

Canadian Forces Experimentation Centre helps secure information with Microsoft RMS

Overview

Country: Canada

Industry: Government

Customer Profile

The Canadian Forces Experimentation Centre (CFEC) is an organization within Canada's Department of National Defence that tests leading-edge technology that can potentially be utilized within the Canadian Forces.

Business Situation

The CFEC was particularly interested in testing solutions that help improve securing information sharing between coalition nations.

Solution

The CFEC tested Multi National Coalition Security System (MNCSS), an information sharing solution that provides mandatory classification marking of all E-mails, attachments and documents created in Microsoft Office.

Benefits

- Improved Communication and Information Sharing
- Enhanced Security and Rights Management
- Look and feel of Microsoft Office
- Helps Reduce Maintenance Costs
- Helps Lower Administration Costs

“The MNCSS can potentially make information sharing easier and quicker as all users are on one network – there is no need to manually transfer information from one network to another.”

John Hewie, Principal Account Technology Specialist, Microsoft Canada Co.

The Canadian Forces Experimentation Centre (CFEC) is the national coordinator for Canada within the Coalition Warrior Interoperability Demonstration (CWID) program. The CWID is an annual international event where coalition nations have an opportunity to review and assess technologies and capabilities designed to solve current interoperability challenges within an international coalition environment. The aim of the Canadian Forces for CWID 06 was to enhance Canada's digital information sharing abilities between its allies. To demonstrate high-level security around its classified information sharing capabilities, the CFEC successfully tested the Multi National Coalition Security System (MNCSS), a solution enabled by Titus Labs Inc. classification software and Windows Rights Management Services (RMS) for Windows Server 2003. The solution provides CFEC encryption when sharing digital files.

Situation

The Canadian Forces Experimentation Centre (CFEC) is an Ottawa-based organization within Canada's Department of National Defence that reviews and tests leading-edge technology that can potentially be used by the Canadian Forces to improve its response to military or other domestic threats.

The CFEC is also the national coordinator for Canada within the Coalition Warrior Interoperability Demonstration (CWID) program. The annual CWID event is an opportunity for Canada and other participating coalition nations to evaluate new and emerging commercial technologies and to develop new ways to meet interoperability challenges and operational requirements. The CWID event uses a global experimentation network to connect military services and government agencies from 23 nations. During the CWID event participating countries explore and measure the effectiveness of applications with potential for strengthening the military, domestic security and public safety. Successful technologies can then be rapidly adopted for operational use.

"The CWID provides an unbiased environment in which to test cutting-edge technologies. This helps the Canadian Forces to learn from its coalition partners in developing better methods to share digital information between nations" said Major Patrick Bailey, who is responsible for coordinating Canada's participation in the event.

The current information sharing solution for coalition partners is a U.S.-based system known as CENTRIX. Sharing classified and sensitive information such as email, documents and files within the CENTRIX system involves multiple wide-area computer networks – the goal is to establish a single

common secure network for transmitting data.

"When it comes to sharing classified digital documents within countries, there is obviously a strong requirement for encryption, security and protection from unauthorized use that is ideally located on a single network. Multiple networks mean more maintenance and administrative costs, which all coalition nations are trying to avoid," says Bailey.

Solution

During CWID 2006, the CFEC tested several Canadian technologies, including the Multi National Coalition Security System (MNCSS). The MNCSS is an information sharing solution which uses classification software from Microsoft Gold Certified Partner Titus Labs and Microsoft® Windows® Rights Management Services (RMS) for Windows Server® 2003 operating system. This system uses tools developed by Titus Labs to provide mandatory classification marking of all e-mails, attachments and Microsoft Office-based documents.

The Windows RMS-based document classification tool works by integrating into Microsoft Word and Outlook® 2003 messaging and collaboration client to help safeguard email and documents in Word from unauthorized use. The MNCSS features a classification toolbar located within Word and Outlook. Using the toolbar, operators can then select the appropriate rights management security level.

"MNCSS is easy to set up and permissions are automatically applied to the documents and e-mails to ensure that only intended coalition members have access," says Charlie Pulfer, VP Product Management, Titus Labs.

