

Technology Inside

ConSentry adds network audit and control software

Written on Monday, February 16, 2009 by HeartDisk

Network access control specialist ConSentry is moving away from pure NAC, and towards providing wider visibility and control over the network. It has developed software that uses the deep packet inspection chips built into its switches and controllers to track and audit all sorts of network activity.

The company has added real-time alerting and correlation capabilities to its InSight Command Centre software, with the aim of identifying questionable applications, devices and network traffic, said CTO Jeff Prince.

A new network monitoring and control dashboard gives the IT manager an overview of the data gathered, plus the ability to drill down to user, application or device level, he added.

"We use the corporate directory for role derivation, and have visibility into the LAN at layer 7 and above," he said. "That includes what files you touch and the messages you send over the network. It is stateful and it tracks flows, so it is also useful for compliance."

Speaking at the NetEvents industry forum in Barcelona, Prince said that potential applications for the new software include regulatory compliance, network management, feeding questionable traffic to an IPS for checking, controlling which applications and servers a user can access according to their role, their location, the time of day, and enforcing security policies on email and IM.

The new software would also have been able to detect traffic generated by the Conficker/Downadup worm, he claimed, although he stressed that it is not designed or intended to be an IDS/IPS.

"The system can also run in monitor mode as well, to test your security policies," he said. "It relies on our high-performance silicon to get deep packet inspection at a low price. That chip means our switch is competitive with HP, Foundry and Cisco, say, but also does deep packet inspection."

ConSentry increasingly finds itself at the point where network management, security management and application management are converging, according to Prince.

He added that network control is far broader now than just PCs - there's increasing numbers of other devices, and compliance is adding the need to trace activity back to users as well.

"We're now focused on providing visibility into the network," he said. "It's not uncommon for a company with 2000 employees to have 5000 or 6000 devices on the network."