



## SECURITY EXPERT DANIEL GEER AND VERDASYS ADVISE SECURING ENTERPRISE DATA, NOT NETWORKS

**WALTHAM, Mass.—March 1, 2010** -- How does a large enterprise maximize the benefit of the latest communications and data-sharing technology, while minimizing the risk of a security breach? A new [report](#) on Enterprise Information Protection (EIP) from Verdasys and an [article](#) in *SC Magazine* by security industry expert Dr. Daniel Geer conclude that, until enterprises learn to connect security directly to data, rather than networks or infrastructure, they will be unable to mitigate the types of breaches recently perpetrated against Google and other companies under Advanced Persistent Threat (APT).

Titled, “***The Enterprise Information Protection Paradigm***,” Geer’s article says a risk-based and data centric approach to security is a paradigm shift away from traditional or infrastructure-centric security because it drives unification of people, process and technology. This unification provides the greatest visibility to data risk, as well as the ability to implement proactive and automated controls to mitigate that risk.

“Data is where the value is; network security has no answer to end-point compromise,” says Geer, who serves as Chief Scientist Emeritus at Verdasys and is the Chief Information Security Officer at In-Q-Tel, the independent strategic investment firm that identifies innovative technology solutions to support the missions of the U.S. Intelligence Community.

Available at [www.verdasys.com/eip](http://www.verdasys.com/eip), the Verdasys EIP White Paper outlines how companies can utilize the EIP methodology to build a strategic data protection program that enables organizations to understand: what sensitive data exists and where; what user is taking what actions with sensitive data; and how to implement real-time automated risk appropriate controls based on the users actions.

Verdasys is using the EIP methodology to help hundreds of Global 2000 organizations protect their sensitive enterprise information. As the foundation of an EIP methodology, the [Digital Guardian](#) integrated platform offers a comprehensive, enterprise-wide security solution that enables greater visibility to data risk, actionable classification of sensitive data, a single policy engine that drives real-time controls including file, remote media and email encryption and eDiscovery and Forensic management.

Digital Guardian has been proven in over 100 production deployments and is the only information protection solution that has been successfully deployed across more than 50,000 machines in a single distributed enterprise environment. Verdasys’ enterprise-wide visibility into data movement and employee activities has led to the interdiction of more than \$700 million in publically disclosed data loss incidents, and is currently safeguarding billions of dollars of corporate and government intellectual property.

### **About Verdasys**

Verdasys, [www.verdasys.com](http://www.verdasys.com), provides Enterprise Information Protections (EIP) solutions that secure proprietary and sensitive data and the integrity of business processes essential for Global 2000 companies to successfully compete in today’s highly collaborative and mobile environments. Digital Guardian, the leading EIP market solution, is a centrally managed data security platform that discovers, classifies, monitors, controls and encrypts sensitive information at rest, in use and in motion across desktops, laptops, mobile devices, email, Web transactions,

terminal servers and enterprise applications. Verdasys customers are the global leaders in financial services, insurance, technology, manufacturing, and healthcare industries around the world. Companies serious about information protection choose Verdasys.

Verdasys is headquartered in Waltham, Mass.

For more information, go to [www.Verdasys.com](http://www.Verdasys.com)