



CounterStorm: Federal Executive Summary

Company Overview

CounterStorm is a leading provider of modular threat detection and mitigation software development kits (SDKs) to security and infrastructure companies, as well as sophisticated government and commercial end users. Headquartered in New York City, the company was formed in August 2001 to commercialize patent-pending technologies developed at Columbia University under grants from the Defense Advanced Research Projects Agency (DARPA). CounterStorm is venture funded, with Novak Biddle Venture Partners, JK&B Capital, and Paladin Capital Group as lead investors. The company has also been awarded Small Business Innovative Research (SBIR) grants by the Homeland Security Advanced Research Projects Agency (HSARPA) of the Department of Homeland Security's Science and Technology Directorate.

Management Team

Steve Gant, CEO, is a veteran technology executive with extensive experience in corporate development, product strategy and market execution at companies such as Trusted Network Technologies, Internet Security Systems, and General Instrument. Bryan Bain, VP of Marketing & Strategy, leverages strong security industry experience at Array Networks, Netilla and Cyberguard to lead marketing and product management. Matt Miller, VP of Engineering, has been with CounterStorm since its inception in 2001, leading the company's product design and development, and quality assurance efforts. Dr. Greg Shannon, General Manager for CounterStorm Government, is the Company's principle investigator for the DHS awards. He joined CounterStorm in 2003 after leading R&D teams at Lucent, Indiana University and other startups.

Market Need

In today's cyber-security landscape, an organization's mission is most vulnerable to previously unreported attacks. Until recently, the only defenses available have relied on

signatures, policies, and rules derived from previously reported attacks. This has left critical enterprise networks vulnerable to zero-day and targeted attacks, especially if the attack is stealthy or slow. Gartner has identified targeted attacks as the top security threat facing businesses in the coming two years. As part of its 2006 Cyberthreats Hype Cycle, the research firm predicts that "by 2008 nearly 40% of organizations will be targeted by financially motivated cybercrime" and urges businesses to invest more in preventative measures. Although no research has been published citing worldwide damage figures, the US Treasury Department has reported that cyber crime has surpassed illegal drug sales in annual proceeds, netting in excess of \$100 billion per year. CIO Insight's 2006 Security Survey data supports this estimate. The survey cites 51% of companies over \$1 billion reporting security breaches in the past 12 months. 45% of companies over \$1 billion report they have been targeted by organized criminals.

To meet the cyber-security challenges of their customers, system integrators must expand their offerings with flexible, modular threat detection and mitigation technologies that can be readily integrated to enhance existing systems or create new offerings. Such modular security components enable integrators to meet their customers' needs and remain competitive in spite of fast-emerging new threats.

CounterStorm's Technologies

CounterStorm has developed a suite of security technologies that are available as a fully-integrated internal network security appliance or as modular components for integration in 3rd party systems. Core intellectual property consists of Active Recognition Technology (ART) a distributed, modular and signatureless threat detection architecture, an integrated correlation engine, and an extensible software platform on which all of these capabilities are delivered. Together, these technologies yield the most accurate signatureless solution in the market today, with field-measured alarm-accuracy levels of 90-99% .

- **CounterStorm-1 Network Security Appliance for non-intrusive protection of internal networks**

- Provides the most accurate detection and containment of new or evolving threats.
- Graphically displays enterprise-wide current threat point and malicious propagation information.
- Automatically quarantines a device or segment when traffic characteristics do not match an approved baseline.
- Robust reporting functionality provides the data to respond to auditor requests and ensure compliance.

- **Statistical Payload Analysis Engine – The Industry’s 1st for Layer-7 Statistical Anomaly Detection**

- Operates at a per-packet level
- Learns the normal content profile of any application on the network
- Doesn’t rely on prior application knowledge, like protocol anomaly detection
- Detects non-scanning and hit-list based attacks

- **Behavioral Attack Recognition Engine**

- Uses behavioral patterns, but no signatures or protocol rules
- Successfully detects zero-day and targeted worms and bots
- Accurately identifies slow/stealthy surveillance activity

- **Distributed Real-Time Correlation across detection engines, sensor appliances, and enterprises**

- This engine correlates data from each of CounterStorm’s detection engines in order to process evidence into actionable alarms in real-time. Sophisticated and proprietary correlation logic synthesizes alert information into highly accurate alarms – dramatically reducing overall false positives.

- **Anomaly Detection Framework**

- Pluggable engine for anomaly detection over packet, session, or flow data
- Independently measures how much individual features deviate from normal
- Trains on dirty data – unsupervised learning
- Used to create multiple detectors for botnet behavior

Competitive Differentiation

CounterStorm is uniquely qualified to provide information security technology to mitigate the risk associated with previously unreported threats. The company’s intellectual property is not theoretical or unproven, but the product of 5 years of industry leading domain expertise in environments with national security implications.

- ART threat detection engines are signatureless. ART employs behavior- and anomaly-based technologies. The real-time monitoring/profiling of enterprise traffic complexity/uniqueness is used to identify statistical or behavioral anomalies.
- ART is self-learning and adaptive, requiring no tuning, minimizing operational overhead.
- ART correlates cross-sensor and cross-site anomalies to detect distributed and coordinated attacks.
- A sophisticated incident correlation engine synthesizes data from each threat analysis engine into highly accurate alarms.
- ART was specifically developed to detect sophisticated, slow and stealthy attacks.

Customer Traction

CounterStorm has received two U.S. Department of Homeland Security (DHS) SBIR Awards totaling \$1.5 million to develop several new innovations and improvements, including the statistical analysis of network traffic and bi-directional application flows. Multiple components of the Company’s Intellectual property have been licensed to BAE Systems (AIT) for use in government projects. Enterprise customer wins include: The Brookings Institution, Warner Music Group and New York Presbyterian Hospital.

Competition

The competitive setting for CounterStorm is complex and crowded. Many technologies are marketed as possessing best-of-breed capabilities for detecting zero-day and targeted attacks but do not match CounterStorm’s level of accuracy and speed of protection:

- Signature, policy, and rules-based technologies such as firewall, anti-virus, and patch management protect the enterprise from all known threats. Relying solely on these technologies will leave the enterprise susceptible to new or unknown exploits or exposed to external threat

during the window between a patch's release and its application.

- Protocol anomaly detection technologies inspect traffic for compliance to RFC specifications. While still a valuable tool to mitigate application-specific buffer overflows, hackers are now engineering attacks that do not violate RFC specifications.
- IPS/IDS vendors market their signature-based products as necessary to attain defense-in-depth, promoting instantaneous in-line blocking of exploits to protect against the sophisticated attacks of today's cyber-criminals. These devices require extensive tuning to minimize false positive alarms. Application-level exploits slip, undetected, past IPS/IDS defenses because they lack signatures.
- NBA(D) systems use both deterministic (signature) but primarily nondeterministic (anomaly) mechanisms to identify suspicious network activity. Most NBAs suffer from high false alarm rates, high detection latency, and offer limited mitigation capabilities. Under the best of circumstances NBA operators cannot react quickly enough to a new exploit to analyze, profile and contain it before wide-spread propagation.

Business Interest

CounterStorm seeks to establish business and technical relationships with "trusted advisors" and system integrators holding government contracts. CounterStorm also seeks sub-contractor opportunities for the development of threat analysis/mitigation solutions being solicited by Federal government agencies.