ARMIS

Public Sector

WHITE PAPER

DISCOVERING AND CLOSING HIDDEN SECURITY GAPS IN ZERO TRUST ARCHITECTURES

What Federal agencies need to know

In recent years, nation-state cybersecurity attacks on the United States' critical infrastructure have accelerated dramatically. In its most recent Digital Defense Report, Microsoft noted that the government is one of the most targeted sectors, comprising 48% of nation-state threat activity.[1] To better protect Federal Government departments and agencies from increasing cyber threats, the president has issued executive orders for shoring up IT infrastructure security, including establishing a Zero Trust architecture strategy. With the exploding numbers of IoT, OT, IoMT, and devices across enterprise environments, however, realizing the full benefits of a Zero Trust architecture is easier said than done because unmanaged assets create a "visibility gap" that can lead to dangerous security gaps. This white paper explores the reasons for the challenges and gaps and how to close them to realize the full benefits of a Zero Trust approach.

The case for Zero Trust

Every day, the federal government relies on IT infrastructure to support and power mission critical activities. But over the past few years, escalating nation-state cyber attacks from China, Russia, North Korea, and others have fundamentally altered the threat environment in federal infrastructure. Continued migration to the cloud, the move to mobile and BYOD, the convergence of IT, OT, and IoT, and the sharp increase in remote work have changed how the government must approach cybersecurity. Today, Federal agencies can no longer depend on conventional perimeter-based defenses to protect critical systems and data.

The good news is there are steps that government agencies can take to help make their networks and cloud infrastructures more resistant to cyberattacks, including the adoption of a Zero Trust strategy. Zero Trust assumes, by default, that no person or device from inside or outside the network should be trusted, and it relies on continuous monitoring of user and device behavior for granting or denying access to resources on the network.

In May 2021, the president issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*. EO 14028 is a government-wide effort to ensure that baseline security practices are in place to migrate the Federal Government to a Zero Trust architecture (ZTA), and to realize the security benefits of cloud-based infrastructure while mitigating associated risks.[2]

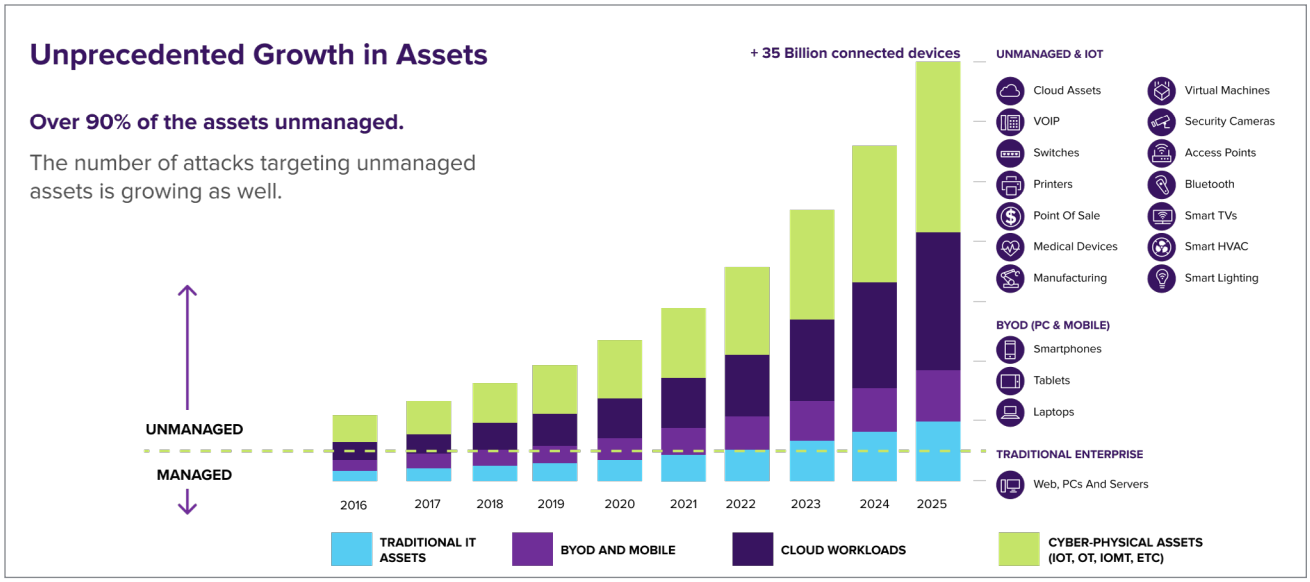
The latest Memo, M-22-09, released by the Office of Management and Budget (OMB), is tied to the Zero Trust strategy outlined in EO 14028 and provides specific goals and deadlines for implementing a ZTA. These deadlines require agencies to achieve specific Zero Trust security goals by the end of Fiscal Year (FY) 2024.[3]

