VPC Flow Logs Are Not Enough

MODERN ENVIRONMENTS REQUIRE A NEW APPROACH TO SECURITY

Lacework™

It started with the network...

Traditional security approaches evolved in static environments. Change was slow because activity was limited, in large part, by the capabilities of available technology resources. But with the advent of new methods for creating and deploying data and applications, and thanks to the dynamic nature of the cloud, organizations are increasingly able to connect widely and quickly to disparate data sources through microservices and other agile architectures. This changed how IT organizations viewed security because these architectures allowed for the rapid and dynamic creation of connections and endpoints. Stable networks, managed servers, and monolithic applications gave rise to network-based tools that delivered security using connection information and packet data.

In the cloud, organizations rely on virtual private clouds (VPC), and to understand the risk potential of your cloud environment, you need a way to track and register VPC activity. VPC flow logs capture data about the IP traffic that moves into and out of your network, and they provide cloud users and administrators with detailed information that can help them identify anomalies and inconsistent behavior that could be the result of attacks or bad actors trying to penetrate their network. Yet, because they cannot scale, are prone to false positives, and due to their inherent limits on file integrity monitoring, VPC logs are not equipped to keep your cloud secure.

But the cloud needs a new approach.

Legacy hardware vendors like Palo Alto Networks have built solutions around VPC flow logs which operate in a way similar to NetFlow logs which are used with traditional hardware like routers and switches. The challenge is that the cloud operating model is completely different; executables come and go instantaneously, network addresses are recycled seemingly at random, and even the fundamental way traffic flows can change rapidly. You have to reset how you think about security in the cloud, and to do so it's important to understand that while VPC flow logs demonstrate some capabilities that are useful for security, an organization should not rely on them for accurate, comprehensive security insights.

Here are eleven ways network-based security tools based on VPC logs fall short when transitioning to the cloud:

#1 VPC LOGS ARE BLIND TO INTRA-VM AND CONTAINER TRAFFIC

VPC flow logs have visibility to all the network data which leaves an EC2 instance but are blind to what happens within the instance. The challenge is that in the new micro-services architecture you might have multiple containers running inside the same instance and their communication will not show up in VPC flow logs. The traffic which stays within the workload for all other applications will, however, not be visible to VPC logs.

CONTAINER NETWORK INFORMATION IS NOT VISIBLE #2

When using container orchestration tools like Kubernetes it's not possible to attribute the traffic to the correct container without being in the right name space. This is only possible with an agent which is able to get the right information on the interfaces and IP addresses for containers. The VPC flow log-based approach will not work with containers.

#3 NETWORK-BASED ANOMALY DETECTION CREATES A LOT OF FALSE POSITIVES

Nothing has confounded network security as much as the demise of static IP addresses and endpoints. Endpoints went from being physical machines to virtual machines, and now containers. Everything is dynamic, and nothing is predictable. This speed means that IP addresses and port numbers are recycled rapidly, making it impossible to know who or what is behind a connection just by looking at network traffic. Existing network and endpoint security solutions based on VPC flow logs are crippled when IP addresses and port numbers can no longer identify endpoints.

The ideal solution is to create a separate behavioral baseline for applications and users. Applications are more predictable than users and mixing them will create lot of false positives, As a result, the VPC flow logs cannot identify if a flow was originated by a user or an application.

Network-based anomaly detection using just port numbers also creates lot of false positives. Consider a scenario where Bitcoin apps use a specific port number; in a DevOps environment, the same application will use random ports, so the chances of false positives is extremely high if alerts are generated only using a port number.

USER ATTRIBUTION IS NOT POSSIBLE #4

At the user level, standard cloud DevOps practices of using service and root accounts have been a double-edged sword. While they accelerate the pace of software delivery, they have also made it easier to initiate attacks from these accounts.

The use of these accounts removes DevOps roadblocks, but they give attackers yet another place to hide. By co-opting a user or service account (and then escalating privileges to root in some cases), cyber criminals can evade identity-aware network defenses. Even correlating traffic with IAM or Active Directory can fail to provide insights into the true user. The only way to get the real user for an application is to co-relate and stitching SSH sessions which is not possible with VPC flow logs.

> *"...standard cloud DevOps practices of using service and root accounts have been a double-edged sword."*

#5 DEEP PACKET INSPECTION DOESN'T WORK

When security that is based on simple network characteristics (addresses and port numbers) failed to stop increasingly sophisticated attacks, the industry responded with DPI (aka "next-gen firewalls"). These tools still add value in the cloud when customers use similar applications (as they do in SaaS models), but in IaaS and PaaS models, applications are usually custom-built. Because next-gen firewalls can't understand custom applications (at least not without a herculean effort to build custom rules), they can't detect attacks.

The other challenge is the growing use of host encryption; trying to use standard network tools at cloud-scale makes any traffic analysis to identify applications extremely difficult.

CYBER KILL CHAIN MOVES BEYOND THE NETWORK #6

In a cloud environment, where network security isn't as effective as it once was, non-network attack surfaces are an even more urgent concern. Here are a few examples that illustrate this point:

- User privilege changes are a key indicator of the attack; these are not visible to VPC flow logs.
- New application launches and changes to packages don't show up in VPC flow logs.
- Changes in launch sequence of applications which can be an important indicator are only visible in an agent-based approach.
- Config file changes are not visible to network logs.

#7 NEFARIOUS ACTIVITY EASILY BLENDS IN

Software increasingly looks like Lego® blocks. Pieces fit together easily and standardized services simplify development and deployment. But there's a security risk hidden in this new approach: cybercriminals using the same standardized services are harder to detect with network only tools.

For example, an AWS S3 bucket used to store stolen data before exfiltration looks the same as an S3 bucket supporting a legitimate app. Standardization makes blending in much easier and the bad guys can hide in plain sight.

