



Keeping The Outside - Outside

Dennis Peasley, Chief Information Security Officer
Herman Miller Inc, Zeeland, Michigan, USA

Challenge

Herman Miller Inc. required centrally enforced security policies for a network spread over more than forty locations worldwide — a system supporting frequent remote connections.

Solution

In 2002, the firm deployed Zone Labs Integrity, working in conjunction with the Cisco 3000 VPN system..

Benefits

Security policies are enforced on a centralized basis, and unauthorized activity is intercepted immediately — from wherever in the world it originates.

Operating System

Windows 2000
Windows XP

Network

Cisco 3000 VPN

Hardware

Dell Servers

Software

Zone Labs Integrity

In a worldwide organization, every employee — wherever they may be — is as close to the home office as a keyboard. Those outside the organization must be kept out — away from valuable information, and prevented from intentionally harming corporate operations. For Herman Miller, Inc., those boundaries are strictly enforced by a network security system anchored by Zone Labs Integrity®.

Herman Miller Inc. is a world leader in office and industrial furnishings — from ergonomic chairs to sturdy desks to the familiar "office cube," an invention the firm pioneered back in the 1960s. Based in Zeeland, Michigan, Herman Miller Inc. serves large-scale clients in both the public and private sector, from more than forty offices around the world.

At the center of the information hub connecting these internationally wide-ranging functions of sales and service, is Dennis Peasley. He's Herman Miller Inc.'s Chief Information Security Officer, and he's focused on ensuring that the company's network remains secure. "We're concerned about outsiders getting into our system to do mischief or maliciously disrupt operations," Peasley explains. "And, we're concerned about viruses getting into our system through unauthorized connections from the inside. We have a lot of people working from home or on the road — we call them 'day extenders'— and they log into the network from remote locations. It's essential that only authorized personnel get access, and that these remote connections are operated under the same tight security precautions as connections from within our office sites."

Last year, Herman Miller Inc. deployed Zone Labs Integrity, working in connection with a Cisco 3000 VPN system. "Zone Labs Integrity gives us the ability to centrally enforce security policies network-wide," says Peasley. "Every computer connected to our system can be scrutinized for malicious or unauthorized activity — we know at all times who's on line, where they're connected from, and what applications they're running while connected. If we find an employee using an unauthorized application — say a peer-to-peer file-sharing program — Zone Labs Integrity makes it easy for us to intercept and

terminate this activity before our data can be contaminated. Running in conjunction with our Cisco VPN, Zone Labs' Cooperative Enforcement technology, included with Integrity, also allows us to ensure that any computer connecting to our network is running the required anti-virus software and is maintaining the required personal firewall protection. If not, that computer is blocked from accessing the corporate network and the user is given instructions on how to come back into compliance with our policies. The system also allows protection of encrypted data being transmitted over the VPN — if you visualize the VPN as the tunnel through the firewall, allowing data to be transmitted and received, Zone Labs Integrity allows us to actually firewall the tunnel itself."

Peasley evaluated several security products and found that Zone Labs Integrity offered far more in the way of centralized protection. "With Zone Labs Integrity," Peasley concludes, "security policies may be enforced on a centralized basis, ensuring both the integrity of our network — and the safety of our data."