud - making hybrid IT environments the most common architecture for today and into the foreseeable future.

Hybrid architectures consist of applications, network, and server components that exist both on-premises and with cloud-providers. In some cases, bandwidth consumption can prohibit migrating some servers, such as consistently utilized applications with minimal scaling or data intensive client / server models, and require companies to maintain both on-premises and cloud environments. These hybrid architectures enable businesses to expand their infrastructure quickly and effectively. They allow for rapid scalability, more predictable costs and significant decrease in budget needs for large expenses like upfront hardware costs, server storage, and maintenance. While this evolution is great for business ROI, it is very difficult for an organization's cyber capability, including its Security Operation Center (SOC) to keep up with a dynamic threat surface.

Cloud migration can be a more effective method of outsourcing IT overhead costs to 3rd party vendors because it offers a more systematic and repeatable model. Rather than interfacing with people in a traditional outsourced IT model, Amazon Web Services (AWS) has created automated and abstracted methods to make "outsourcing IT" a virtually seamless digital experience. The Gartner graphic below [figure 1] depicts the varying levels of management tasks that IT will need to perform, and highlights the tradeoff of each in the areas of control and choice.

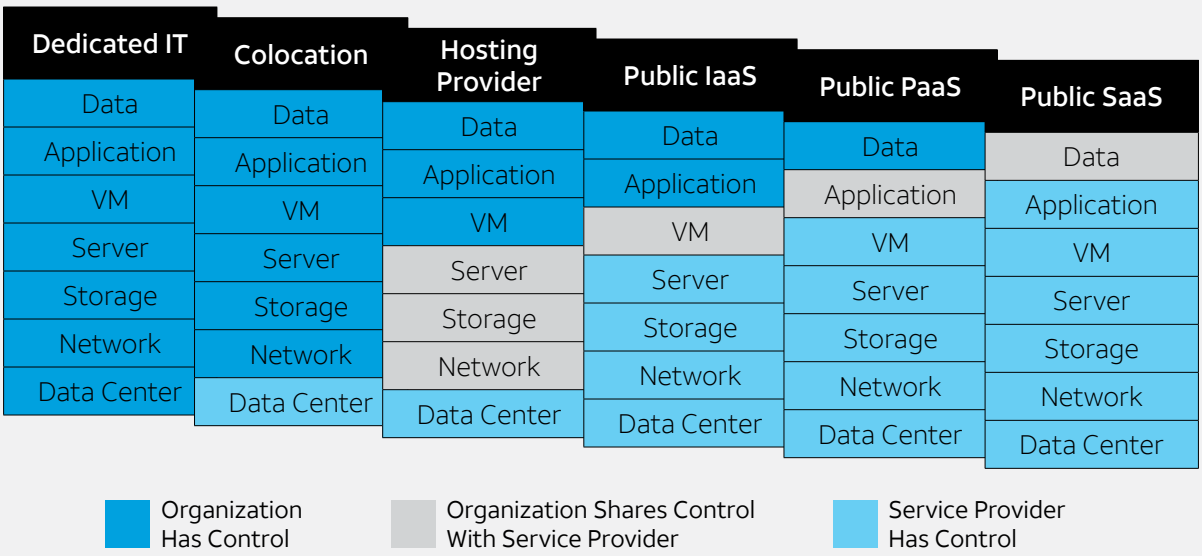
This ever-evolving landscape requires SOCs to adapt from a traditional style of monitoring to a more dynamic system of always-on analysis in order to maintain visibility into the network and effectively protect against threats.

Understanding On-Premises and Cloud Behavior

Traditional on-premises SOCs often utilize a centrally managed logging platform known as a Security Information and Event Management (SIEM) tool. In addition to the SIEM, analysts also utilize several other security components such as firewalls, Intrusion Prevention Systems (IPS), Anti-virus (A/V), and various Threat Intelligence sources. These security tools are the eyes and ears of any SOC. However, in a hybrid environment, many of these tools are either not deployed or cannot be deployed to the cloud portion of the environment due to the inherent abstraction model

Figure 1

Architectural Comparison of Ownership by Cloud



Source: Gartner (October 2016) https://www.gartner.com/BINAVRIES/content/assets/events/keywords/catalyst/catus8/2017_planning_guide_for_cloud.pdf

1. *SolarWinds IT Trends Report 2016: The Hybrid IT Evolution http://it-trends.solarwinds.com/reports/2016/the-hybrid-it-evolution/north-america.pdf*

of the cloud. For example, certain layers of the Open Systems Interconnection (OSI) model are hidden from the end consumer in such a way that traditional data elements like network traffic may not be available for organizations (and their SOCs) to monitor.

