Business Plan

Pelican Security Inc.
14900 Conference Center Drive
Suite 475
Chantilly, Virginia 22030
703-488-9770

Pelican Security Ltd.
3 Tvuot Ha'aretz St.
Tel Aviv 69546
Israel
972-3-648-8454

info@PelicanSecurity.com
www.PelicanSecurity.com

Table of Contents

Executive Summary

Pelican Security is an emerging leader in the client-side Internet security market. Client-side Internet security products protect computer systems from Internet threats like the recent Love Bug virus, which caused in excess of $10B in damage in May of 2000. Pelican's flagship product line, Pelican SafeTnet™, defends corporations from next generation Internet viruses and from hackers who attempt to use Internet technology to gain unauthorized access to vital corporate resources. SafeTnet was the only technology to *proactively* block the malicious actions of the "Love Bug" worm when it first hit and was recently named "Best Internet Security Product" by the readers of Secure Computing magazine.

Unlike outmoded antiviral technology, which is inherently reactive, Pelican SafeTnet's next generation approach provides proactive security protection from both known (previously seen) and unknown forms of malicious Internet code. Reactive approaches are capable of responding to a new threat only *after* it has already occurred. Proactive technologies like Pelican SafeTnet provide superior security because they protect critical resources *before* a new threat can cause any damage. Industry analysts believe proactive security approaches like Pelican SafeTnet will replace reactive antiviral technology in the $1.8B antiviral market.

SafeTnet's unique approach to Internet security works by automatically establishing an access control barrier, called a Dynamic Sandbox™, around Internet applications and mobile Internet code downloaded to the client by Web browsers, email, instant messengers, and other Internet aware programs. The Dynamic Sandbox is a barrier which controls access to corporate resources including data files, applications, network and systems files. SafeTnet's access control rules are based on a centrally defined corporate security policy. Pelican SafeTnet's advanced capability enables corporations to safely conduct business over the Internet without sacrificing the productivity and flexibility provided by mobile Internet technology.

Pelican markets its software in North America to Fortune 1000 corporations. SafeTnet has just completed a very rigorous and successful beta period with several high profile customers. These customers are now beginning large-scale deployments of Pelican products over the next several months. Beta sites and prospective customers include organizations such as a regional Bell operating company, an International cellular and long distance carrier, a Wall Street brokerage firm, a nationwide bank, and a major U.S. Department of Defense organization.

Pelican Security Inc. is lead by a team of seasoned software professionals with a proven track record of taking companies from the start-up stage to successful IPOs. The CEO has an extensive background in marketing and business development for high-tech startups. The CTO has provided the technical leadership and product development expertise for several successful software and telecommunications companies. And the President the company was previously responsible for the strategy and vision that lead two software start-ups to successful IPOs.

The Pelican management team sees rapid growth and high demand in the $3B Internet security market[1]. Pelican's strategy will be to establish itself as the dominant vendor in the client-side Internet security market niche. The client-side Internet security market currently includes a portion of the $100M Internet application security market and a portion of the $1.8B antiviral market[2]. Pelican expects this market niche to grow to more than $3B by 2003 as obsolete antiviral technology is eventually replaced by proactive client-side security approaches. Fortune 500 companies are now actively evaluating the discontinuation of antivirus subscriptions in favor of our approach.

Pelican SafeTnet has been commercially available since February of 2001 and the company has achieved initial sales of approximately $370K in the first and second quarters of 2001. While revenue predictions are uncertain at this stage given the macro economic environment, Pelican believes it will achieve sales of approximately $1.2 to 1.5M in 2001 based on its existing pipeline. The current focus is on developing reference accounts that can later serve as beachheads in their specific market segments. The company expects rapid growth and to achieve profitability in 2002. The company should reach a "steady state" model in 2003 with 100+ percent revenue growth and pre-tax margins above 25 percent.

[1] 2000 market size according to IDC and Frost and Sullivan

[2] 2000 market size according to IDC and Frost and Sullivan

Market

Today, doing business over the Internet is the key to opening new markets and increasing productivity. Whether a corporation's eBusiness strategy is "business to business" or "business to consumer", Internet connectivity is no longer an option; it is a requirement in order to remain competitive. In a recent survey, 43% of corporations were conducting eBusiness in 1999 up from 30% in 1998[3]. That growth rate is expected to accelerate in 2000. Unfortunately the technologies that make eBusiness possible, such as Internet applications and downloaded Internet code, also create new computer security risks that hackers can take advantage of.

Mobile Internet Code

To run an effective eBusiness, organizations need to use powerful tools like mobile Internet code. Internet code is any type of Internet content that can programmatically carry out someone's instructions when downloaded to a client computer. Internet code includes technologies such as executables (*.exe, *.com, *.bat, etc.), Microsoft Office macros, scripts, plug-ins, screen savers, Java applets or ActiveX controls. Internet code can be downloaded into the corporate network by Internet email (embedded or as attachments), Web browsers, FTP, chat clients or by any Internet aware client application.

The vast majority of Internet code is highly beneficial and eBusiness depends on this technology. Without the use of email attachments organizations would be unable to exchange electronic forms of documents, presentations or spread sheets. Without macros many repetitive and time-consuming tasks would have to be done manually. Without tools like scripts, Java applets or ActiveX controls, Web sites would be reduced to static text and graphics with little or no interactivity. Stock quote systems would fail to work, Internet conferencing software would be useless, and on-line order processing systems may be less effective or completely disabled.

Malicious code

Because the Microsoft Windows operating system allows downloaded Internet code to execute with all the user's rights and privileges, hackers can also exploit this technology for malicious purposes. With high profile attacks such as Brown Orifice, the "Love Bug", Killer Resume, ExplorerZip and Melissa all surfacing in the last several months, organizations have become keenly aware of how much

[3] "Issues and Trends: 2000 FBI Computer Crime and Security Survey". Computer Security Institute, March 22, 2000.

damage can be caused by the malicious use of client-side Internet technology. Attacks such as these destroyed corporate information, brought entire networks to a grinding halt, and caused significant losses in productivity. In 1999, IT organizations spent $12 billion worldwide on recovering from malicious mobile code attacks and in lost productivity[4]. In 2000 Damages due **to the Love Bug worm alone are estimated to top $10 billion** and may eventually top all of 1999 damages[5].

While hacker attacks proliferate, the methods to distribute the malicious code grow even faster. Only a few years ago, floppy disks were the primary way of transmitting viruses, and worms were a rarity. Today, email has become the dominant transmission method, and worms and Trojan horses have replaced viruses as the most significant client-side threats. Given this shift, there is not time to wait for an antiviral update. Recent attacks have spread world wide in a matter of hours by exploiting global Internet connectivity.

Hacker Agents

But not all hackers use Internet code to destroy data or cause a loss of service. Internet code can also be used to steal corporate information or gain unauthorized access to key applications, the network or the server itself. With the advent of easily written macro and script-based technologies, it is relatively simple to create stealthy Trojan horse[6] programs that can act as a remote agent designed to do the hacker's bidding. These "hacker agents" can be used to gain unauthorized access to corporate applications and information.

> *"The GIAC (Global Incident Analysis Center) has received several submissions showing large amounts of data being sent, illegitimately, from Windows 98 machines to a Russian IP address (194.87.6.X). The cause is most probably a Trojan horse…"*
>
> Stephen Northcutt, Director Global Incident Analysis Center
> The SANS Institute Flash Alert, July 28, 2000

In a highly publicized incident in October of 2000, Microsoft was hacked by a Trojan horse/Internet worm called QAZ[7]. The QAZ Trojan arrived at a Microsoft

---

4 "Study: Viruses cost $12B in '99", ComputerWorld, January 17, 2000

5 " Attack of the Love Bug", Time Magazine, May 15, 2000

6 A Trojan horse is a computer program that appears to have an innocuous function but in reality has a different, surreptitious purpose.

