Cyberoam

Unified Threat Management

Case Study

Organization
Comyn Ching (Solray)

City/Country
Swansea
United Kingdom

Industry/ Vertical
Manufacturing

We needed a solution that could protect our internal resources from any unauthorised and malicious access, either from the Internet or from any internal user. We were also looking for a solution that would control unproductive surfing.

- Mr. Simon Turner
Group Financial Controller
Comyn Ching (Solray)

http://www.cyberoam.com

Cyberoam Secures the Internet for Solray

Background

Comyn Ching (Solray), the UK's leading name in radiant heating offers practical, reliable and cost-effective solutions for today's most demanding buildings. The Solray design incorporates waterway grids within flat panels, which can be manufactured from a range of materials. The panels are formed into a variety of shapes to create unobtrusive and aesthetically attractive heating and cooling systems. These panels can also be supplied in a range of finishes to blend into or enhance any building interior. The panels can be positioned on walls, placed within suspended ceilings, or even installed within the floor itself.

Solray has completed several design and construction projects for applications such as airports, hospitals, schools & colleges, theatres, prisons or secure units. Their out-of-the-way placement and stout construction makes Solray the most prominent choice in today's market.

The Solray Challenge

The Solray network basically comprised of design, construction and project with no focused gateway security sketch. The company contains the contract document and other client sensitive information and data that can be possibly targeted by attacks from external entities and outside access attempts. The organization, therefore, needed a gateway firewall to regulate user authentication and access control.

Shelter against Intrusions and Misuse

On the Internet, network intruders are sophisticated navigators. They come from outside the enterprise, attacking Internet connections, altering Web pages, and launching denial-of-service attacks. Intrusion attempts can also originate from inside the network, launched by sophisticated assaults that can circumvent or pass through firewalls, transmitting confidential information, or illegally modifying network access privileges. Mr. Turner was concerned about protecting data assets in the LAN such as confidential customer data, drawings, billing records and more from external entities. Therefore, they needed a solution which would be competent at seeing off these threats.

According to Simon Turner, Group Financial Controller at Solray, "We needed a solution that would control unproductive and harmful surfing". The company was facing the following security and connectivity challenges related to its business activities.

Controlling Malware & Spam Numbers

In the absence of gateway anti-virus, users surfing the Web (HTTP), transferring files (FTP) and exchanging mail (SMTP, POP3, IMAP) were constantly exposed to the danger of malware infestation. These malware attacks which often took a blended form through email attachments, PDF, design documents etc had the potential to alter constructive files and demolish significant data. Simple day-to-day activities were often hampered when such malware did infiltrate the system. As a result the productivity suffered as the IT department had to interfere to rectify the situation.

A perimeter level anti-virus solution was required that would protect the network, scan and clean any malware or spyware over Web mail and scan all Web traffic to ensure the contents were safe.

Controlling Surfing Patterns

The company wanted to keep an eye on and limit its users from accessing non-productive sites such as Facebook, Twitter and Myspace. Opening up access to these sites for all users resulted in bandwidth getting "choked". "We wanted the solution to ensure that precious bandwidth is not used up on downloads of audio, video and streaming media and bogus applications like Yahoo Messenger, Skype, MSN and instead, diverted to more productive use", Mr. Turner said. He believes that Internet access is a resource that should not be wasted and so every user's bandwidth usage ought to be distributed and monitored using content filtering. They needed strong web filtering solutions which could control all Internet access and give informative reports on Internet usage.

The Cyberoam Solution

After hunting the market for the right solution, Solray purchased a Cyberoam CR25i Unified Threat Management (UTM) appliance, which was soon deployed in gateway mode at the Swansea Factory, U.K. After deploying the solution, the following benefits were noted:

Cyberoam UTM adds up to a unique identity-based security solution which protects against insider threats by giving absolute visibility into "Who is doing What" in the network and allows creation of user identity-based policies.

User Integration

Cyberoam UTM adds up to a unique identity-based security solution which protects against insider threats by giving absolute visibility into "Who is doing What" in the network and allows creation of user identity-based policies. Mr. Turner used Cyberoam's Active Directory (AD) facility to achieve the task of integrating Solray's users in the network through a wizard to trade in users. Furthermore, the automated single-sign-on (SSO) feature of Cyberoam allows transparent authentication of the end users as soon as they boot their machines.

Complete Perimeter Security

Cyberoam's corporate firewall offered Solray stateful and deep-packet inspection capability to provide granular access control over Internet and network resources. Using this feature the administrator is now able to make identity-based security rules, offering instant visibility and dynamic controls over security breaches. This has enabled Solray to achieve a high degree of granular controls over the user's surfing behavior.

Barricading Intrusions

Mr. Turner used default IPS policies from the firewall rule to protect Solray's corporate network from DoS and spoofing attacks and other exploits. He also used IPS to protect their network, LAN and mail server from these intrusion attempts.

The potent combination of Firewall and IPS protects the Solray's corporate network from DoS, spoofing attacks and other exploits.

With a comprehensive database of 3000+ IPS signatures, Mr. Turner now feels that the company's data is well protected from several variants of spyware attacks, spoofing and DoS attacks in addition to keyloggers, Trojans and more. Cyberoam's promise of security and protection aided them to increase their network efficiency and performance.

The Latest Protection from Virus & Spam

Cyberoam UTM significantly reduced the high incidence of virus attacks, at Solray. Cyberoam UTM's gateway anti-virus and anti-spyware solution ensures real-time protection for Solray's network by delivering clean web and mail traffic.

Recurrent Pattern Detection (RPD) powered signature-less anti-spam technology works instantly on deployment, with minimal human intervention and is language independent. It blocks spam in any language regardless of the content, e.g. image, audio, video or zip-based spam. The anti-spam feature is also equipped with Virus Outbreak Detection. This protects the organization against any zero day attack. All of this means that viruses, worms, Trojans, key-loggers and spyware are now a thing of the past and business downtime is negligible.

Browsing Check Accomplished

Laced with IP Reputation Filters, Cyberoam's content agnostic and language independent technology blocked almost 99.9% of spam mails.

Prior to Cyberoam deployment, there was no control on sites visited by Solray's employees. However, all that changed with Cyberoam's Web filtering feature which ensures protection from inappropriate and insecure Web content, including phishing and other malware-loaded sites. Cyberoam's constantly updated database of millions of sites is divided into 82+ categories which include pornography, P2P, entertainment and job search. By customizing user identity-based policies, the administrator provides selective Internet access and surfing rights based on the user's working needs. "I can now prioritize the organization's bandwidth usage as per business requirements with more effective controls how much bandwidth any particular user can use during any time of the day", said. Mr. Turner.

To Wrap it Up

When discussing his Cyberoam experience, Mr. Turner commented, "We are more than happy with the service which has been provided. One of Cyberoam's most beneficial features is its on-appliance reporting feature that gave us constructive statistical results such as Internet usage patterns, the number of sites which were non-productive or unhealthy and knowing exactly what our users were doing in the network."

Toll Free Numbers
USA : +1-877-777-0368 | India : 1-800-301-00013
APAC/MEA : +1-877-777-0368 | Europe : +44-808-120-3958