



The art of securing your business

COCKPIT2i

Product review

Review was conducted and written by Comsec Consulting group for Jetro's Secure Web Browsing product - COCKPIT2i (July, 2007).

1. Introduction

About Jetro Platforms and its product COCKPIT2i

Jetro Platforms specializes in the server-based computing (“SBC”) and application virtualization sectors and has strong foundations in the SBC world with hundreds of customers world wide. Jetro recently introduced its revolutionary secure web browsing solution COCKPIT2i (COCKPIT to internet) that is designed to provide a fully secured enterprise web browsing infrastructure. COCKPIT2i is different from other security solutions focused on protection against employee browsing risks since it does not protect the network by filtering incoming content but rather keeps all internet content in a central secure area outside the core enterprise network. User browsing activity all takes place outside the network, and only a harmless video-like format enters the corporate network to be presented on desktop monitors. See more at www.jetroplatforms.com

About Comsec Consulting

Comsec Consulting (TASE: CMSC) is a pioneering market leader in providing Information Security & Risk Management consulting services to organizations worldwide. Specializing in the areas of IT Risk Management, Information Security and Physical Security, Comsec Consulting provides all-encompassing services, such as Operational Risk Assessments, Security Design Reviews, and Compliance with International Standards. Founded in 1986, Comsec Consulting operates internationally through six offices in Tokyo, Amsterdam, Istanbul, London, Warsaw and Tel Aviv. Our cutting edge information security services are delivered to over 400 customers around the globe. Comsec Consulting currently employs over 130 consultants, providing a wide range of client tailored, state-of-the-art information security services. At its recent Security Summit, Gartner announced that Comsec is one the top six leading Information Security companies, and the only pure Information Security consulting companies in Europe. The British SC Magazine proclaimed Comsec to be as on of the top 30 leading Information Security companies in the world (and the only Information Security consulting company in that list).

The Company was founded by Mr. Nissim Barel, an internationally recognized security expert, currently serving as President and Chairman of the Board of Directors. See more at www.comsec.co.il

About this document

Comsec was hired by Jetro to conclude a product study and write a design review for its product COCKPIT2i. This document provides is a proof of concept review of COCKPIT2i and summarize its unique value proposition comparing to its competing alternatives and existing products.

Comsec did not actually perform the security tests (infrastructure or application) for the technology itself, but learned the solution and the technology behind it. Comsec studied the product, used it for web browsing and performed a high level review of its interfaces, workflows and concept, and then interviewed customers, analysts, vendors and integrators from selected industries.

2. The Web Access Challenge for Corporations

During the past few years, the use of the internet has become a legitimate business tool. Many organizations today use the internet for business purposes. More and more services are provided over the internet, as well as information regarding various subjects and a number of support services. The possibility to surf the web is offered to company employees. The use of the internet has been proven to increase the company's professional level and also saves time and money.

However, the exploitation or uncontrolled use of the internet may increase the danger of the organization's exposure to various information security risks. In an age where an organization's business activity is based on computerized technology, the organization is threatened by the possibility of damage as a result of a system glitch or shutdown potentially caused by exposure to the internet.

Possible damage to the computer systems may cause the company's internal business processes to cease, and even worse – damage to the provision of services that the company provides vendors, partners and even clients. In extreme cases, a glitch in a company's computer systems may bring to a general shutdown of organizational units within the company – a situation that will harshly damage the provision of services that the company provides, as well as its reputation.

Information security awareness has been growing throughout the past few years. Most of the organizations are aware of the need to secure information and technology from threats that arise from the internet. The recognition of the need for information security leads to allocating resources for protecting the main assets. Furthermore, enforcement of regulations that dictate Information Security standards are obligatory in diverse organizations (banks, insurance companies, credit card companies, medical institutions, etc.). These standards and regulations create the right environment for development of tools, products and solutions that deal with security threats and risks.