The VPC logs cannot distinguish if the traffic going to S3 is from a legitimate app or some data exfiltration.

To detect this activity, you need a behavioral model at the application layer that provides color and context to the activity happening in your environment.

FILE INTEGRITY MONITORING IS NOT POSSIBLE WITH VPC LOGS #8

File Integrity Monitoring is required by many compliance standards including PCI and HIPAA. The file changes can be a leading indicator of an attack. The hackers can change the executable or change the config files or delete the log files. The non-agent VPC flow log only approach will not be able to detect any file level changes.

#9 FILE BASED MALWARE DETECTION IS NOT POSSIBLE

One of the most important indications of a compromise (IOC) is the file hash. However, if there is a known vulnerability, that should be the first thing that is addressed. VPC flow logs, however, are of no help in this regard because they have no information on file hashes or packages.

VPC FLOW LOG BASED APPROACH DOES NOT SCALE #10

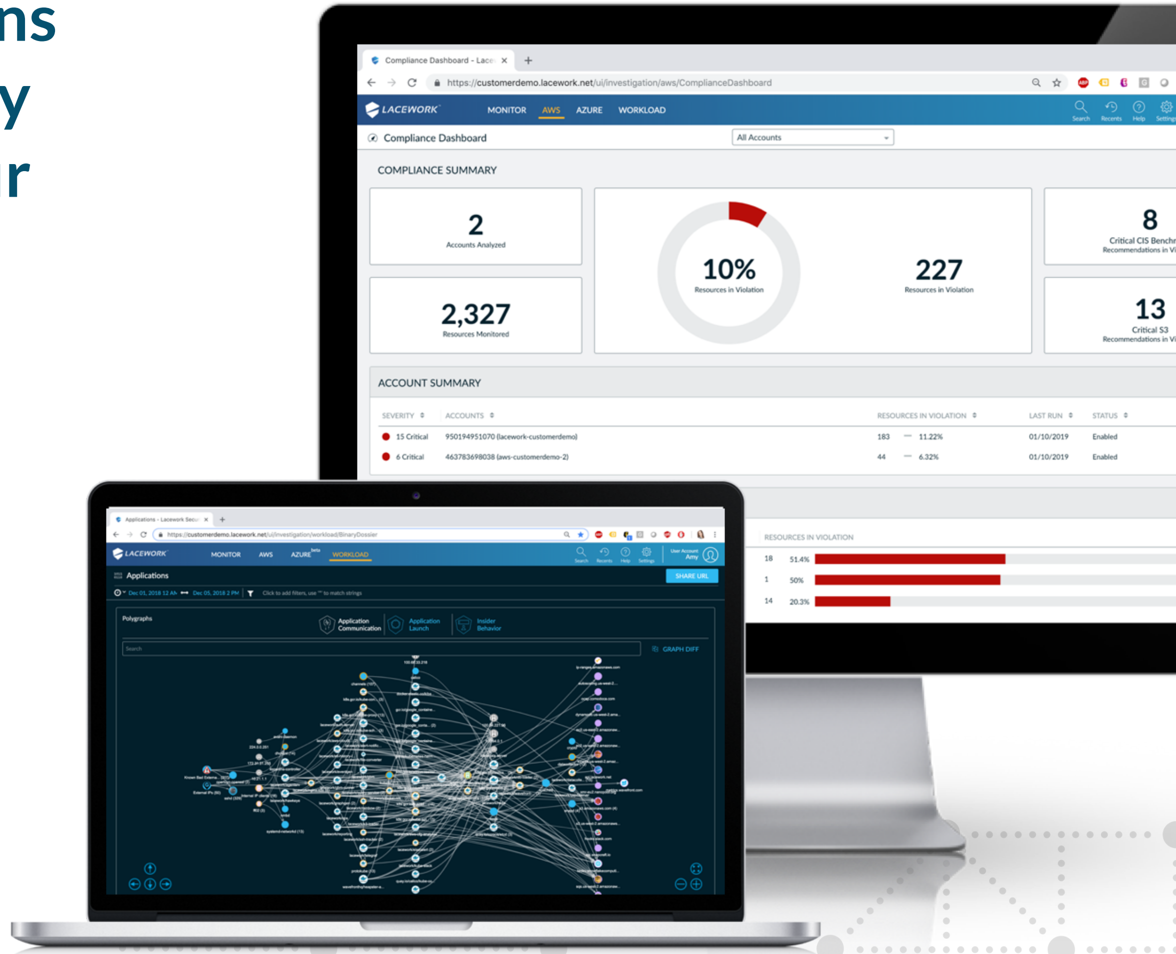
The East-West traffic is 4-5 times the traffic which transits North-South. The challenge is that VPC flow logs can become overwhelmed really fast if they need to be stored and analyzed over a long period of time. The right approach is to move from network logs to a logical apps model. Storing information that tracks a five-tuple talking to another five-tuple is useless as they do not provide the information needed for investigations. The more interesting information is which app to talks to which other app and it does not matter if it happened on one machine/IP/port or thousands of different ones.

#11 THE INEVITABILITY OF AN ATTACK

If any application is open to the Internet it will get attacked. There are hackers which are continuously looking to scan and attack anything which they can find. The challenge is that VPC logs will be alerting on these attacks even though majority of them are false positives. The ideal solution is to identify the front-facing apps and only alert if an attack happens to an app which is not front-facing.

Get actionable recommendations on how to improve your security and compliance posture for your AWS, Azure, GCP, and private cloud environments.

Streamline security for AWS, Azure, and GCP. Gain unmatched visibility, ensure compliance, and enable actionable threat intelligence.



FREE ASSESSMENT

Lacework™