What is Adaptive Security?

What is Adaptive Security and does it really mitigate these emerging threats? What are best practices for implementing Adaptive Security? How does machine learning and analysis help Adaptive Security?

In the digital world, network incidents are developing at an alarming rate. Cyber ??attacks are constantly increasing and the changing security landscape is prompting individuals and organizations to reevaluate their security strategies. Therefore, a modern, context-aware security model called **"Adaptive Security"** is being explored and applied.

So what is Adaptive Security and does it really mitigate these emerging threats? What are best practices for implementing Adaptive Security? How does machine learning and analytics help Adaptive Security? Let's find out through the following article!

What is Adaptive Security?

Adaptive Security is also known as " **Zero Trust** " security where nothing is trusted by default. This ensures consistent monitoring of threats with a flexible approach in which old and outdated security infrastructures are continually replaced by responsive ones.

Renowned Gartner analyst Neil MacDonald described Adaptive Security as:

"Using additional information to improve security decisions at the time they are made leads to more accurate security decisions that support dynamic IT and business environments."

The main premise behind Adaptive Security is the automated implementation of security measures against any detected threats.

Adaptive Security best practices and a 4-layer model

In the true sense, Adaptive Security is part of the following four layers:

Prevent

Prevention is better than cure and the top layer of the Adaptive Security security model is designed with this in mind. This layer isolates all incidents before they arise and outlines the policies, procedures, and prevention tools to defeat any potential threats.

Detect

This class identifies any threats that the defense layer fails to detect. The main aim here is to reduce response times to potential threats by stopping them on the way.

Review, analyze

This layer dug deeper to find any threats missed by the previous class. It is also the place to conduct detailed crash analysis with the help of advanced detection methods and threat analysis.

Guess

Last but not least, the prediction class keeps track of outside events. It provides a thorough risk assessment and alerts IT staff of any suspicious activity.

Information provided by this layer helps to identify successful attacks, predict and prevent similar attacks in the future.

The role of Machine Learning in Adaptive Security

With the rapid transition to cloud-based services, advanced analytics, and Machine Learning play a huge role in protecting Big Data.

Here are some of the main benefits AI and Machine Learning bring to Adaptive Security.

Threat identification

Advanced Analytics and Machine Learning are great at identifying patterns, classifying, and identifying malicious emails, links, and attachments. This assists a lot in identifying new and growing threats.

Threat tracking

The main advantage of incorporating analytics and Machine Learning into your security context is being able to track issues, especially ones that can stop the application for a few seconds and leave no trace. investigate.

Instant analysis of lots of data

AI offers a great opportunity to analyze large amounts of data in the blink of an eye, something that traditional security measures can't do.

This not only ensures real-time detection of threats, but also helps mitigate them by providing a risk-based model.

Ability to use threat stream

Most organizations face data threats from multiple sources and it is difficult to keep track of everything. Thanks to AI and Machine Learning, centralized and intelligent platforms like Anamoly's ThreatStream provide surveys of data from multiple sources.

An example of a threat stream would be an IP address that immediately starts scanning all of your network endpoints. However, with the use of a smart tool, any time an IP behaves strangely, it is written to threat stream for further investigation.

Main benefits of implementing Adaptive Security

Due to its preventive nature, Adaptive Security can detect security problems early. Real-time evaluation of events, users, systems, and network traffic helps to detect security threats early, while automatic responses accelerate the time frame to resolve malicious attacks .

Below are some of the key benefits that can be achieved through Adaptive Security.

Detect risks early

Early risk detection is a key benefit of Adaptive Security. The preventive nature of this security model makes it easy to spot risks before they turn into real threats.

Filter events and priorities

The use of advanced analytics and Machine Learning in Adaptive Security ensures the detection, filtering, and prioritization of security incidents that traditional monitoring systems would not notice.

Solve faster

Real-time evaluation of all users, systems and tools - and a combination of manual and automatic processes - support early risk detection, while automated responses significantly shorten time frame to fix.

Reduce the impact of the attack

Due to its ability to detect threats instantly and resolve it faster, Adaptive Security can shrink attack sizes and limit more widespread damage.

Multi-level monitoring approach is continuously evolving

Adaptive Security provides non-isolated multi-tier monitoring support with just one tool or scale. By examining the Indicators of Compromise, it evolves continuously to face future threats.

The more threat vectors change, the more agile Adaptive Security becomes.

Flexibility and integration with other tools

By design, Adaptive Security is a flexible concept that can work across a variety of tools and platforms. Instead of restructuring the entire infrastructure, Adaptive Security can integrate with any existing system.

You finished reading the article "**What is Adaptive Security?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com