7 "Hackers break into Microsoft's network and may have stolen code for software", The Wall Street Journal, October 27, 2000.

employee's desktop as an email attachment. When activated the worm portion of the Trojan horse spread the malicious code to other Windows desktops inside Microsoft. The Trojan horse was used to steal passwords, which in turn gave the hackers access to the Internal Microsoft network. The hackers were able to access Microsoft's most sensitive data, the source code to its operating system.

> *"… there are some measures Microsoft could have taken. One in particular is a protection against Trojan horse attacks, like the one that started this entire chain of events.* ***Pelican Security*** *sells a product that inhibits all Trojan horse code at the desktop. In other words, the initial security breach would not have happened."*
>
> Steve Hunt, Giga Information Group, "The Microsoft Security Hack reveals strength, not weakness", November 21, 2000

Unfortunately this type of incident is not unique. In March of 2000 it was discovered that another Trojan horse (Anti-Symser) had been used to gain unauthorized access to NATO's network. The hackers were able to steal military plans called "rules of engagement" for Kosovo and subsequently published this information on a public Web site that they had also hacked[8].

Unlike viruses and worms, which are readily apparent because of the damage they do, hacker agents are virtually impossible to detect because the leave no traces behind. Since hacker agents run under the guise of the user, they cannot be detected or stopped by conventional security technology. This stealth code is usually carefully disguised and can be targeted against specific users or organizations. Hacker agents may not get the publicity of their more destructive cousins, but they are potentially a greater problem for a corporation because information is the currency of today's eBusiness economy.

It is possible, for example, to send an email message containing a hacker agent to a specific user, perhaps as an email attachment or embedded in an HTML-based email. As soon as the message arrives at the desktop, the hacker agent then can access the user's local or network documents and sends them by email to an external hacker. In the information contained in those documents represent sales forecasts, merger activity, or private information about an employee; the damage to the company can be severe. Bubble Boy and Brown Orifice are two real world examples of this type of malicious Internet code.

Hacker agents can also be used to implant other Trojan horse programs that can be used to launch a denial of service attacks from unsuspecting computers that

[8] "NATO comes clean on virus problem", InfoSecurity Magazine, August, 2000

can't be traced back to the original perpetrator. Computers taken over by Trojan horse programs, believed to be implanted using Internet code technology, launched many of the recent denial of service attacks, which crippled eBusinesses like Amazon.com and eTrade.

"Back Doors"

New Internet applications such as Instant messengers (e.g. AOL Instant Messenger) and peer-to-peer applications (e.g. Napster, Scour, CuteMX, etc.) can create a "back door" to the corporate network that can be exploited by hackers. These applications can be easily downloaded and installed by anyone with Internet access. Instant messengers may bypass corporate security measures like firewalls and content filtering. Peer-to-peer applications enable anyone on the Internet to gain unauthorized access local hard drives or network drives. Media Metrics estimates that over 900,000 corporate PCs are running Napster, which means that there are nearly a million potential back doors that may be exploited by anyone on the Internet.

Invasion of Privacy

Internet code can also be used to invade privacy by surreptitiously gathering information about the eBusiness user. Hidden applets or scripts running on a Web site can tell where users have been on the Web, what software products they have installed, and even what their Web surfing habits are. This data is ostensibly gathered for the purpose of targeted marketing or customization of Web content, but the potential also exists for the misuse of this information.

Downloadable applications such as Real Player, zBubbles, and the Windows registration wizard are called "ET" programs because they "spy on you and report back by 'phoning home'"[9]. Programs such as these can be used to gather personal information about someone without their knowledge or permission.

The privacy controversy has been highly publicized, especially when it was discovered that firms specializing in this type of tactic could connect a profile with an actual person. No one wants their private information collected without their knowledge no matter how benign the motivation. eBusinesses that expose their customers to this type of hazard risk alienating their customers.

[9] "Who's watching you?" , Time Digital, July 2000.

Client-side Security Requirements

While most corporations have protected the network and server components of an eBusiness system, they have left the front door wide open by completely neglecting the Internet client. The conventional wisdom has been that there was nothing of any significance to protect on the PC. It is erroneously believed that the worse case scenario would mean the information on the local drive would be compromised. Many corporations believe their key business assets are well protected behind an expensive wall of network and server security. But this rationale is flawed and outmoded.

In most cases, the Windows client is the gateway to the eBusiness network. Since Internet code technologies and Internet applications execute at the desktop with all the PC owner's rights and privileges they have access to not only local information, but the network and server as well. Microsoft Windows cannot distinguish between the rights and privileges of the end user and those of an application or piece of Internet code which is executing on the user's behalf.

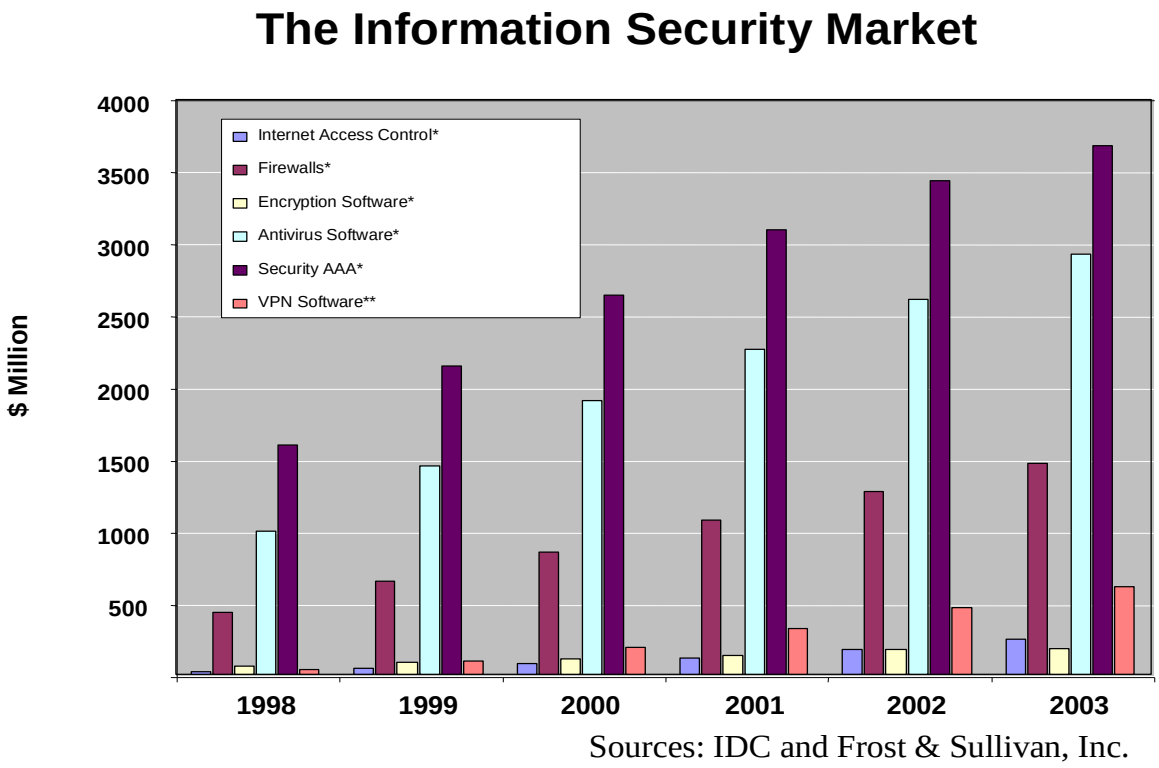
The security exposure created by malicious use of client-side Internet technology creates a need for products that enable corporations to continue to use the power and flexibility of Internet code, while **proactively** protecting key business resources from unauthorized access or destruction. While first generation technologies such as antiviral products have achieved almost a 90% penetration in the corporate market, they do not provide effective protection against new Internet-born viruses like ExplorerZip and Melissa or worms like Love Bug and Killer Resume or Trojan Horses like Brown Orifice. They do not proactively protect eBusiness resources from new Internet code threats; they only react *after* the damage has already occurred.

