

NOTES for the Melior Barbican RNP CyberWarfare Defense Presentation

Explanations, Background, and Guidelines
for your presentation of Melior, Inc.
and the Barbican RNP CyberWarfare Product

January 2005

*(Optional side comments and recommended instructions for the presentation
are shown in the NOTES section in italics)*



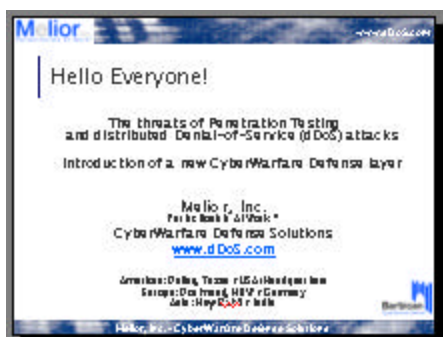
Slide 1 of 24

[PREVIEW DISPLAY SLIDE]

... showing Melior's Mission Statement and summary track record before entering the dDoS market with the new, flagship Barbican RNP product.

Show this slide on-screen, while everyone in attendance is waiting for the presentation to begin.

www.dDoS.com



Slide 2 of 24

[HELLO AUDIENCE - INTRODUCTION SLIDE]

Introduce yourself, your relationship with Melior, and the company itself. Melior is a privately held US company, incorporated in Delaware, USA, with representations in Europe (Germany) and India.

*Note: *all* software development is performed in the United States; the office in India is for this specific market only (Government relations in a proprietary, and highly regulated market).*



Slide 3 of 24

[PRESENTATION OVERVIEW]

With this presentation, I will walk this audience through:

- ❑ the background of Melior, Inc. (*who the company is, why it develops CyberWarfare Defense solutions, and why this company is uniquely qualified to develop such break-through new technologies*),
- ❑ will explain the threats against which Melior defends, explain development and key differentiators,
- ❑ demonstrate the application of the new CyberWarfare Defense layer,

www.dDoS.com

- ❑ show in examples how and where to deploy the defenses,
- ❑ prove where the product is currently in use (examples),
- ❑ talk about the competition (*to set the record straight against the unsubstantiated marketing fluff of other vendors*),
- ❑ provide an outlook on further product development,
- ❑ and conclude with an outlook (*teaser*) of the next generation of Melior CyberWarfare Defense Solutions - against other forms of Denial-of-Service conditions (such as eDoS).



Slide 4 of 24

[ABOUT MELIOR, INC – THE HISTORY - COMPANY BACKGROUND]

Founded with the name „support@tjack.com“ in Münster, Germany, in 1987, at a time when „bang“ (!) style addresses were still commonly used on the Internet, and re-incorporated in Delaware, USA, in 1996, Melior (*latin: „better“*) provided high-end security consulting services to Fortune 100 companies, as well as to Silicon Valley start-ups during the „hey-days“ boom of the Internet.

The larger clients were Bank of America during the merger with Nationsbank (California, 1998), as well as Turner Construction and its German parent company Hochtief AG (Turner in Dallas and New York, USA, and Hochtief in Essen, Germany).

Among other „firsts“ in technology (such as the first „POP“ replication site, mirroring US web-data on servers located in Europe and Asia, *or installing and operating the first free public wireless network in Dallas, Texas*), Melior developed two prototype wireless war-driving vehicles (Truck, California, 1999, and Van, Texas, 2002) for mobile encryption-breaking demonstrations, which were used alongside Melior's own Cray CS6400 Supercomputer and cluster computers.

www.dDoS.com

As part of the consultancy services, the question of how to defend against dDoS attacks was frequently posed to Melior, prompting the initial exploration of available technologies.

Then the first large-scale, and very public Denial-of-Service attack occurred. After the earlier 1999 „Mafiaboy“ attack, performed by a 17-year-old Canadian youth, thus causing outages for several days at CNN, Yahoo, Dell, and several banking institutions, the Internet „root“ servers, providing the key DNS backbone infrastructure, were attacked with a simple ICMP dDoS attack for 5 hours --- twice, on October 21st and 22nd, 2002.

This attack was carefully orchestrated and timed, in order not to exceed the DNS caching timeouts, and demonstrated for the first time that dDoS had become a serious infrastructure risk for the entire Internet, and all the economies increasingly relying on it. Had these attacks lasted longer, the entire global DNS service would have broken down, thus taking down the global Internet.

This event, and the absence of any promising developments of technology to defend against those attacks, prompted Melior to change the company strategy from a service- to a product business, and to begin developing dDoS defense solutions.

Pre-production products were implemented at sites under dDoS attacks as early as summer 2003 (more on those successful defenses later in the presentation).

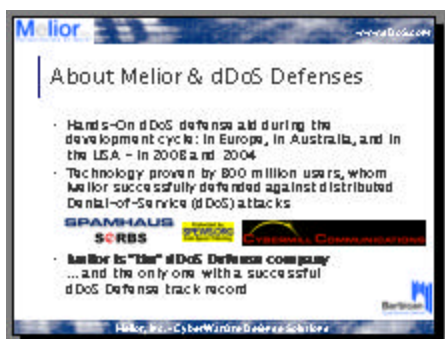
At the RSA Security conference and show in San Francisco, February 2004, Melior made the first public appearance as „the“ CyberWarfare Defense company, when Melior introduced the first, at the time TCP-only, productized technology under the project name „iSecure“.

This new technology was later introduced to the Asian market -in June 2004- at the Networld + InterOp Conference and show in Tokyo, Japan.

In November 2004, Melior announced the full-featured flagship product – Barbican RNP - under the permanent product line name „Barbican“ (referring to the medieval term for a fortification of a gate or gateway – i.e. a firewall), which concluded the initial development cycle for the complete CyberWarfare Defense technology, covering TCP, UDP, and ICMP on OSI network layers 2 and 3, and featuring improved reporting and remote administration capabilities (more on actual attack protection and features -with details- to be discussed later in this presentation).

As of January, 2005, the company is shipping the Barbican RNP (Realtime Network Protection) product.

By the way, the „gate“ part of the Barbican logo purposely reflects the logo of the city of Münster, capital of Westfalia in Germany, to which Melior traces back its origin in 1987.



Slide 5 of 24

[ABOUT MELIOR & DDOS DEFENSES – COMPANY BACKGROUND WITH DDOS EXPERIENCE IN THE FIELD]

During the dDoS technology development cycle, Melior shared news about the project on it's web site (*mostly, to raise additional funding*), but did not otherwise advertise the effort.

In this time, large-scale dDoS attacks were in progress, and the company was contacted often to see if early versions could be used in the defense against those attacks.

One such company (*CyberMill*) ran a popular website (*www.facethejury.com*) with about 2 billion hits a year, and dDoS attacks against this web site impacted their entire online presence. After this ISP had exhausted all other products claiming to defend against dDoS, they turned to Melior, and deployed the first pilot project in Summer 2003. At the time, the code only supported TCP-based defenses, and it turned out to be a good match; the pilot successfully defended against the attack.

