GENERAL DYNAMICS
Mission Systems

PitBull® Trusted Operating System

Cyber Defense Starts with a Trusted Operating System

Isolates Data, Applications, and Interfaces

Provides Foundation for Multilevel Security

Contains Data Loss

Prevents Data Spillage

Reduces Insider Threat Risk

Overview

The PitBull® Trusted Operating System (OS) provides the secure separation and role-based access control required to protect information of multiple levels at the heart of the computing platform. PitBull software enhances Red Hat Enterprise Linux 6® by providing trusted functionality and high assurance.With heightened focus on protecting information from both internal and external threats, PitBull's compartmentalization ensures the integrity and control of data is maintained, while data spillage is contained in the event of a breach. PitBull is a commercial solution that is currently deployed worldwide to protect information and networks.

Features-at-a-Glance

- Adds a fundamental layer of security to ensure integrity for all levels of use
- Isolates applications, network interfaces, data, and users using simple security labels—does not rely on a complex rule set for isolation
- Prevents exploitation of bugs in any one application from damaging the entire system or other running applications
- Controls network resources usable by each application
- Controls and limits all user and administrator accounts—eliminates superuser vulnerabilities by enforcing least privilege and separation of roles.
- Allows for the development of flexible, ironclad security architectures
- Consolidates workstations, eliminating the need for multiple computing platforms
- Installs as an upgrade to an operational system

Security Features:

- Identification and authentication
- Discretionary access control
- Mandatory access control
- Mandatory integrity controls
- Privileges
- Authorizations
- Security flags
- Auditing
- Integrity checking

PitBull® Trusted Operating System

- Advanced secure networking

Industry Standards:

- Exceeds LSPP (EAL4+) Common Criteria requirements
- Provides Bell-LaPadula-based MAC (mandatory access control)
- Supports the MTR-10649 MITRE Label Encoding Format file
- Supports Biba model MIC (mandatory integrity control) based labels

Unique Features:

- MAC and MIC labels supported at the kernel level
- Provides clearances for all system objects to include users, processes, memory segments and files
- Supports roles and authorizations
- Implements poly-instantiated MLS network ports and CIPSO-labeled packets
- Enforces two-man/four-eye login authentication
- Allows for dual operational/configuration system modes of operation
- System integrity checks and integrity databases
- Protects critical system files and services using disambiguated security mechanisms
- Supports labeled printing

with MAC controls

- Enhances and protects audit records

Software Development Kit

The Software Development Kit is included with the purchase of PitBull. The Kit includes libraries, header files, maintenance pages, and software developer manuals required to write PitBull-specific applications or modify existing applications to become PitBull aware.

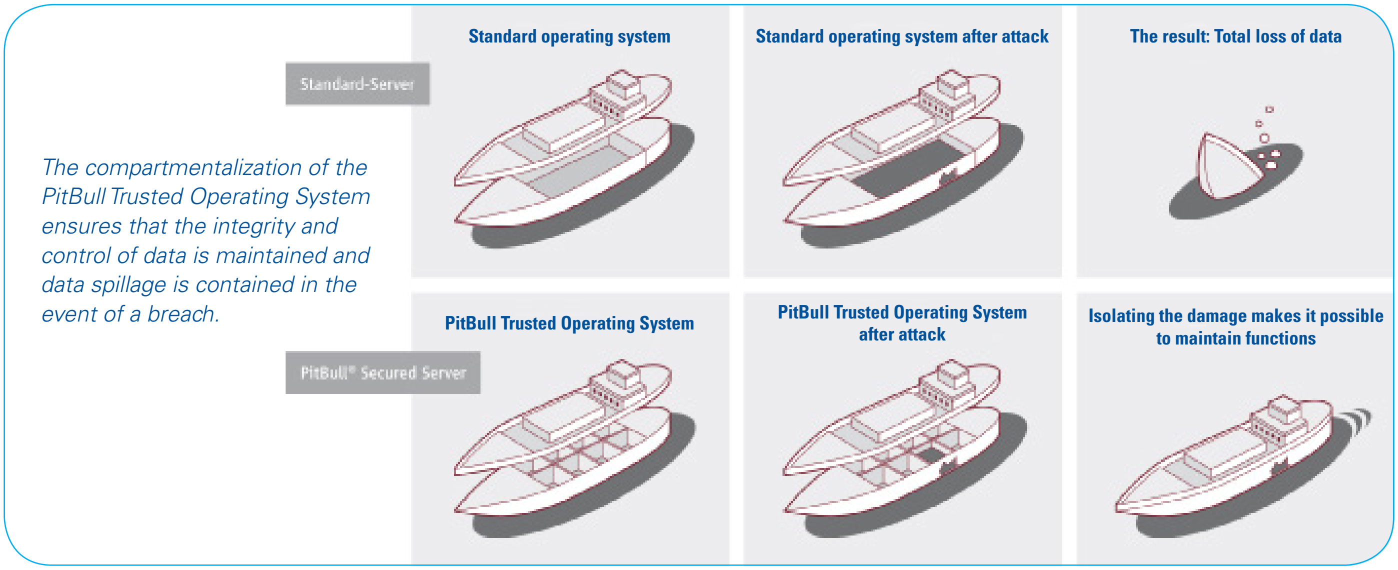
Optional Security Features

Building on the PitBull Trusted OS, the optional security features below allow commercial and custom software to be easily configured into trusted, sophisticated network architecture, securing utilities, tools, and scripts. Other benefits include:

- Streamlines architectures, improves performance, and reduces costs and manpower requirements
- Allows users to securely access back-end applications via the Internet
- Enables a modular architecture tailored to a customer's specific environmental requirements
- **Secure Communications Enforcer:** Tightly integrates trusted programs that pass packets between different security partitions and examines each incoming request and, if validated, directs it to the appropriate service
- **Security Gate:** Trusted software component that mediates limited, secure communication between applications or utilities in separate compartments, without allowing direct access to each other's files
- **Secure Program Launcher:** Allows users without powerful authorizations to execute programs that operate at a high level of security, but only in a limited predefined mannerz

Training

- **PitBull Introductory Training (3-day):** Introductory Training course covers all of the basic PitBull features and commands for users, administrators, software developers, and system architects.
- **PitBull Software Developer Training (2-day):** Designed for software developers who will be writing software for PitBull or adding PitBull security features to existing software. Prerequisite: PitBull Introductory Training


Standard-Server
Standard operating system
Standard operating system after attack
The result: Total loss of data
PitBull® Secured Server
PitBull Trusted Operating System
PitBull Trusted Operating System after attack
Isolating the damage makes it possible to maintain functions

The compartmentalization of the PitBull Trusted Operating System ensures that the integrity and control of data is maintained and data spillage is contained in the event of a breach.

GENERAL DYNAMICS
Mission Systems

gdmissionsystems.com/pitbull • Customer.Service@gd-ms.com
Phone: 1-877-449-0600