A new class of client-side Internet security products is emerging which can control the functionality of Internet applications and downloaded Internet code based on a centrally defined security policy. This class of products applies the well-established concept of application level access control to Internet applications and downloaded code. First generation antiviral products attempt to determine if a given piece of code is "good" or "bad" based upon its similarity to known harmful programs. Application level access control (also known as "sandboxing") functions in a completely different way. Sandboxing products control the Internet application's or downloaded program's access to system and network resources based on a pre-defined security policy.

> Sandboxing technology eliminates the need to ensure that anti-virus protection's up-to-date – just install the software once and forget about it.
>
> Richard Adhikari, PlanetIT

Market size and Growth

The client-side Internet security market is nascent, but expected to grow quickly. In 2000 the overall Internet security market (firewalls, virtual private networks, encryption, Internet access control, and antiviral) is estimated to reach $3B[10]. This market includes some highly successful companies such as Checkpoint (NASDAQ: CHKP), ISS (NASDAQ: ISSX), RSA (NASDAQ: RSAS), Symantec (NASDAQ: SYMC), Network Associates (NASDAQ: NETA), and McAfee (NASDAQ: MCAF).



Sources: IDC and Frost & Sullivan, Inc.

Currently client-side Internet security is not measured (by the IDC and Frost and Sullivan survey) as a separate market segment but is made up of technologies in the Internet application security (Internet access control) and antiviral market segments. Analysts expect the Internet application security market to grow from $100M in 2000 to more than $250M in 2003. The antiviral market is one of the largest components of the over all information security market. According to the

[10] Source: IDC and Frost and Sullivan

IDC and Frost and Sullivan survey, the antiviral market growth is expected to grow from approximately $1.8B in 2000 to nearly $3B in 2003.

Because client-side antiviral technology has not kept up with the Internet, the market is beginning to look for alternative solutions. Despite spending millions on antiviral products, companies are still being crippled by new types of malicious Internet-born code. Almost all of the companies brought down by the Love Bug were running the latest and greatest antiviral products. Many experts have come to the conclusion that the antiviral vendor's after the fact approach to the problem is no longer a viable solution in light of the Internet. These same experts believe that next generation proactive solutions will replace outmoded reactive technologies.

> *"…The underlying technology implemented in traditional antiviral products, pattern recognition, is a technology and market failure in the age of the Internet."*
>
> Jim Hurley, Aberdeen Group

The market for client-side antiviral software is mature with over 90% penetration on corporate desktops. Due to the maturity of the market, a few established players dominate this market segment. Since antiviral software requires constant updating to keep up the ever-changing universe of threats, the antiviral vendor's revenue model is based on reoccurring service fees or subscriptions rather then sales of new software licenses.

Because proactive security approaches such as Pelican's Dynamic Sandbox do not require the constant updating, they can be more cost effective then antiviral solutions. Since Pelican's technology is new and has low penetration, the revenue model for Pelican is based on sales of software licenses. Customer's can purchase a license to Pelican SafeTnet for less cost then a three-year subscription to a desktop antiviral product.

Therefore, Pelican believes that proactive security solutions will eventually replace the vast majority of the client-side antiviral market. Pelican also believes that application level access control (sandboxing) will come to dominate the client-side application security market. Therefore the company believes that the potential market for client-side Internet security will be in excess of $3B by 2003.

Product

Pelican's flagship product, Pelican SafeTnet™ became generally available June 1st, 2000 after several months of beta testing at Fortune 500 customers sites in the US. SafeTnet is based on a "manager/agent" architecture with small

software agent running on Windows-based desktops and a central administrative component running on Windows NT-based servers.

How it works

To protect the eBusiness from malicious Internet code Pelican SafeTnet takes a proactive approach to client-side Internet security. This proactive approach enables Pelican SafeTnet to stop damage to eBusiness resources before rather then after the fact. SafeTnet's approach enables authorized Internet applications to have access to the resources which are necessary for the eBusiness to function while restricting unauthorized access by malicious Internet programs to applications, corporate data, system files and the network itself. This means that SafeTnet does not need to have seen an attack in order to stop it and can protect organizations from any type of malicious code attack even ones no one has ever seen before. Pelican SafeTnet's application security approach enables it to function transparently to the end users while enforcing centrally administered security policy.

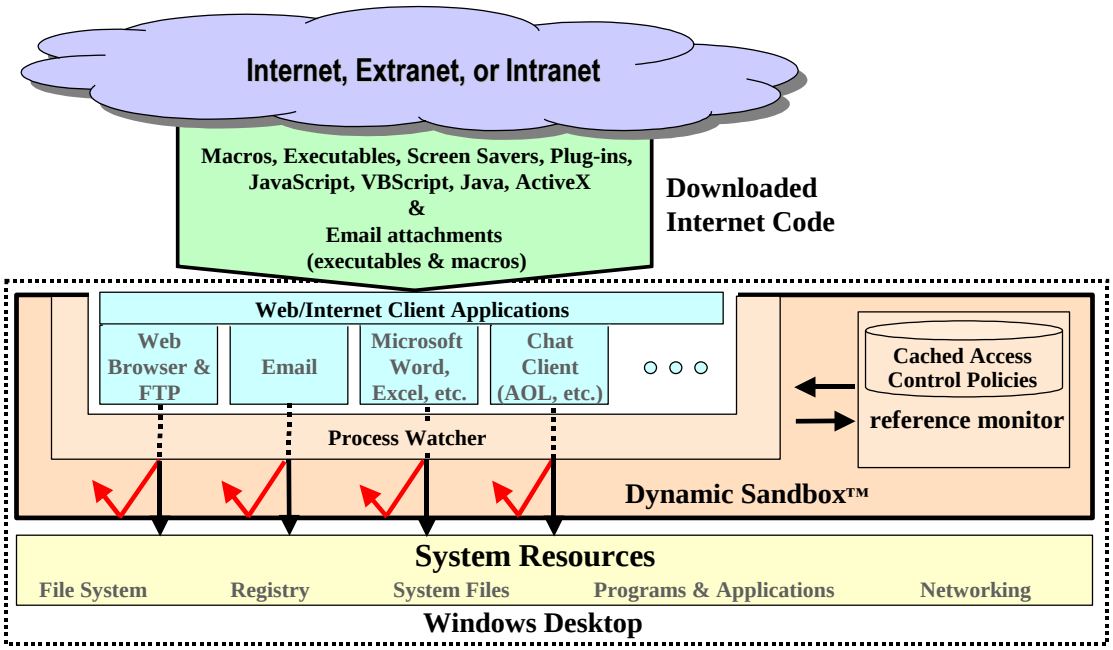
The technology behind Pelican SafeTnet, called **Dynamic Sandboxing™,** starts with the premise that mobile Internet code is a valuable technology that we must allow to be downloaded to a client computer. But while SafeTnet allows Internet code to be downloaded, it places an impenetrable barrier between the executing program and critical corporate resources. This barrier limits or controls what the Internet code can and cannot access. This access control barrier is formed dynamically and automatically whenever Internet code is downloaded to the desktop. The principles behind Dynamic Sandboxing are based on well known application security principles which enables Pelican SafeTnet to overcome many of the limitations of first generation approaches.

Pelican SafeTnet's Dynamic Sandboxing technology controls all of the actions of a downloaded Internet program. SafeTnet automatically watches each of the applications that are capable of downloading Internet code (email, browser, FTP, chat clients, Microsoft Office, extranet applications, etc.) and dynamically establishes a set of access controls around the application when it is executed. These dynamic access controls can intercept the operating system calls and check them against a policy database. If the action is allowed by corporate policy, then the system call is allowed to proceed. If the action is not allowed by corporate policy, then the system call is blocked. Since the Internet code can do nothing (good or bad) unless it first invokes the operating system, it is virtually impossible to bypass the SafeTnet barrier.