In fall 2003, the spammers, which by that point were mostly organized crime, felt that the seven anti-Spam black lists had done enough damage. Their databases of known spammers - used by many governments, universities, and large corporations – allowed for the elimination of about 40% of spam: these blacklisters collect fresh new Spam, identify the sources, and make this data

www.dDoS.com

available for public use in their databases. Customers can configure their mail servers to compare the sources of incoming Spam against these databases, and in turn discard a large number (average: 40%) before it even reaches the intended addressee (*though this is far from being perfect, it is a reliable solution to eliminate a portion of Spam; many anti-Spam vendors use these databases as part of their product set*).

Organized Crime groups, which make a legal profit from Spam, decided to team up with virus-authors, and launched a large-scale dDoS attack (*i.e. „MyDoom“ virus*); the quickly spreading virii took over hundreds of thousands of PCs, formed a huge „bot“ network, and then simultaneously attacked all seven anti-Spam blacklists. Once the attack commenced, all seven went instantly down, and remained inaccessible. Many customers, most notably the US Federal Trade Commission (FTC) did not receive any mail for a day, until they had re-configured their mail servers to no longer compare against the databases, and thus to permit 100% of Spam into their networks. Six out of those 7 blacklists were non-profit organizations, and immediately faced enormous ISP bills, since their traffic pipes were instantly maxed out to the full „burst“ capability, resulting in high monthly bills, which they were simply unable to afford. As a result, three of them shut down permanently, and Melior offered its technology in development to help defend against the attacks.

London-based Spamhaus, the largest of these blacklists with about 260 million users world-wide, and Melior decided that the best way to approach the issue was for Melior to host the Spamhaus online presence, since Melior needed to apply a lot of beta-stage code in the defense, enabling the company to „babysit“ the hosting locally in Dallas. This was a mutually beneficial solution, as it gave Spamhaus a focused and dedicated team to deal with the dDoS attacks, and for Melior, to gain „real-life“ experience with the code in development, and how well it did under dDoS attack.

Besides a few hiccups, this defense was successful, and after many attempts with altered attacks, the Spammers finally gave up (*more information and traffic graphs are available on the Melior website at www.dDoS.com, under „Product History“*). Melior sent units to SORBS and SPEWS in Brisbane, Australia, and US locations, and undertook many other measures to aid in their dDoS defense; as a result, both of those are also still around and serve a minimum of 40 million customers.

Melior offered the same support to Microsoft, when they faced the MS Blaster dDoS attack, threatening their Windows Update domain (prompting even an advisory from the Department of Homeland Security). Microsoft decided to give

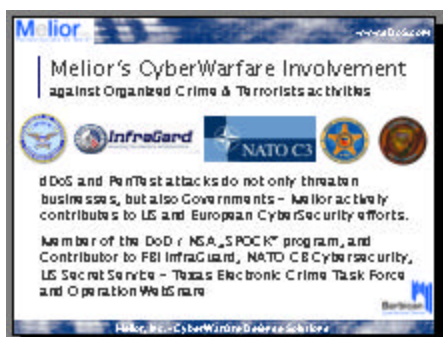
www.dDoS.com

up the targeted domain name instead – moving their hosting to Linux-based Akamai only helped to distribute the patches for the vulnerability exploited by the attack – any additional dDoS traffic would have tipped over even the mighty (and costly) Akamai network.

Had the attack not targeted „windowsupdate.com“, but „microsoft.com“, this story would have been very different.

With this hands-on experience, the code improved drastically, and Melior is the only dDoS defense product vendor with active engagement in the defense against large-scale Denial-of-Service attacks in the real world, and remains to be the only company, which can claim its products actually work!

(Demonstrating with these successful defenses, that Melior was indeed in the process to develop a truly unique, new technology, and not yet another hyped-up start-up with little substance, also attracted a lot of talent to the company).



Slide 6 of 24

[MELIOR'S CYBERWARFARE INVOLVEMENT – WITH GOVERNMENT ENTITIES IN THE US AND EUROPE]

Very early on, Melior recognized that such large dDoS attacks can not only be targeted against commercial sites for the extortion of money, but also be used in political plays.

During the Iraq conflict, arabic news sites (Al Jazeera) were shut down by Denial-of-Service attacks, and the previous Internet Root Server attack in October 2002 also demonstrated, that a dDoS attack on the entire Internet would affect more than just the economies relying on the communication channels the Internet provides.

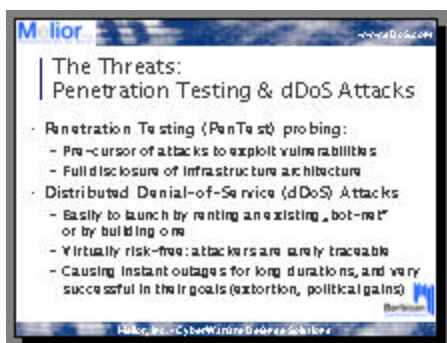
A January 2005 report by the National Intelligence Council on future threats also expects a wide-spread Internet outage caused by terrorists, and thus by political motivation.

In retrospect, the 9/11 attacks were terrible, but the biggest damage was done by the economic slump folloing the attacks; a much easier to accomplish dDoS attack on the Internet would cause a much larger damage, and would not be isolated to the US; but take a large economic toll mostly on the Western World, whose economies depend a lot more on Internet communications than others.

Consequently, Melior engaged with many government agencies around the world to share our goal; with the exposure of successfully defending the anti-Spam blacklisters, Melior also gained attention from the „bad guys“, whose contact and intentions the company instantly reported to the appropriate government channels in each country.

As a US company, Melior naturally does work a lot with US Federal and State Agencies; however, being privately held and with a global focus to introduce a new CyberWarfare layer to network and application security, the company has made an effort to spread government involvement to other countries and NATO as well.

Consequently, Melior was able to send early reports to the US Secret Service, which contributed to the Joint Task Force „WebSnare“, and several other, similarly successful cybersecurity law enforcement issues.



Slide 7 of 24

[THE THREATS – PENETRATION TESTING AND DDOS ATTACKS]

Melior believes Penetration Test probing and Denial-of-Service attacks must be considered in conjunction.

www.dDoS.com

Penetration Testing (PenTest) – or vulnerability probing – can be done very easily, with powerful and free tools, such as NMAP or Nessus (or many others). There is no other viable technology available, which prevents this information from disclosure; any firewall permits traffic, like a Swiss cheese, to go through the permitted TCP ports, and explore what it behind it.

These tools can identify the hardware being used (by the MAC addresses), operating systems, applications, security measures, the number of systems in use, etc. – any system administrator actually looking at firewall and Intrusion Detection System (IDS) logs can tell how many of these probes are being observed every single day.

If run from an internal source within a network, the gathered information is even richer, as few security barriers exist within any network.

With this information, any attacker with malice has a perfect roadmap to identify the best targets; public „bug lists“ provide all the known vulnerabilities, and the attack tools to exploit them are also easily available, due to the powerful search engines and extensive hacker networks for the advanced perpetrator.

Equipped with the roadmap, an increasingly common form of taking advantage of such vulnerabilities is to launch a Denial-of-Service attack. These attacks are surprisingly easy to launch, and bear very little risk of exposure and accountability for the attacker.

dDoS tools are easily available on the Internet; in most cases, the attacker compromises a number of systems with low security settings on the Internet (home PCs running a Windows operating system on a high-speed connection are the ideal target) to form a „bot-net“, or bypasses this step by simply renting one (estimates assume about a million of such bot-nets exist, and up to 70,000 PCs are being taken over each day to be added to them – data from two different studies, as of late 2004).

