

Melior^{Inc.}

Perfectionists At Work

The Melior iSecure System Executive Summary



**Distributed Denial of Service Protection
Network & Systems Cloaking**

April 2003

© Copyright 2003 Melior, Inc.

Tel: 214-421-5975 Fax: 214-421-5951
Toll-free (USA): Tel 888-4 MELIOR Fax 888-TOFAXUS

www.dDoS.com
www.MeliorInc.com

Summary

Melior, Inc., (Latin for "Better") offers the only product, the **Melior iSecure System**, which protects Websites and Enterprise Networks in real time from Distributed Denial-of-Service (dDoS) attacks. These attacks render network devices such as firewalls, routers, switches, and servers useless by attacking the devices with bogus traffic. In addition, **iSecure** offers complete network and systems masking or "*network cloaking*" which prevents hackers from gathering information preceding an intrusion attempt by such methods as IP-Fingerprinting, a standard in every dDoS attacker's protocol.

Since 2000, the product has been successfully developed, tested, and proven to work in Germany and the United States. It is the only product in the market proven to protect against dDoS attacks. It also provides infrastructure cloaking, a unique risk mitigation feature. **iSecure** has been patented in Switzerland and the European Union; patent coverage is pending in the US and all WTO countries.

Melior is currently managing an immediate sales forecast of \$42 million in systems and maintenance contracts to be closed within the first year. Business development activities have led to promising accounts in Fortune 500 companies, public sector, and other organizations.

Melior is seeking at least \$3 million in funding to close these initial contracts, start full-scale production, and have sufficient working capital for penetration into North American and European markets. If able to obtain \$6 million in initial funding, Melior will be able to launch into the most important of the 167 World Trade Organization countries.

The Market for dDoS Products

The current size of the Internet security market is forecasted to be \$13 billion in 2004 for the US alone.¹ The Yankee Group predicts the Host Intrusion Prevention market will grow at a compound annual growth rate of 52.7%, from \$60 million in 2002, to \$520 million by 2007.² Recent highly publicized dDoS attacks have created demand for products to protect against these attacks. In a 1999 dDoS attack, the 17-year-old "Mafiaboy" was able to shut down the websites of Yahoo!, CNN, Charles Schwab, Dell, and others for three full days. The companies were defenseless and forced to wait out the assault. In October 2002, the Internet root servers worldwide were hit by a simple dDoS attack that almost brought down the entire global Internet. The FBI believes the incident was a trial terrorist attack, and has since categorized dDoS as a threat to national security. A subsequent similar attack on the European RIPE system occurred in January 2003. Other attacks include the dDoS attacks on Al Jazeera media and the Tony Blair sites (April 2003).

With limited sales efforts to date, Melior has received interest from some of the largest US and European banks as well as US and German government entities, many of which have trialed competitive products and abandoned them for lack of performance, lack of recognition of unknown attacks, and inability to maintain desired traffic to pass. Subsequent sales efforts will concentrate on the financial services sector, governmental entities, and e-commerce providers. Melior aims to establish the industry standard for security-privacy protection as required by various governmental regulations. **iSecure** complements current security systems already in place, serving as the primary layer of front-line defense, without requiring changes to infrastructure.

¹ International Data Corporation

² "Host Intrusion Prevention is the Last Line of Defense for Networks," Yankee Group, 21 April 2003



Furthermore, Melior recently became a member of the US Department of Defense and National Security Agency (NSA) SPOCK Program. Many dDoS vendors have tried to approach SPOCK and been turned away due to claims that could not be substantiated. Melior is the first Non-Governmental Vendor ("Civil Service Contractor") to join SPOCK, and the first vendor ever to do so upon an introductory meeting. This is a testament of the resounding acknowledgment of iSecure's functionality, and Melior's commitment to "Better" security solutions.

The planned pricing structure is tiered based on the number of Internet connections needing external protection. A large corporate client would typically need 200+ units at an average total cost of \$7 million plus a commitment to ongoing maintenance for at least three years. Smaller customers would require a smaller scale deployment.

	<u>High Discount</u>	<u>Low Discount</u>
Type 1 (100Mbit/sec)	\$ 12,600	\$ 13,500
Maintenance	\$ 3,600	\$ 3,600
Type 2 (400Mbit/sec)	\$ 31,500	\$ 33,750
Maintenance	\$ 9,000	\$ 9,000

** Prices shown net of discount

iSecure Technology

The **iSecure** system currently includes the dDoS protection and Infrastructure Cloaking. The former intercepts known and unknown dDoS attacks in real-time while allowing the normal network traffic to pass without impact. It cannot be detected or compromised because there is no IP or MAC address. Thus completely transparent, iSecure is deployed outside the firewall, and does not violate security policies inside the protected perimeter.

