

Securing new frontiers

Cyberoam is a division of Elitecore Technologies and a leading provider of identity-based Unified Threat Management (UTM) solutions. RWME speaks with Harish Chib, VP New Business Development, Cyberoam



Harish Chib, VP New Business Development, Cyberoam

Perimetre security and endpoint security - are they equally important or is one more so and why?

Perimetre security can stop the attack at the earliest point of the network. It thus stops all attacks at the gateway itself rather than letting it go to the desktops on which end point securities are installed and left much to the whims of individual user. Unified Threat Management solutions prove to be one of the most unique gateway-level solutions, offering protections towards blended threats. Also, the big advantage of the perimetre solutions is that in terms of orders of magnitude they are more manageable, more scaleable, and more robust.

While Network should indefinitely be protected via perimetre security, there is also an increase in the endpoint security based essentially on compliance

with organisational security norms. If a device hasn't proven its compliance to the company's security policies, none of these devices should be able to connect to the company's network. On the basis of the above needs, security vendors are trying to come up with solutions where security compliance is a primary step. Originally a niche market, endpoint security has become a top priority for vendors today.

What solutions are on offer from Cyberoam that takes care of both aspects?

Cyberoam is a leading innovator of identity-based Unified Threat Management appliances and offers a symbiosis of security features including perimetre security through its firewall as well as endpoint level security through its identity-based nature (identifying users in a network) & Custom based signatures to block applications through IDP (Intrusion Detection & Prevention). It also supports multiple security features like identity-based firewall, VPN, gateway antivirus, gateway anti-spam, intrusion detection and prevention and content filtering, as well as bandwidth management and multiple link management – all over a single platform. It thus offers complete Internet security by integrating multiple security technologies against blended and multiple threats, increasing organisational productivity.

What are the major contributors to the endpoint vulnerabilities? How can these be tackled?

The need for compliance to organisational security policies, have given rise to endpoint security technologies. However, there are a number of endpoint vulnerabilities which malicious attackers can utilize and traumatize a network. To list down a few along with their solutions:

■ **O/S vulnerabilities:** Lack of updates in operating systems can sometimes contribute to a major endpoint threat. These cannot be guarded/tracked down at the

perimetre level. Versions Releases of O/Ss have to be installed on a regular basis.

■ **Audit Trails:** Absence of security logs can lead to major vulnerabilities, as it would be impossible to track down activities in a network. Audit logs have to be monitored from time to time to track possible malicious patterns.

■ Restricted Access of Unauthorised peripherals:

The most critical is the exclusion of unauthorised peripherals from the list of vulnerabilities. For eg: USB-based Mass storage devices. Anyone can hook up their USBs and run malicious programs, as most of the computers have unrestricted access in a network. The task of security vendors is thus to guarantee protection against unrestricted peripherals. These should be monitored, reported or blocked.

■ **Missing Security Patches:** Missing updates/patches is a recurrent problem faced at the desktop-level. As and when new patches by vendors are released, they should be taken at a priority, and updated.

■ **Lack of Identification of users that break rules or are noncompliant with policy:** In a large network, lack of identification of the above can lead to serious issues or holes in the security. Users should be identified as and when they create threats in an organisation.

With an increased slant towards endpoint security from many companies, where does perimetre security go from here? Is it true that perimetre security would always lack the depth to tackle many of the new threats?

Endpoint Security can never replace front-line defense of Perimetre security. Endpoint security can only block the threat from entering the desktop machine, and cannot stop the threat from entering the network which is a huge drawback. Endpoint Security, literally means "end-point" which means, it is the last or the contingent defense strategy in a network. Perimetre Security provides extreme protection at the perimetre/gateway level, much before data reaches desktop-level or the last hurdle. There are many products in the Market which attempt to bridge a gap between the perimetre security & the endpoint security.

The future may see solutions that both serve at the perimetre level & the endpoint level. However, perimetre security can never be replicable.