For the attacker, this approach is virtually risk-free. Most dDoS attacks are launched with tools, which modify the source (thus breaking TCP/IP protocol rules), so that at the target site the „sender“ address is incorrect (*this process is called „spoofing“*) and eliminates the option to simply exclude the source: each attack packet has a different sender address embedded, even though it comes from the very same computer in each bot-net.

These „bot-nets“ are then instructed with a single command to attack a target, which then goes down almost instantly.

www.dDoS.com

As a result of some of these targeted attacks, pretty much all British online betting companies, for whose revenue 100% uptime is critical, are paying extortion fees to organized crime groups, or even petty criminals.

What other choice do they have? The extortion fees are much less than moving the infrastructure to a larger environment, in an attempt to „buffer“ the attacks, in turn only forcing the attacker to rent a larger „bot-net“ and to ask for a higher extortion amount.

If a dDoS attack is mounted for political, non-monetary reasons, there is little to be done, since the attacker cannot be enticed by money, but only by political concessions, which in most cases are out of the question for the party being attacked.

Damages so far have been in the billions, with no viable commercially available defense option in sight.



Slide 8 of 24

[BARBICAN RNP TECHNOLOGY – OVERVIEW OF KEY DELIVERABLES]

With Barbican RNP, Melior set out to develop a technology, which had to fulfill the following objectives with no compromises to be a viable defense:

Real-Time Defense

Instant performance is a critical must to intercept PenTest probes, as well as any form of Denial-of-Service attack. Both large- and small-scale cause damage instantly (within seconds at most), so any product with a viable approach to defend against such attacks has to be able to act instantly.

Low-Bandwidth attacks, which target the TCP/IP stack of any device (such as synk4, synk5, and the „shrew“ attacks), most prudently firewalls, have instant

success with only few packets transmitted – so a successful defense had to validate every single packet, before it has the opportunity to reach the desired target.

This leaves the function as an „in-line“ device as the only viable approach – the product had to get all traffic first, inspect the packet and packet flow for validity, and only if found valid, pass it on to the target host. Any other approach, „observing traffic from the sideline“ – as an Intrusion Detection System does, is doomed by design to fail, as not enough time remains to take successful action (regardless, what this action is). „Bad“ (attack) packets have already reached the target, and more likely than not already accomplished their destructive goal.

This approach to build an in-line appliance has its challenges, as it must not introduce noticeable latency, while inspecting both valid („good“) and invalid („bad“) traffic, nor make any mistakes between valid and invalid packets – one of the reasons why it took three years to develop the technology and test it extensively (Quality Assurance – QA- procedures).

Thus **Barbican Real-time Network Protection (RNP)** is an in-line device, does not disrupt valid traffic, introduces little latency (average under 10 ms), and defends against all attacks described in the attack protection.

True „Zero-Day“ Protection

The product needed to be able to defend against *all* claimed attacks, i.e. Operate without signatures, and not only defend against those attacks, which have been previously observed - for two reasons:

1) Defense Capabilities

If the product would only be able to recognize „known“ forms of attacks, a slightly modified attack or one of those attacks, which defy a description in a signature, would easily bypass the defense layer and limit the viability of the product.

Compare to IDS systems or anti-Virus measures: both operate by design on signatures or libraries; any new attack or virus cannot be alerted to or defended against, since without a new definition, signature, or library, the protection is „blind“.

Consequently, Barbican RNP had to work by itself, without external updates, or a definition of attack signatures; instead, it looks at every single packet without prejudice, and applies its own modular ruleset for decision if any given packet is valid and passed on, or invalid, discarded and reported on.

2) Performance

Besides the stringent reason shown above to operate without definitions of attacks, the time it would take to compare incoming traffic against a growing database of signatures invalidates the approach to make the device work in real-time. Invalid or attack traffic has already passed by and accomplished its goal by the time the comparison process between observed traffic and the database is completed; would the traffic be held during this comparison time, the latency introduced in this process would not be acceptable to any customer, and the memory tables holding the information during this time frame would likely quickly exceed the physical limits of the hardware, or escalate the hardware cost. In addition, keeping such tables in memory makes it easier to compromise the system by attacks trying to exceed the physical capabilities of the device.

For this reason, **Barbican Real-time Network Protection (RNP)** operates as a real-time, in-line device (on average under 10 milli-seconds latency), and without any signatures, thus truly providing zero-day protection.

Safety – Barbican RNP is not compromiseable

In deployment as an inline-device, it is mandatory Barbican RNP must not be a risk in itself. Every firewall is vulnerable, since it can be addressed on its MAC and IP-Address directly, and every single firewall available can be instantly attacked and shut down with TCP/IP stack attacks, which target the core communication.

Barbican, on the other hand, has no MAC nor IP address on its Gigabit ports, through which the „live“ traffic flows for validation. It also does not build any static tables internally, which could be indirectly addressed to disrupt the functionality and access to the protected infrastructure.

Barbican RNP has extra network ports for the Administration and Reporting features, which are only to be connected to a secure network, such as the one, on which IDS systems send their alerts, or Security Administrators maintain other systems, outside of normal user bandwidth and access.

Consequently, **Barbican RNP** does not introduce any additional risk to the infrastructure, by being itself vulnerable. By design, it cannot be compromised in any way, and it has no moving parts (no hard disk drive) which might otherwise contribute to a hardware failure (*High-Availability and High-Redundancy Barbican RNP versions are also coming, see that discussion later in the presentation*).

Barbican RNP is not a „black box“, introducing an „unknown“ factor, giving insight into all traffic flowing through it to Melior or others, in either perimeter or internal network defense deployments. With pending security certifications, including source code reviews, and the ability to verify the code to appropriate (mostly Government) customers – proper legal protection for Melior’s intellectual property rights assured – any such concerns can be easily addressed.

Universal Elimination of Invalid Traffic

Though geared to specifically recognize PenTest probes and dDoS attack traffic, Barbican RNP inspects all traffic by validation of valid („good“) traffic – in essence, every packet deemed „NOT VALID“ is considered bad traffic (*for an analogy: Barbican RNP picks the good peas out of the basket of traffic flowing through it, and ignores all the other peas as bad, thus allowing it to perform in real-time*).

In addition to recognizing and discarding the distributed Denial-of-Service traffic the technology is built for, and recognizing and responding to Penetration Testing probes, though this design Barbican RNP goes a lot further: it also eliminates other, not necessarily malicious, yet still harmful „junk“ traffic (such as ‚jabber‘ from broken Ethernet cards), eliminates useless entries in IDS and Firewall logs (thus making these logs comprehensible for the first time and converting them into useful tools for administrators), and thus „cleans up“ a lot of malicious and non-malicious network traffic, which would otherwise propagate throughout the entire network infrastructure (Ethernet Switches and even routers transport such packets without discrimination across „fat“ pipes as well as smaller bandwidth, WAN-pipes).

A New CyberWarfare Defense Layer

As a result, Barbican RNP offers for the first time an additional layer of protection, which recognizes and intercepts traffic otherwise flowing freely throughout all security measures taken – from both external (public) sources, as well as internally.