These directives piggyback on other recent efforts to strengthen Federal security practices, including amendments to Section 889 Part A in the Federal Acquisition Regulation (FAR) which was written to combat national security and intellectual property threats related to the use of equipment and services produced or provided by Chinese state-owned or sponsored companies. FAR 889 specifically calls out Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of those entities) and certain video surveillance products or telecommunications equipment and services produced or provided by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of those entities).[4]

One of the big challenges with effectively implementing a ZTA and complying with rules like FAR 889 is that you can't defend against threats you cannot see. And there are ever-increasing numbers of unmanaged assets that agencies can't see, let alone defend, due to the explosion of end points in the past few years. Moreover, issues **like Log4j** have exposed the hidden threat of outdated devices throughout complex environments like those of federal agencies. To close the visibility gap and secure the mission, agencies need a single, authoritative source of the truth for all organizational assets.

The rise of the Unmanaged Assets

To control access to networks, applications, and data, and to authenticate users and manage access, Zero Trust architectures rely on a variety of technology building blocks. The problem is that most security and management tools fall short when it comes to seeing let alone securing unmanaged assets. And that's a significant issue, given how fast devices are proliferating. Unmanaged device types vary widely and can include anything fromIP phones and cameras to streaming media players to switches and routers to printers and smart TVs...



While organizations have been busy adopting Zero Trust controls for users and managed computers, the number of unmanaged assets in network environments has been growing exponentially. Not only are these devices nearly everywhere now, they are also vulnerable and have attracted the attention of bad actors. In fact, attacks on unmanaged and IoT devices increased 300% in 2021.

Zero Trust Building Blocks

Having clarity into "everything" that is connected to your network is the foundation of a Zero Trust environment. NAC/802.1x was developed to solve this problem, but for OT, IoT, and IoMT it falls short. With NAC/802.1x, all that is collected for unmanaged assets is an IP address, or (less often) a MAC address. The type of device, manufacturer, operating system, chip set, and– most importantly–its vulnerabilities remain unknown.

Moreover, a tricky aspect of Zero Trust is that you also don't know what you don't know with respect to managed assets. For example, even endpoint detection and response (EDR) solutions monitoring managed assets, such as laptops, desktops, and servers, may be missing or have misconfigured agents that leave them vulnerable to attack.

At the end of the day, it is simply not possible to successfully deploy a Zero Trust approach without an understanding of ALL the devices on the network. To further complicate the situation, enterprises typically have several different networks that need to be carefully monitored, including corporate, guest, wireless, administrative, and building networks.

OT environments also provide some unique challenges as they typically are not as mature from a cybersecurity perspective as traditional IT environments. Just consider the list of long-known vulnerabilities highlighted in the recent OT:ICEFALL report, none of which represent a "Zero Day" attack vector. In OT environments, Supervisory Control and Data Acquisition (SCADA) networks and Programmable Logic Controllers (PLCs) are also more vulnerable to attacks and are often overlooked or only protected by point solutions. Given the sheer number of ongoing cybersecurity attacks today by nation-state actors, strengthening cybersecurity in OT environments is especially critical.

