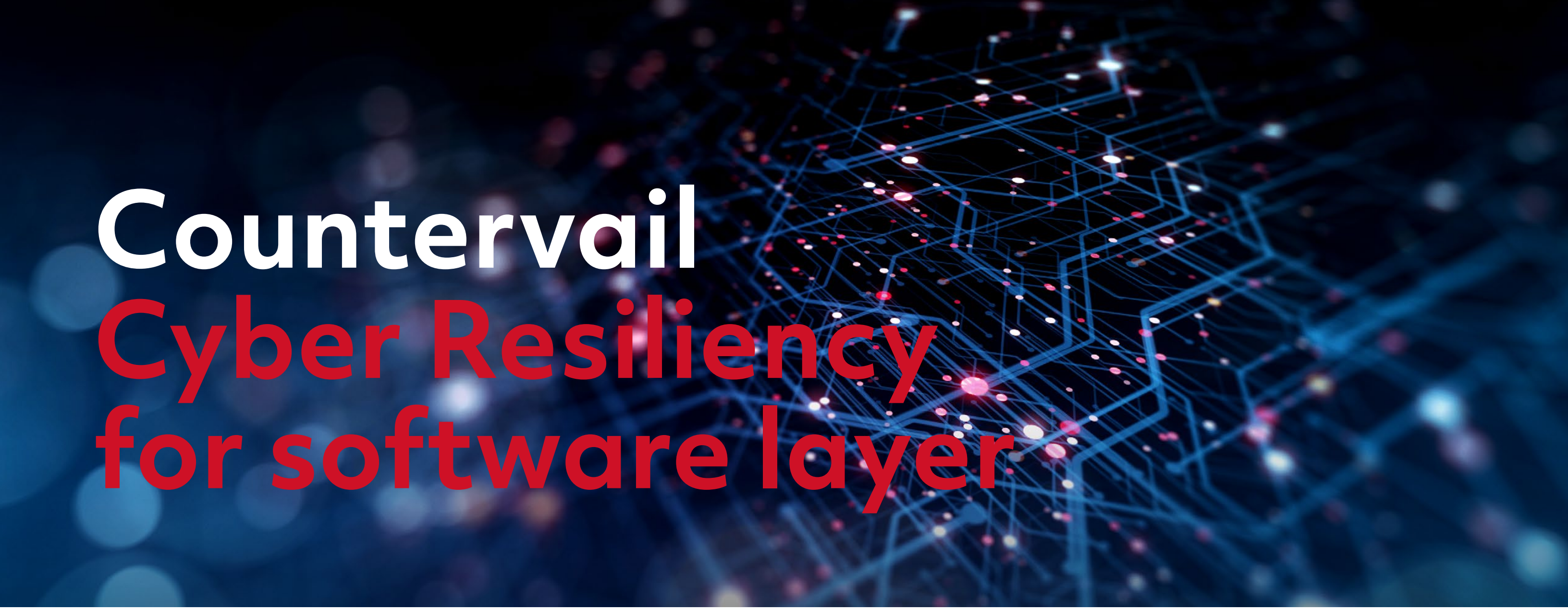

Countervail
Cyber Resiliency for software layer

As cyber threats against corporate and military systems continue to grow, system administrators are in need of advanced capabilities to authenticate computer applications and data. This is especially important because today's computer infections can change and compromise data anywhere, and often go unnoticed.

We need to maintain the integrity of the execution environment

Countervail, designed by leading cybersecurity company Raytheon Technologies, is a cyber-resiliency solution to this problem, providing an authenticated execution environment while limiting the attack surface of the platform's operating system.

The software solution bolsters the cyber resiliency of mission critical- and support- systems by ensuring the integrity of operating systems, applications and data. It is customizable to address an array of deployment use cases.

The Countervail solution

Countervail from Raytheon Technologies is an off-the-shelf cyber-resiliency product that reduces the risk of advanced cyber threats by preventing all untrusted or modified binaries from running on a protected system. As the sophistication of cyber threats continues to grow, the need exists for advanced capabilities like preventing untrusted execution on a target platform. Countervail's solution: Assume that the system should only operate as it was intended by actively protecting its configuration.

This solution can be procured through Raytheon Technologies' GSA IT Schedule 70 contract #GS-35F-204GA.

KEY CAPABILITIES

- Validates and maintains integrity of the operating system, allowing it to only operate as intended
- Authenticates signed files (applications, libraries, drivers, and data) prior to and during execution and provides integrators the ability to sign trusted applications and control the entire execution environment
- Blocks any attempts to execute unauthorized applications and logs all security events
- Detects possible attackers who have gained system access and/or administrative privilege and provides options for protecting Risk Management Framework (RMF)/Security Technical Implementation Guide (STIG) controls
- Actively protects signed files from being modified or deleted

EVERY SIDE OF CYBER

How it works

Countervail applies protection measures after application compilation and before deployment to the end system. It does not require access to or modification of application source code, reducing development and deployment time.

Instead, Countervail provides customers complete control over what applications and data are deployed into their fielded environments and creates a baseline. Additionally, it ensures system integrity after deployment by comparing attempted changes to the baseline and actively prevents baseline modifications.

Its threat model assumes the adversary has bypassed NIST 800-53 controls and has gained root-level access to a system and then protects against these attackers, even if they are an insider. It cryptographically verifies all user- and kernel-space binaries that are run on the system. Execution authentication can be further enhanced by allowing the system integrator to prevent all interactions of trusted binaries with untrusted data files. Countervail prevents all users from deleting, moving or modifying attributes of protected Linux system files, and blocks unauthorized updates or Operating System rollbacks.

It can also be used to lock important configuration files into place, ensuring that the system operates only in its intended configuration. Additionally, Countervail can be deployed with Boot Shield to provide a comprehensive hardware and software security solution, from early boot to mission execution.

When deployed together, Countervail offloads crypto operations to the Boot Shield card, which also provides continuous runtime memory monitoring of operating system internals and sensitive code elements.

Countervail updates safely and easily, and provides secure updates to applications, libraries, data and operating system patches and drivers. Countervail provides support for modern Linux and Windows operating systems.

Countervail

Raytheon
Intelligence & Space
1100 Wilson Blvd.
Rosslyn, VA 22209-2249
cyberresiliency@raytheon.com
raytheon.com/cyber/countervail

Raytheon Technologies

www.RTX.com