Melior has named this new protection the „CyberWarfare Defense“ layer, as the technology incorporated in Barbican RNP truly is, what the name „Barbican“ suggests for the last several hundred years: "a fortification at a gateway or drawbridge on the approach to a castle“.

Though the technology is truly unique, and could command any price, Melior purposely offers each Barbican RNP system at a very aggressive price, to allow deployment of this protection in an affordable manner on a large scale, for the protection of online presences, perimeter defense, and throughout networks

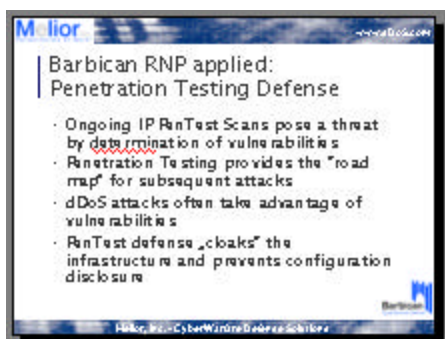
internally.

(But before pricing is discussed, let's first look at the technology itself.)

Instant Operation – Reporting

Barbican RNP does not require a learning curve, configuration, or even a change in the infrastructure. Once unpacked and rack-mounted, existing Ethernet connections are plugged into Barbican RNP (not even extra switch ports are necessary), and Barbican RNP instantly protects: „plug & protect“.

Optionally, an admin and reporting connection can be used, to configure a target host for Barbican RNP to send standard „syslog“ event messages to; most customers have asked for this feature to collect events from multiple units deployed across perimeters and internally, and correlate the data sent from Barbican RNP units and other security systems used in a layered defense architecture.



Slide 9 of 24

[BARBICAN RNP APPLIED: PENETRATION TESTING DEFENSE]

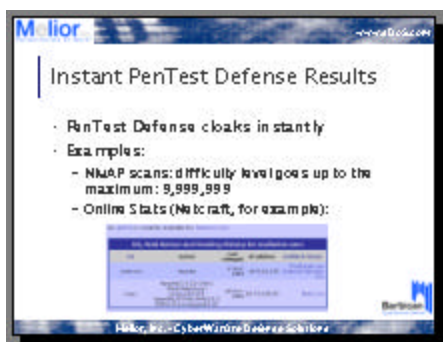
As previously discussed, Penetration Testing and Denial-of-Service attacks need to be considered together. The ongoing scans, as every security administrator knows, provide a scarily detailed map of the probed infrastructure, which in turn is the perfect roadmap for subsequent attacks – dDoS attacks or otherwise.

An active PenTest defense, such as provided by Barbican RNP, essentially blocks all such probes, and thus „cloaks“ the infrastructure, not revealing any information available through such probing.

Of course, this defense must go hand-in-hand with other „best practices“ of system security. A badly configured web server, which produces error pages showing its server configuration and operating system platform, can still reveal

www.dDoS.com

some configuration – yet for Barbican RNP, returning a web error page is not „invalid“ traffic – just shows a sub-standard security approach.



Slide 10 of 24

[INSTANT PENTEST DEFENSE RESULTS]

Simply by plugging in Barbican RNP, all penetration testing probes are intercepted by Barbican RNP, which responds actively: reporting all probed ports as „open“, yet not revealing any other information. The targeted infrastructure never responds to the probes.

Barbican RNP also adds a randomized portion to the probe, so it cannot be fingerprinted itself.

Existing Intrusion Detection Systems (IDSs) can be fine-tuned to listen to Barbican RNP responses, allowing to trace the attacker and take counter measures: PenTest probes always come from valid Ips (i.e. Never spoofed), since the attacker needs to receive the results from the probe.

As a result, the attacker is left with no gain from the probe: the results are worthless. If the attacker uses a probing tool such as the popular NMAP program, and turned on the option to assess the level of difficulty to compromise the probed site, the level of difficulty recognized by NMAP instantly goes up to the maximum of 9,999,999 – a typical difficulty level for a well-administered site hardly ever exceeds 200,000 on this scale.

Online survey company NetCraft (UK) also gathers some information by probing the infrastructure.

In this example, the lower entry (June 2002) is prior to deploying Melior's PenTest Defense, and clearly shows the operating system (Linux). The probed server itself, behind a commercial firewall, which does not intercept any such

probe, had not been specifically configured, and by default shows the exact server configuration, down to the patch level of the software.

In the entry above (August 2003), Melior's PenTest Defense has been plugged in inline, and no longer is the operating system available: „unknown“. To demonstrate proper „best practices“ for other components, the probed web server has been properly configured, and simply shows „Apache“ (a configuration step, which a higher-level security administrator could also eliminate) – Melior wants to demonstrate the benefits of PenTest Defense, deployed by a standard system administrator with no special security training.



Slide 11 of 24

[BARBICAN RNP APPLIED: DDOS DEFENSE]

By simply plugging in Barbican RNP dDoS attacks are instantly identified, discarded, and reported on (*via syslog, from all deployed Barbican RNP units across the protected perimeter – see „How to Deploy“ later on in this presentation*).

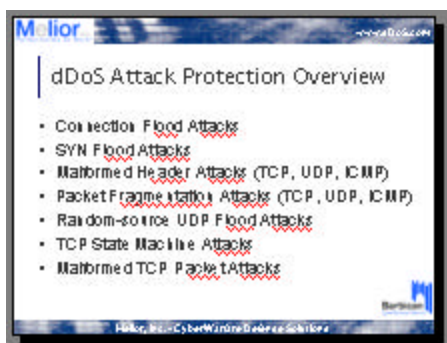
Barbican RNP does not simply throttle all traffic, but inspects every packet flowing through it, and instantly – in real-time, with typically less than 10ms latency – passes it on or discards it. Thus valid traffic spikes are permitted, which do occur normally – the short-term IPO traffic at a banking institution, the CNN news article catching the interest of millions, a popular article on eBay, for instance.

Even during a dDoS attack, normal operations continue to function, as if there was no dDoS attack present.

If the customer chooses to collect data from Barbican RNP in a central location for further analysis, this data and its correlation can then be helpful to demonstrate the successful deployment of CyberWarfare Defense in the mix of

www.dDoS.com

security measures – important to demonstrate compliance with the Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, and for security budgeting purposes (*this is an important aspect to CEOs, CFOs, and other executive staff*).



Slide 12 of 24

[DDOS ATTACK PROTECTION OVERVIEW]

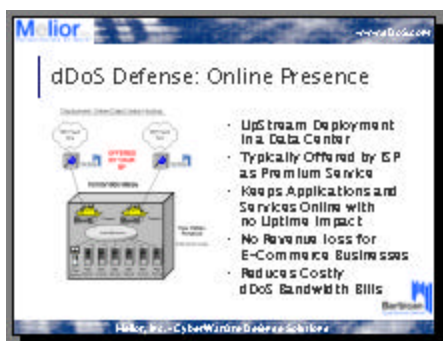
An overview of the kinds of attacks, against which Barbican RNP defends:

- ❑ **Connection flood attacks:**
The attacker exhausts the target's resources by creating a large number of unused connections to the target.
- ❑ **SYN flood attacks:**
The attacker exhausts the target's resources by starting a large number of connection "handshakes" that it never finishes.
- ❑ **Malformed header attacks (TCP, UDP, ICMP):**
The attacker attempts to take down, take over or degrade the performance of a target by sending packets whose headers contain invalid data.
- ❑ **Packet fragmentation attacks (TCP, UDP, ICMP):**
The attacker attempts to take down the target using packets deliberately crafted to take advantage of faults in certain operating systems or network devices.
- ❑ **Random-source UDP flood attacks:**
The attacker consumes the target's network resources by originating a large number of UDP datagrams that appear to come from random origins.
- ❑ **TCP State Machine attacks:**
The attacker attempts to take down or degrade the performance of a target by performing protocol actions out of expected order, or in ways that "confuse" the target device's network communication system. -

www.dDoS.com

❑ **Malformed TCP packet attacks:**

The attacker attempts to take down, take over or degrade the performance of a target by sending packets that contain various kinds of invalid data.



