MixMode®

THE INEFFICIENCES OF LEGACY TOOLS

CLOUD SECURITY VS. ON-PREM

Why Traditional On-Prem Solutions Won't Work for Securing The Cloud

www.mixmode.ai | +1 (858) 225-2352 | info@mixmode.ai |

OVERVIEW

In an era of digital transformation, cloud computing has emerged as a cornerstone of business operations, enabling organizations to scale rapidly, drive innovation, and achieve operational agility. It's also revolutionized the way organizations store, access, and manage their data and applications.

The rising tide of sophisticated cyber threats, evolving regulatory requirements, and the potential impact of security breaches have elevated the importance of cloud security to unprecedented levels. As more critical business functions and sensitive data are migrated to the cloud, the need for robust cloud security becomes paramount.

As a result, the security landscape has evolved, necessitating a shift in security practices and approaches. Organizations across industries are recognizing that the adoption of comprehensive and proactive cloud security measures is no longer a luxury but an essential safeguard to protect their valuable assets, maintain customer trust, and ensure business continuity.

But cloud security differs significantly from traditional on-premises security in several key ways.

This eBook explores the pressing need for cloud security in today's landscape and the key differences between traditional and cloud security.

INFRASTRUCTURE OWNERSHIP

In traditional on-premises environments, organizations have direct control over the entire infrastructure stack, including physical servers, network devices, and data centers. In contrast, in cloud environments, the underlying infrastructure is owned and maintained by the cloud service provider (CSP). This distinction affects how security measures are implemented and managed.

Infrastructure ownership is a critical aspect of cloud security. When a company uses a cloud service, they are essentially trusting the cloud provider to protect their data and infrastructure. However, it is important to understand who owns and is responsible for the security of the underlying infrastructure.

In some cases, the cloud provider may own and manage the infrastructure, while in others, the customer may be responsible for managing and securing their own infrastructure within the cloud environment.

Understanding infrastructure ownership is crucial in ensuring the security of cloud-based systems and preventing potential data breaches or cyber attacks.

RESPONSIBILITY DISTRIBUTION

Cloud security is complex and requires a clear understanding of the roles and responsibilities of each party involved. In a cloud environment, the responsibility for security is often shared between the cloud service provider and the customer.

- **The provider is responsible for securing the infrastructure, including the physical data center, network, and hardware.**
- **The customer is responsible for securing their data and applications within the cloud.**
- **The distribution of responsibility must be clearly defined and agreed upon to ensure that both parties understand their obligations and can work together to maintain a secure environment.**

Effective responsibility distribution is critical for ensuring the safety and security of data and applications in the cloud.

NETWORK PERIMETER

The cloud has revolutionized the way businesses operate by providing a flexible and scalable infrastructure that can be accessed from anywhere. However, this flexibility comes at a cost - the concept of a physical perimeter is blurred.

Traditional on-premises security heavily relies on securing the network perimeter through firewalls, intrusion detection systems, and other boundary defense mechanisms. In the cloud, the concept of a physical perimeter is blurred due to the dynamic nature of resources and the ability to access services over the internet.

Cloud security focuses more on securing individual resources and applying network security controls within the cloud environment. With resources being dynamically provisioned and services being accessed over the internet, traditional security measures such as firewalls and intrusion detection systems are no longer sufficient.

Instead, organizations need to adopt a more holistic approach to security, one that involves continuous monitoring and advanced threat detection across the entire infrastructure.

DATA LOCATION AND ACCESS

In traditional IT environments, there is a clear physical perimeter that can be secured with firewalls and other measures that utilizes localized data storage with limited data movement. However, in the cloud, resources are dynamic and can be accessed over the internet from anywhere in the world.

Data can be distributed across multiple regions or data centers, potentially crossing international boundaries. This raises concerns about data sovereignty, compliance with data protection regulations, and the ability to maintain consistent security controls across various locations.

This also blurs the concept of a physical perimeter, making it more difficult to secure data and prevent unauthorized access.

As a result, businesses must adopt new security strategies and technologies that are designed specifically for cloud environments.

SECURITY CONTROLS AND TUNING

In the traditional on-premises security model, organizations have to deploy and manage a range of security tools and appliances to safeguard their networks and data. This can be a complex and time-consuming process, requiring specialized expertise and resources.

In the cloud, security controls are typically implemented through software-defined configurations, APIs, and cloud-native security services provided by the CSP. This requires organizations to adapt their security tooling and processes to the cloud environment.

It's important to choose a cloud security provider that delivers a more scalable, flexible, and cost-effective security solution in the cloud.

VISIBILITY AND MONITORING

Organizations may not have direct control over the underlying infrastructure in a cloud environment, making it difficult to detect and address issues. Additionally, the complexity of cloud environments can make it challenging to identify the root cause of problems.

