

Organization

ITE Distribution

CountryDubai
UAE, Asia**Industry/ Vertical**

Information Technology



We are a company with a rapidly expanding footprint and multiple business centers, ITE Distribution's individually deployed security solutions like firewall and anti-virus were resulting in a steep increase in its Capital and Operational expenses.

-Mr. Manoj L Daswani
IT Manager
ITE Distribution.

<http://www.cyberoam.com>

Cyberoam Security fortifies ITE Distribution, Dubai Network**About ITE Distribution**

ITE Distribution is an 18-year-strong, IT distribution company headquartered in Dubai, UAE. With a product portfolio that includes Belkin, Iomega, Kingston, Labtec, Logitech, Palm, Peachtree, Symantec, Targus and Tucano, ITE has distinguished itself as THE RETAIL distributor across markets. Its longstanding association with vendors has led to product penetration and market share growth across the region. Its distribution territory includes the GCC, the broader Middle East region, the entire African continent as well as the CIS countries. In addition to the main office in Dubai, ITE maintains logistics centers in the Jebel Ali Free Zone and Johannesburg.

The organization was looking for a solution that could provide them with hassle-free Internet security, control over internal and external attacks and indiscriminate Internet surfing, and real-time, intelligent enterprise-wide reporting.

The ITE Distribution Challenge

A company with a rapidly expanding footprint and multiple business centers, ITE Distribution's individually deployed security solutions like firewall and anti-virus were resulting in a steep increase in its Capital and Operational expenses. Deploying and operating these diverse security solutions was a complex exercise requiring special expertise. In spite of the higher costs and expertise required to manage these solutions, they often fell short when required to co-ordinate and launch an effective counter-offensive against blended threats.

Firewall Limitations

ITE Distribution's infrastructure is built on a hub and spoke network between multiple branch offices and the head office, protected by a firewall. However, growing Internet traffic and lack of access control soon exposed the limitations of the access control mechanism. The company realized that blanket corporate access policies are restrictive, but relaxing these policies had left its network exposed to the risk of intrusion and hacking. In addition, absence of Internet usage accountability resulted in unrestricted Internet surfing, often to malicious sites that infected the system with spyware and adware.

High Connectivity Costs

The company had deployed site-to-site VPN connectivity using leased lines to link remote offices for information access. It didn't take the company very long to realize that leased lines are an expensive access option that was resulting in its operating expenses escalating out of control. The only way to rein in connectivity costs is by allowing staff to securely use public infrastructure to communicate data.

Unrestricted Surfing

IT Manager, Manoj L Daswani was perturbed by unprotected and unrestricted Internet surfing which was making the organization increasingly vulnerable to security threats. As he put it, "One of the biggest dangers we faced was from the entry of malware from unregulated surfing." Apart from the obvious risks that these malicious threats posed, unchecked surfing had a considerable impact on productivity and network performance. Downloading and transmitting of non-business related data was putting an enormous strain on infrastructure and lowering network availability and response times for legitimate activities.

Messaging Risks

Messaging systems are a critical component of any business, but as email usage increased, so did the risk of infections to the system. Spam entering the system was creating problems at multiple levels – they were clogging the mail server, eating into the storage space, and sapping bandwidth.

Spam entering the system was creating problems at multiple levels – they were clogging the mail server, eating into the storage space, and sapping bandwidth

The company also faced blended threats from emails embedded with links to malicious or compromised websites. These blended email threats have emerged as the most dangerous and adaptive form of malware attacks. Apart from the cost in terms of wastage of storage and bandwidth, the bigger hit was on productivity, as employees spent precious time weeding out unwanted mails.

Before zeroing in on Cyberoam, TPI had done a preliminary testing on two other solutions. The company uses a number of business applications that are hosted on the Internet and needed a comprehensive and unified security solution that could protect it from external and internal threats and provide seamless and secure connectivity between branch and corporate offices. As Mr. Daswani put it, “We needed a system that offered full business flexibility and guaranteed against performance loss when faced with multiple blended attacks.”

The Cyberoam Solution

After pilot and careful analysis of Unified Threat Management (UTM) technologies from various vendors, ITE Distribution decided to install Cyberoam’s ICSA and Checkmark certified, identity-based UTM firewall. ITE Distribution purchased three CR appliances: CR250i - Jebble Ali (Head Office), CR50i, and CR25i – Dubai (Branch offices, and deployed all three in gateway mode. They also used 10 VPN roaming users.

