Securing Your Cloud Workloads

Many forward-looking organizations are moving some or all of their compute resources over to Infrastructure-as-a-Service (IaaS) providers like AWS, Microsoft Azure or Google Cloud. They make the shift to take advantage of the flexibility of elastic compute resources and lower costs that IaaS offers. This migration has rendered many on-premise data centers obsolete, as well as the security strategy used to protect workloads in those data centers.

The Need to Protect Public Cloud Workloads

There are several issues related to migrating a data center to the cloud. Chief among them is that migrating security controls is too often an afterthought, something to be considered only at the end of the migration process.

What many data center managers fail to realize is that with AWS' shared security model, they are responsible for securing everything running on the AWS infrastructure. They incorrectly assume that because Amazon has locked down the infrastructure that it is also securing the workloads running on top of that infrastructure.

Instead, organizations need to deploy security controls designed specifically to protect public cloud workloads from attack. Consider the following attacks that can result in data exfiltration:

1. A bad actor targets your servers in public subnets in your virtual public cloud (VPC) on AWS
2. A bad actor gains a foothold in your internet-facing assets by exploiting a misconfigured server with open ports
3. A bad actor performs lateral movement to find servers in your private subnet
4. A bad actor compromises servers running in your AWS instances and downloads data

The built-in security controls in the AWS environment can provide some visibility and protection against these attacks but cannot block all of these malicious activities. Those tools also lack the ability to provide threat visibility across your cloud and on-premises environments.

The Migration of Threats to the Cloud

Unfortunately, attackers are well-aware of enterprises’ migration to the cloud and the complexity of migrating both workloads and security controls into a shared security environment like AWS. They 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.

There are several common mistakes that organizations make when migrating workloads to the cloud:

- **Believing that security is the provider’s responsibility**: Infrastructure providers like AWS are specific in delineating what aspects of securing the platform are their responsibility and what are the customers. Unfortunately, many organizations are not familiar with the IaaS shared responsibility model and, unlike a SaaS model (like Salesforce), they don’t realize that they are responsible for any applications or services installed on top of the infrastructure.

- **Expecting that what worked on-prem will work in the cloud**: Workflows and processes operate differently in the cloud than in on-premises environments, yet organizations sometimes operate on the assumption that the cloud versions of their on-premises security controls and processes will operate in the same way.
• **Failing to migrate security controls along with workloads:** As organizations migrate workloads, another issue is that they fail to embrace the same “Defense-in-Depth” approach as they did with their on-premises environments. The strategy of deploying multiple security controls at the edge and internally increased the likelihood of detecting threats.

• **Migrating incomplete or inconsistent security policies:** Some organizations migrate existing workloads to the cloud in a “lift and shift” approach, in which they move the workload “as-is” and do not rearchitect the workload to reflect the new cloud architecture. Although fast, this practice often fails to incorporate the latest cloud security controls, leaving the workloads exposed.

Here’s one such attack scenario that bad actors are using to target workloads in the public cloud:

1. An attacker exploits a vulnerability in a web server that is deployed in AWS and thereby gains shell access to it.
2. The bad actor performs a scan of the internal network that is accessible from the web server and discovers the existence of a phpmyadmin instance on a database server.
3. The attacker acquires access to the database server by leveraging default/weak passwords in phpMyAdmin (an open source admin tool), and as a result, obtains full access to the database content.
4. The attacker extracts the full database content and copies it back over to the web server, preparing it for exfiltration.
5. Finally, the attacker uploads the database content to an external server and monetizes their target’s data by selling it to a competitor or launching secondary attacks against the victim’s customers.

Multi-stage attacks such as the one described above pose a serious security problem to enterprises. Many companies have invested heavily in security capabilities for their on-premises assets and data centers. However, these solutions often offer little or no protection of cloud workloads. As a result, enterprises can’t defend themselves against threat actors that target their infrastructure.

**Limitations of Cloud Workload Protection Platforms**

To adequately defend their cloud workloads, enterprises are turning to a category of security controls known as cloud workload protection platforms (CWPP). CWPP products meet the unique requirements of protecting server workloads in public cloud infrastructure as a service (IaaS) environments. According to Gartner and Forrester, CWPPs typically provide a set of key capabilities to meet those security requirements that include:

- Network visibility
- Network segmentation and firewalling
- Malware protection
- Intrusion detection and prevention (IDS/IPS)
- Application control and workload verification against a baseline
- System and file integrity measurement, attestation, and monitoring
- Supplemental memory and exploit protection; privilege monitoring of processes
- Data analytics for kill chain identification, rapid alert prioritization, and investigation

However, organizations need more than just visibility into the internal cloud traffic that other CWPP products provide. In the attack scenario discussed above, any security strategy for protecting cloud workloads that lacks visibility into malicious traffic entering the cloud environment is incomplete. Organizations need the ability to see both the initial targeting of an asset in their public cloud and the subsequent lateral movement as the attack spreads to prevent data exfiltration:

- A perimeter-focused tool would potentially see the exploit targeting the vulnerable system, but miss the internal scanning, access to the database, and data harvesting.
- A network-focused tool will see the lateral movement after the compromise of the web server but not understand that the scanning is related to compromise and likely treat it as normal network activity.
- The perimeter-focused tool would see the data exfiltration but not realize the data was from a compromised database and likely permit the data breach.
The Lastline Difference

Lastline® recognizes the limitations of certain cloud workload protection models to detect and contain sophisticated threats. Our Lastline Defender™ for Cloud product provides immediate visibility into threats and intrusions across your public cloud workloads. You gain high-fidelity insight into malicious activity entering and operating within your AWS environment, enabling you to respond faster and more effectively:

- **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

Lastline Defender for Cloud delivers the network visibility and detection you need to stop advanced attacks before they disrupt your business. Lastline Defender for Cloud is part of the Lastline Defender product family, enabling you to deploy a single solution to protect cloud and on-premises environments from advanced threats.