Security threats are an ever-present concern when using the internet. Browsing the internet can be exploited as a backdoor for malicious code. Firewalls, anti-virus, anti-spyware software, etc. must be operated at all times. However, no matter how well protected your system is and how careful you are, browsing the internet places your system and corporation at risk. The internet is a public network that exposes the user to a global integrated network.

According to a 2006 FBI study, approximately 65 percent of organizations that deploy these traditional security measures still have their networks or data compromised by viruses and other malicious attacks.

In addition, risks such as: Phishing ,Pharming ,Spyware, Adware, Malware, Reverse Tunneling, Hidden Frame, Browser and O.S. Security Breaches, all renew themselves within a short time period and make identification and defense difficult.

The following are the major risks that arise from browsing the internet from corporate networks, many of them are new terms for new risks that were recently introduced to the world:

1. **Phishing** is a criminal activity using social engineering techniques. Hackers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing attacks are known to be carried out through bogus emails or a malicious redirection in a trusted website. Also IM (Internet Messaging) is known to be a security risk. For example, website forgery can be carried out using a Cross Site Scripting (XSS) attack that will convince the attacked user to validate his credentials against a trusted website while in fact a script running in the background is sending those credentials to the hacker.
2. **Pharming** is a hacker's attack aiming to redirect a website's traffic to another (bogus) website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. The idea is that the hacker will change the IP address for a known website URL name (DNS record). A successful attack will result in a misconfigured host file or a DNS server that directs the user to the hacker website. The hacker website would then be able to collect the user inputs including his verification credentials.
3. **Spyware** is computer software that collects personal information about users without their informed consent. Personal information is secretly recorded with a variety of techniques, including logging keystrokes, recording Internet web browsing history, and scanning documents on the computer's hard disk. This attack output may vary from personal data theft to a wide organizational data rip. An internal end user who browses the Internet from the organization's internal workstation is subject to these kind of attacks.
4. **Adware** (Advertisement Software) is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used. Adware sometimes is used as spyware.
5. **Malware** is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a combination of the words "malicious" and "software". The expression is a general term describing a variety of forms of hostile, intrusive, or annoying software or program code, such as Computer Viruses, Trojan Horse, Malicious Worm, etc.
6. **Reverse Tunneling Attack** is based on the idea of creating a tunnel (TCP session) from an internal workstation (within the organization information network) to an external (Internet) machine through legitimate firewall rules (HTTP, FTP, etc.), by using the created tunnel to connect the internal workstation from the external machine. A successful attack would expose the internal segment of the organization (where the workstation is placed) to an external malicious user.
7. **Hidden Frame** – Attacking the end user workstation (that is part of the internal network), using a hidden frame within the legitimate web page that contains a malicious code that can be exploited locally on the workstation, exposing the internal segment to security threats.

- 8. Browser and O.S. Security Breaches** – New software bugs and security vulnerabilities in the browser application are constantly discovered. These bugs are published on the Internet, on hacking sites, and are the basis for new hacking attempts and attacks. New security breaches are usually fixed and Microsoft occasionally publishes software updates. Immediate amendments of specific and urgent breaches are addressed by ad-hoc “Hot-Fixes” (Hot-Fixes for breaches in Microsoft’s various systems are released constantly and sometimes daily). Un-updated systems which are used for browsing may be exposed to many security threats.

Traditionally, organizations have sought to protect against external security risks with a combination of firewalls, intrusion detection/prevention software and anti-virus software. With the growth in spyware, key logging applications, and phishing sites, and the proliferation of blended attacks on computing networks, combined with the rapid increase in employee use of the internet, organizations are finding that existing security measures leave significant time and technology gaps in their protection. For example, anti-virus software provides protection from e-mail borne viruses but does not prevent the possible theft or corruption of corporate data by spyware and offers only limited protection against viruses that proliferate via peer-to-peer networks and instant messaging.

