
Inside the fight to secure
air-gapped environments

Inside the fight to secure air-gapped environments

Thank you for downloading this Broadcom Article. Carahsoft is the distributor for Broadcom cybersecurity solutions available via NASPO ValuePoint, North Carolina Endpoint Protection Contract 208M, Software Solutions and Services – OMNIA Partners, Public Sector, and other contract vehicles.

To learn how to take the next step toward acquiring Broadcom's solutions, please check out the following resources and information:

For additional resources:
carah.io/BroadcomResources

For upcoming events:
carah.io/BroadcomEvents

For additional Broadcom solutions:
carah.io/BroadcomSolutions

For additional cybersecurity solutions:
carah.io/CybersecuritySolutions

To set up a meeting:
Broadcom@carahsoft.com
571-662-3260

To purchase, check out the contract vehicles available for procurement:
carah.io/BroadcomContracts


Adobe Stock | Gorodenkoff

Inside the fight to secure air-gapped environments

Air-gapped and disrupted, degraded, intermittent and low-bandwidth (DDIL) environments safeguard the Department of War's most sensitive missions. Isolated from the internet to reduce exposure, these systems store information that could cause significant damage to national security if undermined — from weapons platforms to strategic intelligence, design blueprints and troop movements.

"In addition to being targets for the theft of their critical information, these environments are exactly what a large global adversary would want to compromise or take offline ahead of launching a major attack," said Garrett Lee, vice president of public sector for Broadcom's Enterprise Security Group (ESG). "Each of these specialized environment types requires a tailored security configuration to narrow the threat surface and offer visibility and command and control."

However, meeting those unique demands can be difficult. Many agencies that have embraced cloud security in other domains find that SaaS-based tools cannot extend adequate protection to disconnected networks because they require constant internet connectivity. Legacy security technology, meanwhile, can be cumbersome to manage and update, creating inefficiencies that further widen the risk surface.

Perhaps more concerning is the common misconception that isolation alone is enough to deter attackers.

"Often with air-gapped environments, a false sense of security can lead to a relaxed posture toward risk," Lee said. Insider threats are a particularly underestimated vector, whether from unintentional errors or malicious actors seeking to exfiltrate classified data. Contractors also pose challenges, and lapses in this area have already triggered supply chain trust issues, mission impact and contract losses.

This means implementing Data Loss Prevention programs across all control points to prevent sensitive data from leaving an environment, whether by accident or by design.

Zero trust rigor is equally important. Security teams must retain transparency in disconnected states, with continuous monitoring of user behavior, system and application access, data usage and removable media policies. Agencies also face the burden of running proprietary applications on end-of-life operating systems, leaving them to pay steep fees for extended security updates.

"Employing a positive security model for these legacy OS to prevent threats is a considerably less

PRODUCED BY: NEXTGOV/FCW | SPONSORED BY: Symantec. by Broadcom | Carbon Black. by Broadcom | carahsoft.

expensive strategy than paying the vendor's ransom," Lee explained.

Balancing mission continuity with security

For defense leaders, the question is how to enforce strict protections without jeopardizing operations.

"If you are air-gapping systems, you have already taken measures to limit mission risk to those systems, but you should focus on only allowing what is explicitly and clearly necessary for mission continuity," said Lee. "The mission comes first, but security needs to essentially only support the mission. Nothing more, nothing less."

Agencies need security toolsets capable of enforcing highly specific, often unusual, rules. Without that level of granularity, organizations risk not having adequate controls in place or imposing restrictions so rigid they interfere with essential functions and, in effect, assist the adversary.

"Integrate security from the start, not as an afterthought," said Lee. "Ensuring agencies have a great endpoint protection solution with a layered defense approach remains pivotal here just as it is in broader enterprise environments."

Application Control solutions can provide the positive security model approach and granularity needed to enforce strict protections without impacting the mission.

Broadcom's comprehensive approach

Broadcom's Symantec and Carbon Black cybersecurity solutions are built for air-gapped and DDIL environments that cannot depend on cloud connectivity. Unlike SaaS-only tools, the solutions provide endpoint, data and network defenses that function in disconnected or austere conditions.

"Our suite is battle-tested in air-gapped environments," Lee said. "From the attacker's perspective, infiltration, persistence and exfiltration are all thwarted. Running commands and scripts is not possible due to the positive security model in place — allow what is good and block all else."

Core capabilities include data loss prevention to counter insider threats, application control that blocks unauthorized scripts and executables, and device control with granular USB security to ensure a single compromised drive cannot escalate into a larger breach. Broadcom also delivers unfiltered endpoint detection and response data, making it impossible for attackers to hide in recording gaps.

The Symantec and Carbon Black global intelligence network strengthens defenses, providing unmatched visibility into emerging threats. These insights facilitate faster detection, stronger mitigation and fewer false positives, helping administrators maintain operational integrity without drowning in noise.

Futureproofing for evolving threats

Performance remains a top concern in resource-constrained environments, but Broadcom has developed its suite to minimize overhead. Lightweight architecture and simple workflows help practitioners identify security pitfalls, then test and implement new rules quickly without impacting end users.

By adapting layered defenses to the realities of air-gapped and DDIL environments, Symantec and Carbon Black solutions help the Department of War secure vital systems against increasingly sophisticated threats.

"Our goal is to bring zero trust principles to help agencies allow what is minimally necessary for the mission to fully function," Lee said. "Enable the mission, but not the adversary."


Adobe Stock | aLListar/peopleimages.com

To learn how Broadcom can help your agency to secure air-gapped environments, visit **www.carahsoft.com/broadcom**.