SOLUTION BRIEF

Gain Detailed Asset Intelligence Eliminate Known & Unknown Risk

Deep Situational Awareness In Merger and Acquisition Scenarios

During a merger or acquisition (M&A), due diligence requires that IT and security managers from the acquiring firm assess the IT infrastructure of the business that is going to be acquired. This typically starts with a detailed inventory of the new organization's devices, applications, and systems. It also requires understanding the risks associated with the new organization's assets, and that you develop a plan to mitigate these risks once the two environments are integrated.

Traditional security products are not well-suited for this use case. For example, the information in inventory systems like IT Asset Management (ITAM) and Configuration Management Databases (CMDB) is usually out-of-date and incomplete. Network scanners can miss devices, or worse, can disrupt critical devices causing costly downtime. Discovery products that require agents, like Endpoint Detection and Response (EDR) and systems management products (e.g. Microsoft SCCM) are costly and difficult to deploy, and they're ineffective for unmanaged, IoT, medical, and industrial devices that can't host agents.

The Armis Centrix™ Agentless Device Security Platform

Armis provides the detailed asset information and risk assessment you need to complete due diligence confidently and to secure newly acquired infrastructures seamlessly—all without ever touching or scanning any devices. Armis requires no agents and no additional hardware, so it can be up and running in a new environment in minutes.

Armis uses multiple, non-intrusive methods to discover and classify every managed, unmanaged, and IoT device in the environment.

See and understand devices in an unfamiliar environment

Armis Centrix™ makes it easy to inventory and quickly understand another organization's infrastructure—including distributed organizations with multiple locations. Armis discovers servers, laptops, smartphones, VoIP phones, smart TVs, IP cameras, printers, HVAC controls, medical devices, industrial controls, and more. It can even identify off-network devices using Wi-Fi, Bluetooth, and other IoT protocols in your environment— a capability no other security product offers without additional hardware.

It analyzes device characteristics and behavior to detect risks and threats by monitoring wired and wireless traffic on your network and in your airspace. If Armis detects a threat or a compromised device, it can alert or quarantine the device automatically, keeping your critical business information and systems protected from unacceptable risk.

The comprehensive inventory Armis generates provides a depth of information that gives you and your team a complete understanding of the infrastructure you're acquiring. The Armis device inventory includes critical information like device manufacturer, model, serial number, location, username, operating system, installed applications, and connections made over time. This gives you a clear picture of device, application, and system that come with the organization you're merging with or acquiring.

Evaluate risks

Armis takes the effort out of assessing vulnerabilities in the infrastructure you're acquiring. It compares device characteristics against a baseline of over 3.5 billion devices in the Asset Intelligence Engine to determine each device's unique level of risk. Risk scores include factors like device and manufacturer reputation, and any known asset criticality that is unique to your organization vulnerabilities.

The risk analysis Armis Centrix™ provides helps your team quickly understand and plan so they can be ready on day one for a new, expanded attack surface. Create policies that categorize known devices by type or level of risk, helping to maintain the security posture of your infrastructure.

Identify and respond to threats across the environment

Once the corporate merger is complete and network infrastructures have been connected, Armis keeps the combined infrastructure secure. It continuously analyzes devices and their behaviors to identify new risks and threats. It works with your existing security ecosystem to block or quarantine suspicious or compromised devices automatically. This provides peace of mind that an attack on any device—managed or unmanaged—can be stopped, even if your security team is busy with other priorities.

Armis Centrix™ integrates with switches and wireless LAN controllers, enforcement points like Cisco and Palo Alto Networks firewalls, and network access control (NAC) products like Cisco ISE and Aruba ClearPass. It integrates with your SIEM, ticketing systems, and asset databases to allow these systems and incident responders to leverage the rich information that Armis Centrix™ provides.

M&A Process	Pre - Acquisition	Post - Acquisition
Identification	Conduct a comprehensive inventory of devices, applications, and systems. Identify any risks associated with the organization's assets.	Continue identifying new devices, monitoring existing devices, and managing risk in the new environment. Extend security and policy controls over newly detected devices.
Evaluation	Prioritize risks and identify those that could impact the organization. Strategize between the two parties on how to mitigate risks.	Continue to assess risk and make comparisons across environments and over time. With the new corporate footprint, capacity plan based on load, needs and risk. Sunset legacy products that are no longer needed or are too outdated to run safely.
Integration	Create policies that segment known devices based on device type or risk. Enable policies that proactively catch and stop unknown or risky devices.	Continue to execute policy-based protections to block unknown or risky devices. Add anomaly based protection and develop a triage based vulnerability and patch management system to address critical CVEs first.

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, 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 stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform

Industries

Solutions

Resources

Blog

Try Armis

Demo

Free Trial