Slide 13 of 24

[DDOS DEFENSE: ONLINE PRESENCE]

Most online presences for content web sites and e-commerce applications are hosted in data centers, in which the customer rents space in cabinets or cages for their own equipment, and ISPs provide Internet connectivity typically by way of 100 Mbit/s or faster Ethernet connections on copper or fiber wiring.

The customer's infrastructure setup is usually fairly similar: firewalls protect against basic attacks and limiting the number of TCP, UDP, and ICMP ports, on which the outside world can communicate with the systems deployed in the customers' space, and a variety of network- and load balancers, as well as a number of application servers.

Location of any online presence is usually chosen for environmental redundancies, as well as for availability of a multitude of Internet feeds.

The customer pays for the space used within the data center (fixed cost), as well as for the amount of traffic delivered to and from the infrastructure by the ISP (dynamic cost). Usually the dynamic bandwidth cost has a fixed minimum price (subscription rate), with the capability to „burst“ from the minimum rate to the full capacity of the medium (the „pipe“).

If the customer comes under „bandwidth flooding“ dDoS attack, the amount of traffic delivered to the pipe typically goes to the maximum, resulting in saturation of the pipe by invalid traffic, thus overwhelming the transport capabilities through the pipe, and resulting in maximum revenue for the ISP. For the revenue aspect, no ISP has a business interest to defend the customer against such Denial-of-

www.dDoS.com

Service attacks (and Service Level Agreements –SLAs- typically exclude dDoS attacks), nor does the customer usually have other leverage to request action to be taken by the ISP without compensation.

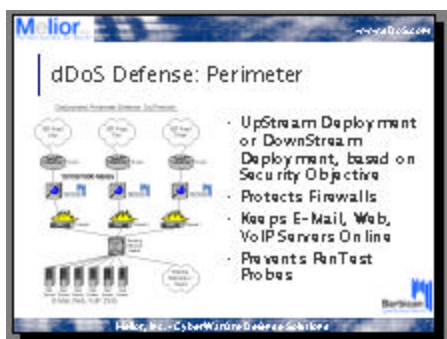
In order for **Barbican RNP** to defend against all attacks (see brochure on „Attack Protection“), including the costly flooding of the bandwidth pipe, it must be installed „upstream“, i.e. on the ISP end of the traffic delivery medium, prior to the point of measurements for bandwidth cost.

To provide the ISP with a business incentive, ISPs typically prefer to purchase **Barbican RNP** units, and offer their deployment and usage as a premium service to the customer, to offset the lost revenue for the additional dDoS, PenTest, and junk traffic.

As a customer, you would want to choose your co-location provider from a list of ISPs, who deploy and offer **Barbican RNP CyberWarfare Defense Solutions** as an add-on service. If you already have an online presence in a co-location facility, and your ISP is not on the list of Melior resellers or premium providers (see our web site), you may want to work with your ISP to consider offering this defense as a premium service.

The cost benefit is obvious: compare the rates of ongoing bandwidth cost exceeding your monthly subscription rate, and the cost of damages, outages, and vulnerability exploitation (PenTest - against which your current security measures do not defend) against the cost of **Barbican RNP** units (or their premium service cost by the ISP).

You will find **Barbican RNP** amortizes very quickly.



Slide 14 of 24

[DDOS DEFENSE: PERIMETER]

Most medium and large networks are set up in a similar architecture design, following a „best practices“ approach established - until now:

One or more Internet connections are shielded by firewalls, protecting against basic attacks and limiting the number of TCP, UDP, and ICMP ports, on which the outside world can communicate with the systems made available for public access, or on which services using the Internet can communicate (out-bound e-mail, web surfing, Voice-over-IP, DNS, etc).

Penetration Tests probes for vulnerability probing are not intercepted, and the infrastructure is open to attacks and compromises. Each firewall is addressable and runs – like any other device accessible from the Internet – on a TCP/IP stack, which in itself is vulnerable.

With freely available tools, any individual, group, or competitor with malicious intent can determine the exact configuration of the customer's infrastructure (with tools such as NMAP or Nessus), and attack it at will to disable individual components or shut down devices and access to and from the entire infrastructure. A simple stack attack on the firewall will disable all communications instantly.

Barbican RNP defends against these attacks (*please see brochure on „Attack Protection“*), including the PenTest probes (to also protect the on-premise router, it must be installed „upstream“, i.e. on the ISP end of the traffic delivery medium – *please consult our brochure on on-line presence defense*).

As a customer, you will want to eliminate the risks of vulnerability exploitation and direct attacks on your infrastructure by shielding your firewall(s), network devices (switches, routers), and servers, now that CyberWarfare Defense Solutions have

www.dDoS.com

become available with Barbican RNP v1.0. The benefits are obvious: compare the cost of cost of damages, outages, IT staff usage, and vulnerability exploitation (against which your current security measures do not defend) against the cost of Barbican RNP units (or their premium service cost by the ISP).

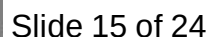
Benefits for uptime and application availability, such as:

- ❑ Web Services
- ❑ E-Commerce Services
- ❑ E-Mail Services
- ❑ Telephony Infrastructure (Voice-over-IP / VoIP)
- ❑ Domain Name Service (DNS)
- ❑ File Transfer (FTP) Services

Benefits of decreased IT staff costs due to:

- ❑ Drastically reduced log sizes in firewalls and Intrusion Detection Systems (IDS) - less IT staff time spent to review logs efficiently
- ❑ Reduced need to rebuild firewalls, servers, desktops, and other devices from TCP/IP stack attacks
- ❑ Reduced costs from compromises from worm/virus attacks
- ❑ Reduction/Avoidance of follow-up costs of vulnerability exploits due to elimination of Penetration Testing for yet-uninfected systems (IT staff time spent to keep up with system patches)
- ❑ Budget benefits from improved reporting on valid vs. invalid network traffic

You will find Barbican RNP amortizes very quickly.



Most networks in corporations and governments are set up in a similar architecture design, following a „best practices“ approach established - until now:

Some high-security conscious sites deploy firewalls also internally between LANs and WANs, and in front of internal application farms, to control access to resources within the infrastructure; however, the cost to deploy and maintain firewalls and their policies is too cost-prohibitive in most cases to actually implement.

Penetration Tests probes for vulnerability probing are not intercepted from external or internal sources, and the infrastructure is open to attacks and compromises. Each firewall is addressable and runs – like any other device accessible from the Internet – on a TCP/IP stack, which in itself is vulnerable – and the same is true for network devices (switches, routers, VPN gateways), servers, and desktop PCs.

