Public Cloud Workloads at Risk

Bad actors target your workloads in infrastructure-as-a-service (IaaS) environments like AWS. They are well aware of enterprises’ migration to the cloud and the complexity of migrating both workloads and security controls into a shared responsibility security environment. They also understand that data center managers too often deploy internet-facing workloads in the cloud without the same levels of protection that they deployed in the on-premises data center.

Attackers employ a range of techniques to penetrate your cloud infrastructure, launch new instances, and move laterally to launch attacks on other workloads, before ultimately harvesting your data. These techniques include:

- Targeting your servers in public subnets in your virtual public cloud (VPC) on AWS.
- Exploiting a misconfigured server with open ports to gain a foothold in your internet-facing assets.
- Moving laterally in your public cloud to find servers in your private subnet which you thought were safe (because they do not have a route to the internet).
- Compromising servers running in your AWS instances and downloads data.

Detect Threats Entering or Moving Laterally within AWS

Lastline Defender™ for Cloud is the first native cloud Network Detection and Response (NDR) solution that delivers unmatched visibility of advanced threats in both your internal and external public cloud traffic in AWS. You can deploy Lastline’s industry-leading AI-powered threat detection to protect your public cloud workloads, without the need to deploy agents or collectors.

Lastline Defender for Cloud provides immediate visibility into threats and intrusions across your public cloud workloads, enabling you to detect and contain sophisticated threats before they disrupt your business. You gain immediate visibility of malicious activity entering and operating within your AWS environment so you can respond faster:

- **Inbound Exploits of Cloud Workloads:** Prevent attacks against vulnerable applications and services in public clouds
- **Malicious Lateral Traffic:** Detect when an attacker scans for other workloads and prevent discovery of additional services and block lateral movement and connection to an unusual port
- **Data Exfiltration:** Detect and block anomalous data access before a bad actor can exfiltrate the data

Accelerate Your Response to Cloud Workload Threats

Lastline Defender for Cloud uses a combination of three complementary techniques to detect the advanced threats that other tools miss and eliminate false positives:

- Leverage the knowledge in our Global Threat Intelligence Network to scan traffic metadata and payloads for variants of known threats
- Apply unsupervised ML to your network traffic to detect protocol and traffic anomalies
- Use supervised ML to automatically create classifiers that recognize malicious network behaviors and previously unknown exploits

Most AI-based network security products implement less accurate techniques. These probabilistic approaches lead to many false positives and hours of follow-up investigation.

Applying AI to network traffic will inevitably detect anomalous patterns of behavior, because that is what it’s designed to do. Unfortunately, it is virtually impossible for these other AI-based tools to understand if the detected anomaly is malicious or benign. After all, not all anomalous activity is malicious, and not all malicious activity is anomalous.
Lastline is different. Our solutions utilize AI that is automatically trained both on network traffic and malicious behaviors. This unique combination enables deterministic detections and eliminates false positives. This means more effective enterprise security with fewer resources.

Securing Your Workloads

You need the ability to see both the initial targeting of an asset in your public cloud and the subsequent lateral movement as the attack spreads to prevent data exfiltration. Lastline Defender for Cloud provides both an in-line perimeter sensor and VPC flow analysis for comprehensive threat detection and response:

- **Perimeter**: Delivers full packet (DPI) visibility into any malicious content in the access/egress (“North/South”) traffic between the internet and your cloud workloads.
- **VPC Flow**: Analyzes VPC Flow logs to support the monitoring of metadata of internal (“East/West”) traffic, including network anomaly detection, connection on unusual ports, and data transfer anomalies.

Protect Your Entire Network: Cloud and On-Premises

Lastline Defender for Cloud is part of the Lastline Defender NDR platform that detects and contains sophisticated threats before they disrupt your business, on-premises or in the cloud. The Lastline Defender platform delivers the cybersecurity industry’s highest fidelity insights into advanced threats entering or operating in your entire network, enabling your security team to respond faster and more effectively to threats.