

# ConSentry Bolsters Security at Network's Edge

May 9 2007

---

The startup's new line of Ethernet switches are designed to control user access and secure every port on the network for enterprise branch offices.

Many networking vendors are pushing the idea of moving more intelligence to the edge of the network. But ConSentry Networks is taking that idea to a greater extreme when it comes to securing access at the network's edge.

The startup on May 7 introduced a new line of Ethernet switches built to control user access and secure every port on the network in an economical way for enterprise branch offices.

Declaring death to the wiring closet as it is known today, ConSentry also announced a new universal endpoint interoperability initiative to work with different endpoint vendors to ensure that a user coming into the network is identified and that the appropriate policies are applied to that user.

"How [wiring closets] have been built is now under siege. They have open access on all ports, there's no automated way to separate guests and contractors from employees, there's no control over how and what users are accessing, there's no knowledge of the endpoint - whether it's managed or unmanaged, safe or healthy - and there is no ability to contain the threat of malware," said Dan Leary, vice president of marketing for ConSentry, in Milpitas, Calif.

ConSentry's universal endpoint interoperability initiative is intended to cover all types of endpoint, managed or unmanaged, without the requirement to add more agents. It allows customers to leverage their existing investments in endpoint security but centralize control over access.

For managed endpoints, ConSentry's secure switching architecture works with security and access frameworks such as Microsoft's Network Access Protection and the Trusted Computing Group's Trusted Network Connect; anti-virus offerings from Symantec/Sygate, McAfee and Trend Micro; and client endpoints from regional providers such as Criston in France and NTT Data Intellilink. In addition, the ConSentry third-generation security and control software provides enforcement for those vendors' products.

ConSentry also extended its architecture to embrace unmanaged desktops, including Linux and Mac client operating systems as well as Windows, through a dissolvable agent.

ConSentry's security software, embedded in its LANShield switches and in its centralized InSight Command Center console, "starts with knowing who the user is and making sure their PC posture is good," Leary said.

Then application fluency adds the ability to perform user and behavior analysis. It works by going back to the identity store and learns as the user enters the network "their role in the organization, and [ it can ] understand the applications that are running. The intersection of that data builds a picture of what's happening on the network," Leary said.

Such understanding, which can be used as a foundation for creating access policies, is "a missing piece from others that just look at IP addresses or ports. This allows that policy decision to be made," he said.

The new LANShield CS-4024 24-port switch for branch offices provides Gigabit Ethernet connectivity and POE (power over Ethernet). It is due in the third quarter and starts at \$5,995.

*Copyright 2007 by Ziff Davis Media, Distributed by United Press International*

Citation: ConSentry Bolsters Security at Network's Edge (2007, May 9) retrieved 5 May 2024 from <https://phys.org/news/2007-05-consentry-bolsters-network-edge.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.