3. What is COCKPIT2i

Traditional internet browsing requires a direct HTTP link from the user’s browser to an external website, thereby potentially allowing undetected harmful code to penetrate and travel throughout the enterprise network. Currently available network security products that address browsing risks focus primarily on identifying malicious objects coming through open ports in order to eliminate them.

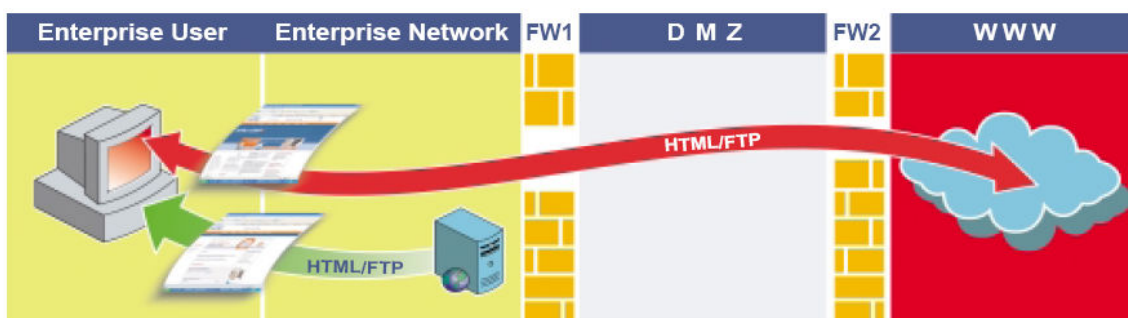


Image 1 - Browsing the internet using traditional web browsing.

COCKPIT2i is a server-based virtual browser that enables web browsing from a DMZ area outside the corporate network. It transfers SRDP, a video-like format, to users instead of HTML, images, files, print files, and software objects. COCKPIT2i Master Server manages the user’s access

permissions, and COCKPIT2i Gateway manages browsing virtualization activities. All ports, including the HTTP and FTP ports, are closed to enterprise users at the firewall. Data, files, images, scripts, and active code therefore cannot travel in and out of the enterprise network.

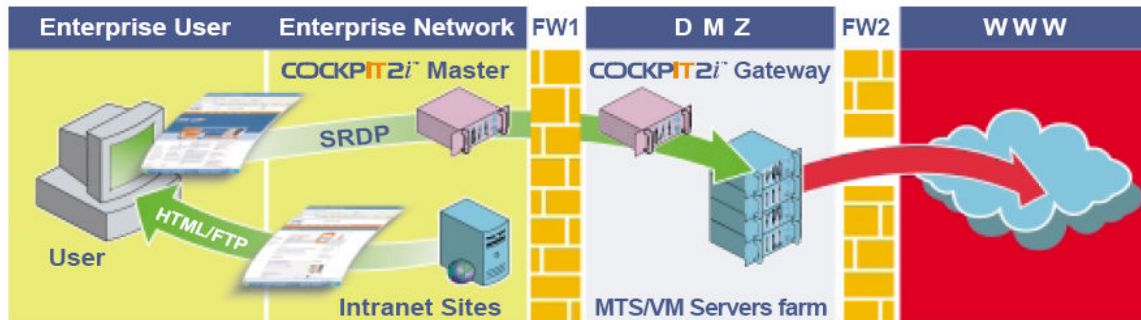


Image 2 - Browsing the internet using COCKPIT2i for remote browsing.

4. Overview of COCKPIT2i Workflow

With its innovative architecture and unique visualization technology, Jetro COCKPIT2i represents a new approach for allowing safe and centrally managed employee web browsing from within corporate networks. Instead of filtering web data, the product keeps all web data outside the enterprise network and does not allow any potentially harmful elements to enter the network.

