



SBIR Commercialization Assistance Program

Policy-based Recovery on Virtualized Enterprise Networks (PROVEN)

Business Opportunity:

Increasing threats of cyber warfare, terrorism, natural disasters, and other forms of disruption, have resulted in comprehensive Continuity of Operations (COOP) strategies taking on increased emphasis. As Department of Defense (DoD) architectures become more net-centric and globally distributed, our dependence upon continuously available distributed services continues to grow, emphasizing the need for robust COOP and cyber defense solutions.

Unfortunately, existing COOP solutions are typically complex, inflexible, costly, and lacking in capability, as demonstrated by long delays, ranging from hours to days, between failure and full restoration of critical operations. PROVEN provides the technology to solve those problems and provide cyber defense and COOP within the SOA paradigm and net centric environments. The PROVEN solution is based upon enforcement of semantic policy, which defines continuity requirements in terms of the meaning of integrated data, the operational processes that depend on the data, and the underlying services used to execute those processes.

The commercial market size is estimated to be greater than \$15 billion. As of 2004, IDC forecasted the security and business continuity market is to exceed \$16 billion by 2008. In 2006 over \$200 billion dollars was spent by U.S. businesses on physical and logical security products and services (Security Magazine). The Yankee Group projects SOA-related spending to hit \$11 billion by 2010, including infrastructure, applications, and security.

PROVEN is in the early stages of Phase II development and Securboration is looking for strategic partners to leverage the SBIR Phase II Enhancement program for full-scale development, and deployment to provide value added to our partner's programs.

Company Background:

Securboration was founded in 2001 to address collaboration needs of the DoD. Securboration has worked since that time to pioneer techniques to transform data into knowledge and enable exchange of that knowledge within collaboration processes in large-scale customer environments. Securboration currently has 24 employees, who are based in Florida, Georgia, North Carolina, Texas, and Virginia. Company revenue from research contracts for 2008 was approximately \$2.8 million, and 2009 revenue is estimated at \$4 million. Securboration currently has approximately 18 open contracts, mostly Small Business Innovative Research (SBIR) contracts that are either in Phase I or Phase II. Two Phase III contracts are pending; these will provide commercialization opportunities for technology developed on several of those ongoing efforts.

Industry Problem:

DoD Directive 3020.26 requires all DoD Components to have a comprehensive and effective continuity program that ensures DoD Component mission essential functions continue under all circumstances. While not bound by the DoD Directive, private industry shares the same

rationale for ensuring continuity of operations. Much of the impetus for COOP planning focuses on responding to potential attack, particularly terrorist and cyber attacks. However, once solutions are put in place to address those threats, those same solutions will also help with more benign impacts to continuous operation, such as routine building renovation or maintenance, mechanical failure of building systems, failure of Information Technology (IT) and/or telecommunications installations, fire, and inclement weather or other acts of nature (e.g., Hurricane Katrina).

Few threats pose the significant danger that cyber warfare creates to critical infrastructure. One element that underlies the danger of cyber attack is the relatively limited investment required to engage in such attacks. Cyber warfare can be conducted from almost anywhere, with a very limited investment in simple and readily available computing equipment. The very enticement to system deployment over the internet – widespread availability and access – has also created its greatest vulnerability. McAfee cited in its 2007 annual report that “approximately 120 countries have been developing ways to use the Internet as a weapon and the targets are financial markets, government computer systems and utilities.” PROVEN is focused on cyber defense, which involves actions taken to monitor and protect information systems and computer networks and detect, analyze, and respond to unauthorized activity within them. Cyber defense must not only protect systems from external adversaries but also from exploitation from within, and is now a necessary function in all operations.

Technology:

For maximum effectiveness, semantic technologies can be used to infer recovery policy dynamically and procedures based on the semantic meaning of that enterprise data. Policy-based service management across a virtualized network promises to lead to increased automation, improved network performance, and reduced labor needed to establish, maintain, and reestablish a network.

PROVEN is a software application that works seamlessly in a service-oriented architecture to essentially monitor the current operational and computational situations and compare them to requirements that it maintains within its internal policy model. In this manner, as the operational environment changes, from major events such as cyber attack or natural disaster to more mundane situations such as staffing shortage or needed system maintenance, PROVEN can dynamically relocate services to maintain COOP and/or adjust priorities and permissions based upon defined policies. For example, following a natural disaster, non-essential services may be reduced in priority, and essential services elevated in priority. PROVEN monitors the operational environment, and uses its policy model to determine how to control the deployment and execution of services over the grid.

Advantages and Differentiating Features:

PROVEN presents several advantages over existing techniques. First, its policy model uses advanced computational reasoning techniques to align operational needs with computational resources. In traditional COOP, this reasoning is substituted with manual actions and/or a priori definitions, which inhibit responsiveness to change and result in inconsistencies that develop from a lack of situational awareness.

PROVEN’s key innovation is its flexible approach to continuity of operations that leverages a semantically consistent model of the operational environment to proactively define and execute policies, including during times of conflict and/or crisis, to maintain mission essential services at all times. This semantic model defines and enforces policies across the entire SOA, and all

services are automatically managed and executed in accordance with the defined policies. The use of semantic technologies to infer recovery procedures and policy dynamically are based on the semantic meaning of enterprise data. This approach overcomes the limitations of current data-centric approaches, which rely on known static structures and procedures and a greater degree of human intervention to support recovery.

Stage of Development:

To date, a needs assessment, proof of concept, feasibility, and initial prototyping of the system have been completed. The first generation prototype is being expanded under the ongoing SBIR Phase II effort. Securboration is currently working with a commercial grid computing software provider, Data Synapse, to provide the underlying grid infrastructure.

Competing Technologies:

Current approaches to maintaining COOP commonly rely on large caches of redundant hardware and operational capability. Often scaled down or redundant complements of hardware are utilized to re-establish operational capabilities at fixed alternate sites. Competing technologies (at least those known to exist in the unclassified realm) tend to be reactive to threats, which in many cases, means the system or capability is lost for a time and recent transactions are often compromised.

Applications:

- DoD systems are required to maintain operational capability but are under constant threat of cyber attack, and in the private sector, systems must maintain data integrity and are under constant threat of malicious intent (e.g., hackers, identity theft, etc.).
- Maintaining systems and capability in the face of natural disasters or other catastrophic events, ensuring mission critical data is available to groups that depend on that data.
- Reallocation of critical services and capabilities during times of peak demand or emergency.

Benefits:

- The ability to respond proactively to existing and emerging cyber threats while maintaining the capability of critical systems within the DoD net-centric enterprise.
- Provide the level of proactive response necessary to maintain continuity of business operations in critical corporate information technology environments.

Intellectual Property:

The IP associated with the semantic processor capability is currently protected as trade secrets. The company continues to evaluate its IP position to determine if filing patents to provide additional enforced protection is appropriate.