With freely available tools, any individual, group, or competitor with malicious intent can determine the exact configuration of the customer's infrastructure (with

Melior, Inc. CyberWarfare Defense Solutions, 1501 Beaumont Street, Dallas, Texas, USA

tools such as NMAP or Nessus), and attack it at will from external or internal sites to disable individual components or shut down devices and access to and from the entire infrastructure. A simple stack attack on a firewall, router, or Ethernet switch will disable all communications instantly; attacks on servers and applications will disrupt those equally quickly.

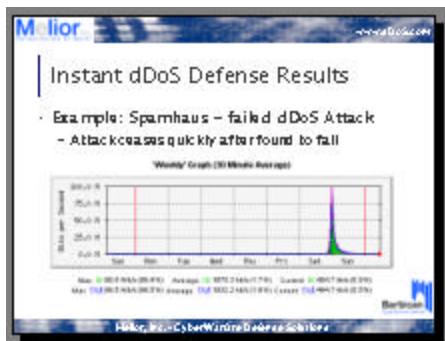
In addition, user desktop PCs are often compromised by virii, worms, and other forms of malware (studies have shown 40% of desktops in US Fortune 100 companies are compromised), and the malware spreads very quickly across the entire infrastructure, contaminating other LANs, remote sites via WANs, and server farms.

Even simple invalid and „junk“ traffic (such as jabber from malfunctioning network devices; i.e. bad traffic without malice) flows freely across the LANs and WANs, eating up resources. While on a 100 Mbit/s or faster local network this extra traffic is not as much noticable, it often easily saturates the smaller wide-area network connections, and leads – with growing networks – to costly upgrades of such connections.

Barbican RNP defends against both invalid, non-malicious traffic, as well as against malicious attacks from internal and external sources (*please see brochure on „Attack Protection“*), including internal or external PenTest probes to exploit vulnerabilities in local or remotes sites as preparation for targeted attacks.

As a customer, you will want to eliminate the risks of internal and external vulnerability exploitation and direct attacks on your infrastructure by shielding your firewall(s), network devices (switches, routers), desktops, and servers, now that **CyberWarfare Defense Solutions** have become available with **Barbican RNP v1.0**.

The benefits are obvious: compare the cost of cost of damages, outages, IT staff usage, and vulnerability exploitation (against which your current security measures do not defend) against the cost of **Barbican RNP** units (or their premium service cost by the ISP).



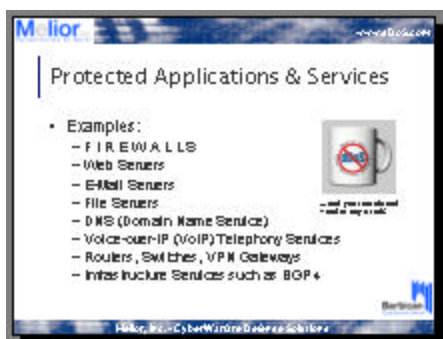
Slide 16 of 24

[INSTANT DDOS DEFENSE RESULTS]

Simply by plugging in Barbican RNP – here in an online presense defense example – dDoS attacks no longer have an impact.

As this example from Melior's Spamhaus dDoS defense shows, a 100 Mbit/s dDoS attack was launched against Spamhaus, yet failed to make a dent – the website and anti-Spam blacklist database remained operational, with no impact to access the data.

Consequently, after a few hours, the attacker gave up – they tried again several times in similar fashions, each time altering the tools and their approach. Yet none of these attacks made an impact, and finally no more dDoS attacks were observed.



Slide 17 of 24

[PROTECTED APPLICATIONS AND SERVICES - EXAMPLES]

dDoS attacks can be geared against specific network devices, operating systems, applications (for instance: web servers, E-Mail servers, DNS, Voice-over-IP telephony services, infrastructure services such as BGP4) in either broad-scale attacks, overwhelming services or bandwidth pipes, or specifically targeted against known or emerging vulnerabilities.

In the initial v1.0 release, **Barbican RNP** is geared to protect against OSI Layer 2 and 3 attacks; however, many attacks targeting applications on OSI Layer 4 and above can be recognized and thus defended against on the lower levels.

Melior has several modules in development, addressing CyberWarfare Defenses against OSI Layer 4 and above attacks, which will become available for easy installation on existing **Barbican RNP** platforms by the customer.

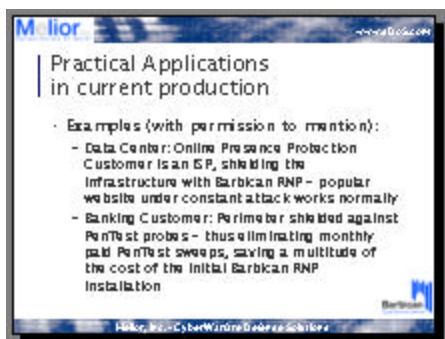


Slide 18 of 24

[BARBICAN RNP – THE APPLIANCE]

Picture of the Barbican RNP appliance with standard features.

www.dDoS.com

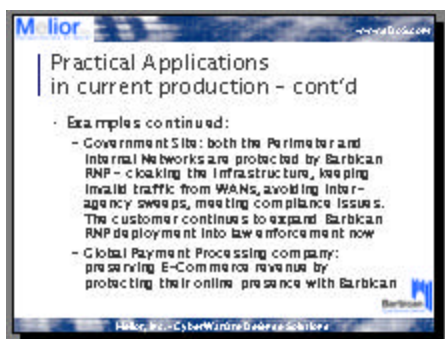


Slide 19 of 24

[PRACTICAL APPLICATIONS – EXAMPLES]

These examples are self-explanatory. Many Barbican RNP customers choose not to disclose their implementation of the CyberWarfare Defense layer, yet (obviously) recognize the need for it, driven by various reasons:

- ❑ Compliance issues
- ❑ Uptime and Availability Concerns
- ❑ Cost savings and Amortization



Slide 20 of 24

[PRACTICAL APPLICATIONS – EXAMPLES CONTINUED]

Other motivations for the implementation of the CyberWarfare Defense layer are:

- ❑ Homeland Security Compliance
- ❑ Preserving the Basis of Revenue Generation in Online, Internet E-Commerce businesses

Slide 21 of 24

take counter measures – by default this implies the Cisco solution cannot act in real time, and bad packets do enter the network. For some low-level and dynamic bandwidth attacks, which also defy signatures, a few packets in a short burst are sufficient to cause the desired damage (synk4, synk5, the shrew attacks, etc.) – Cisco's solution is by design unable to defend against those.

True Zero-Day Attack Defense

One of the key differentiators and key goal of product development of Barbican RNP was to keep it signature-free. Barbican RNP never compares traffic against known form of attacks; all attacks are „new“ to Barbican RNP. It validates the traffic based on universal rules, which do not require updates or definition by the customer; thus enabling Barbican RNP to successfully defend against all forms of attacks as described in our product feature overview.

