sageza

Instant Insight
October 26, 2004

Cisco Drives Secure Network through Integration with Partners

By Joyce Tompsett Becknell

Cisco has recently made announcements about joint security development with Computer Associates, Microsoft, and IBM. The announcements involve integration of vendor security offerings with Cisco's Network Admission Control (NAC), a Cisco-sponsored initiative that uses network infrastructure to enforce security policy compliance on networked resources. NAC is part of Cisco's Self-Defending Network strategy to increase network intelligence for automated recognition and response to security threats. The announcements include:

- Computer Associates has just joined the NAC program, and will integrate Cisco's Trust Agent with its eTrust PestPatrol Anti-Spyware and eTrust Antivirus solutions. These products will provide the first NAC-compliant virus and spyware protection. CA intends to continue using the NAC framework and related technologies by integrating other eTrust threat management solutions.
- IBM and Cisco are extending their global security alliance by integrating IBM's Tivoli security policy compliance software with NAC technologies to automatically comply, quarantine, and remediate at-risk devices, including portable and desktop clients and wireless devices.
- Microsoft and Cisco agreed to share and integrate the Microsoft Network Access Protection (NAP) program with Cisco's NAC. They are working on interoperability between NAP and NAC architectures, and integration of embedded security capabilities from Cisco with those from Microsoft's Windows. The companies have also both committed to driving industry standards in network admissions and access control to help drive broad market adoption.

Net/Net

Security has been and continues to be an important area of computing for many companies today. Survey after survey ranks it high and indicates that companies are willing to dedicate the money and resources needed to increase it. The universal thorn in the side of enterprises and security vendors alike is that meaningful security is as much about policies and practices as it is about products. A secure product functioning in an insecure environment is no better than an insecure product that can render the most secure environment vulnerable. Until now, security products have mostly focused on detection and alerts rather than on responding to actual problems. The best they could offer was to block access or quarantine devices. IT managers could receive hundreds of pages of alerts and notices, but the burden of responding and understanding the impact on the business were left to the humans running the system. Additionally, most vendors thought in terms of their own architectures and product capabilities, while IT managers had to think in terms of global heterogeneous networks. The introduction of demand-driven computing architectures and methodologies, where more and more devices can interact and affect each other's behavior, has exacerbated security concerns. In the world of the mainframe-led data center, where one system's operating system and firmware were able to control virtually all resources, security was more manageable. In an open systems world with distributed intelligence and limited cognizance between technologies, no one vendor has been able to dictate standards, and customers have relied on patchworks of products and capabilities to achieve advanced levels of security within their IT infrastructure.

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Milan +39 02·9544·1646

Cisco first articulated its vision of the future network with its Architecture for Voice, Video, and Integrated Data (AVVID), which was a standards-based integrated vision for the network that offered the ability to create network services combining different data types. In essence, this was about integrating the transport layer. This vision has evolved to the Intelligent Information Network, which argues that the various pieces of intelligence embedded throughout the network should be managed and coordinated to provide a holistic view of the network, leading to the network virtual organization (NVO), an organization that responds on demand to changing business needs and can collaborate with other NVOs. Cisco believes companies are currently integrating network services and will eventually move to application-oriented networks and services. The security arm of this is the Self-Defending Network Strategy, which provides for secure infrastructure, advanced security technologies, and system level solutions.

Sageza believes this approach to addressing network security has significant merit. Networks are the technology all enterprises share in common and are the interface point between whatever other technologies are deployed. In addition, without an integrated network that functions as a continuum of services, it is difficult to achieve the vision of demand-driven computing that companies like IBM and Microsoft have articulated. The collaboration between these vendors is crucial to their success. Users do not need to spend more time shuffling between competing sets of standards, trying to work out which will solve their problems more efficiently. The time has passed when a single vendor can leverage its market weight to drive standards. The increasing interoperability and integration of technologies demands that standards have to be established and developed in collaboration. Without that common framework, standards are denigrated to brochureware or exist only in a single vendor's microcosm. Security in particular requires devices and systems to have common methods of sharing information, responses to threats, and ways to recognize each other in multiple contexts.

These announcements, however, are only a beginning. Many more vendors, most of them smaller and specialized, will have to become involved in the process, and users will have to work with vendors to develop best practices that combine secure policy and procedures with secure integrated products. Since different groups of employees use the network differently depending on industry and company size, companies will need flexibility in determining the levels of security they need and appropriate responses to perceived threats. Flexibility is one of the most difficult things to achieve from a security vantage; it requires a combination of physical integration, complete knowledge of business risks, and integrated intelligence that can be trained to respond reliably and predictably. Cisco's commitment to driving security through partnerships and common standards is a sign that they understand the implications of their vision and that they will not likely be successful creating an architecture for a secure network using only their own inventions.

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 96587
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Milan +39 02·9544·1646