- When enterprise users browse to local corporate sites, such as company portals, or web applications, or open local files, they automatically use their desktop browser.
- When users attempt to follow a link to external websites, the local browsing window is automatically and seamlessly replaced with the COCKPIT2i remote browsing window. Users continue their browsing session but the browsing actually is executed at a remote environment in the DMZ secured area.
- When the remote session is opened for users, they continue to have access to their settings, cookies, history, favorites, and links. The local desktop browser and the remote browser activated for the current session function seamlessly together.
- The remote session is anonymous. The browsing sessions on the DMZ contain a random set of username and password for each session to ensure user's privacy and data safety.
- COCKPIT2i provides a seamless printing experience; it rebuilds all print files to XPDF on the server side and redirects it directly to the relevant printer. The product does not allow a transfer of print files or original office or PDF documents.
- COCKPIT2i does not allow downloads or uploads of files, and the user has the option to email them using the enterprise's central email system.
- COCKPIT2i is fully integrated with corporate network directory (AD) services.
- An unmatched powerful web browsing experience is achieved using Jetro's patented technologies for hardware/software load balancing, seamless remote windows emulation, visual media streaming, Smart link recognition, content redirection, remote printing and flash banners handling.

When implementing Jetro's secure browsing solution, the IT manager gains the comfort knowing

that the FTP/HTTP ports are closed while still allowing the users a powerful browsing experience. The network manager gains full control over users browsing permissions and all monitoring capabilities. No other product can provide a similar level of protection for a full web browsing user experience. The only method to provide a similar load of security is either to prohibit employee web access or to enable employee web browsing only on separate desktops that connect directly to the web without going through the corporate network.

5. Competitive Analysis

Numerous network security products and procedures exist to protect organizations against the growing risks of web browsing. Current solutions include firewall with web proxies, content filtering, and server/client side anti-malware solutions. These lines of defense attempt to identify and destroy incoming malware from the web. Other products try to isolate the browsing environment (using a virtual machine) on the desktop to separate the browsing environment from the user desktop and corporate network.

We identified five types of approaches / products that enterprises currently use to protect against the risks of employee web browsing and how to monitor employee browsing manually.

Existing Concepts – Description and Advantages/Disadvantages:

1. Physical network separation involves separating the network into two different physical network segments and only allowing enterprise employees to have access to the internet from workstations that are not connected to the enterprise network. All threats (known and unknown) are dealt with in a different physical environment. It is impossible for anything to travel between the two networks. Implementing this solution requires two workstations for each user or a separate workstation for groups of users that provides internet access without going through the corporate network. This separation is hard to implement and force. It usually requires isolating the "internet" workstation in such a way that a user would not be able to unplug it from the network and re-plug his internal corporate workstation instead, or just use it to download malicious files and transfer them to the corporate information data network. Physical method separation is costly, difficult to administer, and reduces user productivity and satisfaction

2. Terminal browsing can be achieved by architectural design and terminal server implementation in order to try to provide secure remote browsing from a separated segment (Demilitarized Zone). Microsoft Terminal Server, VM servers, Jetro COCKPIT-SBC or Citrix PS4 are products that can be used for such a solution. Using such technologies usually requires dual management for both environments and few implementations we were facing ended up with poor performance. The terminal solution has many security holes, management, monitoring, performance and user experience gaps that make it very difficult to successfully deploy as a web browsing solution.

Citrix PS4 (on top of Microsoft Terminal Server) – by installing a terminal server the organization's DMZ, a user may browse the internet remotely and safely. Users will connect using Remote Desktop (RDP/ICA) to the terminal external servers. This way, any threats (known and unknown) will be dealt with outside the organizations' network. Terminal solution alone (With or

without Citrix PS4) was not design for such use and it has many security holes, management and monitoring issues, performance and user experience gaps that make it very difficult to successfully deploy as a web browsing solution, it will require a lot of hardware, and will result with poor performance, no integration to local browser and therefore low user satisfaction.

3. Web proxy - is a device that offers a network service to allow clients to make indirect network connections to other network services such as web servers. Usually used in organizations as a device that inspects internet browsing activities and performs an active enforcement of the browsing policy (such as URL inspection based on white or black lists, deep content inspection for malicious HTTP content that is based on known attacks (signatures) etc.). A proxy solution is considered to be a good security solution for browsing access control and even a good content inspection for malicious internet packets. However, it cannot guard the internal workstations or servers from being exposed to security issues that arise while browsing the public internet. Below are selected companies who make web proxy solutions.

