SOLUTION BRIEF

Armis Network Visibility, Segmentation and Enforcement

Enterprises often have significant challenges in managing network visibility, segmentation, and enforcement. The complexity of large enterprise networks, with their intricate and dynamic interconnections, can hinder the ability for IT & security teams to adequately map network traffic patterns and identify potential security risks. This inability to fully understand communication structure and patterns of the network, makes it difficult to see what an asset is actually doing, impacting the ability to generate proper segmentation recommendations and enforce security policies.

Understanding the Network Starts With Assets

Key to understanding the network is the ability to identify, classify and profile each and every asset that connects to the network. While oftentimes, data about managed assets exists in existing IT & security tools such as EDR systems, many assets such as IoT, OT, IoMT, and other unmanaged assets do not. Here, it is essential to be able to discover and inventory those assets along with the other classically managed assets that can accommodate a security agent.

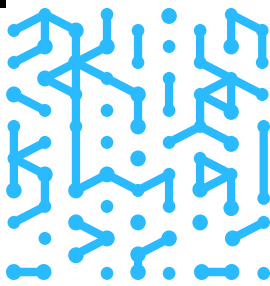
A primary way to identify these assets is by analyzing network traffic which satisfies the top use cases most important for network visibility, segmentation, and enforcement.

Detailed Network Visibility

Network visibility is crucial for IT & security teams to maintain a secure and efficient network infrastructure. Insights gleaned from an asset's network communications empowers teams to make informed decisions about network management, capacity planning and security. Inspecting and analyzing the network traffic of all assets gives IT & Security teams a visual diagram of the network with an overlay of detailed asset connections information such as IP connections, traffic, services and hosts complete with risks associated with the network connections-related risks.

Action Based on Network Policy Violation or Match

When a policy violation occurs, IT & Security teams need the ability to take enforcement actions to address the violation and maintain the security and integrity of the network. Enforcement can be automated in the form of creating alerts or sending a trigger to an existing network enforcement system such as WLC, firewall, NAC and switches. Other instances may require the manual creation of Access Control Lists (ACL) which can be pushed to the enforcement system.



Intelligent Network Segmentation

Enterprises have complex networks with numerous interconnected systems and devices. Implementing effective network segmentation requires a thorough understanding of the network infrastructure, its components, and their communications patterns. The inability to manage these complex networks leads to misconfigurations, incomplete segmentation or security violations. IT & Security teams need tools that can display network traffic information to make segmentation implementation easier while also providing granular control over network access to improve network security posture.

Enrich Native Network Access Tools/Systems

The task of creating ACLs and rules for network enforcement can be a long and arduous task and those systems may not have all the information required for an enforcement operation. IT & Security teams can greatly benefit from having recommended rules or more complete information available to automatically enrich the creation and pushing of those rules.

The Armis Solution

Armis Centrix™ provides complete network visibility mapping asset connections & communications across all environments. With Armis' network traffic analysis and deep packet inspection capabilities, IT & security teams can visualize network communications and display asset risks in order to more efficiently manage network segmentation and security policy enforcement. Armis shows detailed information about IP connections, traffic, services and host communications. From these comprehensive insights, IT & Security teams can intelligently segment networks or take any number of enforcement actions including creating Access Control Lists (ACL) or sending triggers to existing network enforcement systems such as WLC, firewall, NAC and switch.

Summary

Armis Centrix™ offers a single-source-of-truth for all data sources and creates a map of the connections & communications of every asset on the network. By leveraging network traffic analysis, organizations can more easily understand what assets are communicating to what other assets or systems. This allows IT & Security teams the ability to streamline proper segmentation of their networks while also maintaining a strong security posture, reducing their attack surface, and protecting their brand.

ARMIS.

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011