Armis is unique in its ability to discover all IT, IoT, OT, and IoMT assets in the enterprise, alert on their vulnerabilities, and provide unified, real-time asset insights through a single user-friendly dashboard.

Top 8 contributors to Zero Trust security gaps

1 | *Lack of visibility* into connections between IT, IoT, OT, and IoMT devices and network services makes it nearly impossible to segment assets.

2 | *Poor CMDB data quality*, especially when it comes to IoT and OT devices whose data may only include an IP address.

3 | *Multiple versions of the truth* because different security and management tools focus on different types of assets.

4 | *Configuration challenges* with data controls, such as encryption, on unmanaged assets.

5 | *Weak or missing security controls and inherent vulnerabilities* in unmanaged assets because most device manufacturers focus on ease of use and don't design security controls into devices.

6 | *Missing context* in Security Orchestration, Automation and Response (SOAR) tools for what assets are doing versus what they should be doing.

7 | *No controls* since workload controls don't apply to unmanaged assets.

8 | *No behavioral logs* because unmanaged assets don't produce logs for consumption by User and Entity Behavior Analytics (UEBA) and other types of tools looking for suspicious activity.

How to Apply Zero Trust to Unmanaged Assets

The principles of Zero Trust are the same for unmanaged assets as they are for managed assets. In short, you need to know:

- What each asset is (asset inventory)
- What data and which applications and network resources each asset needs to access
- What software vulnerabilities and other risks each asset contains
- Whether each asset is behaving "normally" for the context of the asset

When you have near real-time intelligence on every asset, you can feed the information into your Zero Trust security policy enforcement system, which can then grant network access to data and resources as appropriate to the asset. This intelligence is equally important to enabling your Zero Trust security policy enforcement system to automatically remove network access or send an

alert when assets exhibit unusual or anomalous behavior. The ability to perform digital forensics and incident response (DFIR) on unmanaged assets is also essential. Add together all of these capabilities and you've got a strong Zero Trust security system that works for unmanaged assets.

To obtain all the knowledge listed above without disrupting asset operations, you need a security system that:

- Does not use agents
- Does not perform disruptive or dangerous network scans
- Works with all assets, no matter how little attention the manufacturer gave to security when they designed the asset

Comprehensive Visibility and Intelligence for *Every* Asset

The Armis Asset Intelligence platform is an agentless SaaS platform that automatically collects and analyzes asset data, delivering the industry's most comprehensive asset intelligence platform. Through hundreds of pre-built integrations, Armis seamlessly works with your existing IT management and security solutions and your network infrastructure to discover, classify, assess, and continually monitor every connected IT, OT, IoT, IoMT, cloud, and 5G asset—managed or unmanaged—in your environment in support of Zero Trust security. It also helps to improve and streamline governance and compliance-related processes. For example, Armis can detect and report on the manufacturer of and chipsets in assets, helping to pinpoint the physical location of any devices from Chinese technology firms that deviate from FAR 889 requirements.

Core to the Armis platform is our Collective Asset Intelligence Engine, a groundbreaking knowledgebase that tracks and analyzes the attributes of over two billion assets worldwide. The Collective Asset Intelligence Engine learns how assets are used and then monitors what assets are doing versus what they should be doing. For example, it understands the difference between a tablet used to check-in visitors in the lobby versus one used for driving a video conferencing solution. It also continuously maps connections and communications between assets and services, learning the relationships and dependencies between, and the importance of, assets across your environment. And it can detect threats with a high degree of accuracy by comparing real-time behavior with established baselines, triggering alerts or actions.

Armis and Zero Trust

Legacy security solutions are focused on managed devices, but are not designed for unmanaged or IoT devices. Armis is purpose built for unmanaged devices, and yet provides an overlay protection for managed devices.