Blue Coat Systems. Blue Coats' proxy solutions are implemented at the internet gateway to protect internal users and networks from spyware, phishing attacks and inappropriate web usage. Blue Coat products perform policy enforcement on content, users, applications and protocols.

PineApp™. PineApp's Surf-SeCure can be implemented as either a proxy or a bridge. It provides real-time filtering and packet inspection. Surf-SeCure integrates spyware and anti-virus scanning capabilities, web surfing protection layer and active URL content filtering.

Websense. Websense's Web Security Suite is a device that acts as a proxy. The product protects against spyware, malware, phishing attacks, bots, key-loggers and backchannel communications. Much like a proxy, the Web Security Suite blocks threats before they reach the network internal computers.

Finjan. Finjan offers Vital Security solutions for businesses and organizations. It is a device that acts as a proxy. The product protects against malicious attacks by abnormality of behavior. Much like a proxy, the Finjan Suite blocks threats before they reach the network's internal computers. In addition

4. Secure local web browsers represent a new group of web browsers that have improved security capabilities. They withhold some security mechanisms that allow end users to browse the public internet in a more secure manner. Most lack centralized management capabilities and require daily updates. Moreover, most solutions, such as Microsoft Internet Explorer and Mozilla Firefox, withhold security features that enterprises might find desirable. Nevertheless, the security risks of exposing the organization's local workstations to attempted hacking will still exist as long as the local user is using the browser application locally. Security breaches that may be used with low privileges can still affect the system, and yet the solution does not cover the corporate needs for network security, monitoring and management.

Firefox. Firefox is an open source web browser, created by thousands of software developers around the globe. It has unique protection against spyware. Firefox maintains automatic updates and preserves users' privacy by clearing stored personal information.

Internet Explorer 7. Internet Explorer 7 provides more security through a new architecture and features that help defend against Malware and phishing. It better protects against URL exploits and ActiveX malicious code. Like Firefox, Internet Explorer 7 allows the user to delete private information and history data.

Amust 1-Defender. Amust provides protection in various types of scenarios by preventing the installation of Malware. It also limits the activities that Malware can do. 1-Defender enforces "SafeInternet mode" to known internet applications (Explorer, Outlook, MSN), by employing Least Privileged User Account (LUA) that does not reduce Windows usability and flexibility, while making internet experience safer.

5. Local virtual browser. With local virtual browsing, enterprises require desktop users to access the internet on a hosted basis with a guest operating system that cannot affect the local operating system directly. A guest virtual O.S. executes the browser application and therefore all browsing security risks are isolated at the virtual local guest system. Issues enterprises face with local virtual browsers include:

- Limited to no centralized management / updating / policy enforcement capabilities
- End users must have administrative permissions to enable virtual environment
- Virtual operating system can become "backdoor" to corporate network
- Difficult to deploy (must implement on all enterprise desktops)
- Not seamless to users
- Requires change management / training
- HTTP ports remain open for each user

VMWare / Virtual Desktop Infrastructure. Leading solution for virtual machine implementation. It allows a user, who already has Windows OS installed on his hard drive, to theoretically install as many other different OS as he wishes. By installing a separate OS, the user can isolate his client's computer from the virtual machine, thus allowing him to use a virtual environment for internet browsing.

MojoPac. Transforms a simple USB memory drive into a portable Windows XP session. It is private, secured and easy to install and use. The portable session has its own unique user and environment configuration, and is completely isolated from the Host PC, thus preventing malicious software from jeopardizing that PC.

GreenBorder Pro. Keeps all interactions with a website and its associated content and programs away from the Host PC. The application keeps all the system files and resources invisible, protecting them from being remotely accessed or modified. All downloaded information (videos, applications, documents) are opened in a protected and isolated environment.