The Microsoft Windows RMS component of MNCSS serves to help safeguard digital

information from unauthorized use. With this system in place, selection of the classification and releasability of the information within is required before the document can be saved or the email can be sent.

Benefits

During CWID testing, the MNCSS proved to be an ideal tool to help improve security and rights management and enhance data sharing between coalition nations. “Secure information sharing is very important with coalition countries. Every country has information they consider classified that they would not want to share with other countries,” says Bailey.

Enhanced Security and Rights Management

Based on classification levels set by CFEC users, documents and email are encrypted via Microsoft Rights Management. Only authorized members of the community of interest with the appropriate security credentials will be able to view the information.

The MNCSS features the same look and feel as the Microsoft Office desktop environment, allowing users to associate classification levels with enforceable rights management (RMS) policy. These policies can restrict the distribution, printing or copying of documents in Microsoft Outlook and Microsoft Word.

The Titus Labs product will prevent any distribution of emails while a recipient from outside the flagged community of interest is in the distribution list. Administrators can also configure the Document Classification product to automatically apply RMS permissions based on the selected classifications to control viewing, distribution, printing and retention of the document.

“RMS provides us with an added layer of assurance. This is the level of security that the CFEC seeking, and helps them do their

work with a higher level of confidence,” says John Hewie, Principal Account Technology Specialist, Microsoft Canada Co.

For example, the selected classification markings are automatically inserted at the top and bottom of the document and in the email subject field. Even if the user does not manually select these markings, it will be enforced before the email can be sent or the document can be saved.

The tool did a good job of restricting the sending of email to only specific communities of interest based on the releasability marking, recalls Bailey. This feature prevents the sending and forwarding of an email to recipients outside the community of interest indicated in the releasability tag. The solution also features enterprise-class encryption capabilities, which prevents unauthorized users from being able to view the message.

Improved Communication and Information Sharing

Organizations such as the CFEC require a cost effective method to exchange information both between themselves and with other allied countries and the MNCSS system allows coalition members to share information. “MNCSS successfully met its CWID objectives and other than for sorting out a few installation issues, there was no technical support required,” says Bailey. During the CWID, users received on-site training and found the system to be intuitive, easy to use and quick to set up and deploy, adds Bailey.

“The MNCSS can potentially make this information sharing easier and quicker as all users are on one network — there is no need to manually transfer information from one network to another,” says Hewie.

For More Information

For more information about Microsoft products and services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada Information Centre at (877) 568-2495. Customers who are deaf or hard-of-hearing can reach Microsoft text telephone (TTY/TDD) services at (800) 892-5234 in the United States or (905) 568-9641 in Canada. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information using the World Wide Web, go to: www.microsoft.com

For more information about Titus Labs products and services, call (613) 820-5111 or visit the Web site at: <http://www.titus-labs.com/>

For more information about Canadian Forces Experimentation Centre products and services, call (613) 949-6751 or visit the Web site at: <http://www.dcds.forces.gc.ca/cfec/>

The document classification tool can also be used within other public sector environments including intelligence and law enforcement, adds Pulfer. "These organizations can benefit from the solution to help prevent sensitive information and confidential email messages from intentionally or accidentally getting into the wrong hands."

The solution can potentially enable multiple CENTRIX networks to be collapsed into a single network, helping to reduce costs and administrative workload.

"The general consensus was that MCNSS made the process of classifying data part of the thought process rather than being an afterthought or an optional step. It will also help us communicate with our allies and share information with them, which is a crucial capability for Canada as we build our defence policy around international partnerships," says Bailey.

Microsoft Office System

The Microsoft Office System is the business world's chosen environment for information work, providing the programs, servers, and services that help you succeed by transforming information into impact.

For more information about the Microsoft Office System, go to: www.microsoft.com/office

© 2007 Microsoft Corporation. All rights reserved. This case study is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. Microsoft, Example: Active Directory, Windows, the Windows logo, Windows Server, and Windows Server System are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Document published January, 2007

Software & Services

- Microsoft Word
- Outlook® 2003
- Windows Rights Management Server 2003

Partners

- Titus Labs

Microsoft®