Cisco skirts around the issue in their product literature, but claims to defend against *„even Day Zero attacks that have never been seen before“*, however does state that in order for the system to work, policies need to be defined (*„an interactive mode allows users to review and approve recommended actions and policies prior to activation“*) – i.e. a policy must exist defining the kind of „Zero-Day“ attack observed in order to catch it: this is not TRUE „Zero-Day“ attack protection (*but marketing fluff*).

Safe against Compromise

The Barbican RNP „IN“ and „OUT“ ports do not have a MAC-, nor IP Addresses, thus the product cannot be directly addressed, other than from it's third, secure admin port, which is only to be connected to a safe, separate network connection (same as the reporting & alert channel for an IDS system). Thus Barbican RNP cannot be compromised.

The Cisco solution does have separate admin ports as well, but in order for it's product to work, the monitor and defense ports on the product have to be addressable (*„diverted traffic“*) – which allows hackers to address both units directly, and attempt to compromise them.

Note: Cisco's Guard XT product ships with default „root“ passwords enabled; if the customer fails to read the announced patch and does not change the root (superuser) password, each product can be easily taken over by an attacker scanning for fingerprinted Cisco devices (see also the section on Penetration testing defense).

Penetration Testing Defense

As an „inline“ device, Barbican RNP recognizes and intercepts Penetration Testing (PenTest or probing) attempts, and actively responds to them, reporting the probed ports as open, yet not revealing any information. To avoid fingerprinting of the Barbican RNP unit itself, it also adds a randomized portion to the response. This behaviour prevents the customer's infrastructure configuration and potential vulnerabilities from being revealed by probes, thus making it a lot more difficult to launch targeted attacks against the customer's site. It can also aid IDS (Intrusion Detection Systems) deployed at the customer site to track down such probing attempts, as these attacks are never spoofed (the attacker must receive the information he or she is seeking). IDS systems can be fine-tuned to watch and alert to such responses generated by Barbican RNP.

Cisco's solution does not offer this feature.

Note: one of Melior's testimonial clients (Dallas Telco, Federal Credit Union) illustrates in their testimonial, that the PenTest defense feature saves them substantial funds by decreasing or eliminating the need for recurring PenTest Sweeps to demonstrate proper implementation of security practices. The cost of each unit amortizes in about six months due to this feature alone.

Hardware Failure Protection

Contrary to the Cisco solution, Barbican RNP does not run off a hard disk drive, the most likely piece of hardware to fail in production (spinning constantly at a minimum of 5,400 rpm). The only moving parts in a Barbican RNP system are the cooling fans; even if all of them fail (CPU- and power supply fans), the unit can continue to work, and alerts to this failure by an error condition light on the front panel of the unit.

Melior is in the process to offer additional versions in a High Availability (HA) configuration, very similar to the HA version offered for the previous, iSecure, product. This HA version has redundant power supplies and fans. A ship date has not yet been announced.

Proven to Work against dDoS Attacks

Even with the might and marketing power of Cisco, the company has been unable to demonstrate successes in the defense against distributed Denial-of-Service (dDoS) attacks; at this time (January 2005) Cisco has only one reference client (Rackspace, an ISP in San Antonio, Texas).

Melior, on the other hand, has successfully defended the anti-Spam blacklists (Spamhaus, SORBS, SPEWS) as well as a very popular website (www.facethejury.com) with earlier, much less sophisticated product versions, beta-software, and other means: with a combined user base exceeding 300 million users globally, in large companies, universities, and governments.

Reference Customers

Cisco lists San-Antonio-based RackSpace as their only reference client. RackSpace offers both the Cisco solution as well as the Arbor Networks product for a premium cost to their customers.

One such customer (a global Internet payment processing company) went to RackSpace, as they were continuously victimized by dDoS attacks. After moving their hosting to RackSpace, they came under dDoS attack again: however, both products in use at RackSpace were even in conjunction unable to defend, and RackSpace had no other choice but to “null-route” the traffic, essentially routing the customer’s traffic into no-man’s -land, thus disconnecting the customer from the Internet. After this experience, the customer then purchased an iSecure product from Melior.

In comparison, Melior shows testimony from several clients, proving successful dDoS defenses for prominent and critical services, and a large user base, exceeding 300 million users.

Note: at this time, Melior remains the only company being able to make any such claims to have successfully defended against dDoS attacks.

Connection Flood Attack Protection

SYN Flood Attack Protection

Spoofed Attack Protection (TCP/UDP/ICMP)

DNS Attack Protection

Both products defend against these attacks; these capabilities are mentioned in the overview to show Barbican RNP falls in no area short of the Cisco product.

TCP State Machine Attacks

Barbican RNP defends against these attacks, which are popular to exploit known and documented vulnerabilities in TCP/IP stacks, by which every single Ethernet device on TCP/IP functions. Specially crafted attacks can compromise the stack by „confusing“ it’s communication abilities, thus essentially shutting the device (such as a firewall) down.

Cisco makes no claims for such capabilities.

www.dDoS.com

Malformed Header Attacks

Barbican RNP recognizes and intercepts attacks by malformed packet headers, which consist of invalid data not recognized by the target TCP/IP stack, thus shutting the targeted device down (firewall, web server, etc).

Cisco makes no claims for such capabilities.

Packet Fragmentation Attack Protection

Similar in concept to the malformed header attacks, Barbican RNP recognizes and intercepts attacks by other, specifically crafted parts of the packet to exploit known OS and network device vulnerabilities. This defense capability is in essence very different to recognize and defend against than malformed header attacks, thus listed separately.

Cisco makes no claims for such capabilities.

HTTP "Get" Attack Protection

Barbican RNP in it's v1.0 release operates strictly on OSI layer 2 and 3; for feature lock, Melior does not claim any specific application level defense methods on Layer 4 and above.

However, many such attacks create „flood“ conditions, which are recognizable at the lower level, and Barbican RNP does defend against some of these attacks. In addition, additional modules, which will become available for installation on the deployed Barbican RNP product by the customer, are under development, including specific modules to address application layer attacks; among those is a module for the „get“ attacks.

Note: Cisco claims to defend against this application layer attack; Melior does not, however, at this time have any proof this statement is correct. We recommend to encourage the customer to compare both products in a lab environment, and compare results.

BGP Attack Protection

BGP4 attack protection falls into the same category as the HTTP „get“ defense. While Cisco makes no other statement as to the actual BGP defense capabilities, Barbican RNP defends against some of the „network connection reset“ attacks, which are often used in a BGP table „poison“ attempt. Future application layer modules will become available, expanding the defense capabilities of Barbican RNP in this regard to the application level.

Note: in this context you can mention Melior, Inc. owns the domain name „bgp4.com“ from the previous 11 years as a high-end security services provider, thus minimally insinuating our capabilities and knowledge to develop such additional BGP4 defense modules.

Instant Protection without Configuration / Learning

Barbican RNP allows the customer to unpack the unit, mount it in the rack, and immediately start using it with instant protection, as Barbican RNP does not require any learning curve or pre-configuration („plug & protect“). As an in-line device, Barbican RNP also does not require any changes to the customer's infrastructure, not even additional ports on an Ethernet switch.

Cisco's Guard XT product requires the definition of policies and configuration, which slows down deployment, and makes it more tedious; it is likely to require adjustments to the customers' infrastructure, and may require up to 4 additional Ethernet ports on customer switches.

