Melior Inc.
Perfectionists At Work

iSecure

CyberWarfare Defense

1st Legal
Attn: Audy Gilstrap
403 West Loop 820 North
Fort Worth, TX 76108
Via e-mail *gilstrap@1stlegal.com*

Monday, May 5, 2003

**PROPOSAL FOR Secure Co-Location in Melior data facilities protected by iSecure CyberWarfare Defense**

Dear Audy,

Thank you for your interest in Melior, Inc. and the opportunity to introduce to you our unique distributed Denial-of-Service defense tool, iSecure, which enables us as the exclusive provider of hosting solutions safe against dDoS attacks, and fully cloaked from nefarious hackers, protecting the configuration of servers and other network devices.

In the following proposal we offer an immediate solution, which we hope you will select to keep 1st Legal's website and data applications permanently on the Internet without any interruptions.

We are readily available to work with you at any time to migrate your site and applications.

Sincerely,



Matt Gair
Co-Founder and Vice President Strategic Business Development

Melior Inc.
Perfectionists At Work

iSecure

CyberWarfare Defense

# PROPOSAL FOR CO-LOCATION OF 1ST LEGAL SERVERS

## Current Issues

At the time this proposal was written, 1st Legal has expressed interest to cease a relationship with its current vendor and to retain Melior, Inc. to Co-Locate one rack of servers with 2MB of bandwidth and managed security services.

## About Melior, Inc. – Background

Melior, Inc. is a highly specialized computer security company with a long history of providing high-end security solutions, with its roots dating back to 1987 to Germany. In 1996, Melior moved to the United States, and has recently – with the development of iSecure – transformed from a services company to a product company with augmenting services.

Melior is headquartered in Dallas, Texas, USA, with offices and technical personnel in Europe and India.

Melior has a rich background in infrastructure and security; it has built a $20m data center in San Jose (Silicon Valley, 1998/1999), designed and implemented the worldwide infrastructure for the Macromedia Shockwave Downloads (1995/1996), linked merging banks together (Bank of America & Nations Bank, 1998), deployed the first Point-of-Presence co-lo replication servers on the Internet (1996), and made recently Internet history again by launching the first dDoS-safe hosting environment and demonstration web server (2003).

Melior is currently the only company on the Internet to offer a fully cloaked hosting solution, which is safe against all forms of Denial-of-Service attacks (bandwidth flooding, network attacks, and application-level attacks).

## About Melior's iSecure CyberWarfare Defense Product

iSecure was developed to protect against Denial-of-Service attacks, one of the oldest and easiest forms of Internet attacks, and also the most devastating. In its distributed form, a dDoS attack is launched from a source behind many "handler" or agent systems, and can only be stopped by the attacker.

All other solutions in the market have taken the approach to combine existing technologies in an attempt to defend against dDoS attacks, by using Intrusion Detection Systems (IDS), Quality-of-Service systems (QoS) to detect attacks and throttle traffic. These systems fall short by design, as they are:

- Signature based (recognize only known forms of attacks, and of those only attacks for which signature files can be written; new attacks are not recognized)
- Slow (the very best response time is 4 minutes, typically 15-45 minutes – the damage is already done within a few minutes or less)
- Often require human interaction, further slowing response time down

- Even in the event of successful detection and reaction, network traffic is throttled, which means the dDoS traffic is overwhelming the desirable traffic: in essence, the dDoS attack is still successful
- Effective only against flooding attacks, no solution for network- or application attacks

**Product Description**

iSecure is a stand-alone system, deployed either upstream in the carrier-grade version, or locally in front of the firewall (no security policy violation). It functions as an in-line scanner, inspects the bit-stream traffic and reacts in real time (defined as 6 nanoseconds to 6 milliseconds). It does not use a signature base, but has an intelligent decision engine, which is able to detect "good" and "bad" traffic. Without the need of a signature base, it defends successfully against known and unknown attacks.

iSecure is currently available in three versions for real-time throughput at true 100 Mbit/s, 400 Mbit/s, and 1 Gigabit/s (1,000 Mbit/s).

It has been fully developed, tested in various environment, has never produced "false positives", works right out of the box, and (optionally) allows for additional configuration, and an administrative interface.