Fortress Grand Virtual Sandbox 2.0. Allows unknown applications to be run in an isolated environment. These applications will not have access to private files, system resources and computer configuration.

6. Findings

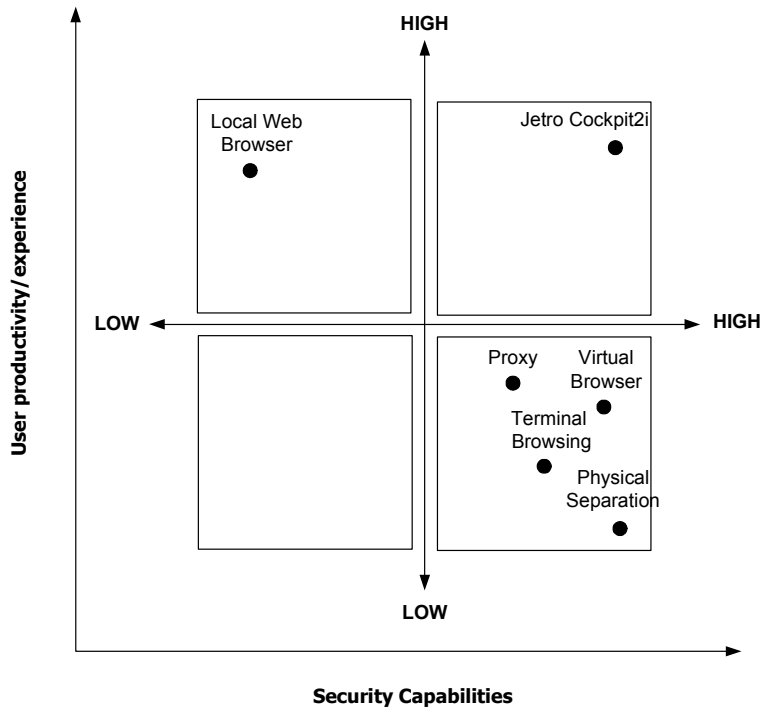
The following table compares the five major approaches to protecting against employee browsing risks / managing employee browsing activity based on three main criteria:

- 1) Protection against employee web browsing risks
- 2) Management, monitoring and control of employee web browsing
- 3) User productivity and web browsing experience

Network Security Concepts	Physical Separation	Terminal Browsing	Web Proxy	Secure Desktop Web Browsers	Local Virtual Browser	Jetro's COCKPIT2i
Sample products/vendors	Two separate networks & separate workstations for web browsing	<ul style="list-style-type: none"> • Terminal Server • Citrix PS4 • VM 	<ul style="list-style-type: none"> • Blue Coat • PineApp • Radware • CheckPoint 	<ul style="list-style-type: none"> • Internet Explorer 7 • Firefox • Amust Defender-1 	<ul style="list-style-type: none"> • VM ware • Mojopac • GreenBorder • Fortress Grand Virtual Sandbox 	COCKPIT-to-Internet from Jetro Platforms
<u>Protection</u> against web browsing risks.	High	Medium - High	Medium - High	Low	Medium	High
<u>Management</u> , monitoring and control.	Low	Low - Medium	Medium	Low	Low	High
<u>User productivity</u> and web browsing experience.	Low	Low	Medium	High	Low - Medium	High
Summary	High Cost, low user productivity and poor satisfaction. High security if well implemented and forced on all users.	Medium-High level of security, very low user experience and Productivity; High deployment cost making it not attractive.	High level of security against known threats, low protection against new ones. limited user experience.	New generation of browsers still provide low security against the growing threats and have no centralized monitoring and no web usage control.	Low to Medium security; deployment difficulties; low productivity.	Maximum level of security; good user experience; high productivity; good centralized monitoring and web usage control.