As a result, organizations need to invest in tools and strategies to ensure they can monitor and manage their cloud environments effectively. This includes leveraging automation and analytics to gain greater visibility into their infrastructure to quickly identify and address issues as they arise.

They need to ensure they have proper visibility into their cloud infrastructure and implement advanced, scalable solutions to detect and respond to security threats effectively.

DETECTION AT SCALE

On-premises security solutions are limited in scalability due to physical hardware limitations and the need for manual updates and maintenance. This means that as your business grows, you may need to constantly purchase and install new hardware to accommodate increased security needs.

In contrast, cloud security solutions offer much greater scalability because they can be easily scaled up or down as needed, without the need for additional hardware. However, some of these solutions may face scalability issues.

This means that as the amount of data and traffic increases, the security solution may struggle to keep up and may become less effective. This can be a serious problem for businesses that need to ensure the confidentiality, integrity, and availability of their data at all times.

It's important for organizations to carefully evaluate the scalability of their chosen cloud security solutions to ensure they can handle their growing needs.

SUMMARY

Understanding these differences is crucial for organizations to effectively design and implement security measures in the cloud. By embracing cloud-native security practices, leveraging CSP-provided security services, and adopting a comprehensive approach that aligns with the shared responsibility model, organizations can navigate the unique challenges of cloud security and protect their assets in the dynamic and ever-evolving cloud environment.