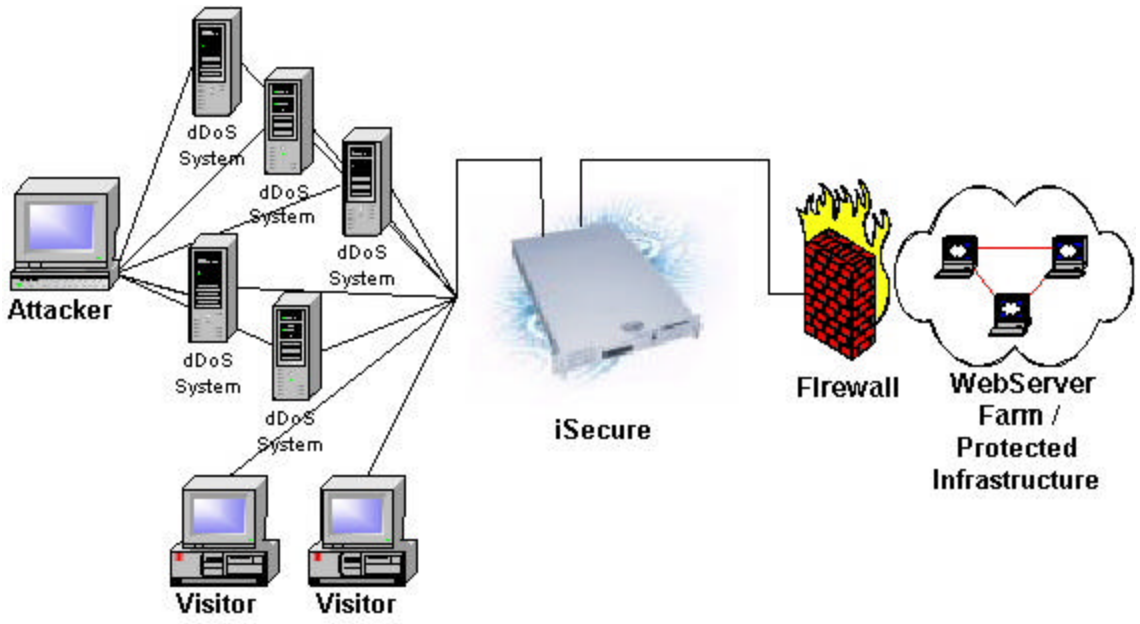



*Figure 1 – Deployment Overview*

**Functionality: distributed Denial-of-Service Defense**

"Bad" traffic is defined as (distributed) Denial-of-Service attack, malformed packets, reconnaissance traffic, spoofed IP numbers, and so forth. Upon detection, it drops the "bad" traffic, while letting the "good" (valid) traffic through.

Detection and Routing of packets is performed in real time (6 nanoseconds to 6 milliseconds at full bandwidth utilization). Valid packets are allowed through to the firewall and the protected infrastructure, while invalid packets and Denial-of-Service attack traffic is discarded.

The protected infrastructure works at normal performance and is not affected by the attack. Visitors from the Internet to the site have access to the content without impact, while the Denial-of-Service attack has no effect:

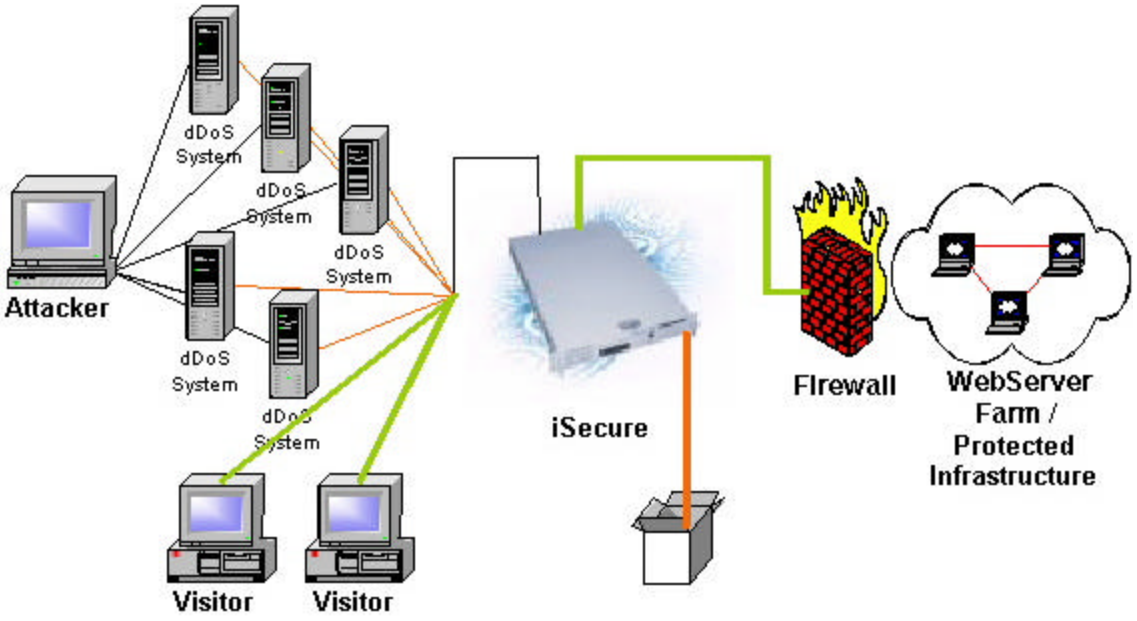



*Figure 2 – distributed Denial-of-Service Defense*

iSecure defends against all three types of distributed Denial-of-Service (dDoS) attacks:

- Bandwidth Flooding (such as ICMP floods)
- Network Attacks (such as "ping echo" attacks)
- Application Attacks (mixing with port 80 or port 53 traffic)

By covering all three forms of attacks, any dDoS attack from simply script attacks to sophisticated, targeted attacks by any level of expertise of the attacker, as well as with a large number of dDoS "handler" systems, remains unsuccessful.

**Functionality: Infrastructure Cloaking**

iSecure also offers another unique functionality: infrastructure cloaking. As the first step of every hacker is first to launch information gathering probes to determine which firewalls, servers, and configurations are in use, making this information unavailable is the first line of defense against attacks of any kind.

All existing solutions in the market are unable to provide this layer of protection. Every firewall limits the number of available ports, however must keep those ports open, which are necessary for communication with the public (visitors). These open ports offer the ability for a hacker to launch exploit and reconnaissance tools. The firewall itself also remains open for mapping and exploitation.

iSecure recognizes any attempt to gain information of the infrastructure it protects, and responds with all ports as “open”, and does not reveal any configuration information. While the production infrastructure performs without impact, no information is revealed to probing attempts, and the attacker has to guess which systems are actually deployed – leaving only guesswork as to which vulnerabilities may exist for exploitation.

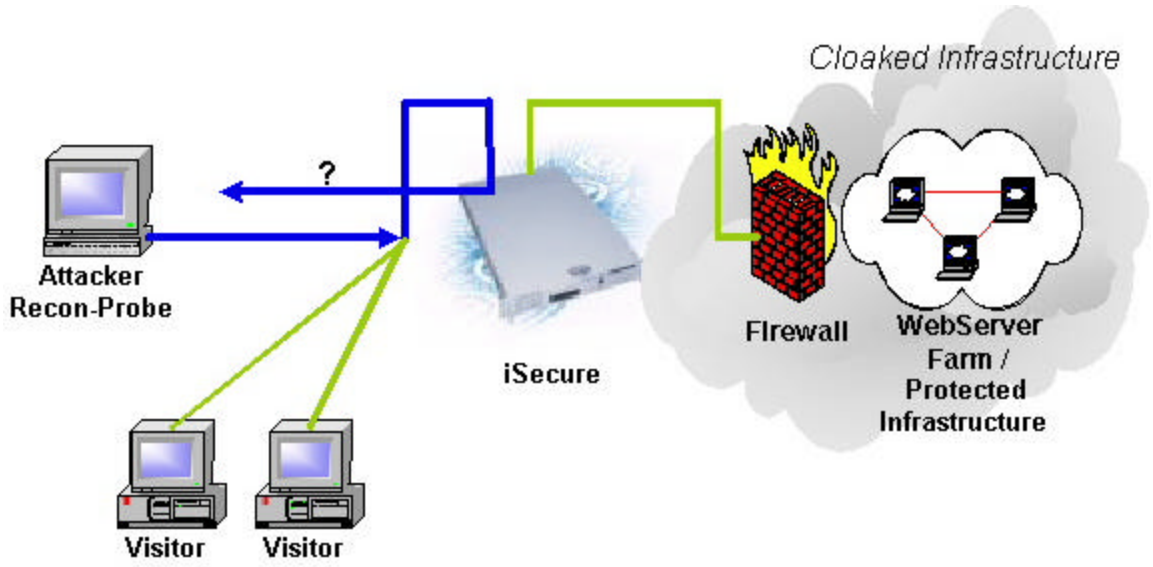



*Figure 3 – Infrastructure Cloaking Overview*

This unparalleled cloaking feature is the basis of disabling attackers from launching targeted attacks. All Melior hosting services are protected by it.

**Demonstration & Proof**

Melior provides many means to prove our security claims for distributed Denial-of-Service Protection and Infrastructure Cloaking:

- ✓ Providing Melior's technical White Paper
- ✓ Demonstration Video for live access on the Internet (streaming media)
- ✓ Demonstration Video on DVD (all region codes) in high-resolution, by request
- ✓ Live Online Demonstrations on our demo system on the Internet
  - demonstration by Melior Technical Staff
  - live test by external parties
- ✓ Live Demonstration at the Melior Data Center in Dallas
  - on Melior-provided attack- and target systems
  - customers can bring their own test tools, attack- and target machines
- ✓ Live Demonstration at a customer site
- ✓ Providing documentation from extensive tests performed at large financial and commercial institutions in the United States and Europe

Melior, Inc. was also just accepted as a member to the SPOCK program, which is a forum consisting of the US Department of Defense, various US Government Agencies, and US Government contractors.