The key to gaining visibility into cloud environments without the traditional processes and tools lies in effective training and situational awareness for the SOC team. Cloud architecture training will allow the staff to understand the nuances and capabilities of the cloud, including serverless computing, API security, security groups, and establishing an organization's overall security policy configuration requirements. **Training on the new cloud toolset is equally important in educating analysts not just on the architecture, but on the additional functionality that is now available through these tools.**

Engineers who are responsible for securing both on-premises and cloud environments must understand the types of activity and threats unique to each environment. Normal behavior in an on-premises environment may not be normal behavior for cloud environments, and vice versa. One example of this distinct difference in network behavior is interactive logins (i.e., users logging into a server via a Graphical User Interface (GUI)). On-premises servers typically have many logins by various administrators, however, this behavior becomes atypical in a cloud environment. Most cloud production systems are constructed from build scripts and have no need for interactive logins -- if a change is needed to a cloud

system, the build scripts are modified and the system is rebuilt from a clean image. **A SOC analyst must be able to understand the difference between on-premises and cloud behaviors and the context around an event in either environment in order to react accordingly. This variance, although small, could be the difference between a full compromise and blocking an attacker.**

The main lifeblood of any SOC function is environmental data, specifically event logs. Comprehensive logging is one capability imperative to a SOC in order to track network activity, gain deeper operational context, and maintain accountability of users and resources. However, this basic service does not translate cleanly from an on-premises log to a cloud log. An on-premises logging solution collects logs centrally from all devices for correlation based alerting on predefined use cases. This is typically not the

A SOC analyst must be able to understand the difference between on-premises and cloud behaviors and the context around an event in either environment in order to react accordingly.

case for cloud environments since log data may not be readily available. If logging is available, it is generally stored in a cloud storage system. Two options to reconcile this issue are to push cloud logs back into the on-premises logging solution (i.e., an authoritative log), or to extend your traditional logging infrastructure into the cloud. Both approaches have potential drawback, which could include increased data transfer costs for your company or sluggish performance while searching for logs. These issues represent a real security management challenge. How can a SOC provide the same monitoring capabilities for on-premises and cloud systems?

Use Case Variances

Simply taking on-premises use cases from your SIEM tool and applying them to a cloud based environment can lead to false positives, or worse, false negatives. **SOC functions must create and manage two separate use case libraries which address threats in both environments, maintain an up-to-date asset management inventory, and know where the boundaries of on-premises and cloud exist for their unique hybrid environments.**

Misconfigurations - AWS S3 buckets (data storage container) utilize security groups or roles to restrict access and protect data. A SOC function must know how to build a use case to alert on unencrypted and publicly accessible buckets. Misconfigurations of S3 buckets can result in public disclosure of sensitive information and have been the root cause of several recent data breaches.

Network Visibility - Basic firewall alerting is another problematic issue when logging cloud events. In traditional on-premises monitoring, clients own the networking infrastructure and are thus able to configure monitoring of logs. In most cloud environments, the cloud provider typically owns the infrastructure which enables them to manage the physical components of cloud services. By outsourcing these management responsibilities, corporations sacrifice absolute visibility into network traffic, but are able to operate more economically and with shared risk responsibility.

Machine Learning - Correlation engines, an integral part of traditional on-prem SIEMs, rely on complex rules that trigger alerts based on a sequence of events across more than one log source or device type. While correlation rules are often more advanced than simple pattern matching use cases, they often require significant resource overhead (expensive, powerful servers) and expert tuning skills to build appropriate use cases and alerts. **With the transition to hybrid environments, the introduction of scalable machine learning services to such complex use cases can enable automated responses and anomaly based alerting, in turn removing false positives that require significant analyst time to evaluate.** These capabilities not only improve the average response time of alerts, but also allows SOC analysts to focus on triage rather than detection.

Managing Assets

A cloud-based system's ability to autoscale based on demand has led to new methods of managing assets. Servers are often treated as disposable assets and may spin up or down with unique hostnames and IP addresses as needed to scale for demand. When you take this logical resource approach along with physical on-premises asset management, you've created a rather complex puzzle for Hybrid SOCs.

To tackle this issue, SOCs must develop new tool sets which use APIs to see to it that cloud systems are discovered and properly configured. On-premises vulnerability scanning, for example, will utilize a port scan to map a network and host environment, and compares this against a library based on known vulnerabilities. This capability does not operate in the same manner in cloud

environments. Scanning externally accessible IP ranges and systems theoretically can be done the same way, but scanning entire Virtual Private Clouds (VPCs) cannot.

Port scanning is typically against the terms of services for cloud providers, forcing vulnerability tools to use APIs to pull this information. Information which had been readily collectable must now be collected in API calls, and in this case, vulnerability checks. These are generally conducted at system build time, rather than an ongoing vulnerability scanning procedure.

While patch management is not a SOC function, monitoring systems via vulnerability management for missing patches is part of understanding the weaknesses in a network that can allow attackers to exploit bugs and gain unauthorized access to an organization's network. On-premises systems often plan monthly downtime in order to implement key patches. In the cloud, companies can "roll" the systems, which builds a new fully patched system at build time. The system is then run against vulnerability and configuration checks. Once a system passes all security checks it is then promoted to production. This process occurs daily or weekly, allowing code to move to production quicker and more effectively, while also eliminating downtime for the business. The cloud approach to patching is extremely useful and efficient when it comes to tackling zero day vulnerabilities like heartbleed and eternal blue (WannaCry).

Improving Protection with Tools, Training and Next Generation Security Mindset

Forward thinking SOC functions must realize they are not just first responders, but also cloud security analysts and architects. They must be able to perform log analysis across a wide variety of tools and platforms, as well as understand how to collect and run cloud based tools to obtain the information they are looking for through scripts and APIs. They must also have knowledge on how to recreate instances in the cloud, what a build script looks like, what services a company subscribes to and the context around each alert to accurately determine the threat level. SOC staff must also have knowledge on how to script, which is typically lacking in today's Tier 1 SOC personnel. The end result and business impact is that qualified SOC talent will become harder to find and on-going training will be required in order to perform their job functions appropriately.

For more information about AT&T Cybersecurity Solutions and Threat Manager, visit here.

Share this with your peers