For example, suppose a Microsoft Word document containing a macro arrives as an email attachment. Pelican SafeTnet knows that a potentially dangerous Internet code has been downloaded because it was watching the email client. If

the user double clicks on the document to open it, a Dynamic Sandbox is formed around the email client application (since that was the process that spawned MS Word). As the embedded macro makes a system call, the Dynamic Sandbox intercepts the request and checks it against a locally running policy database. If the macro attempts an action which violates a centrally defined corporate security policy, (such as modifying system files, sending email, modifying sensitive registry keys, and deleting documents, etc), that action is automatically blocked by SafeTnet and a notice given to the user that a policy violation has occurred. If the action is authorized, then the macro functions as it would normally.

Dynamic Sandboxing Architecture



The advantage of SafeTnet's Dynamic Sandboxing approach is that it can deal with any type of client-side Internet threat, known or unknown, because it does not depend on pattern recognition or heuristics. Furthermore, SafeTnet works with all types mobile programs including macros, scripts, executables, and applets. Because it operates at the client operating system level, it will work even if the Internet code is encrypted or compressed. SafeTnet functions equally as well for network users and mobile users. Finally, since Pelican SafeTnet provides a fine-grained approach to application level security, it can give legitimate Internet code access to authorized resources while restricting

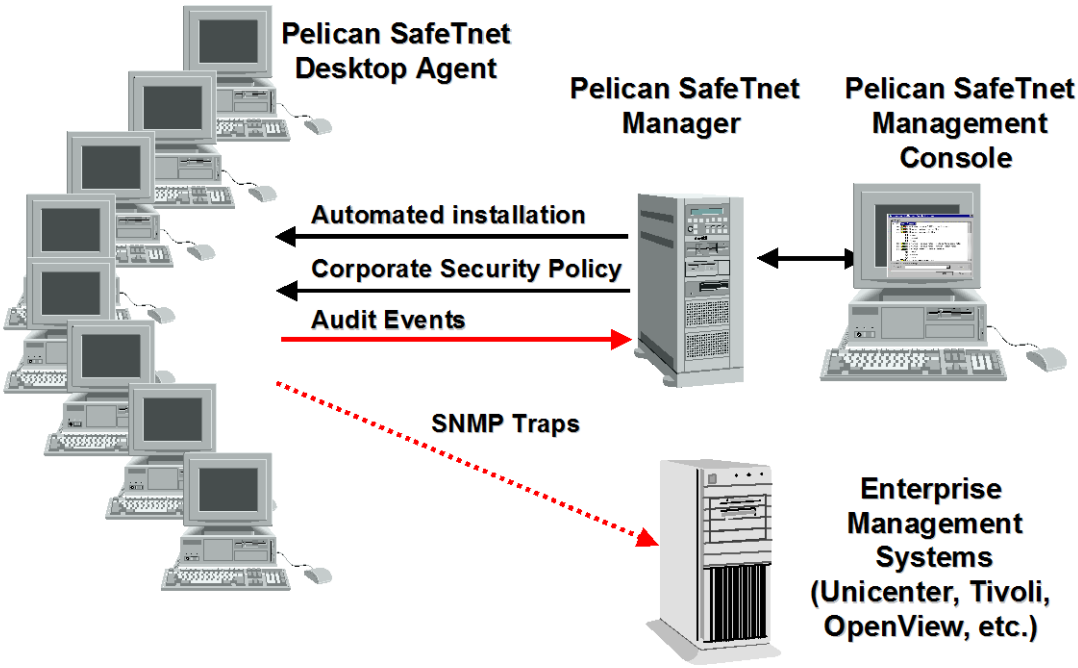
malicious program's access to unauthorized resources. First generation products have no granularity; they simply block or allow the downloaded code to run. SafeTnet's granularity enables eBusiness applications to take advantage of powerful Internet technologies without exposing their owners to dangerous side effects or consequences.

Central Administration and Auditing

Pelican SafeTnet was designed from the outset as an enterprise solution, focusing on the need for central administration and scalability. The access control policies for the Dynamic Sandbox are defined centrally by security administrators and cannot be changed or overridden by end users. These policies are easy to set up through a point and click interface and the local policy definitions within SafeTnet's desktop agents can be automatically updated every time the user logs into the network. Pelican SafeTnet's policies deny access to all critical system resources by default. Explicit access can be granted to a given resource by a specific type of active content through modification of an existing policy or creating a new one.

Policies can vary by the channel that downloads the Internet code (Web, email, FTP, chat, etc.) or by the source of the downloaded code (URL). Policies can also vary by user group. Some groups can have more restrictive policies while other groups are given greater flexibility. SafeTnet's central administration facility is integrated with the Windows NT user database so users and groups do not have to be recreated. Once set up, SafeTnet requires very little administration or updates.

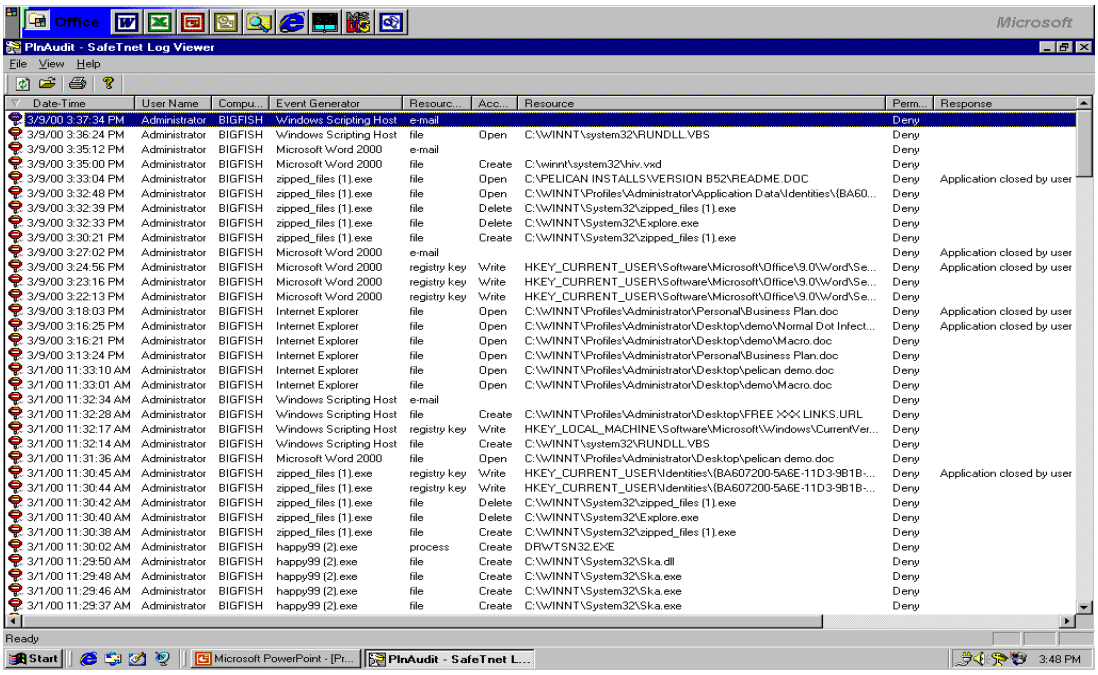
Central Administration & Auditing



Pelican SafeTnet provides security administrators with a centralized, detailed log of all suspicious events caused by downloaded active content. Since SafeTnet monitors access to key system resources, it is able to collect critical events from each user's desktop and display them on the administrator's console or an enterprise management console such as CA-Unicenter, Tivoli TEC, or HP OpenView.

This detailed audit log enables security administrators to stay on top of the Internet threats by monitoring the behavior of intrusive Web applets, detecting viruses, worms, and Trojan horse attachments, and even helping to determine the source of an Internet code attack.

