

Cyberoam proves to be more effective for Yokogawa than top security vendors



Case Study



Organization

Yokogawa India Ltd.

Country

India, Asia

Industry/ Vertical

Electronics and Software



Corporate Profile

From being primarily a provider of Process Automation Systems and Products, Yokogawa India Limited (YIL) is today positioned as a Comprehensive Solutions Provider of Enterprise Technology Solutions (ETS). Established in 1987, YIL has created the state of art global engineering center and manufacturing center in Bangalore. They have a strong marketing and service network across India. They also have a breadth of competencies to meet the technological requirement of the Indian Process Industry. They excel in turnkey project execution in Process Automation and Enterprise Integration, with core competencies in Design and Engineering of Process Control Systems, Implementation of Extended Enterprise Applications and more.

The Yokogawa Challenge

Highlighting the need for replacing their existing CheckPoint solution, Mr. Manoj Kumar, the Deputy Manager - IT at Yokogawa said, "We need to provide Internet access to our users for business purposes and to ensure speed and security of content. The existing Checkpoint system was not effective at addressing our business challenges".

According to Mr. Kumar, the issues that they faced were:

Need for Web and Application Filtering

Mr. Kumar desired to ensure that the users at Yokogawa use the Internet for productive, work-related activities only. He wanted to prevent users from accessing unproductive, harmful and malware-laden websites which can expose the company's network to cyber threats. One of the most important vectors of worry was the productivity. The productivity might be affected while spending precious time in unproductive surfing and downloading. "Restricting uploading/downloading of streaming media, which occupied precious bandwidth, was our main concern", Mr. Kumar said.

User Accountability Issues

Mr. Kumar desired that each and every network activity of all the users should be properly accounted, irrespective of the way or the device they use to connect to the network. "The need for us was deployment of a proper user accountability solution which could log and monitor the entire browsing pattern of a user", said Mr. Kumar.

Virus and Malware Threat

Unrestricted and unmonitored surfing often provides an entrance for Malware to enter the network. These malicious objects like Trojans, Viruses, and Spyware etc. enters the network quietly and often takes a blended form, like infecting the network through email attachments. Often, these attacks have the potential to cost an organization a great deal of time, money and productivity of their employees.

The Cyberoam Solution

After having dissatisfactory experience with major security products including CheckPoint, FortiGate and SonicWALL, Yokogawa was looking for a product that could solve their business challenges more effectively. After a thorough evaluation, they were impressed with Cyberoam's award-winning Layer 8 technology. They purchased One (1) CR 2500iNG appliance and deployed it at their office in Bangalore, India in Gateway Mode.

After deploying Cyberoam in the network, the benefits that they notice are:



"Cyberoam has given us more value against money than the leading security vendors combined"

Mr. Manoj Kumar
Deputy Manager - IT
Yokogawa India Ltd.

Seamless AD Integration

Cyberoam's Active Directory integration feature allows the appliance to map users and groups from ADS with Cyberoam for the purpose of authentication. This enables the appliance to identify network users transparently. Cyberoam communicates with Windows Directory Services to authenticate users based on groups, domains and organizational units. Mr. Kumar uses Cyberoam's AD authentication along with Local authentication to provide Identity-based security for around 1,500 users.

Mr. Kumar said, "Thanks to Cyberoam's AD Integration feature, mapping users between our AD Server and the Cyberoam appliance is now a piece of cake. Unlike CheckPoint, Cyberoam's AD Integration feature just works".

Identity-based Authentication, Authorization, and Audit

Cyberoam's Layer 8 Technology allows Mr. Kumar to design identity-based policies, which extends throughout the network, irrespective of the device used by the employees to connect to the network. Cyberoam Security appliances offer identity-based AAA (Authentication, Authorization, and Audit) allowing control and visibility of who is connected to your network, using what device and what they are accessing.

Safe, Productive Surfing Unleashed

Cyberoam's Checkmark Certified Web and Application Filtering feature allows Mr. Kumar to instantly block undesirable web sites and application, and enforce acceptable usage policies on all employees. Cyberoam blocks all unauthorized uploads/downloads, P2P applications, pirated audio and video streaming using a Content Filtering database of more than 100 million websites, categorized into 89+ categories. Moreover, the feature is coupled with Bandwidth Management feature, which ensures bandwidth availability and data transfer

limit based on duration and schedule of access for specific web categories and applications.

Cyberoam delivers comprehensive control and visibility over more than 2,000 applications. Unlike age-old port-based classification mechanism, Cyberoam classifies applications based on their risk level, characteristics and technology, offering granular controls. This stops sophisticated application-layer threats right at the network perimeter, ensuring Application Security. Mr. Kumar said, "Not only Cyberoam helps us block unproductive/harmful content, it also provides us granular Bandwidth Management at individual Website and Application level".

Gateway Anti Virus

Cyberoam's Checkmark Certified Anti Virus and Anti Spyware prevent entry of Malware and Spyware at the entrance itself ensuring clean Mail (SMTP, IMAP and POP3) and Web (HTTP, HTTPS, FTP) traffic. They provide real-time protection against constantly emerging cyber threats resulting in maximum network uptime. It also blocks attachments for specified file types like executables, media files, password-protected files etc. before any Malware affects the network.

Superior Reporting

Cyberoam network security appliances deliver in-depth reporting over the appliance, eliminating the need for an independent reporting solution and minimizing the resultant security investment and operational expense. Over 1200 in-depth reports offer real-time visibility into user and network activities over dual dashboards – Security dashboard and Traffic dashboard. This in turn yields Yokogawa with high security, optimal network performance and helps them meet regulatory compliance requirements. "When it comes to On-appliance Reporting, no one comes close to what Cyberoam offers", Mr. Kumar said.

Thanks to Cyberoam's AD Integration feature, mapping users between our AD Server and the Cyberoam appliance is now a piece of cake. Unlike CheckPoint, Cyberoam's AD Integration feature just works.

To Conclude

Mr. Kumar said, "After introducing Cyberoam into our network, we have been able to save cost on bandwidth and increase Internet surfing speed and productivity. Cyberoam has given us more value against money than the leading security vendors combined".

Toll Free Numbers

USA : +1-800-686-2360 | India : 1-800-301-00013

APAC/MEA : +1-877-777-0368 | Europe : +44-808-120-3958

Copyright © 1999-2013 Cyberoam Technologies Pvt. Ltd. All Rights Reserved. Cyberoam and Cyberoam logo are registered trademark of Cyberoam Technologies Pvt. Ltd. Although Cyberoam has attempted to provide accurate information, Cyberoam assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Cyberoam has the right to change, modify, transfer or otherwise revise the publication without notice.

