STOP™

Greater Security and Ruggedness, with Lower Development Costs

STOP is a high assurance operating system, designed from the ground up with security as its core focus. It is available to third-party developers as a platform for security-critical applications.

Developed exclusively in the U.S., STOP is a closed-source operating system. Field proven, STOP supports the Joint Strike Fighter program and several guards on the U.S. DoD/IC Unified Cross Domain Services Management Office (UCDSMO) baseline list.

STOP for Secure Application Development

STOP supports many Linux® API calls, allowing third party developers to port their applications to a higher assurance platform. Developers choose STOP to differentiate their products in today's competitive market. Customers also choose STOP to minimize total cost of ownership. For more than 35 years, STOP has not required a single critical security patch. STOP has flexible licensing options available for Enterprise and Tactical deployments as well as versions for individual workstations and development environments.

STOP for Cross Domain

The granular access controls and robust security features of STOP give users moving data between enclaves the assurance that classified information has been labeled correctly.

Built-In Security Features

Certifications

- Common Criteria EAL 4+
- FIPS 140-2

MARKET READY	STOP is integral to BAE Systems XTS® Guard 5 cross domain solution and is available as a stand-alone OEM product to Government and commercial customers, including third-party application developers.
PRICING	Trials are free. Flexible options exist for OEM partners: license model includes Software Development Kit (SDK) license and runtime licenses.

FOR MORE INFORMATION

11487 Sunset Hills Road
Reston, VA 20190
www.baesystems.com/csp
cybersecurityproducts@baesystems.com

Unique Security Features
- Smaller attack surface
- Instant revocation without reboot
- Buffer overflow protection by default
- Kernel integrity checks
- Native full disk encryption
- Remote shutdown

Minimal Developer Training Required. Support for:
- Linux API
- Database, web server, web browser and more applications
- Common libraries and developer tools, like Make and GCC
- X Windows GUI

Multiple Access Control Options
- Mandatory Access Control (MAC) includes Multi-Level Security (MLS) models that enforce traditional high-security information flow requirements and protect critical system resources from unauthorized modification, along with Role-Based Access Control (RBAC) which allows flexible permission-based access controls

Unique Security Features
In contrast to conventional operating systems that tack-on security features, STOP has security capabilities and development processes designed at the core of its DNA, including:

Smaller Attack Surface
Less than 1/10th the size of the Linux kernel, reducing the risk of compromise and minimizing the cost of security certifications.

Multiple Access Control Options
STOP provides system administrators with flexible security policy options. Administrators can choose between Mandatory Access Control, Role-Based Access Control and Discretionary Access Control.

Instant Revocation
When a security policy is changed, STOP responds immediately by applying real-time security configuration updates without requiring a reboot. Unique to STOP, this feature provides greater assurance and convenience for your mission.

Buffer Overflow Protection
Many potential threats, such as stack smashing, are mitigated through the use of all available compiler security options, NX (no execute), and ASLR. Runtime integrity monitoring is used to protect executables, security policies, configuration files, and other valued assets.

Flexible Auditing
Customizable configuration of auditable events ensures accountability. Fine-grained selection criteria allow the collection of all necessary and relevant records.

Extensive System Integrity Checks
Not only is the STOP kernel checked for integrity at startup, its kernel crypto-modules can also be checked at startup and on demand. The kernel utilizes a variety of features to guard itself against unauthorized modifications.

Flexible Deployment Options
STOP is portable, flexible and mobile in its deployment options without compromising its security certifications. STOP can be deployed on a wide variety of platforms, beyond traditional server environments, including:
- Single-Board Computers (SBCs)
- Virtual appliances
- Embedded devices

Native Full Disk Encryption
STOP encrypts each block of the file system, including a pre-boot environment that ensures encryption at rest and at initial startup.

Minimal Training Required
The STOP Linux-like Application Programming Interface (API) makes it easy for Linux-proficient developers and security professionals to operate.

About Us

BAE Systems Cybersecurity Products portfolio is focused on enterprise defense and the protection of information. We protect the world's most sensitive information with innovative solutions such as STOP™ secure operating system, our class-leading cross domain products, the Data Diode Solution™ and XTS® Guard 5, and our Secure Information Broker Appliance, SIBA.