Security Capabilities vs. User experience and productivity

The traditional argument against more security for the corporate network is the reduction of user's productivity. It is very hard to balance between those two requirements; generally higher Network security reduces user productivity. Jetro solution succeeded to combine those issues as shown in the following chart:



* While with existing security concept user is paying with productivity and browsing experience, COCKPIT2i provides an impressive user web browsing experience with seamless windows. It does not force unnecessary restrictions, and at the same time is providing the highest possible level of network security.

Customer's viewpoints

Comsec interviewed selected existing COCKPIT2i customers, potential customers, vendors and integrators as well as senior IT personnel at a few targeted industries. Here is a collection of their feedback that best represent the general impression of the product and its offering:

- "We used to have physically separated networks and computers for browsing the internet. The COCKPIT2i approach provides us with the same level of security but with a seamless browsing experience to our users "
- "Jetro's Secure Browsing solution is a very unique solution, which strongly defends the internal LAN by separating it from the "browsing area" that is placed in a Demilitarized Zone. "
- "This new product deals with our concerns and problems through two main issues – security and functionality."
- "The product "removes" the internet surfing from the internal LAN to the external Demilitarized Zone. The product uses different network resources such as directory

services and physical devices. In case of security glitches the browsing area is infected leaving the internal network safe. "

- "COCKPIT2i combines the benefits of other products' approach and provides an integrated solution for security browsing; actually it is the only product that deals directly with the risks and threats that arise from surfing the internet. "
- "When we used to have external Information Security services and Remote Proxy access, users were blocked when attempting to browse certain internet websites. In addition, the Proxy also disables the use of security protocols such as HTTPS, SSL, etc. thus the users had difficulties while browsing the internet."
- "We use the products can be used as a data clearance device and eliminate unsafe files from entering the internal LAN. "
- "We tried to use Terminal Servers for secure browsing; but it denied the use of links that are sent by email. The link is connected through the local browser and cannot reach the destination. "
- "We will gain better performance using COCKPIT2i by reducing the consuming resources, such as Flash and reducing the administrator's need for dealing with problems at the end user computers. "
- "COCKPIT2i provides centralized management capabilities including monitoring and auditing. "
- "As a Bank institution we tried to use MTS with Citrix 4.0 and other products in order to provide secure browsing. This attempt failed due to functionality problems. The Terminal servers were overloaded due to the lack of ability to control large internet applications such as Flash."
- "We tried using separate work stations for browsing; but did not succeed in preventing users from copying information between the internet station and the network station. During an Information Security Risk Assessment that was conducted, external, many unsafe web-based files were discovered on the user's (network based) work stations".
- "COCKPIT2i is the only product that can provide us with the level of security achieved by separate network segments but without its downsides."

7. Conclusions

The Problem

Providing internet access to corporate users became a real concern in every organization. It seems that this concern will rapidly grow when using new web functionality and updated technologies.

The Product

Jetro's COCKPIT2i manages two browsers for each user. A local web browser at the user's desktop for local data and a remote terminal-based browser located outside the network for web browsing. The two browsers act like one for the user and when the user attempts to access the web, COCKPIT2i seamlessly redirects the session to the remote browser that projects the browsing data as video to the user's monitor.

How is it different?

Existing network security solutions try to identify the malicious objects (coming through the open ports at the Firewall) in order to eliminate them. Those detection and filtering solutions require daily updates and while they may provide good protection against known threats, they provide insufficient (if at all) protection against new and unknown threats.

COCKPIT2i does not deal with the different threats coming from the internet; it simply keeps them all outside the network and does not let any data in.

Value Proposition

We have chosen Jetro COCKPIT2i as the product that best provides a solution for organizations to securely browsing the internet! This is a brand new concept that provides an unmatched security to the organization and high comfort to the IT personnel.

COCKPIT2i in its current functionality will not allow enterprises to replace existing network security and infrastructure solutions that address the risks of employee web browsing and the desire to control / manage employee web browsing. As such, only those organizations who will be willing to pay for this level of security will want to evaluate COCKPIT2i for their needs.