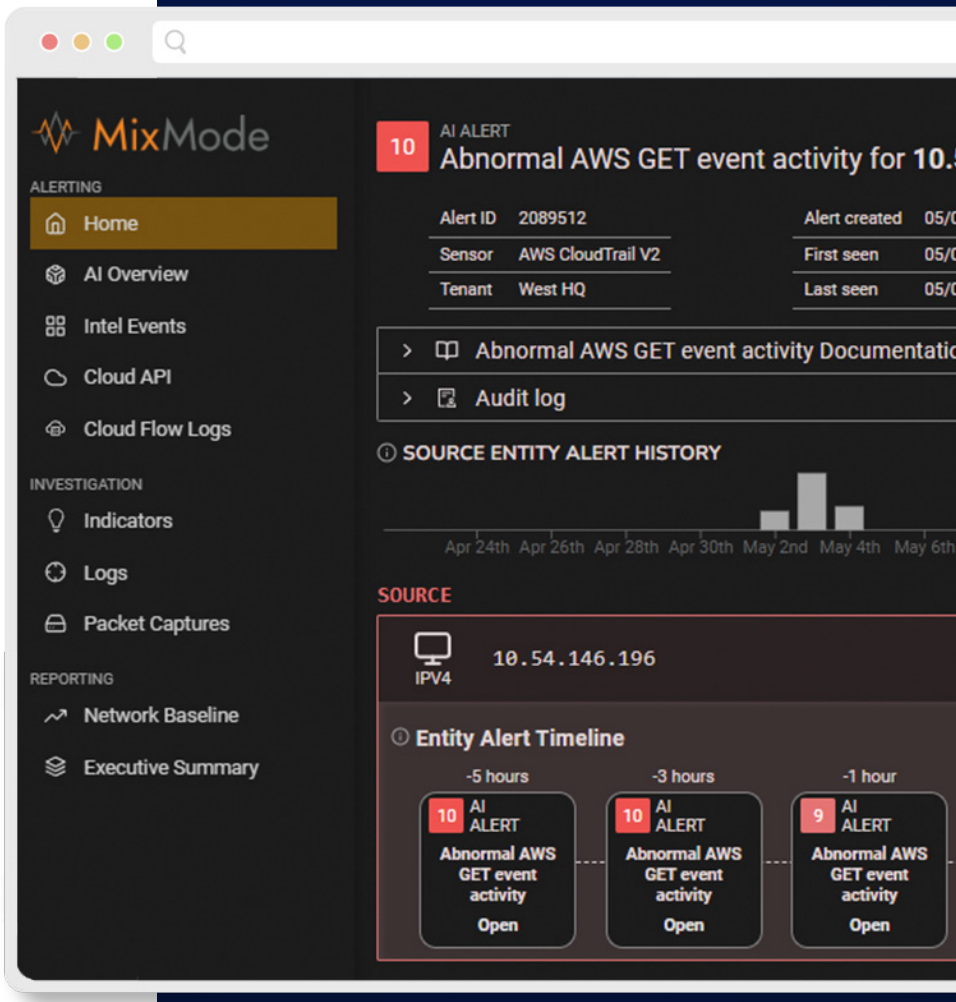
MIXMODE CLOUD DETECTION AND RESPONSE

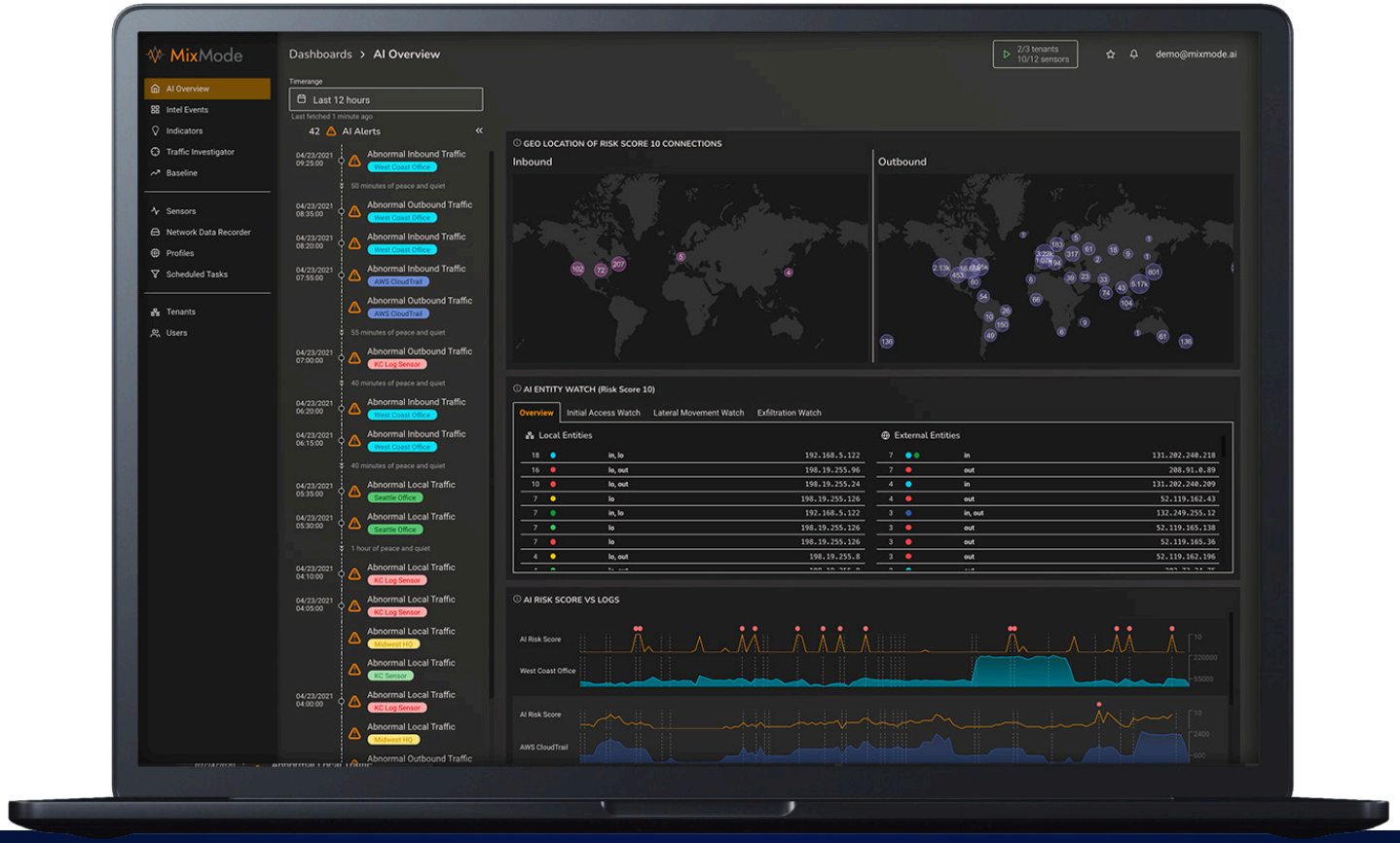
MixMode's Cloud Detection and Response Solution provides real-time protection for your entire cloud infrastructure, capable of ingesting and analyzing large volumes of diverse cloud data from multiple sources.

MixMode continuously monitors your environment and correlates cloud traffic with log data, SIEM logs, and threat intel feeds, delivering comprehensive visibility and real-time threat detection that ensures the defense of cloud applications and infrastructure against both known and unknown threats.

- **Proactively identify and resolve threats sooner, including active, novel attacks that other platforms miss.**
- **Reduce false positives and automate manual processes to focus on what matters.**
- **Streamline visibility while up-leveling existing investments.**
- **Ingest and analyze large volumes of data in real-time without increasing spend.**

No rules. No tuning. No limits.





MixMode®

CONTACT US TO LEARN MORE

www.mixmode.ai | +1 (858) 225-2352 | info@mixmode.ai | © MixMode, Inc.

Cloud Security Statisitcs Source: https://www.resmo.com/blog/cloud-security-statistics