Raytheon, an RTX Business

Electronic Armor® Cyber resiliency for software layer

As threats against U.S. military systems continue to grow in scope and sophistication, many government programs and prime contractors recognize the need for significantly stronger security mechanisms to protect mission-critical systems. These systems are increasingly software dependent, making them a desirable target for adversaries to exploit.

Cyber-resiliency solutions

These systems also present inherently unique cyber-protection challenges because of their often remote deployments and detachments from managed networks, which makes detection, adaptation and response to evolving cyber threats difficult.

Although commercial information assurance processes and tools can prevent some basic or even moderate attacks, they cannot serve as the only layer of defense for mission-critical systems.

Stronger security mechanisms are needed to protect critical technology and ensure systems continue to operate as designed in cyber-contested environments.

The Electronic Armor solution

The Raytheon's Electronic Armor (EA) offers an integral solution for cyber resiliency and technology protection.

The EA prevents reverse engineering and protects the confidentiality and integrity of data and applications from attackers who have bypassed traditional information assurance controls and/or gained escalated privileges on a system. The solution assumes root-level attackers are already on your systems.

Among its many features are the hardening of the operating system, providing data at rest and runtime protections, preventing execution of unauthorized applications and preventing modification/introspection of sensitive applications and data.

KEY CAPABILITIES

- Hardens operating system (capability removal).
- Protects data at rest and runtime.
- Prevents execution of untrusted software.
- Prevents modification/reverse engineering of applications.
- Provides autonomous event detection and response framework.

Electronic Armor

Electronic Armor leverages advanced techniques such as just-in-time decryption, decoys, false paths and active defenses that keep critical applications and data secure while ensuring overall mission resiliency.

Electronic Armor does not require access to program source code, allowing for smooth deployment to legacy and new systems. The solution seamlessly integrates into existing security architectures. The collective features of EA can be tailored to fulfill the unique requirements of each specific deployment. It has been field deployed since 2009 and supports modern and legacy versions of Microsoft® Windows®, Linux, and VxWorks.

How it works

EA's operation includes offline and runtime elements. Prior to deployment, offline tools are used to fingerprint and tailor the system to the hardware environment, so it actively responds to threats in a way that supports the mission. The tools are also used to encrypt and package applications, libraries and data for use in the trusted environment.

During runtime, EA is loaded into memory and establishes a trusted execution environment through hardware and environmental checks. Once it has established that the environment is safe, trusted applications and data are now allowed to be loaded into the memory. The system is then continuously monitored and actively defended by EA as the applications are allowed to carry out their mission while thwarting would-be cyberattacks.

Electronic Armor

Contact
Raytheon, an RTX Business
1100 Wilson Blvd.
Arlington, VA 22209
cyber.services@rtx.com

www.RTX.com/cyber

Raytheon
An RTX Business