All this information and links to the demonstration video are available on our web site.
Last weekend, we concluded the process to move the last of our California data centers to the Dallas data center, to provide this production environment also with iSecure protection.

**About Melior's Hosting Solutions**

Since 1996 Melior provides highly secure, and highly available websites to customers in Europe, the United States, and Asia, for customers spanning a wide field of industries.

With iSecure, our Hosting environment is safe against distributed Denial-of-Service attacks, and fully cloaked.

We provide solutions for high volume customers, and customize the environment to meet our client's demands. Each hosting environment is carefully designed to perform best for each customer. This includes single or distributed sites, consideration for content delivery to different regions on the globe, appropriate peering agreements, path redundancy, and other vital components.

Melior provides log analysis and trending for up to one year of traffic, which is daily updated, and available via web browser.

**Reliability**

Melior provides high uptime, for both the infrastructure in itself, as well as traffic management to and from the internet. Redundant servers for web hosting, DNS, E-Mail, etc ensure that even hardware failures do not impact system performance.

**Melior, Inc.**
United States of America – Europe – Asia
US HQ: 1501 Beaumont Street, Dallas, Texas 75215
www.MeliorInc.com – www.dDoS.com – www.BGP4.com – www.Secure.SH
Tel +01-214-421-5975 Fax +01-214-421-5951

All systems run on highly reliable UNIX platforms, which support all applicable server extensions, including all Microsoft-specific extensions.

Our qualified staff is ready to assist with configuration and setup of customized web content.

**Availability**

We offer highly available systems either in a single data center, or load balanced across multiple data centers. We own the domain BGP4.com, which stands for the routing protocol which runs the entire Internet backbone (Border Gateway Protocol v4), and offers a redundant infrastructure with distributed Domain Name Servers (DNS), redundant routing access, and dynamically updated configurations.

Our 7x24 support staff guarantees that any arising issues are promptly addressed, and our customers get the best support, true to our company motto: “Perfectionists At Work.”

All Melior hosting solutions are protected by our iSecure product, and thus safe against Denial-of-Service attacks, ensuring no service interruption occurs due to outside interference.

**Security**

With Melior’s extensive and proven security consulting experience since 1987, all our own systems for hosting solutions are completely secured and locked down. We deploy the most effective firewall, web server, and e-mail systems, use extensive encryption and LDAP authentication systems, and ensure that our customers get the full benefit from our experience.

Melior has experience in hosting media sites, e-commerce and health care sites, and other industries which rely on secured systems to protect customer and vendor data, as well as avoid changes or defacements of content.

**Secure Management by Customer**

Our customers have the ability to manage their own configuration for DNS hosts, e-mail accounts, and web content configuration. Melior staff is also readily available to perform any configuration as requested.

Customer access for management and content uploads/changes is SSL encrypted and authenticated via LDAP, to make sure only approved changes occur. Melior also monitors access closely, as a fail-safe check for unauthorized access attempts.

All access and changes are recorded, and logs are maintained for an extensive period. If any unauthorized access attempt is observed, Melior records all forensics information and initiates or assists in legal action as requested by the client.

**Proposed Solution: Immediate Co-location/Hosting in Melior Facility**

To make 1st Legal content immediately available, Melior will provide one 18-inch rack within its facility.

With this location and provider change, the 1st Legal servers are protected against Denial-of-Service attacks, and reside on a high-availability platform to handle the traffic of a high-profile web presence. Melior will ensure that upstream bandwidth flooding is protected as well by our co-location provider.

**7x24 Support Available via US (Dallas) or India (New Delhi)**

Due to time differences, we provide support out of our US location in Dallas as well as from India. Our support goes beyond technical considerations; we are also available to handle media events, business issues, and related support, should this become necessary.

Melior can quickly scale up operations in India or Dallas to meet increasing demands for customer support.

**Pricing**

- One 18-inch rack
- 2 MB Bandwidth
- iSecure protected hosting with Melior managed security (dDoS safe and cloaked)
- Melior support

Name your price; and we'll see if we can do it.

***For Melior, Inc.***

Thomas J. Ackermann, Founder and CEO
Matt Gair, Co-Founder and Vice President Strategic Business Development
John Danchak, Enterprise Sales