ARMIS®

SOLUTION BRIEF

Closing Agency Enterprise Asset Visibility Gaps

The Continuous Diagnostics and Mitigation (CDM) program established the Federal Dashboard to consolidate summary information from each agency-level dashboard to form a picture of cybersecurity health across all civilian agencies. Comprehensive visibility across all IP Addressable devices enabled by highly reliable data quality is a top priority and a prerequisite for program success.

However, despite the tremendous efforts of the CDM program over the last decade, it continues to fall short of providing complete contextual visibility. The remaining gaps are caused, in large part, by a rapid increase in unmanaged and undermanaged devices across the enterprise. Due to the explosion of endpoints in the past few years, many federal agencies are experiencing a "visibility gap" where IT and security leaders can't see all the vulnerable assets within their environment.

To make matters worse, it is well-documented that unmanaged IoT/OT devices are now being actively targeted by nation states. Coupled with rising tensions between Russia and the rest of the world, this leaves U.S. critical infrastructure under increased threat of cyberattacks. These malicious cyberattacks can have damaging effects on lifeline services such as water, power, healthcare services, and supply chains.

New Dashboard Uncovers a Lack of Visibility and Unknown Vulnerabilities

The CDM program has upgraded to a new dashboard that implements Elasticsearch. Elasticsearch powers search solutions for thousands of companies worldwide to find documents, monitor infrastructure, and protect against security threats. As agencies have transitioned to this new dashboard, more unmanaged and undermanaged devices are being revealed.

This has brought into focus the extent of the current visibility gap, which is a serious threat to federal networks and our country. The biggest challenges to data quality include a lack of profiling of IT/OT devices and a lack of deduplication/rationalization of IP devices identified by different tools. The President's FY23 budget – in addition to EO 14028 and M-22-09 - calls for significant additional CDM funding to address current gaps in Endpoint Detection and Response (EDR) tooling capabilities.

While it is expected that CDM DEFEND will be a significant programmatic and contractual mechanism for addressing improved asset visibility, the visibility gap is only getting bigger. Currently, EDR technologies are primarily focused on agent-based technologies and there is a need to fill gaps for unmanaged and undermanaged devices to enable detections of IOC/IOAs.

Closing the Visibility Gap: Asset Discovery and Agentless EDR with Armis

	Managed devices	Unmanaged & IoT devices	Off-Network devices
Device controls	●	○	○
Networks Controls	●	◐	○
Visibility and analytics	●	○	○
Security automation & orchestration	●	◐	○
Data controls	●	○	○
People Controls	●	○	○
Workloads	●	N/A	N/A

Over the past few years, security managers have rapidly adopted EDR systems that provide continuous monitoring of managed devices. Unfortunately, traditional EDR systems don't work on unmanaged devices because they can't accommodate security agents. The Armis agentless EDR security platform solves this problem by covering the gaps left by traditional agent-based EDR solutions.

Armis continuously monitors the state and behavior of all devices on your network and in your airspace for indicators of attack. When a device operates outside of its known-good profile, Armis issues an alert or triggers automated actions. The alert can be caused by a misconfiguration, a policy violation, or abnormal behavior such as inappropriate connection requests or unusual software running on a device.

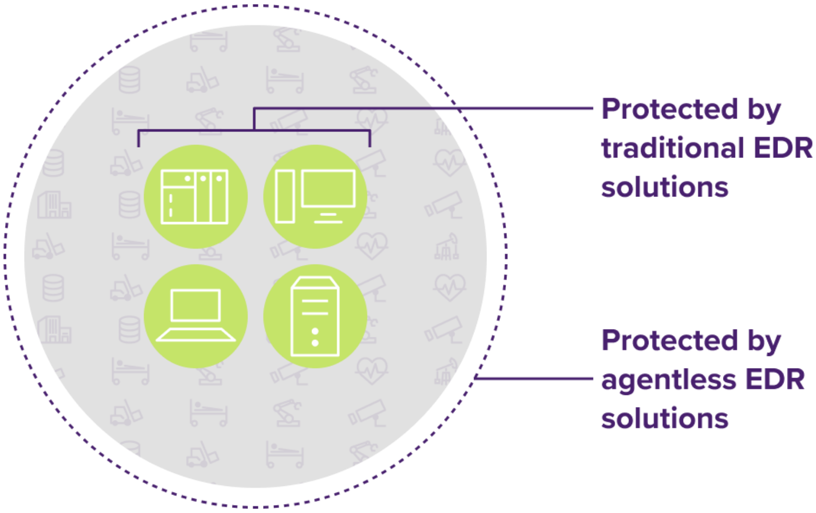
The Armis platform is completely agentless, which simplifies and speeds deployment. And it is also completely passive so that it won't disrupt the operations of devices. Everything works in real-time, so the discovery of assets, identification of issues, and automated enforcement are immediate and continuous.

Why Armis?

- **Comprehensive**
  Discover and classify all devices on your networks.
- **Agentless**
  Nothing to install, no configuration or device disruption.
- **Passive**
  No device scanning or network impacts.
- **Frictionless**
  Installs in minutes using existing infrastructure.

Agencies must achieve a consolidated view of their risk posture. This requires a clear risk status and vulnerability posture for every device and possible attack path, and the ability to rapidly respond to incidents.

Ready to learn more and harden your defenses by closing the visibility gap? Visit landing page, or email cdm.defend@armis.com for more information.


Protected by traditional EDR solutions
Protected by agentless EDR solutions

By 2024, up to 90% of devices will be unmanaged

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

1.888.452.4011 | armis.com

20220427-1