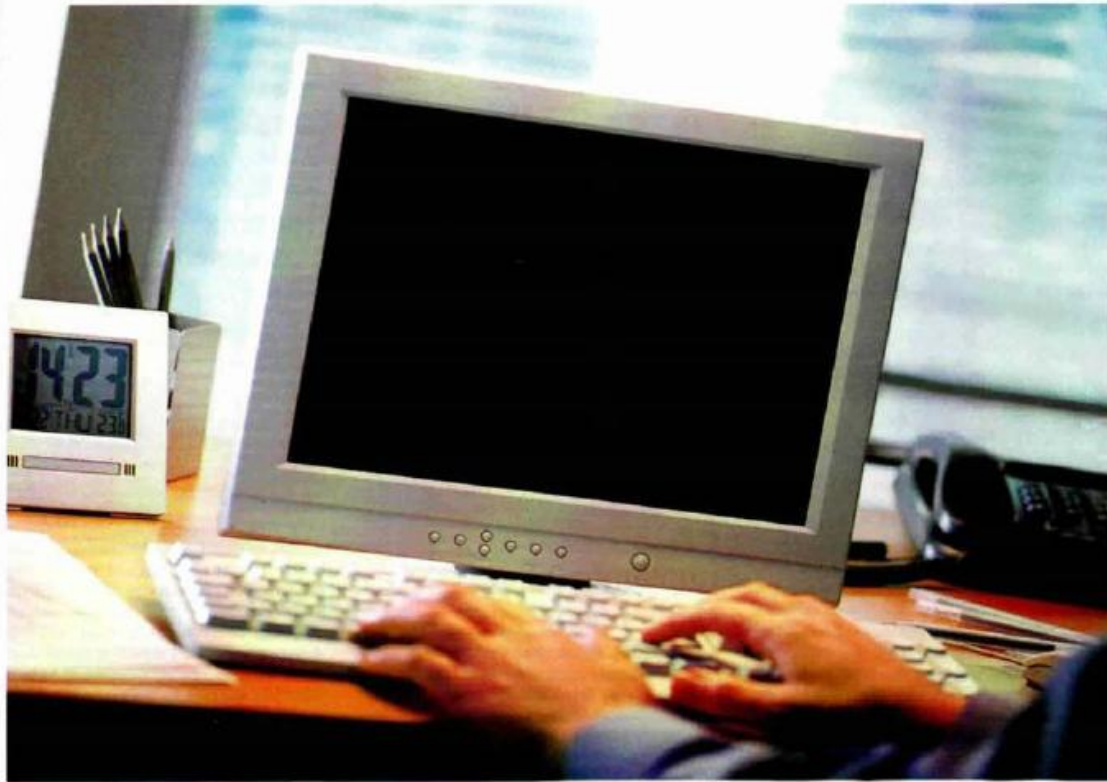


CASE STUDY



MISSION SECURITY

Security is a crucial aspect for any organization, more so for one dealing with IP. Nucleus Software addressed its security concerns by deploying Websense security tools.

BY MEHAK CHAWLA

In an era where the sophistication of threats is fast outpacing the preparedness of organizations, CIOs are becoming increasingly paranoid about security breaches and unplanned data sharing. Rajesh Garg, Vice President & Head - Information System Support, Nucleus Software, was no exception to this rule.

Data being posted on various sites, resumes being shared, source code being carried about on laptops, copying data to USB drives etc have become a common phenomenon across organizations. It is a cause of concern for companies like Nucleus Software that deal with confidential customer data. "As a solutions provider to the leading banking and financial services players in the country, Nucleus Software has always dealt with sensitive and confidential data," ex-

plained Garg.

Given the nature of work, allowing Internet access for various functions like sales and marketing, recruitment and HR became an imperative for Garg and his team. There was another challenge—the developers and pre-sales consultants needed to store product source codes and the details of various products and services on their machines.

This made it imperative for Nucleus to deploy an effective mechanism to protect its IP and client information.

Traditional anti-virus remedies that were readily available in the market did not do the trick as Garg thought that his organization required a more comprehensive solution to be deployed while ensuring zero access hassles for employees.

After successful evaluation of the

CASE STUDY

WE HAVE BEEN ABLE TO REDUCE LEAKS WITHIN THE ORGANIZATION BY 95% WITHIN TWO MONTHS OF THE DEPLOYMENT



RAJESH GARG,
VICE PRESIDENT &
HEAD - INFORMATION SYSTEM SUPPORT,
NUCLEUS SOFTWARE



WE CREATED A SERIES OF SECURITY PATTERNS TO BE DEPLOYED AT THE GATEWAY LEVEL BASED ON 200 SOURCE CODE PATTERNS FROM NUCLEUS

SURENDRA SINGH,
REGIONAL DIRECTOR - SAARC & INDIA,
WEBSense INC

product offerings from various vendors in the market, Nucleus zeroed-in on the Websense suite of DLP solutions to meet the company's security requirements. The Websense solution included predefined rules as well as customization features to ensure the protection of Nucleus' IPR.

Solution configuration

The Websense security tools were designed and customized to allow Nucleus' administrators to control, restrict and track the flow of sensitive information sharing within the organization. The tools would also enable the IT team to restrict employees from visiting non-business

Web sites.

According to Surendra Singh, Regional Director - SAARC & India, Websense Inc, Data Security Suite Manager, SMTP Gateway, Web Security Gateway Manager, Proxy, Remote Filtering Server, End Points and Remote Filtering Client were deployed.

