Prioritize and Execute: Getting DOD to Zero Trust Faster

Data, applications and workloads represent some of the most critical pieces of our nation's network, but they are often the least protected.

Mark Sincevich
Federal Director
Illumio

If federal defense leaders needed proof of national cyber insecurity, the exponential growth of cyber threats, including the SolarWinds breach and Colonial Pipeline ransomware attack, stand as bold reminders of the need for a cyber overhaul.

Attention is turning to Zero Trust strategies with the recent Executive Order on cybersecurity as a catalyst for security momentum. The Defense Information Systems Agency's (DISA) "Zero Trust Reference Architecture" that embeds security throughout the architecture, instead of only at the perimeter, bolsters this momentum.

President Joe Biden's 2022 budget request to Congress also includes $10.4 billion for Department of Defense cybersecurity, including Zero Trust efforts. Now, DOD agencies and commands must prioritize the components of Zero Trust that will deliver the most immediate security impact.

Prioritizing Mission-critical Assets

Federal leadership has been trying to tackle several aspects of Zero Trust at once, spending a tremendous amount of time on other Zero Trust pillars, such as ICAM (identity, credential, and access management), devices and network security. While each is an important part of an overall Zero Trust architecture strategy, they will not protect the DOD's high-value assets if an attacker is already inside the network.

Dave McKeown, Deputy CIO for cybersecurity and the DOD's Chief Information Security Officer (CISO) explained that we have long understood that an increasingly determined adversary will eventually find a way to breach our perimeter and layer defenses.

Therefore, we must assume the adversary is already on our network and deny by default by assuming compromise.

Data, applications and workloads represent some of the most critical pieces of our nation's network, but they are often the least protected. The National Security Agency's (NSA) report "Embracing a Zero Trust Security Model" directs agencies to shift their security philosophy and to architect security from the inside out to guard mission-critical assets like applications and workloads with Zero Trust segmentation (also known as micro-segmentation).

When a workload is properly segmented, it can appear cloaked or invisible to an attacker. It is crucial that defense agencies prioritize this pillar and execute the strategy by starting with a single critical application or a small number of workloads. This will help them keep their high-priority data secure, even after a breach happens.

Breaches will inevitably occur; the key is doubling down on protecting mission-critical assets like applications and workloads to stop the lateral movement of a cyber attack so agencies and commands can continue to focus on the mission.

When a workload is properly segmented, it can appear cloaked or invisible to an attacker. It is crucial that defense agencies prioritize this pillar and execute the strategy by starting with a single critical application or a small number of workloads. This will help them keep their high-priority data secure, even after a breach happens.

Zero Trust Segmentation For An Immediate Security Impact

To properly secure defense environments, teams must identify their critical applications and workloads, often found in the data center, on the cloud or in hybrid environments. It is essential they create visibility into how applications and workloads connect to one another. After all, they can't secure what they can't see.

Visibility will allow teams to react quickly to threats and changes in workflow. They can then architect their security from the inside out, as the NSA directs, by applying and enforcing Zero Trust segmentation.

Zero Trust segmentation is decoupled from the network, allowing teams to lock down and separate key assets at the speed of the mission. The NSA advises agencies to focus first on protecting critical assets and then securing all paths to access them.

Zero Trust segmentation policies use allow lists that indicate which applications and workloads are permitted to connect. If a connection is not explicitly stated, it is denied by default. This fortifies the network to ensure attacks cannot spread. Zero Trust segmentation blocks unnecessary movement automatically, which keeps critical assets secure.

Defend Forward With Zero Trust Architecture

When it comes to cyber attacks, if agencies need to chase the enemy, sharing threat intelligence, then the damage is already done. Agencies must defend forward with Zero Trust segmentation to not only minimize the spread of attacks but also prevent future cyber catastrophes.

As the DOD prioritizes the Applications and Workloads pillar as the most important piece of their Zero Trust strategy, they will see an immediate security impact. This approach will dramatically reduce the application attack vector by protecting critical applications and workloads even while agencies continue to improve the network.

And as Mr. McKeown said about Zero Trust Architecture: Our networks will be exceedingly more secure, the war fighting mission will be defended, and our adversaries will have to dedicate significant resources only to achieve very small gains.

Learn more at www.illumio.com. ■

About The Author

Mr. Sincevich has more than 30 years experience helping IT firms serve the Federal marketplace. He joined Illumio where he started the Federal and Federal System Integrator (FSI) Business from scratch. Illumio is a cybersecurity software company that enables Zero Trust Segmentation in Defensive Cyberspace Operations. The company helps agencies, commands and organizations achieve Zero Trust and prevent attacker lateral movement by (i) providing real-time visibility, (ii) reducing the dynamic attack surface, and (iii) enabling faster implementation all through host-based micro-segmentation. Illumio is FIPS 140-2 validated, is on the DHS CDM APL and is NIAP Common Criteria Protection Profile Certified. Illumio can be placed in multi-vendor hardware environments, using existing infrastructure to improve agencies' cybersecurity postures and effectively accomplish their missions.