The underlying technology for iSecure follows a radically different concept than all other attempts to solve the problem of dDoS defense, all of which represent combinations of existing technologies, such as Intrusion Detection Systems and traffic management tools, and proven to be ineffective for this purpose. Developed by senior security specialists, iSecure consists of two integral new and patented technologies: a bitstream inspection engine and an intelligent decision engine, providing real-time detection and defense (real time = 6 nanoseconds to 6 milliseconds under full bandwidth load) by deterministic allocation of "good" and "bad" traffic.

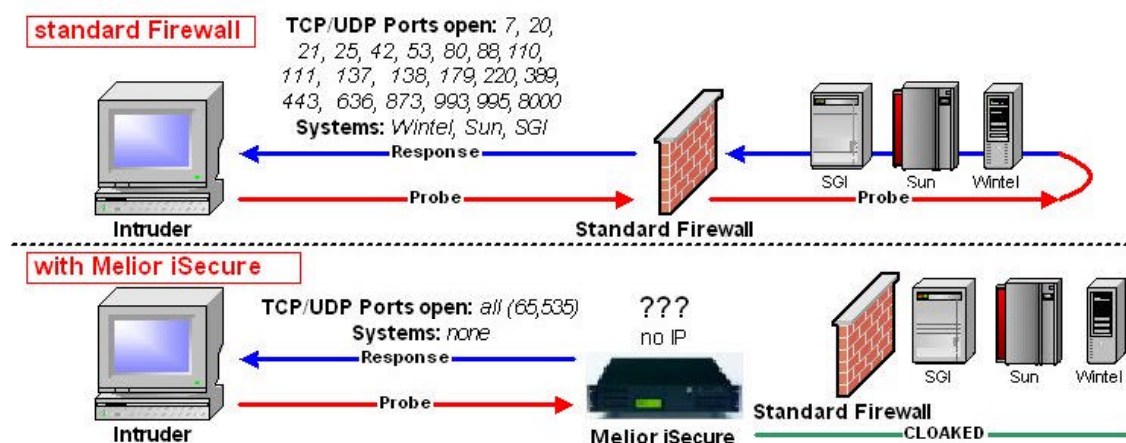
The bitstream engine monitors and analyzes each packet header flowing through iSecure, which works as an inline scanner, and feeds the information to the decision engine. The decision engine processes the information in a parallel matrix through an algorithm designed for Denial of Service defense, thus being able to determine very quickly if each packet is "good" to pass, or "bad" to be dropped. This decision process does not rely on a signature base, and thus defends against both known and unknown form of attacks. All tests have produced no false-positives, confirming iSecure's unique algorithm for TCP, UDP, and ICMP inspection and decision really works. iSecure works stateless, thus offering no vulnerability to attacks (as seen in other products based on TCP intercept), and allows for faster processing.

The same technical principle will be adapted to different applications of the bitstream inspection engine (focusing on both packet header and payload) and decision engines geared for other purposes, by which the parallel decision matrix engine makes pass/drop decisions to defend against content-based threats, currently planned for anti-virus defense and combating "Spam" E-



Mail. Both applications offer the benefit of defending against known and unknown attacks without definitions of "signatures" or "libraries", thus independent from anti-virus developments.

The Infrastructure Cloaking protects against any information-gathering probe from external parties by recognizing and intelligently responding to such probes, offering an unprecedented first line of defense:



History of Melior

Founded in 1996 as a Delaware C-Corporation, Melior is a high-end infrastructure and security service provider and architect. In 2001, as a contractor for Turner Construction, Melior managed IT operations and re-designed the nationwide network infrastructure. In 1999, Melior integrated the first link between Bank of America and NationsBank during their merger.

Current management:

Thomas J. Ackermann, Founder, iCEO

Matt Gair, Co-Founder, VP Strategic Business Development

Boni D. Bruno, Chief Technology Officer - CISSP, IAM

Rachel Fefer, Director of Strategic Business Analytics

Joyjit Sarma, Melior Inc. Ltd – India

Jim Potter, Group Director, Pacific Rim

John Danchak, Director of Enterprise Sales

Evan K. Langlois, Technical Solutions Architect

Christopher Brice Turner, Network Security Advisor

(individual background information on the Melior, Inc. web site)

Financial Summary

Melior is seeking at least \$3 million in initial funding from investors. Within thirty days of receiving this level of backing, Melior will execute its North American and European Sales campaign. If able to obtain \$6 million in initial investor support, Melior will launch a global campaign in the most important of the 167 WTO countries where the iSecure patents will be enforced.

EBITDA generated from a conservative sales forecast demonstrate the ability for rapid and profitable growth.

