ENFORCING C2C AS PART OF A SUCCESSFUL ZERO TRUST FRAMEWORK

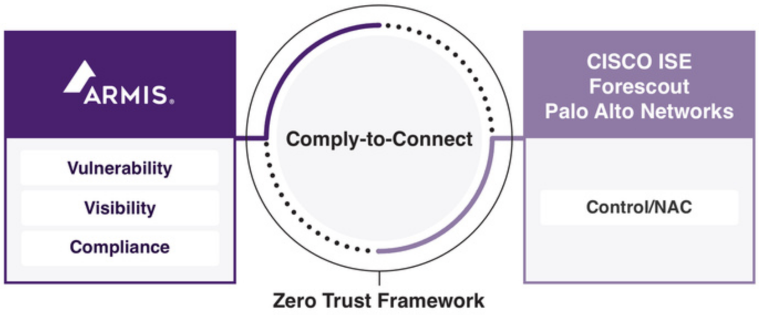
The Department of Defense (DoD) Comply-to-Connect program, or C2C, began as a congressionally mandated five-year cybersecurity program passed into law through the FY 2017 National Defense Authorization Act (NDAA). Evolving from the beginning, C2C has become the backbone of the DoD's Zero Trust policy.

With the current environment of heightened geopolitical tensions and ongoing concerns with China's goals in Asia, cybersecurity is critical for our servicemen and women being able to perform their missions. Previously, C2C had only been focused on traditional, managed IT resources. This was in part due to the sole reliance on Network Access Control, NAC, and 802.1x, an IEEE standard for port-based network access control. While NAC is effective for controlling access to traditional IT resources, it does nothing to secure the growing cyber asset terrain which contains critical assets (OT, IoT, IoMT, & ICS) in operational environments.

The updated C2C program has requirements to provide coverage of all assets on a DoD network, not just reporting an IP Address as NAC can do for some IT resources. C2C is a component of a broader Zero Trust architecture. C2C enforces compliance requirements and so strengthens the overall security posture within a Zero Trust environment. It aligns with Zero Trust principles by ensuring that devices connecting to the network meet a minimum level of security hygiene. This meets the Zero Trust objective of verifying the trustworthiness of all devices, regardless of their previous access rights or location.

Armis can uniquely provide a Zero Trust solution across all of these environments. The Armis Intelligence and Security Platform is a FedRAMP and IL4 Authorized solution and is agentless. This means fast deployment for government clients, who can be up and running day one.

DoD Comply-to-Connect Zero Trust Architecture



Comply-to-Connect is the Foundation of DoD Zero Trust

One of the key challenges C2C faces as it becomes a key part of the DoD Zero Trust solution is achieving visibility to ALL assets on the network. As stated above, NAC solutions only work for IT resources. This leaves large segments of assets unseen and unprotected. These assets must be accounted for because they are potential threat vectors. Nation-state actors have been specifically targeting these unmanaged assets recently. Many of these unmanaged assets are running end-of-life Operating Systems, are misconfigured, or have other vulnerabilities. Armis can provide 100 percent visibility into all of these environments and identify corresponding vulnerabilities.

Armis can quickly enable C2C to have total visibility into all DODIN assets and meet the challenging Zero Trust mandate from DoD. Further, Armis real-time Compliance and Vulnerability capability across all assets gives the DoD never before awareness and enables the vision of C2C to be reality.

Ensuring You Can Determine the Device Security Posture

The dangerous reality is that most organizations do not have enough information on unmanaged assets to be able to determine if a network asset meets a desired security posture in real-time. You can't protect what you can't see. Detailed information is required of an asset to be able to determine if it is in compliance with the required DoD cybersecurity posture. Often agencies attempt to manage this visibility gap manually by having personnel track down the required information from disparate sources. This process is inefficient, costly, and most importantly cannot keep up with fluid, real-time environments. Additionally, all asset detection/inventory capabilities must work at scale and real-time to provide the required Zero Trust solution.

Closing the Gap

In order for C2C to meet its mission requirements, awareness of assets in all environments is required, and more critically, awareness of the vulnerabilities of these assets. Further, for OT and IoMT environments traditional scanning approaches do not work and can cause denial of service, just the opposite of the intended outcome.

The Armis Platform has bi-directional integration with NAC and 802.1x. It can automatically notify the NAC that an IT asset needs to be moved to a remediation network at any time. NAC solutions only evaluate IT assets the first time they see them, yet many of these assets can stay on the network for weeks at a time.

Conclusion

C2C is an approach that focuses on ensuring that only compliant and secure devices are allowed to connect to a network. This approach is crucial for maintaining a strong security posture, especially in environments where a wide range of unmanaged devices, including OT, IoT, and IoMT assets, are present.
The Armis Platform provides several key capabilities that can quickly assist organizations in implementing and enforcing C2C:

1. Device Discovery and Inventory
2. Risk Assessment
3. Policy Enforcement
4. Vulnerability Management
5. Threat Detection and Response
6. Compliance Reporting

It's time to realize the full potential of the C2C program and achieve a critical step towards a Zero Trust architecture for the DoD. To get to a Zero Trust future, agencies must achieve a total view of their risk posture that is timely and accurate. Armis can make such risk awareness a reality. Call us at 888-452-4011 or visit www.armis.com/public-sector to learn more.

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.

About Armis

The Armis FedRAMP platform is completely agentless, which simplifies and speeds deployment. It discovers and classifies every device across any environment, including connected devices on and off the environment that most traditional agent-based tools miss. Armis provides a complete, comprehensive, and detailed inventory of an agency's IT, OT, IoT, and cloud assets so agencies can visualize and secure the entire attack surface. The Armis platform allows agencies to detect threats by comparing real-time asset state and behavior and to respond with ease to create automated, policy-based actions such as triggering vulnerability scans or segmenting dangerous devices. Everything works in real-time, so the discovery of assets, identification of issues, and automated enforcement are immediate and continuous.

1.888.452.4011 | armis.com/public-sector

ARMIS®
Public Sector