INTRUSION DETECTION VS INTRUSION PREVENTION SYSTEMS: WHAT'S THE DIFFERENCE?

Network intrusion refers to unauthorized activity within an IT infrastructure network. The purpose of unauthorized network activities range from espionage and exploitation to data leaks and network downtime. According to the 2018 Verizon Data Breach Investigations Report that studied more than 53,000 security incidents around the world, most network infringements attempts successfully compromise the network within a few minutes. Two-thirds of the security incidents occurred months before they were discovered.

As a consequence, organizations victimized by sophisticated cybercrime incidents lost mission-critical business information, incurred significant financial losses and faced costly lawsuits due to security non-compliance. It is therefore critical to both detect and prevent network intrusions proactively, before the impact escalates beyond control.

Intrusion Detection and Intrusion Prevention both refer to a different set of tooling and practices applicable at different stages of the cyber security kill chain for network security and protection. Both technologies are designed to analyze and understand networking activities that have the potential to damage the security posture and health of a computer network. They may be designed to work together with a suite of technologies, protocols and mechanism to maintain optimal standards of security.

What is an intrusion detection system?

Intrusion Detection System (IDS) refers to the technology that passively monitors the network to identify anomalous activities and traffic patterns. The activities may encompass inbound and outbound network traffic posing threats from within and outside of the network. The IDS is configured to detect traffic anomalies in reference to organizational policies of user access and privileges. In response to unauthorized network activities and incidents, the IDS system can alert appropriate personnel or technologies to act against the detected threats.

A simple open source IDS solution may detect intrusions by comparing the network traffic information to databases of known attack signatures. In this case, the effectiveness of the IDS solution is limited by the digital signatures of known network exploits available and updated at the time of network intrusion. Sophisticated commercial Intrusion Detection Systems rely on advanced technologies including machine learning algorithms designed to understand baseline network traffic operations and identify anomalous incidents in real-time. IDS capabilities embedded within an external networking hardware equipment can be used to detect suspicious traffic activity to and from a specific device in real-time, whereas hosted IDS solutions may be used to evaluate traffic at a holistic network level close to real-time depending upon the technology capability and configurations.

Unlike a firewall, IDS solutions are not designed to block data packets once a suspicious activity is detected. Instead, IDS complement the overall security system of the organizations so appropriate response can be launched to reduce the risk of security infringement. The purpose of the IDS system typically involves gathering useful understanding on potential threats that are likely to impact network security.

Understanding intrusion prevention systems

Intrusion Prevention System (IPS) refers to the technology solution that actively responds to a potential threat by blocking the network traffic or unauthorized associated actions at various levels of the system. An IPS solution typically controls the network access and acts as a sophisticated firewall-like technology with built-in IDS capabilities to prevent the attacks from happening in the first place. The IPS solution offers advanced capabilities such as analyzing network incidents and identifying patterns of potential threats before taking preventive action. Unlike a firewall that only identifies packet headers and rejects the data from entering the network, the IPS system analyzes the entire packet and correlates the information with known events of high network security risk. It then blocks the data based on specific organizational policies pertaining to user access and privileges. An IPS system may also be configured to take no action against specific threats, making it similar to an IDS solution.

IPS systems are also available as hosted IPS solutions that protect the organization at the holistic network level as well as Network-Based IPS solutions designed to protect individual networking devices. The principle of operation of both technologies is similar and each can be configured to meet the unique monitoring needs of the network architecture.

Which is better: IDS vs IPS

The choice between IDS and IPS technologies comes down to the use cases, IT budget, compliance requirements, network architecture and the overall security strategies, among other factors. IDS

solutions can help your organizations evaluate the internal user behavior as well as potential threats originating from the outside. It can be used to identify infections and virus leading to information leakage. IT security personnel can also use the technology to identify configuration errors, scan for Shadow IT or unauthorized apps, and other clients and servers involved in traffic routing, information flows and network access.

An IPS technology can also be used to address these problems by preventing unauthorize network activities by itself, but the role of the technology must align with the organization's security strategy in thwarting these risk vectors. For instance, an organization may have lined up a series of security layers that analyze potential network intrusions to strategically understand the risk, root causes and taking preventive action. They may also need to understand the risk of an apparently unauthorized traffic and information flow across the network. Perhaps there may be a rogue employee attempting to gain access to sensitive business information or a legitimate networking attempt by an app to serve a sudden spike in traffic critical to business growth. Either way, organizations may need more than just a standalone IPS solution to realize the best course of action. If organizations don't need to actively block the network traffic identified as a potential intrusion and already have appropriate security measures in place, then additional investments in IPS over an IDS solution may not justify the choice.

Research suggests that cybersecurity risks are on the rise. The threats are coming from all directions – from disgruntled employees within the organizations to cybercrime underground rings and state-sponsored actors. The attacks are not only financially motivated but are also used as a symbolic representation of political activism, among other reasons. It is imperative for organizations to understand the impact of the threat and take proactive action in mitigating risks of network intrusions. By detecting and preventing network intrusions proactively, organizations can achieve these goals and save their business as well as users from the unforeseen consequences of cyber-attacks.