



Information Assurance

XTS-400™ Trusted Computer Guard

Working to become a dependable partner of choice

BAE Systems Insyte's information security products enable classified information sharing, while enforcing network segregation. Highly evaluated, these products provide unrivalled data security and are available off-the-shelf or as part of a total system solution.

The XTS-400 trusted computer system is ideal for hosting trusted guard and server applications providing files, data and applications with unparalleled protection from malicious users and rogue software.

It is evaluated at common criteria EAL5 augmented by both the USA's National Security Agency and the UK Communications Electronics Security Group (CESG).

Robust operating system

The XTS-400's STOP™ operating system incorporates a high-assurance kernel to enforce the system's security and integrity policies.

The multi-level secure kernel ensures that information, processes and devices stored and running on the system at different sensitivity levels cannot intermingle in violation of the system's mandatory security model. The operating system also provides the capability for regrading objects (changing their security or sensitivity level), subject to customer-defined, configurable security policy. Because the XTS is evaluated at such a high level, data can only pass from one security domain to another through the security policy specified by the customer.

The operating system also includes:

- X-Windows graphical user interface
- Linux® programmatic interface
- A multi-level file system
- TCP/IP networking.

Trusted applications with high assurance

The Linux® - like programmatic interfaces of the XTS-400's Secure Trusted Operating Program (STOP™) operating system enable developers to port of develop applications easily on the system. These applications reside, for the most part, outside the system's Target of Evaluation (TOE), making them easier to certify and accredit while deriving a high degree of security and integrity from the underlying mandatory protection mechanisms in the TOE.

Several trusted software applications available for the XTS-400 have been accredited and are operational. These include trusted guard applications that provide strict control over the automated sharing of information among differently classified networks.

Commodity applications with high security

The Linux® Application Programming Interface of the XTS allows it to host Linux® - compatible applications, typically requiring no software reengineering. This capability increases the utility of the XTS by taking advantage of the many existing applications that can benefit from the security of being run on a high assurance server.

Life-cycle engineering expertise

BAE Systems has several application development groups that specialise in the development of high assurance guards and other applications that run on the XTS. These groups are experience in the entire life cycle of development, including requirements analysis, development, documentation, certification, deployment, and support. They can help field the systems by providing installation, configuration, accreditation support, training, and help desk support to enable the customer's XTS system to meet their mission requirements.

BAE Systems has experience in working both with prime contractors and directly with agencies. BAE Systems can act in every role from product supplier to full development partner through various contract vehicles.

Our capability

BAE Systems has developed sovereign assurance information management capability for the UK government's Information Assurance Technical Programme (IATP).

An in-depth understanding of Information Assurance (IA) lifecycle requirements are required before government, military and coalition partners can share information across security domains, nationally and internationally. To develop this understanding BAE Systems provides:

- Initial IA study/analysis and risk assessment
- Understanding of the information community
- Development of appropriate technology and process
- Management of solution evaluation, certification and accreditation
- Continued support - addressing the risk of emerging threats and leveraging new IA technology.

BAE Systems has delivered secure, trusted operating systems and databases based on mandatory access controls (MAC) and multi level security (MLS) for several years. Subsequent developments have seen the adoption of domain based security techniques, data diodes supporting one-way information transfer and a variety of firewall based solutions (de-militarised zone).

These capability enhancements meet evolving operational needs allowing sensitive MOD operational data to be shared securely, at both fixed and deployed locations, across all services.

Our approach

BAE Systems applies a building block architecture approach and has leveraged the XTS-400 capability to develop common guarding solution functionality.

Guard solutions are constructed from existing software suites hosted on the XTS-400 and may include third-party supplier capabilities such as:

Trusted re-grade and release between security domains of differing sensitivities

- Policy-based filtering
- Content checking, eg malicious code, dirty words or white list
- Syntax/schema validation
- Commercial anti-virus engine integration
- Label based sensitivity mediation/network identity mediation (mandatory access control)
- Handling of encrypted data.

Bespoke development

In some cases bespoke development solutions are needed to meet specific security needs. A dedicated team undertakes highly-specialist development activities and manages solutions through evaluation and certification. This includes all phases of the delivery lifecycle; requirements capture, system design and development, integration & test, and evaluation.

FOR MORE INFORMATION CONTACT:

BAE Systems Integrated System Technologies Limited
Victory Point
Lyon Way, Frimley, Camberley
Surrey, GU16 7EX, United Kingdom
Telephone +44 (0) 1276 603000
Fax +44 (0) 1276 603001
email insyte@baesystems.com
www.baesystems.com/insyte

Copyright © BAE Systems 2010. All rights reserved.

This publication is issued to provide outline information only which (unless agreed by BAE Systems in writing) may not be used, applied or reproduced for any purpose, or form part of any order or contract or be regarded as a representation relating to the products or services concerned. BAE Systems reserves the right to alter without notice the specification, design, price or conditions of supply of any product or service.

04.10.Insyte.BC222408.01.v12