SafeTnet Administrator's View of Mobile Code Events



Benefits

Pelican SafeTnet provides the final line of defense against malicious Internet code and eliminates the threat from new, Internet attacks that other methods can't prevent. Instead of reactive antiviral "cures", SafeTnet prevents the "disease" from occurring in the first place. This enables eBusinesses to take advantage of all kinds of Internet technology without the fear that their eBusiness resources will be compromised by an Internet code attack.

> *"What sets the Pelican product apart…is the central management and policy-based enforcement at the desktop. The 'once and for all' nature of Pelican Security's product makes it the winner in the desktop security battle"*
>
> Steve Hunt, Security Analyst, Giga Information Group

Availability and Pricing

Pelican SafeTnet is currently available for Windows 95, 98, NT, and Windows 2000 desktops. The SafeTnet Administrative Server runs on Windows NT servers with Windows 2000 support scheduled for the end of 2000. SafeTnet is priced from $30 to $60 per desktop depending on quantity purchased. The SafeTnet Administration Sever is priced from $2,000 to $5,000 depending on quantity.

Strategy

Sales and Marketing strategy

Pelican's market strategy is to establish itself as the leading vendor in the client-side Internet security market niche through the use of direct sales to large corporations. Pelican believes that a direct sales channel is the best way to launch a new technology in the corporate market place and establish a leadership position. The company's direct sales organization will target Fortune 1000 corporations, primarily in North America, where the Internet is critical to their business strategy. The direct sales organization will focus on selling site license deals with average transactions in the $100K range and above.

While Pelican SafeTnet is applicable to any organization connected to the Internet, Pelican's early goal will be to establish a referenceable customer base in financial services, telecommunications, and government organizations. Once this base is firmly established, Pelican will expand its industry focus to manufacturing, retail, pharmaceutical, and other industry niches.

Pelican has established a 14 step sales process that is currently used in order to manage and track progress with each customer. The process begins with identifying qualified prospects from the target markets. Pelican's team is using a variety of marketing tools to generate qualified leads. These programs include public relations (press and analysts), trade shows, speaking opportunities, on-line seminars, and limited advertising.

Raw prospects will be qualified by an internal telemarketing organization whose function is to identify the more qualified prospects and move them through the early stages of the sales cycle. Once a prospect has reached a sufficient interest level, the lead will be turned over to the direct sales force. Prospects will then proceed through discrete phases which would include on-site demonstrations, controlled testing of the product, paid pilots on a limited number of desktops, paid large-scale pilots and eventually full purchase and deployment.

When Pelican has established a leadership position in Internet application security, and Dynamic Sandboxing technology is more recognized, it will begin to transition to a "multi-channel" approach to the market in order to reduce its cost of sales. The company's goal will be to have a healthy balance between direct and indirect channels. Pelican assumes that some direct sales will always be necessary to deal with large corporations desire to purchase direct from the vendor. However, indirect channels such as OEMs, VARs, and distributors can provide a more cost effective way to market Pelican's products and a gain wider "footprint" which will allow to reach a broader customer base.

One of the company's first priorities will be to establish strategic relationships with possible OEM partners such as security software vendors, systems software vendors, application software vendors, hardware vendors and large consulting companies. OEM partners will enable Pelican to leverage its technology across a wider customers base while giving the company increased credibility. The company believes that there is significant opportunity to bundle its Dynamic Sandboxing technology with other vendor's products or to grant non-exclusive licenses to use its technology as an embedded component of another vendor's hardware or software solution.

Examples of potential partners:

- System software and hardware vendors: IBM/Tivoli, Microsoft, Sun, HP, Compaq, Dell, Gateway, BMC, CA, Bullsoft, etc.
- Security software vendors: ISS, RSA, Symantec, Network Associates, F-Secure, e-Security, Content Technologies, Tumbleweed, etc.
- Application software & content vendors: AOL/Netscape, Bloomberg, Siebel, etc.
- Consulting companies: Big Five, SAIC, Global Integrity, Booz-Allen, CSC, etc.

The company's next priority will be to establish strategic relationships with value-added resellers (VARs) who provide Internet security solutions. Before Pelican can embark on this course of action it will need to have established referenceable customer base and the infrastructure to support VARs. VARs can bundle Pelican's technology with other products or services to create a more comprehensive solution for the customer. VARs will also enable Pelican to reach additional market segments that would be difficult or not cost effective for a direct sales organization. Examples of this type of partner would include Checkpoint resellers like Network Access Solutions, Qwest, and Uunet/MCI.

VARs will also allow Pelican to reach corporations outside the North American market. The company's initial foray into the European and Asian markets will likely be through VARs whose primary focus is on Internet security solutions. This will require an expansion of the company's support infrastructure and modifications to its product in order to support other languages besides English. In many cases the right international VAR will take on the international language modifications in return for special considerations in the distribution of the products.

In recent discussions with its corporate customers Pelican has received indications that there may be a market need for a single-user or consumer version of SafeTnet. While the company intends to remain focused on establishing Pelican SafeTnet in the corporate market, it may choose to offer a

consumer version of the product. However, a consumer version will require completely different sales and marketing approach as well as some modifications to the desktop agent.

Initially Pelican will market the consumer product through the Web using Web-based advertising and email promotion. Early customers for a consumer product might also include users of the corporate product who want to have a similar solution on their home computers.

Pelican intends to explore the possibility to use strategic partnerships as another way to reach the consumer market (for example through OEMs). Not withstanding the above, a consumer product is a secondary strategy, which cannot take away from our primary mission of selling to the corporate market.

Product Strategy

Pelican's product strategy is to dominate the client-side Internet security market by providing advanced products which deliver security functionality missing from the Windows operating system. The first step in that process is to establish the Company's implementation of application level access control (Dynamic Sandboxing) as the preferred solution to the Internet code problem. This problem provides a compelling reason to deploy the technology and gives us a foothold in corporate accounts.

However, Pelican's vision is that application level access control is a solution to a wide range of Windows security issues. The fundamental problem that application level access control solves is that Windows (including Windows 2000) cannot distinguish between an authorized user at the keyboard and an application executing on the user's behalf. Any application executing under the Windows operating systems (client or server) runs with all the user's rights and privileges. This problem is virtually unique in the computer industry. Almost all other operating systems (MVS, VMS, Unix, etc.) support application level access control either natively or through third-party add-on software.

Pelican plans to release additional products that use the same basic application level access control architecture as Pelican SafeTnet. Future uses of application level access control might include an independent access control "wrapper" around off-the-shelf or custom client applications. This access control wrapper would enable the customer to determine what resources the client application can and cannot access independent of the user's rights and privileges.

For example, AOL Instant Messenger has met with limited success in the corporate market place largely because of security concerns. Using Pelican's

application level access control technology we could create an independent "wrapper" around Instant Messenger that would allow the corporation to determine exactly what resources the Instant Messenger application could have access to. This would benefit AOL by making Instant Messenger more attractive to corporate customers and would benefit the corporate market place by making their networks more secure.

Other applications of the Company's technology might include securing eCommerce applications running in a Windows environment. There are products on the market today that provide add-on security for eCommerce applications, but these products are still based on server-side security, not client-side security. For example, the Company's technology could be used to wrap a client application (which may actually be a downloaded ActiveX control) in an access control layer that would restrict the resources the application could access on both the client and the server. This would create a more flexible and secure eCommerce applications.

Pelican believes that products of this type may have a higher perceived value to the customer and therefore may command a higher per unit sales price then the SafeTnet product. In addition, there is virtually no competition for Windows application level access control products, the Company would have the market mostly to itself.

Competition

There are two basic approaches to solving the malicious Internet code problem: Reactive solutions and proactive solutions. Antiviral vendors and content filtering vendors are reactive solutions because they can respond to new threats only after they have already occurred. Sandboxing and Microsoft's Authenticode are proactive solutions since they can prevent new types of attacks before they can cause any damage.

The antiviral market is a well established and dominated by two major players – Network Associates (McAfee) and Symantec (Norton), which together have 70% of the antiviral market. The content filtering market is relatively new with several vendors jockeying for position. Authenticode is a Microsoft technology and, while it is touted by Microsoft as a general-purpose security solution, it has not been adopted by many other vendors. Sandboxing is an emerging market with three vendors currently selling Sandboxing products: Finjan, Aladdin (eSafe), and Pelican Security.

