10 Reasons VPC FLOW LOGS

Won't Keep Your Cloud Secure

VPC LOGS ARE BLIND TO INTRA-VM & CONTAINER TRAFFIC

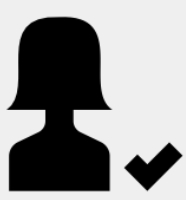
With multiple containers running inside the same instance, their communication won't show in VPC flow logs.

NETWORK-BASED ANOMALY DETECTION CREATES FALSE POSITIVES

Dynamic nature of the cloud means that endpoint security solutions based on VPC flow logs are crippled when IP addresses and port numbers can no longer identify endpoints.

USER ATTRIBUTION NOT POSSIBLE

The only way to know real user data is for application to co-relate, stitch SSH sessions. Not possible with VPC flow logs.



DPI DOESN'T WORK

The use of host encryption that tries standard network tools at cloud-scale makes traffic analysis to identify applications difficult an ineffective.

CYBER KILL CHAIN MOVES BEYOND THE NETWORK

Not visible in VPC flow logs: user privilege changes, app launches, app sequence changes, config file changes.

NEFARIOUS ACTIVITY BLENDS IN

Service-based architectures make it easy to mimic legitimate activity; VPC flow logs can't distinguish between authorized activity and hacking attempts.

FILE INTEGRITY MONITORING NOT POSSIBLE

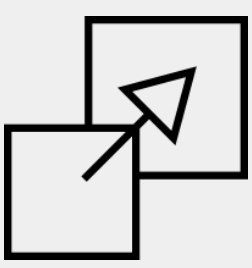
File-level changes not detectable, yet file integrity monitoring required by many compliance standards.

CONTAINER NETWORK INFORMATION NOT VISIBLE

When using container orchestration tools like Kubernetes it's not possible to attribute the traffic to the correct container.

NO FILE-BASED MALWARE DETECTION

VPC flow log have no information on file hashes or packages.



DOES NOT SCALE

VPC flow logs can become overwhelmed fast because of pace of traffic in the cloud.