Cluster Support for High-End Bandwidth Defense

Cisco claims cluster support for its product as a differentiator for the capability to address high-end traffic throughput, yet does not offer any information how this clustering works.

The clustering capabilities are true for Barbican RNP as well; depending on the customer's network architecture by deployment of additional load balancers, or by splitting the traffic connections across several parallel Barbican RNP units.

Note 1: Barbican RNP's throughput is guaranteed at 400 Mbit/s per system, and connections of speeds up to one Gigabit/s on the network layer. There is no indication the individual Cisco Guard XT systems alone or in conjunction are able to process faster; by design, it is likely to perform slower. Encourage the customer to compare both products in a lab environment.

Note 2: Higher bandwidth than 1 Gigabit/s per connection is very rare, and usually only found in environments such as Akamai, Google, and backbone ISPs. The vast majority of Internet connections in the target markets for both products is 100 Mbit/s or slower; with actual throughput needs - including spike traffic – usually not even coming close to physical connections.

Reporting to SYSLOG Monitors

Both products offer the ability to log to standard 'Unix'-style „syslog“ collectors and monitoring devices, a standard requirement for large organizations. These customers usually have proprietary or off-the-shelf data interpretation engines,

which prepare the data collected from various sources in an appropriate format for the customers' needs.

Cisco offers other products for those „off-the-shelf“ collector programs; Melior may in the future offer a similar collector product, combined with a central, enterprise-wide Barbican administration utility; however, any standard ‚Unix‘-based syslog collector will perform well for both products.

List Price

Barbican RNP retails for \$18,000 list price in the Americas, and Euro 18,000 elsewhere; Melior seeks to protect the reseller margins, and not undercut prices to establish a „street price“.

The cost for the Barbican RNP product is purposely low – Melior could sell the unique technology at a much higher price, but we recognize the need for this new CyberWarfare Defense layer across a wide range of perimeter and internal networks, and would rather deploy more units at a lower cost to the customer, thus making the implementation of this additional protection affordable.

The Barbican RNP list price includes the first years' maintenance cost, renewable at \$3,600 per year.

Cisco's product consists of two units, each listed at \$90,000, and at a maintenance cost of \$10,800 per year for each unit, bringing the total cost to \$201,800.

Note 1: the initial cost of the Cisco product (11.2 times more than each Barbican RNP unit) is a major competitive advantage. The customer can purchase over 11 Barbican RNP's with better defense capabilities for each Cisco unit; the deployment cost in staff and required infrastructure changes for the Cisco solution widens this gap even further.

Note 2: Barbican RNP offers many other benefits, decreasing staffing costs by eliminating PenTest sweep costs, reducing junk traffic and log sizes on firewalls and IDS devices, thus allowing to budget for lower staffing costs; the Cisco solution requires policy decisions and reviews, thus is more likely to increase staffing costs.

Note 3: Due to the significantly lower cost of Barbican RNP, the customer can much easier afford to deploy Barbican RNP units in front of WAN links (thus reducing bandwidth cost by eliminating „junk“ traffic), and between subnets in their user-base LANs (thus reducing the risks of compromised desktops to

spread, and allowing the customer to keep contamination isolated on networks between internally deployed Barbican RNP units – see also deployment examples for Barbican RNP).

Additional Pointer

These additional tid-bits of information may also help augment your pitch:

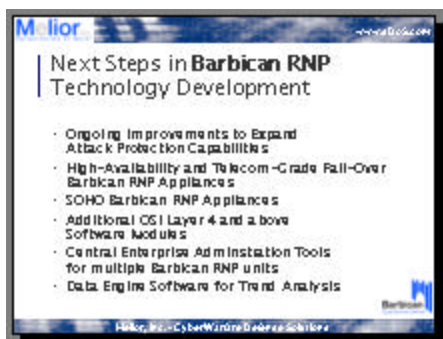
“Developed by Cisco Systems”

Cisco prominently displays their in-house development of the “Cisco Guard XT” product.

In fact, this is the identical product formerly known as Riverhead, which Cisco acquired and simply re-branded (similar to the Ethernet Switches from Kalpana and Grand Junction, which made up Cisco’s initial offering for that market by simply repainting them and adding a Cisco label; or NTI’s “PIX” firewall). Upon the Riverhead acquisition, in which Cisco previously held a 10% stake, Cisco stock took a hit, as analysts wondered why Cisco spent \$39 million on a technology, which had already been proven to not work well, and to not offer a viable dDoS defense.

As in the previous acquisitions, it is likely to take Cisco at least a year to fully integrate the acquired staff and combat retention, until “Guard XT” customers can expect improvements to the product.

Compare to Melior and Barbican RNP customers: we developed the product in record time (despite several delays in our initial launch target), and Melior does nothing else but concentrate on product development for CyberWarfare Defense solutions against various Denial-of-Service conditions, with no integration issues hampering progress and continuous product improvements.

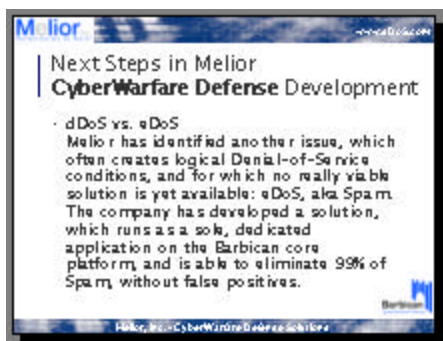


Slide 22 of 24

[NEXT STEPS IN BARBICAN RNP TECHNOLOGY DEVELOPMENT]

This technology development outlook specific to the Barbican RNP platform is self-explanatory.

Melior has little intentions to give away development projects in progress, but wishes to assure customers that the product is constantly improved; all updates are covered by the mandatory service & maintenance agreement (first year included in the purchase price).



Slide 23 of 24

[NEXT STEPS IN MELIOR CYBERWARFARE DEFENSE DEVELOPMENT - eDoS]

The above is true – „Barbican eDoS“ applies a similarly new technology approach to finally address the problem of Spam, which is yet another Denial-of-Service issue on a more logical level, and also a transport medium for malware, often used in the first step of dDoS attacks to build the „bot-nets“.

Before Melior brings this new product to market, Melior intends to become the market leader in the dDoS arena first, against which the company is up against few competitors, which a much better product.

www.dDoS.com

To succeed in the anti-Spam market, which is crowded by more than 200 vendors, none of which offer a truly viable commercial or public-domain solutions, the company needs the reputation and credibility gained by becoming the market leader in the dDoS field, and earn the funds for the necessary expenses to enter the eDoS (anti-Spam) market.

At this time, Melior has chosen not to offer a release date for the eDoS product.



Slide 24 of 24

**[PRESENTATION CONCLUSION –
LEAVE THIS SLIDE ON-SCREEN AS „TAKE AWAY“]**

This concludes the Melior Barbican RNP CyberWarfare Defense presentation.

I thank you for the time you spent with me - I hope the presentation has given you substantial information on the risk of PenTest and dDoS attacks, and I made a convincing case to show there is, for one, a valid defense option, and for another, the need to defend against more than those two – all firewalls and servers are vulnerable against attacks, and by not acting NOW, they remain to be an enormous risk in themselves, if they are not protected to perform the tasks they were implemented for.

More information is available from me, or from Melior directly on their web site (including this presentation).

Thank you!