Antiviral

Antiviral technology has been around almost since the advent of the PC and has been fairly effective against conventional viruses that are spread through infected floppy disks. However, antiviral technology has not proven to be a reliable solution to the malicious Internet code problem. Antiviral products did not initially detect malicious Internet code such as Melissa and ExplorerZip (and their variants), and it was days before they were able to provide the updates to their antiviral definitions. Virtually all of the corporations that were crippled by recent attacks like the Love Bug worm were running the latest antiviral software.

Network Associates (through their McAfee subsidiary) and Symantec (through their Norton subsidiary) dominate the antiviral market with over 70% market share[11]. Since antiviral vendors collectively have over 90% penetration in the corporate market their business model no longer relies on sales of software licenses. Instead these vendors charge their customers a "service" fee or subscription for access to the latest virus definitions. McAfee has carried this one step further in creating McAfee.com that uses an Application Service Provider (ASP) model for generating revenue. Analysts estimate that it costs corporations approximately $30 per user per year for the antiviral vendor's

[11] ICSA research

service fees and internal costs associated with keeping the virus definitions up-to-date[12].

Although the major antiviral vendors are large software companies with significant resources at their disposal, Pelican Security doesn't believe their current technology is competitive to Pelican's Dynamic Sandboxing technology.

The pattern matching approach used by the antiviral vendors is orthogonal to Pelican's approach. Antiviral products attempt to determine if a given piece of code is "good" or "bad" based on how similar it is to a known example of "bad" code such as a virus. Pattern matching limits antiviral vendor's detection capabilities to attacks that have occurred before. If a malicious code attack has not been seen before, the antiviral software will not detect it.

In addition, not all "bad" Internet code is a virus and not all "good" Internet code is safe to run. SafeTnet's Dynamic Sandboxing approach instead controls what the Internet code can and cannot do. The downloaded program in question may or may not be "malicious". It may in fact be a virus, worm or Trojan horse. Or it may be a legitimate piece of code that is simply trying to do something that violates corporate security policy. In either case Pelican SafeTnet will block any action that is in violation of the security policy whether or not the code is a virus. In this sense SafeTnet is "anti-hacker" instead of "anti-virus".

The key difference between Pelican SafeTnet and antiviral products it that antiviral technology is inherently reactive while SafeTnet is inherently proactive. Antiviral products depend on scanning files and comparing the pattern of that file to the pattern of a known virus. This means that the antiviral vendors must have seen the virus beforehand in order to capture the signature of the virus. Once they have the virus signature, they can then detect other instances of the same virus code. The after-the-fact nature of antiviral technology makes it ineffective against new types of attacks.

> "New viruses are discovered at the rate of over 300 per month. Many of these are not detected using the older DAT files [signature files]"[13]

Antiviral technology is also unsuccessful against variations on existing threats. Since changing the virus, encrypting it, or simply compressing it with one of the innumerable compression tools (such as WinZip) can easily alter the pattern of a file, the virus scanner may not detect the new pattern. Symantec, a leading vendor of antiviral products, acknowledges this problem in a recent article:

---

[12] Gartner Group

[13] McAfee Web site

> "Symantec believes that the [Wall Street brokerage firms] were hit by a new version of ExplorerZip that appeared late last week. The only difference was that the virus arrived as a compressed file, so existing virus scanners could not catch it"[14]

Of course the antiviral vendors are aware of this limitation and in recent years have begun to supplement pattern recognition with what they call *heuristics*. Heuristics are a set of rules for determining if a piece of code is a potential virus; they do so by judging how similar the pattern is to known virus code. These rules are static (they are set in advance by the vendor) and tend to give a lot of false positives. At best, heuristics are guesses at whether the mobile code is good or bad, and because the rules are based on known viruses, it is still a reactive approach.

> "The problem with anti-virus software is that it's inherently reactive. We have artificial intelligence for identifying viruses, but virus writers are good at getting around heuristics."[15]

However, the biggest problem with antiviral technology is that it is only designed to detect and remove viruses; it is not designed to control access to eBusiness resources by Internet code. Antiviral products can only block the code completely or allow it to run, they cannot provide granular access which would allow authorized mobile code to have legitimate access to protected resources while restricting the access of unauthorized or malicious code.

Content filtering

The content filtering market is relatively new with several vendors jockeying for position. The best known vendors include the major antiviral players, Network Associates and Symantec, but also include lesser known vendors such as Trend Micro and Content Technologies.

Content filtering technologies work at the email or Web gateways and attempt to "filter" undesirable content such as malicious mobile code, hate speech or pornography. Content filtering solutions are attractive solution to the malicious Internet code problem because they promise to block malicious code at the enterprise perimeter and prevent it from entering the network at all.

---

[14] Vincent Weafer, director of Symantec's Antivirus Resource Center "Investment banking firms fall victim to virus", CNET News.com, November 30, 1999

[15] Dan Schrader, Vice President of New Technology at Trend Micro, Inc. quoted in ComputerWorld

However, content filtering for malicious mobile code is at best only a partial solution. To detect malicious mobile code, the content filtering gateways rely on the same pattern recognition approach as desktop-based antiviral products.

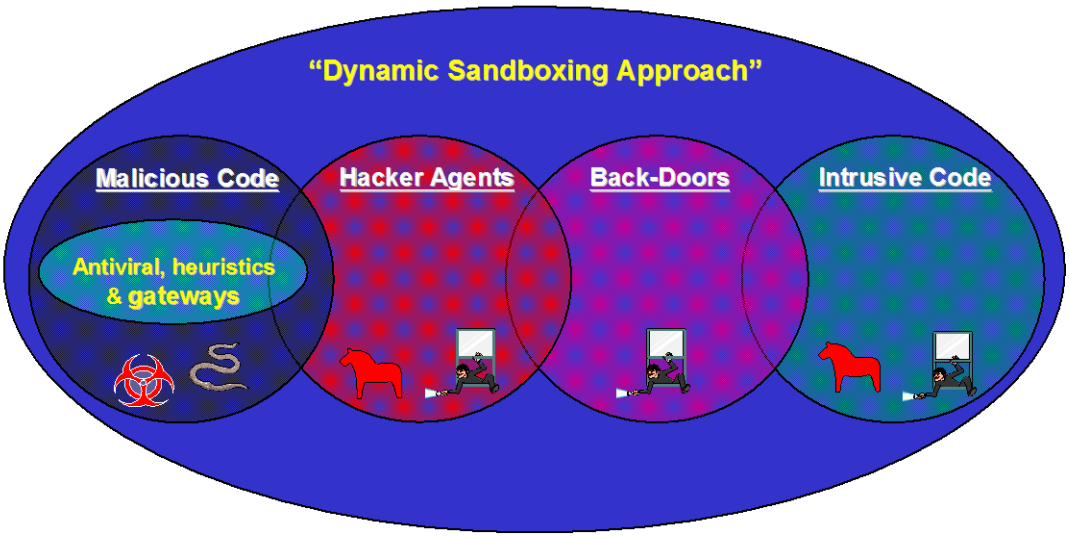
Most email gateways have the ability to run email attachments through an integrated antiviral engine. Internet firewalls can also filter Web content by routing downloaded executables and, in some cases Java applets, to an antiviral engine for inspection. However, since this approach is based on pattern recognition, it is also inherently reactive. While it can filter out well-known threats, variations on old threats and new threats can pass through the filtering process. Content filtering is impractical with many common technologies such as scripts embedded in HTML pages, HTML-based email and ActiveX applets. Content inspection at the Web gateway also creates a bottleneck that can significantly increase browser response times.

