GENERAL DYNAMICS
Mission Systems

CrossingGuard®XD

Virtual Cross Domain Transfer Solution

SABI Certified Cross Domain Transfer Solution

Software-based, designed for secure virtualized environments

Built for tactical deployments with SWaP constraints

Supports uni/bi-directional data transfer requirements

Security based on DoD standards and NSA guidance

Increases operational and cost efficiency

Meets NIST SP 800-53 rev 4, CNSSI No. 1253 and CNSSI No. 1253F Cross Domain Overlay

Overview

The ability to access and share information anytime and anywhere is critical to any mission – the warfighter in a tactical environment requires the ability to do so with minimal equipment due to Size, Weight and Power (SWaP) constraints. General Dynamics offers a low SWaP, trusted cross domain access and transfer solution that is ideal for tactical platforms and sensors.

CrossingGuard®XD is a software-based virtual guard designed for tactical mission environments that require cross domain processing at the mobile edge where low SWaP is critical. Built on open standards, CrossingGuard®XD enables uni- and bi-directional data transfer between adjacent security domains based on pre-defined message rule sets and filters.

CrossingGuard®XD can be employed on any trusted virtual platform including General Dynamics' Trusted Embedded Environment (TEE) Cross Domain access solution. TEE is a software-based bare-metal Type 1 hypervisor and separation kernel that utilizes Intel® hardware-assisted virtualization to enable multiple operating systems to run and be viewed simultaneously on the same computer.

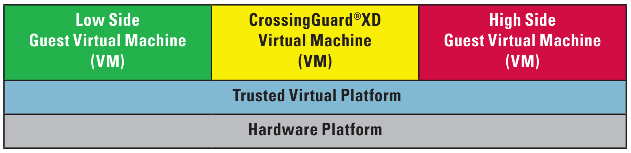
By collapsing the footprint, users realize increased operational efficiencies including rapid mission response time as well as significant cost savings associated with decreased equipment, infrastructure and lifecycle savings.

Crossing Guard®XD

Built to Meet Tactical Mission Requirements

Typical cross domain access and transfer solutions are hosted on hardware appliances that require platform power and space which are costly to purchase and maintain. The CrossingGuard®XD core framework is designed for virtual environments requiring:

- Modularity to support flexible software components and pre-defined rule sets based on mission need
- Embedment into existing or new infrastructures minimizing footprint and reducing SWaP
- Extensibility, driven by configurable policy
- Adaptability for new features, filter engines, workflows



Low Side Guest Virtual Machine (VM)
CrossingGuard®XD Virtual Machine (VM)
High Side Guest Virtual Machine (VM)
Trusted Virtual Platform
Hardware Platform

Core Security Features:

CrossingGuard®XD executes in its own virtual machine and utilizes an assured uni-directional pipeline architecture. It features Security Enhanced Linux® (SELinux) protection as part of its trusted computing base and Secure Inter-Process Communication (SIPC) message processing. This assures the guard is an independent, protected entity with limited and controlled interfaces shielded from other processing on the same computing platform. The secure transport uses standards based protocols such as Transport Layer Security (TLS) over TCP/IP along with certificate based mutual authentication. Other security features include:

- Built-in self-tests and trusted boot
- Fail secure (terminates outside connections upon attack)
- Mandatory Access Control (MAC) protection based on SELinux policy
- Firewall capabilities
- Anti-virus/malware checking
- Covert channel prevention mechanisms
- Automated filtering rules to re-grade security classification of network-based messages
- Secure auditing
- Support for Raise-The-Bar initiative

Other CrossingGuard®XD Features:

- Runs 'headless' for autonomous operations; can be configured to support limited admin functions
- XML sanitization, data transformation, content filtering and normalization
- Supports various pre-defined data filtering and message formats
- Digitally-signed XML schema validation
- Configurable protocol engines
- Interchangeable transport protocols with current sessions of varying types due to abstracted interfaces
- Optional virtual machine interfaces
- Support for interoperability with high and low Online Certificate Status Protocol (OCSP) responders for digital signature path validation
- Support for SNMP v3 for status monitoring (Gets and Traps)

Technical Specifications

- Certifications
  - SABI Certified
- Operating system
  - Linux. Hardened per STIG and un-needed RPMs have been built out which reduces the attack vector
- Domains supported
  - Two adjacent security domains, i.e. Unclassified / Secret (SABI) or Secret /Top Secret (TSABI)
- Policy enforcement
  - SE Linux policy, CrossingGuard®XD policy and use of SIPC for distinct uni-directional flow through the assured pipeline architecture
- Data transfer capabilities
  - Secure Transport uses the Transport Layer Security (TLS) protocol over TCP/IP along with certificate- based mutual authentication
- Data filtering capabilities
  - Currently supports MIL-STD 6017/A/B Variable Message Format (VMF), NTP, JBC-P, FOS, ASCII & Binary program specific filter components, USMTF, JPEG, XML and Misc. File Types (L to H): .ppt, PDF, CSV, NMEA/GPS, .wav, and BMP
- Operational Mission Environments
  - Top Secret and Secret or
  - Secret and Unclassified, or
  - Secret and Secret/Releasable

Previously, multiple pieces of equipment were needed to view/access applications of different security levels such as Battle Management Software and weather maps.

TEE and CGXD enable users to run and view those applications simultaneously on one single platform.

GENERAL DYNAMICS
Mission Systems

info@gd-ms.com • GDMissionSystems.com
US & Canada: 1-877-449-0600 • Global: Your AT&T Country Code + 877-466-9467 • DSN: 312-282-1048