ZERO TRUST PILLAR	MANAGED DEVICES		UNMANAGED / IoT		OFF NETWORK	
DEVICE CONTROLS	●	◑	○	●	○	●
NETWORK CONTROLS	●	◑	◑	●	○	●
VISIBILITY & ANALYTICS	●	◑	○	●	○	●
SECURITY AUTOMATION & ORCHESTRATION	●	◑	◑	●	○	●
DATA CONTROLS	●	○	○	●	○	●
PEOPLE CONTROLS	●	○	○	●	○	●
WORKLOADS	●	○	N/A	N/A	N/A	N/A
		ARMIS.		ARMIS.		ARMIS.

● FULL COVERAGE ◑ PARTIAL COVERAGE ○ NO COVERAGE ADDITIONAL COVERAGE

The Armis platform also provides the most comprehensive, unified asset inventory and device discovery available today. It enables your agency to quickly drill into the details of every asset, including make, model, OS and firmware versions, owner, physical location, known vulnerabilities, risk to the organization, and more.

The combined capabilities in the Armis platform are foundational for Zero Trust approaches; your Zero Trust systems can rely on trusted, real-time data from Armis to make better decisions about risk and network access. And this agentless approach starts delivering value within hours as opposed to agent-based solutions which can take weeks–and still not see or protect unmanaged assets.

Why Armis?

- Rapid, easy agentless deployment. Most customers are up and running in one hour.
- Unparallelled visibility. See ALL assets, managed and unmanaged. Contextual intelligence. Our Collective Asset Intelligence Engine has more intelligence on asset behavior than any other provider.
- Thoughtful integrations. Works seamlessly with your existing workflows and systems.
- Continuous Diagnostics and Mitigation (CDM) program approved.
  Armis is on DHS's CDM Approved Product List.

A 'Live Map' of your assets

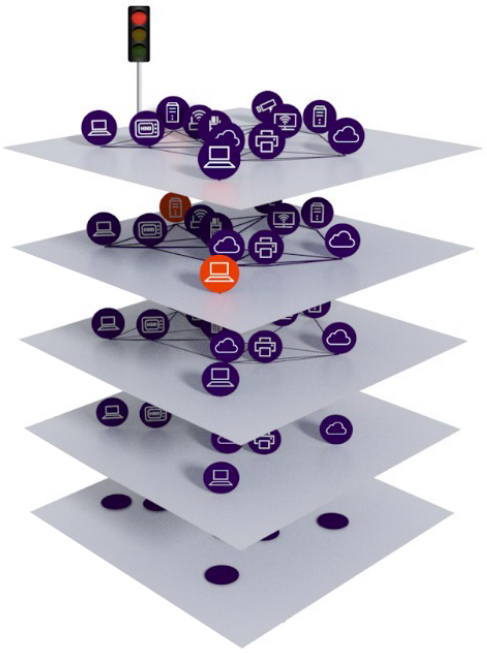
Manage, Secure, Automate, Orchestrate

Detect Vulnerabilities, Risks and Threats

Map Relationships and Connections (Context)

Profile, Context, Enrich (Asset Intelligence)

Asset Discovery (Unified across all Sources)



Conclusion

The recent Zero Trust-related executive orders are an acknowledgement that the threats to federal infrastructure have never been greater. But agencies can't meet the Zero Trust challenge without seeing 100% of their connected assets.

Implementation of a strong Zero Trust security architecture now requires that you also apply Zero Trust principles to the multitudes of managed and unmanaged, IT, OT IoT, IoMT, Cloud, and 5G assets that pervade the modern enterprise. These assets don't accommodate security agents or produce logs, and they are not easily patched. To realize the full promise of Zero Trust, you need specialized capabilities for seeing and non-disruptively monitoring every asset. And those capabilities must integrate with your other Zero Trust tools and processes.

To learn more about Zero Trust solutions and how the Armis Asset Intelligence Platform can support your mission, visit https://www.armis.com/zero-trust.

Sources

1. Microsoft Digital Defense Report, Microsoft Corporation, October 2021.
2. Executive Order on Improving the Nation's Cybersecurity, The White House, May 2021.
3. M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, Office of Management and Budget, January 2022.
4. Federal Acquisition Regulation: Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment, Federal Register, July 2020.

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.

armis.com

info@armis.com

20220308-1

ARMIS®