Integrated Security Delivered

The CR250i UTM firewall appliance is installed at the company’s head office in Dubai. Cyberoam’s Multiple Link Manager ensures uninterrupted and seamless connectivity to business applications by monitoring link availability of multiple WAN connections and transfers traffic from a failed to a working link. It provides a distinct cost advantage over solutions that use multiple appliances to manage traffic over multiple links. The CR50i and CR25i appliances are deployed at the company’s branch offices and provide affordable secure remote connectivity to corporate resources including Mails, Database, ERP, and CRM. The three appliances work in tandem to provide enterprise-wide security while ensuring continuous business continuity.

The Wall of Fire – Firewall

ICSA and Checkmark - dual certified Cyberoam’s stateful inspection firewall now cordons off the organization’s network and guards its resources against any unauthorized access. The firewall ensures that the entire gamut of applications and other servers deployed in the DMZ are not accessed by any unauthorized intruder. This ensures that all the business critical resources are well protected.

Intrusions Arrested

Today, ITE Distribution relies on Cyberoam’s sophisticated Intrusion Prevention System (IPS) to keep its network protected at all times. With over 3000 in-built signatures that are automatically updated to protect against the most current threats and the capacity to deploy custom IPS signatures, Daswani is confident that he has the solution which provides a strong defense against a range of network attacks. “Cyberoam’s uncompromising commitment to security and protection helped us improve network efficiency and performance”, he says with satisfaction.

Acting as an application firewall, the IPS controls all the applications that are used to access the Internet. Unauthorized Instant Messaging (IM) and Peer-to-Peer (P2P) applications are now well controlled and the risk of any information leaking out from them is curbed.

Spam Busted

Controlling spam is no longer a continuous battle for Mr. Daswani and his team, as Cyberoam’s anti-spam solution leverages language independent and content agnostic RPD technology to protect the customer’s network against virus and spam.

ITE Distribution needed a system that offered full business flexibility and guaranteed against performance loss when faced with multiple blended attacks.

The firewall ensures that the entire gamut of applications and other servers deployed in the DMZ are not accessed by any unauthorized intruder. This ensures that all the business critical resources are well protected.

Unauthorized Instant Messaging (IM) and Peer-to-Peer (P2P) applications are now well controlled and the risk of any information leaking out from them is curbed.

Controlled and productive surfing translates to improved productivity as time is now spent on business-related access and not wasted on meaningless and unproductive browsing.

More importantly, Cyberoam's gateway anti-spam and anti-virus solutions significantly improved system efficiency by reducing the number of messages that needed to be processed and stored. It reduced bandwidth consumption for non-business activities and boosted productivity as employees no longer spent hours cleaning their mail boxes of junk, spam, and phishing mails. IT is able to focus on core activities, as e-mail originated malware is eliminated from the system.

Browsing Controlled

With granular filtering of Websites across 82 categories, Cyberoam provides policy-based control on Internet surfing by employees. Controlled and productive surfing translates to improved productivity as time is now spent on business-related access and not wasted on meaningless and unproductive browsing. Curbing unauthorized downloads of IM, P2P, and other applications has reduced the chances of malware infecting the system and resulted in a drastic fall in calls to the IT helpdesk.

Reporting Streamlined

The IT team is able to better manage the security of the network through Cyberoam's comprehensive enterprise-wide reporting. They are able to easily and quickly identify threats and fine tune the system to respond to any suspicious activity, thereby improving network security and efficiency. ITE's top management is kept abreast of network usage and security information through a single customizable page on the dashboard, while HR is able to measure employee performance and behavior by analyzing their browsing patterns.

Customer Speak

ITE Distribution is happy that they chose Cyberoam as it has delivered a flexible, comprehensive, and customizable UTM solution that has efficiently addressed their security concerns and effectively reduced connectivity and operation costs.



USA - Sales Toll Free: +1- 866-663-2927 | Support Toll Free: +1-877-380-8531

India - Sales: +91-79-66065606 | Support Toll Free: 1-800-301-00013

EMEA/APAC - Sales: +91-79-66065787 | Support: +91-79-66065777

Copyright © 1999 - 2008 Elitecore Technologies Ltd. All rights reserved. Cyberoam and Cyberoam logo are registered trademark of Elitecore Technologies Ltd. Although Elitecore has attempted to provide accurate information, Elitecore assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Elitecore has the right to change, modify, transfer or otherwise revise the publication without notice.