Furthermore, if the email or Web content is encrypted, content filters cannot recognize even known threats. The use of encryption is becoming wide spread in eBusiness applications. Many Web sessions are now encrypted using SSL. Mobile users often connect to the corporate network using an encrypted VPN "tunnel". There is increasing use of encrypted email or email signed with a digital signature which also alters the pattern of a known virus.

Perhaps the biggest reason why content filtering is only a partial solution is that the concept of a clearly defined enterprise perimeter is a myth. Because of mobile users and extranet partners, there is really no clearly defined boundary to the enterprise. Mobile users of eBusiness applications typically connect to the Internet through a local ISP. The content they download is not scanned by the corporate content filtering gateway and therefore mobile users are exposed to all Internet threats - as though there were no content scanning. By definition, extranet partners are given internal access to the corporate network, yet we cannot control what content enters their network.

Finally, like their antiviral cousins, content filtering solutions only block or allow mobile code, they do not work by controlling access eBusiness resources. Content filtering gateways cannot insure mobile code has legitimate access to some resources while restricting access to others.

Dynamic Sandbox vs Antiviral Positioning



Microsoft Authenticode

Authenticode is Microsoft's approach to mobile code security. Authenticode applies a digital signature to executable programs (such as plug-ins) or ActiveX controls. This digital signature verifies the identity of the author and ensures that the code has not been modified or tampered with since it was signed. Authenticode does **not** guarantee that the mobile code is harmless or benign. It has even been demonstrated that a programmer can get an Authenticode digital certificate for even the most malicious of applications.

In addition, the controls over the level of security, what sources will be trusted, and even the choice to use Authenticode are governed by the end user. The user must make a decision whether or not to accept active content from an "un-trusted" source. Unfortunately, when asked for a response, end users often click away heedless of the potential consequences. Worse yet, end users can turn off the entire Authenticode mechanism leaving no control over what active content is downloaded. While Microsoft has come up with a tool kit that corporations can use to turn off these controls in Internet Explorer, all the user has to do is re-install a new copy to circumvent this configuration.

Surprisingly enough, Authenticode was not designed to work with executable email attachments, Microsoft Office macros, many plug-ins, scripting, and other types of active Internet content. In some cases, VBScript attacks have exploited legitimate, digitally signed ActiveX controls for illegitimate purposes. This was the mechanism used in some of the highly publicized "safe for scripting" attacks in late 1999 and early 2000. The controls that were exploited all had valid Microsoft Authenticode certificates. In the recent high profile malicious code outbreaks including Love Bug, Melissa, Happy '99, and ExplorerZip, none of them were prevented by Authenticode.

Other Sandboxing vendors

Finjan Software Ltd.

Finjan, a venture-backed, Israeli-based software company and was the first to introduce Sandboxing as an approach to the malicious mobile code problem. In 1997 they launched a desktop product called SurfinShield™ that sandboxed Java applets. However that product met with limited market success. In 1998 they introduced a gateway solution that worked in conjunction with a firewall to block malicious Java applets and ActiveX controls. This product had some limited commercial success but is readily confused with antiviral and content filtering products.

While Finjan had the right idea in using access control techniques to solve the mobile code problem, their implementation was flawed. The first versions of SurfinShield worked only with Java and ActiveX. While Java and especially ActiveX presented a serious theoretical security threat, there were few if any real world examples of malicious Java and ActiveX code. The first serious mobile code threats to emerge were Microsoft Office macros (such as Melissa), executables (such as ExplorerZip), and scripts (such as the Love Bug). SurfinShield provided no protection against these threats. The most recent release of SurfinShield has added limited support for executables but still doesn't support macros or scripts. Statistically macros and scripts are the most common types of mobile code exploited by hackers representing 80% of all mobile code threats[16].

In addition, Finjan's method of sandboxing replaces Windows system files and modifies applications such as Internet Explorer. This means someone running SurfinShield is no longer running a standard version of Windows or IE, but rather a modified variant. Because a Finjan customer is running a proprietary version of Windows, supporting a PC running Finjan's products is virtually impossible.

[16] "Fifth Annual ICSA Labs Computer Virus Prevalence Survey: 1999", ICSA, 1999

Because of this, most large organizations reject implementing software that modifies the operating system. The company believes this has been the most significant barrier to the acceptance of Finjan's products and will present a serious sales obstacle in the future.

Aladdin (eSafe)

Aladdin Knowledge Systems inc. is a publicly traded (NASDAQ:ALDN) software company based in Tel Aviv, Israel. In 1998 Aladdin acquired another Israeli company called EliaShim whose U.S. subsidiary was known as eSafe Technologies Inc. EliaShim was an early antiviral vendor with limited market success in some parts of Europe. In 1997 they introduced a sandboxing product for Java and ActiveX called eSafe Protect.

ESafe Protect was initially targeted at a consumer market. The product combined sandboxing for Java and ActiveX with the EliaShim antiviral product and a crude personal firewall. Because it was designed for a single user, it had no central administration and management capability. It also was very intrusive with a management interface that was too complex for a home user. The product met with limited commercial success due to the fact that Java and ActiveX never materialized as a significant security threat and other antiviral products were easier to use, less intrusive, and were more frequently updated.

In 1999 they introduced a version targeted at the corporate market called eSafe Enterprise. It appears as though this product might have been afterthought since they tried to retrofit the consumer product rather then develop a new version. The client software retains its intrusive user interface (lots of dials, buttons and flashing lights) and is still focused primarily on mobile code downloaded by a Web browser. Sandboxing of email attachments is not automatic and they do not sandbox scripts and Microsoft Office macros. They did add central deployment, central administration of security policies, centralized collection of audit events, but the design is not scalable to a large enterprise.

eSafe Enterprise is a much weaker product functionally then Finjan's because sandboxing of downloaded executables is manual, not automatic. However, the biggest drawback to eSafe's product is the built–in antiviral scanner. Most corporations have already made a commitment to an antiviral solution and find this functionality to be redundant. In most head to head competitions at customer sites, eSafe usually comes in behind Finjan's SurfinShield. While the Company does compete aggressively with Finjan, it almost never runs into eSafe as a serious competitor.

Competitive Summary

	SafeTnet	Desktop Antiviral	Gateways	Finjan	eSafe
Blocks known viruses, worms & Trojan Horses	Yes	Yes	Yes	Yes	Yes
Blocks unknown viruses, worms & Trojan Horses	Yes	No	No	Partial	Partial
Control access to critical resources by macros	Yes	No	No	No	No
Control access to critical by scripts	Yes	No	No	No	No
Control access to critical resources by executables	Yes	No	No	Yes	Manual
Control access to critical resources by Java	Yes	No	No	Yes	Yes
Control access to critical resources by ActiveX	Yes	No	No	Yes	Yes
Access control by policy	Yes	No	No	Yes	Partial
Works without modifying the operating system	Yes	Yes	N/A	No	Yes
Centrally administered policy	Yes	Partial	Partial	Yes	Yes
Central logging and alerting	Yes	Partial	Partial	No	No
Integrated with enterprise management systems	Yes	Partial	Partial	No	No

Executive Team

Irit Rapaport, co-founder and chief executive officer

Irit Rapaport is the co-founder and chief executive officer of Pelican Security. With over fourteen years' high technology experience, Rapaport oversees the strategic direction of the company.

Prior to co-founding Pelican Security, Rapaport has been a director of business development in ELISRA Holdings Ltd. Her responsibilities included; pioneering and leading the process of creating ELISRA Holdings Ltd.-the spin-off of several start-up companies from ELISRA- finding and assessing new investment opportunities and negotiating and managing private placement agreements within Israel and the United States. She was also responsible for negotiating OEM contracts and strategic large sales accounts.

Prior to ELISRA, Rapaport held the position of vice president of marketing and strategy at ULTRAMIND. In this position she negotiated contracts with distributors and marketing and sales firms within the United Kingdom and Israel. Rapaport also co-managed private placement and financing strategies for the company.