Implementation challenges

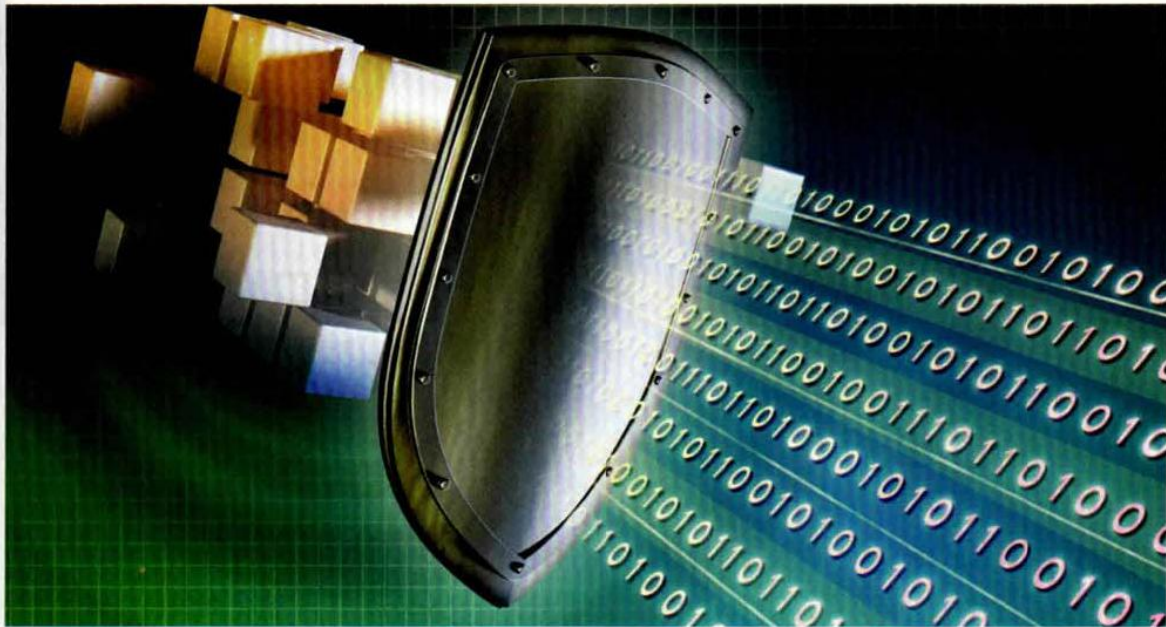
Singh explained that the implementation and deployment of a DLP solution was not easy. The solution had to be customized and tweaked as per Nucleus' re-

quirements in terms of levels of scrutiny. "Based on 200 patterns of source code from Nucleus, Websense created a series of security patterns to be deployed at the gateway level. In addition to the source code, critical HR policies, financial documents and marketing collateral, were fingerprinted. This meant that the gateway would screen these documents and clear them for sharing via mail only after receiving the relevant approval," elaborated Singh.

Garg corroborated that challenges were aplenty and some of them necessitated serious brainstorming. "As is often the case with beta stage product implementations, we faced a few challenges

Security infrastructure

Role	Version	Model
Websense Proxy Server	Web Content Gateway 7.5.0	Dell Power Edge R710
Websense SMTP Server	Microsoft IIS 6.0 SMTP Server	Dell Power Edge R710
Websense Web Security Gateway	Web Security Gateway 7.5	Dell Power Edge R710
Websense Data Security Suite	Data Security 7.5	Dell Power Edge R710
Websense Remote Filtering Server	Remote Filter 7.5	Dell GX 620



which required us to go back to the drawing board and resolve the concerns," he said.

According to Singh of Websense, "A key challenge prior to the deployment was to determine the parameters that would define the algorithms and also serve as the gatekeepers. Nucleus Software wanted specific parameters and security checks for the source code and languages used within the organization. Such patterns and information were not available in the Websense DSS repository as the company policies do not allow sharing of vital information with a third party."

To facilitate the availability of source code, sample files were made available to the Websense engineering team following the receipt of the required security and management approvals. This helped create patterns, which were then tested with a

variety of source code files specific to the language and technology in which the pattern was developed.

Patterns with low success rates were fine-tuned. These iterations continued for several months before the DLP solution was approved, accepted and implemented within Nucleus' Noida campus.

Calculating RoI

"After deploying Websense Data Security Suite and Security Gateway, we have been able to monitor and prevent the leakage of sensitive data," said Garg.

Post implementation, the awareness levels about IP have risen significantly within the organization. Earlier, while selected users were given Internet access based on business justification, other employees accessed the Internet from

kiosks. This was primarily due to security concerns.

With the deployment of Websense solutions, Internet access has been granted to all the employees. In addition, the implementation has also drastically reduced non-business Internet usage during business hours.

"During the POC period, numerous activities were traced for sending and sharing sensitive data outside the confines of the organization. Initially, these practices were close to 25-30 per day, but now these incidents have become almost negligible after the implementation of the product and fine tuning of the policies. We have been able to reduce leaks within the organization by 95% within two months of the deployment," said Garg.

The entire cost of implementation was recovered within two months. This ROI was calculated on the basis of the investment made on the product and the time spent by the employees on non business usage during the business hours. By cutting down on non-productive usage, Nucleus Software saw a 52% saving in Internet bandwidth.

Also, the 35 odd computers that were previously used as Internet kiosks for employees were rendered redundant as a result of this implementation. This resulted in direct savings of \$25,000, concluded Garg.

mehak.chawla@expresindia.com

PATTERNS WITH LOW SUCCESS RATES WERE FINE-TUNED. THESE ITERATIONS CONTINUED FOR SEVERAL MONTHS BEFORE THE DLP SOLUTION WAS APPROVED, ACCEPTED AND IMPLEMENTED WITHIN NUCLEUS SOFTWARE'S NOIDA CAMPUS