SECURITY FOR LABORATORY DEVICES

NON-DISRUPTIVE CYBERSECURITY FOR PHARMACEUTICALS AND LIFE SCIENCES

THE UNSEEN CYBER ATTACK SURFACE

In the pharmaceutical and life sciences industries, three areas of the business lack robust security controls because the devices in these areas are not visible to traditional security tools.

- **R&D labs.** These are hotbeds of innovation. Researchers and scientists are given latitude to use the instruments and applications that they want to use, often without prior review by the security team. As a result, the security team cannot adequately monitor or secure these instruments.
- **Manufacturing labs.** Validation requirements, outdated devices, old software applications, and the general sensitivity of the manufacturing lab environment make traditional, agent-based security systems difficult to apply. In addition, known software vulnerabilities in these labs are rarely patched because downtime is too costly to the business.
- **The enterprise.** Common devices such as IP video cameras, HVAC systems, smart TVs, etc. are being connected to the enterprise network on a daily basis. All of these “Enterprise IoT” devices are vulnerable to attack, but they can’t easily be patched, and they can’t be secured or monitored by onboard agents. They are risks waiting to be attacked.

Each of these areas are blind spots for your security team, putting you at greater risk for cyber attack. The impact could be very serious:

- An attack on lab equipment can lead to delays in product development and manufacturing, potentially causing hundreds of millions of dollars in losses.
- An attack on research computers can lead to theft of intellectual property and lost strategic advantage.

Until recently, a good security solution for these areas was not available. That’s now changed.

THE ARMIS PLATFORM

COMPREHENSIVE
Discovers and classifies all devices in your environment, on or off your network.

AGENTLESS
Nothing to install on devices, no configuration, no device disruption.

PASSIVE
No impact on your organization’s network. No device scanning.

FRICTIONLESS
Installs in minutes using the infrastructure you already have.

THE ARMIS SOLUTION

The Armis agentless device security platform allows security teams in the pharmaceutical and life sciences industries to properly secure all connected devices and computing resources—without any disruption to the business. Armis requires no agents or additional hardware to deploy, so it can be up and running in minutes to hours. Armis provides the following security benefits.

Visibility

Within minutes of being deployed, Armis shows you things in your environment that were previously unknown and invisible, such as connected devices that do not have security agents installed. Armis discovers and classifies every managed, unmanaged, and IoT device in your laboratory and manufacturing environment including connected laboratory instruments, automation equipment, thermostats, locks, lighting, HVAC controls, personal smartphones, and more.

Proactive Risk Mitigation

Armis not only shows you every device in your environment, but how risky it is. Armis generates a risk score for each device based on factors like software vulnerabilities, known attack patterns, and the behaviors of each device on your network.

In addition, Armis continuously monitors the state and behavior of all devices in your environment for indicators of attack. Armis compares real-time device activity to established, "known-good" baselines that are stored in the Armis Device Knowledgebase. When a device in your environment operates outside of its known-good profile, Armis issues an alert or triggers automated incident response.

Automated Incident Response

When Armis detects a threat in your environment, such as a misbehaving device, Armis can alert your security team and trigger automated action to stop the attack. Through integration with your switches and wireless LAN controllers (WLC), as well as your existing network control points like firewalls and network access control (NAC) systems, Armis can restrict access or quarantine suspicious or malicious devices.

Non-disruptive Deployment

The Armis platform requires no agents or additional hardware to deploy, so it can be up and running in minutes to hours, without any disruption to your existing computers, lab instruments, or research scientists.

ASSET DISCOVERY

- Identify all connected devices in laboratory and manufacturing environments.
- Make, model, OS, IP, etc.
- Connection and activity history
- Device location
- Integrate with asset inventory systems (CMMS, CMDB)

RISK MANAGEMENT

- Passive, real-time, continuous risk assessment
- Extensive CVE and compliance databases
- Risk-based policies

THREAT DETECTION

- Detect changes in device state or behavior
- Detect behavior anomalies
- Detect policy violations

INCIDENT RESPONSE

- Quarantine devices automatically
- Integrate with firewall, NAC, SEIM
- Reduce malware dwell time
- Improve incident response

ABOUT ARMIS

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.

20200124-1

ARMIS

1.888.452.4011
armis.com