Beginning her high technology career with the Israeli Defense Forces, Rapaport led the Army's fiber optic communications programs as program manager of the Signal Corps. Her responsibilities included managing commercial contractors, defining system specifications as well as issuing requests for proposals. She received an honorary discharge as Captain.

Rapaport holds a B.Sc. degree in Electrical and Electronic Engineering from Tel Aviv University. She also holds a M.B.A. from Institut Europeen d'Adminsitration des Affaires (INSEAD), Fontainbleau, France.

Gilad Golan, co-founder and chief technology officer

Gilad Golan is the co-founder and chief technology officer of Pelican Security. With over ten years of high-technology experience, Mr. Golan is responsible for the company's strategic technical direction.

Prior to Pelican, Golan co-founded Menta Software, an application server that allows remote users to connect and use applications that execute on LAN-based servers. Prior to Menta Software, Golan held the director of business development position at CommTouch Software, a developer of e-mail client solutions for the Internet. While at CommTouch, Golan played a key role in

product design and development. He maintained full responsibility for product marketing, including strategic partnership management with ComTouch's distributors and OEMs.

Previously, Golan served at the National Semiconductor in Israel as the product applications manager for Voice Products. In this position he developed voice processing product lines and leading compiler optimization techniques. In addition, he worked in the company's Munich office in the marketing center as a Staff Engineer and provided expert support to major European customers.

Golan holds a B.S. in Computer Science from Technion, Israel Institute of Technology.

Pete Privateer, president

Pete Privateer is the president of Pelican Security. Privateer has over twenty years of experience in the software industry with an extensive background in high-tech and Internet/network security and a solid track record in building successful startup companies. At Pelican Security he is responsible for the overall strategy and operation of the company.

Prior to Pelican, Privateer co-founded and held the position of senior vice president of operations at AXENT Technologies (AXNT). While in this position he led the company's profitable transformation from a VMS utility product company into a $100+ million computer security company. Prior to AXENT, Privateer was one of the original employees of KnowledgeWare where he was responsible for the overall strategy and vision. Through his efforts, KnowledgeWare developed into a $140 million publicly traded company that was eventually acquired by Sterling Software in 1994.

Privateer graduated with a Bachelor of Science in Physics from The University of Florida.

Risk Factors

Short Operation History

The company was founded in the beginning of 1997 and had no previous operating history. The company will have to undergo a quick growth and expansion in order to achieve its goals.

Competition

The company plans to gain a leading market position using its unique technology, protected by intellectual property laws. Competitors may try to achieve similar functionality using a different technology that does not infringe the company's rights.

Different approaches exist today to the problem of Internet application security. There is no assurance that the company's proposed solution will be adopted by the market. In addition, some of the companies competing with Pelican Security have greater financial resources.

Development Risks

The company has a product in limited availability stages; however, significant research and development efforts are still needed. Software development schedules are notoriously volatile, and product release dates may slip. Time to market is a crucial element of success in today's dynamic software environment. If the company doesn't complete its product offering fast enough, its chances to succeed might be impaired.

Market acceptance of the product

The field of Internet application security is still at its early stages. In spite of the growing concerns in corporations to various security issues, a significant PR and marketing effort will be needed in order to educate the market. The company believes that it can greatly benefit from previous efforts made by companies such as Finjan and other organizations concerned with the issues of network security. Still, there is no assurance that the market will accept the company's products.

Dynamic Security Market

The market for security products is at an early stage of development. The awareness and need for such products is a recent phenomenon. As the market for Internet application security products is only beginning to develop, it is difficult to assess the size of this market, the appropriate features and pricing structure to address the market, the optimal distribution strategy and the competitive environment that will develop. Failure of the security market to grow or failure of the company to properly assess and address such market would have a material adverse material adverse effect on the company.

Intellectual property and Proprietary Rights

The company relies on its technology for the success of its plan. The company will protect its technology by international patents whenever necessary. If the company's application for patent otherwise fails to protect the company's technology, it is exposed to greater competitive risks.

Dependence on Key Employees

The company depends on several key employees for the execution of its business plan. Unplanned termination of employment by any of them may adversely affect the timely execution of the plan.

Financials

Quarterly Profit & Loss - Q1 & Q2 2001 Actuals & Q3-4 2001 Projected

	Q1/2001		Q2/2001		Q3/2001		Q4/2001		Total 2001	
	K$	% of Revenue	K$	% of Revenue	K$	% of Revenue	K$	% of Revenue	K$	% of Revenue
Worldwide Product Revenue	**$340**	100%	**$12**	100%	**$300**	100%	**$600**	100%	**$1,252**	100%
Cost of goods	$8	2%	$8	67%	$8	3%	$8	1%	$32	6%
Gross Margin	**$332**	98%	**$4**	33%	**$292**	97%	**$592**	99%	**$1,220**	94%
R&D	$741	98%	$500	33%	$450	97%	$450	99%	$2,141	43%
Sales & Marketing	$882	259%	$500	4167%	$400	133%	$450	75%	$2,232	71%
G&A	$287	84%	$250	2083%	$225	75%	$250	42%	$1,012	17%
Total Expenses	$1,910	562%	$1,250	10417%	$1,075	358%	$1,150	192%	$5,385	131%
EBIT	**-$1,578**	-464%	**-$1,246**	-10383%	**-$783**	-261%	**-$558**	-93%	**-$2,492**	-37%

Three Year P&L Projections

	2001		2002		2003	
	K$	% of Revenue	K$	% of Revenue	K$	% of Revenue
Worldwide Product Revenue	**$1,252**	100%	**$7,000**	100%	**$15,000**	100%
Cost of goods	$32	3%	$140	2%	$300	2%
Gross Margin	**$2,218**	177%	**$6,860**	98%	**$14,700**	98%
R&D	$2,141	171%	$2,350	34%	$3,150	21%
Sales & Marketing	$2,232	178%	$3,250	46%	$5,975	40%
G&A	$1,012	81%	$1,125	16%	$1,625	11%
Total Expenses	$5,385	430%	$6,725	96%	$10,750	72%
EBIT	**-$2,492**	**-199%**	**$135**	**2%**	**$3,950**	**26%**

Management discussion of financials

The above figures represent the consolidated financials (in U.S. Dollars) for both Pelican Security Ltd. and the subsidiary Pelican Security Inc. The first and second quarter figures represent actual revenue and expenses. The first quarter of 2001 was the first quarter in which significant revenue was booked. Revenue figures for Q3-Q4 2001 are projections based on the current prospective customers in the sales pipeline.

Product revenue shown above is from software license sales and maintenance only. The company has assumed no revenue from consulting fees. Software license sales are assumed to come from only one product, Pelican SafeTnet, the company has not built in revenue assumptions from future products into this model. Revenue recognition will follow the U.S. Federal Accounting Standards Board (FASB) guidelines for revenue recognition in a software company.

Projected product revenue is dependent on meeting product development milestones, having customers willing to deploy large numbers of licenses, and early customers that are willing to act as references to future customers. Failure to meet product development objectives or customer objectives will likely result in

a slipping of product revenue into a future quarter or may result in lost sales altogether.

Maintenance is bundled with each software order and is priced at 15% of the current list price prior to any discounts. Pelican assumes that maintenance will be approximately 18% of the software license sale on average. Maintenance is recognized at 1/12 per month starting from the third month of the sale (the first three months of maintenance are included free of charge) in accordance with FASB guidelines.

The cost of goods line includes the actual cost of the production of the product (CD, packaging, documentation, etc.) and the cost of post sale support.

License fee revenue is assumed to come 100% from direct sales in 2001. All revenue from indirect sales is assumed to be booked as net to the company. No royalties or commission will appear in the cost of sales line item even if substantial future sales result from indirect channels.

R&D expenses reflect only the costs for development and maintenance of the current Pelican SafeTnet product line and do not reflect cost for development of additional products.

In April of 2001 the company substantially reduced it expenses through substantial cuts in R&D, Sales and Marketing and G&A. The reduced expenses are reflected in the Q2-Q4 expense numbers.