Reconnex Announces iGuard Is On GSA Schedule; Appliance Fills White House Data Security Mandate

Reconnex Partners with Summit Government Group for Government Sales; Federal Agencies Can Use iGuard to Comply with White House Directive to Protect PII

MOUNTAIN VIEW, Calif., September 27, 2006 - Reconnex, the expert in information protection, today announced that its iGuard content-monitoring appliance is now on the General Services Administration (GSA) schedule via its strategic partnership with Summit Government Group, which enables government agencies and departments to purchase Reconnex products. The company also announced that government departments and agencies can use the iGuard to comply with the recent directive from the White House Office of Management and Budget (OMB) to protect Personally Identifiable Information (PII) in motion and at rest. The Reconnex appliance provides 100 percent visibility to monitor traffic leaving and entering the network and discover electronic threats, both unknown and known.

"We're committed to helping government agencies find and remediate risks to their networks. While the White House OMB directive emphasizes PII, agencies also need to protect against leakage of other highly sensitive information such as intelligence and even images and photos," said Faizel Lakhani, vice president of marketing at Reconnex. "The Reconnex iGuard is uniquely qualified to deal with such a broad range of information because it can monitor every application and every protocol across every port. Reconnex already has several government customers, but being on the GSA schedule via our partnership with Summit makes it much easier for us to reach new customers, and Summit is recognized for its superior sales and marketing expertise."

Reconnex is part of Summit's ChannelSelect program, which offers clients both GSA Schedule Agent and Teaming level participation, enabling Reconnex to properly position its products, increase its visibility in the government marketplace, and improve its overall effectiveness in selling throughout the complex public sector. The program optimizes the government sales schedule, minimizes channel conflict, leverages government procurement contracts while maximizing margin potential, and decreases manufacturer administrative overhead.

Reconnex Solution Enables NIST Compliance

The White House OMB security directive to protect PII is based on risk assessment guidelines published by the National Institute of Standards and Technology (NIST) in Special Publication 800-53, which includes a checklist of four steps required to safeguard PII. By using the Reconnex solution at every step, government agencies can discover, capture, identify, and remediate security problems.

Step 1: Confirm identification of PII protection needs. Reconnex's free 48-Hour e-Risk Rapid Assessment™ checklist helps government agencies find out if the security of their PII is at risk.

Step 2: Verify adequacy of organizational policy. Reconnex's e-Risk assessment examines all traffic leaving and entering a network over the course of two days, enabling government agencies to discover if sensitive information is at risk and if employees are using the network inappropriately.
Step 3: Implement protection for PII being transported and/or stored off site. The Reconnex platform provides real-time, comprehensive visibility into information crossing the network. If a PII leak is discovered, agencies can quickly find out what happened and remediate the problem. Plus, security personnel can analyze stored information about all data flowing over the network to discover previously unknown risks.
Step 4: Implement protections for remote access to PII. Reconnex uses Samba server monitoring and protocols such as FTP to ensure that PII is not put at risk.
About the Reconnex iGuard

A sophisticated, accurate solution for ensuring that sensitive data does not leave government agencies via their networks, the Reconnex iGuard also enables agencies to look back to find out if sensitive data has already left the network and determine how it left, so they can fix the problem. The Reconnex iGuard is the only content-monitoring appliance with electronic risk protection capabilities that allow agencies to capture, classify, analyze, and temporarily store all network content; perform historical analysis on the captured content to detect unknown threats; and correlate with known threats. Only the iGuard provides 100 percent visibility into network use because it monitors all information entering and leaving the corporate network.

About Reconnex

Reconnex is the leader in information monitoring and protection appliances designed for any organization – including enterprises, government agencies or educational institutions – that wants to protect its brand, maintain compliance, or secure sensitive information. Reconnex's simple-to-deploy appliance delivers accurate detection while protecting an enterprise before, during, and after any threat to corporate privacy or intellectual property. A privately held company based in Silicon Valley, Calif., Reconnex protects information for over one million users today.

For more information about Reconnex, please visit www.reconnex.net