The product provides value to two types of organizations: 1) those who do not currently allow web browsing access from the same network/desktop and would provide access if they could do so with an acceptable level of protection and an acceptable ability to manage and control browsing activity and 2) those that already allow employee web browsing but want a higher level of security and greater ability to centrally manage and control employee web browsing. The first group will be the quickest to adopt COCKPIT2i technology, exactly as happened when Checkpoint introduced its Firewall-1 solution to the world.

The Business Opportunity

We know that there is a growing concern and therefore larger budget spent by corporations in order to secure their network and protect their business and brand. Enterprise network security spending estimate of \$38billion, from which spending on software is about \$13 bn. We roughly estimate that the COCKPIT2i market has the potential to grow to around \$1b US over the next 5 years and triple that during the following 5 years. This market will grow even faster when it will be relevant for SMBs and not just the larger corporations and this will happen when it will be available (As Jetro plans in its roadmap) as a series of appliances targeted for a different size of customers. Jetro's future appliance will also contain other integrated capabilities that will prevent phishing and other threats. We believe that the first customers to adapt this new technology will come from those more security oriented industries such as the government, financial services and insurance. We also believe that it may take few years until a browsing server solution such as COCKPIT2i will become affordable enough in order to be an alternative for traditional browsing and a mainstream in second tier industries and SMBs. New regulations, such as those which are now materializing in Europe (Bazel2) for Government and Financial services and then in other parts of the world will push the market to adopt Jetro's unique offering.

Jetro's effort to partner with global leaders in this industry is definitely a key factor in its execution plan and we believe (talking to some of those potential players) that this scenario is likely to materialize in the near future.

Main Conclusions

The internet is not going to be safer but much riskier; all layers of content inspection and filtering will never match the growing risk to enterprise network. Given the continuing worldwide adoption of the Web as a mass communication, entertainment, information and commerce medium, providing web access to enterprise employees become a top tier enterprise productivity resource.

We compared the different types of solutions to protect the corporate network from the internet and have found that each type of solution has its disadvantages. While a combination of different solutions may provide a fair solution, it still exposes the network to many risks. **We have found that COCKPIT2i, which was designed specifically for enterprise secure web browsing, provides the best performance, manageability and usability, while maintaining the highest possible level of web access security for its customers' networks.**

COCKPIT2i's foundations are based on the already proved technology of Jetro's COCKPIT its SBC product. This provides COCKPIT2i with a high level of credibility and maturity, which is important in Enterprise sales, but of not lesser importance for Jetro; it provides Jetro with important competitive advantages against potential new players, who may wish to join this market.

8. About Comsec review team

Following are the Comsec team members who were directly involved in the COCKPIT2i review:

Mr. Yuval Birman is Comsec's Infrastructure Security Division Manager. Yuval is an expert in infrastructure and application security. Over 10 years of experience in finance, online gaming and Internet trading security sectors. Yuval managed Information Security projects for various applications. These projects included diverse Internet technologies and inter-organizational applications.

Mrs. Sharon Cohen Head of the High-Tech and Telecom Sector Division, with responsibility over a large number of High-Tech and Telecom accounts. Mrs. Sharon Cohen specializes in the Information Security market, with 10 years of experience in various High-Tech and Telecom companies.. Sharon experience includes information security, IP and ISP systems, large information system architectures, and more.

Mr. Asaf Bergerbum is a senior Information Security Consultant / Technology Leader. With over 7 years of experience in information security, Asaf is an expert in Microsoft technologies, operation systems, servers hardening and many security products deployment.

Mr. Amit Hayun, Project Manager – Finance Division. Expert in Terminal Server approach, 10 years of experience.

Mr. Shlomi Arditi has over 10 years of experience in the Information Security market, and information technologies. Shlomi is an expert in communication equipments. In the framework of his position and a Project Manager in Comsec's High-Tech and Telecom Division, Shlomi is responsible for a team of technical consultants that carry out diverse Information Security services.