<u>Revenue</u>	Year 1	Year 2	Year 3	Year 4
Type 1 Units	\$ 8,415,000	\$ 11,475,000	\$ 20,250,000	\$ 33,750,000
Maintenance Type 1	\$ 2,340,000	\$ 5,400,000	\$ 10,800,000	\$ 19,800,000
Type 2 Units	\$ 14,737,500	\$ 16,875,000	\$ 25,312,500	\$ 33,750,000
Maintenance Type 2	\$ 4,050,000	\$ 8,550,000	\$ 15,300,000	\$ 24,300,000
	\$ 29,542,500	\$ 42,300,000	\$ 71,662,500	\$ 111,600,000
<u>Expenses</u>				
COGS (7% of Sales)	\$ 2,067,975	\$ 2,961,000	\$ 5,016,375	\$ 7,812,000
Royalty (15% of HW Sales)	\$ 3,472,875	\$ 4,252,500	\$ 6,834,375	\$ 10,125,000
Sales/Operations (1%)	\$ 295,425	\$ 423,000	\$ 716,625	\$ 1,116,000
G&A (5% of Sales)	\$ 1,477,125	\$ 2,115,000	\$ 3,583,125	\$ 5,580,000
	\$ 7,313,400	\$ 9,751,500	\$ 16,150,500	\$ 24,633,000
EBITDA	\$ 22,229,100	\$ 32,548,500	\$ 55,512,000	\$ 86,967,000
				\$ 197,256,600

Investment Evaluation Synopsis

- ❑ **Product Risk:** Fully developed, tested, proven, and patented (pending in final formal step). Additional validation/recognition: SPOCK, customer testimonials.
- ❑ **Market Risk:** Exclusive access to dDoS and cloaking markets, as competing products are not effective, and thus are not selling. This bears repeating: *there is not a single other product that offers effective dDoS protection, and none offers cloaking*. Each market (dDoS and cloaking) is estimated to be worth several billions of dollars in the long-term given the large number of potential customers seeking to protect their network infrastructure.
- ❑ **Financial Risk:** Melior would be profitable with the first large sale (200+ unit to any financial or other institution) or sales to about 30 customers for small and mid-size deployments. With a gross profit margin around 80%, no subsequent funding would be required.
- ❑ **People Risk:** Staffing progress has been steady. Heidrick &Struggles is working to augment the existing management team and has identified several candidates for the position of CEO; additional high-profile team members are in the pipeline. Steady technology history (existing global infrastructure and security service business, expertise, staying power) since 1987. Melior is in the process of setting up an independent, outside Board of Directors as well.



- ❑ **Patents Set:** With international agreements, iSecure patents apply in all member states of the European Union (and Switzerland), and all 167 WTO countries, including the US. It should also be noted that an additional, redundant process (filing) was done in the US. The broad way the iSecure patents were defined and accepted, Melior, Inc., has patent protection to an extent at which any other vendors may be forced to pay royalties if they wish to sell into WTO countries (including EU, CH, and USA).

Future *the potential to become a market leader in existing markets of:*

- ❑ **Future Signature (library) free Anti-Virus protection:** For all other products, everyone needs to download libraries to catch known forms of viruses; by applying the same principle as for dDoS defense (interchangeable Decision Engine), iSecure protects against known and unknown forms of viruses, with no need to download software or updates. The shortcomings of competing products, and why they work only in a limited fashion, is because they work on signature-(library) based detection and have to frequently download updates to recognize and be successful against virii. The iSecure advantage in the anti-virus market is the library-/download-free virus detection; contrary to the dDoS functionality, the virus defense is easy to accomplish.
- ❑ **Future SPAM E-Mail Defense:** We will apply the same principal iSecure technology to determine which e-mail is "bad" (SPAM, unsolicited), and which is "good". This will be accomplished with a new, different iSecure decision engine being developed by Melior, which will be geared towards eliminating SPAM e-mails.
- ❑ **Exclusive access to capture the IPSEC protection market:** With the next revision of iSecure, we will be able to protect IPSEC devices such as VPN gateways, which are currently totally exposed (outside fire wall and DMZs). No other product offers this functionality, and, as we go forward, we will develop and replace different decision engines (the current one is geared towards dDoS attacks) to enable a broader reach into the market on a granular/content level.
- ❑ **Exclusive additional potential in the market of Network Cloaking:** Cloaking as a stand-alone solution has yet to be delivered by any other vendor. This feature alone is the most powerful risk mitigation solution available and clearly represents a market unto itself.

Summary

Melior, Inc., is the first to deliver a solution to an ever-pervasive problem threatening Internet and network security worldwide. With one time funding of \$3 million or \$6 million (and without subsequent funding requirements), Melior and its investor partners can quickly capitalize on this opportunity and become the industry standard for dDoS security and network cloaking, with long-term growth opportunities in additional markets (IPSEC protection, anti-virus, SPAM, etc).

