Monash Technology Report

The Future of Security Technology, Part 1

November 25, 2002

Obligatory Disclaimer

Obviously, everything in this report is just a prediction. I could be wrong about any or all of it. But I think there's an excellent chance it's correct.

Introduction and Summary

Over the next 2-4 years, most of what we now think of as information security technology will merge into five classes of products:

- Integrated *security appliances*
- Centralized *network security management software*
- Real-time *identity management servers*
- DBMS and database-related software, which will take significantly increased responsibility for ensuring information security. The most important example is *office/collaboration applications, which will be ported to DBMS platforms.*
- General client-side security products, whether software-only or hardware-based.

By way of contrast, most other classes of security product will be marginalized, especially "point products" in categories such as firewalls, intrusion detection, or even antivirus. Specialist vendors that flourish in these sectors will do so primarily via an OEM route. But most specialist vendors will disappear (or be transformed via merger) in a process of extreme market consolidation. Due to Wintel inertia, however, client-based software may be an exception to this general trend.

This document is part of the Monash Technology Report continuous information service, and is meant to be used in conjunction with our personal consulting services. Although we send it to certain professional investors, some of whom are our clients, it is not an investment research report and should not be relied upon to make investment decisions as if it were. Opinions are our best judgment at the time of publication.

In support of these assertions, the following arguments are briefly laid out below:

- Appliances already dominate large parts of the security market, especially the firewall/VPN sector. An explosion in processing power requirements will accelerate this trend.

- *Intrusion detection systems,* as currently deployed, suffer from four fundamental problems:

  1. They don't work well.
  2. Even if they did, they wouldn't be good for much.
  3. Their performance is inadequate.
  4. Their total cost of ownership is excessive.

  To address these problems, IDS technology will necessarily evolve in at least two directions: *intrusion protection*, integrated into firewall appliances, and better IDS, integrated with other network management tools.

A follow-on Part 2 of this report (and more parts if necessary) will cover other arguments in support of the overall thesis, including:

- Longstanding weakness in the AAA market is due primarily to cost-of-ownership issues. At least on the server side, these can and presumably will be solved using techniques (both in technology and in corporate politics) analogous to those used in data warehousing.

- Office/collaboration applications (such as Microsoft Office, Microsoft Exchange, and Lotus Notes) will run over mainstream DBMS (i.e., SQL Server, DB2, and Oracle). Thus, the same industrial-strength levels of security used to protect financial data and customers' proprietary information will also be available to messages and other documents.

- Microsoft still doesn't have its priorities straight, and the outlook for general client-side security is consequently disturbing.

This document is part of the Monash Technology Report continuous information service, and is meant to be used in conjunction with our personal consulting services. Although we send it to certain professional investors, some of whom are our clients, it is not an investment research report and should not be relied upon to make investment decisions as if it were. Opinions are our best judgment at the time of publication.

Appliances Are Taking Over

Appliances are already the dominant delivery platform for firewalls and VPNs *(virtual private networks).* That's true today, no matter what market research firms may say to the contrary. At least, it's true if you define *appliance* to include routers, switches, cable modems, and anything else that's not a general-purpose computer.

To see this, just consider the leading vendors in the firewall and VPN categories, which in some order seem to be:

- Check Point -- over 50% appliances*
- Cisco -- almost all appliances
- Netscreen -- all appliances
- Nortel -- all appliances
- Sonicwall -- all appliances
- Watchguard -- all appliances
- Linksys, Netgear, and 3COM -- all appliances
- Symantec -- betting its future strategy on, and probably getting its current firewall/VPN growth from, appliances
- Secure Computing -- an exception; a niche vendor still selling either software packages or "appliances" that are really just generic Dell servers

That's dominance.

** Check Point actually says that "over 40%" of its revenue is associated with the Nokia platform. But since OEM revenue is presumably discounted vs. end-user licenses, Nokia alone probably represents over 50% of Check Point's market penetration on an apples-to-apples basis.*

And it's not just firewall/VPN. Antivirus is showing signs of going the same way. At least in its early releases, Symantec Gateway Security is a pretty silly product if you think of it as a "firewall plus other stuff" appliance. Who would want a niche high-end firewall combined with a mainstream antivirus product combined with some low-end IDS and content filtering? But if you view SGS as "antivirus plus other stuff", it makes a lot more sense. Everybody needs antivirus, after all, and ill fitting though they are, the other parts might nonetheless actually be useful. Network Associates is going the AV appliance route too, building an appliance that will run McAfee Antivirus, Sniffer (not a big surprise), and IDS from market leader ISS (Internet Security Systems).

Actually, as will be discussed in future reports, there's some reason to think AV will wind up being very tightly integrated into messaging systems and spam filters. This could interfere with running AV on appliances. But if that tight integration doesn't happen -- and perhaps even if it does -- I think network-based (as opposed to client-based) AV may well wind up running overwhelmingly on appliances rather than general-purpose computers.

Other categories of security software are also going onto appliances. Indeed, a whole host of venture-backed startups want to integrate every conceivable kind of security (AAA sometimes excepted) onto a single high-performing box.

And this appliance trend makes all the sense in the world. As everybody knows, appliances have three inherent advantages over generic software solutions:

1. Ease of configuration (important both because configuration is very costly and because bad configuration leaves security holes) and management.
2. Greater integrity (it's tougher to hack an appliance than it is to hack a general purpose computer that happens to run security software).
3. Performance.

Those are big advantages indeed.

Performance requirements are exploding

Of the three major benefits to appliances cited above, two seem beyond dispute. But the third, performance, is the subject of some misunderstanding and debate. Many industry observers seem to argue "Hmm. Today's appliances work at better than T1 or 100 MB (or whatever) speeds, and that seems wholly adequate. So no more performance will be needed any time soon."

That argument is fundamentally flawed, however, for several reasons:

- Even if throughput requirements are capped for a while, much more complex processing is needed than is now used. Thus, stresses on performance will be much greater. Indeed, performance is going to be a critical factor in delivering the highest level of security protection.

- At large enterprises, throughput requirements aren't capped anyway. Intranet protection, aka *network segmentation,* is causing throughput needs to skyrocket.
- Enterprises (and resellers) who invest in a strategic technology supplier want to be assured that there's a smooth path to higher levels of performance than they happen to need today.
- Even if they've been slow to take off, *managed security services* are a good idea for vendor and customer alike. Service providers will definitely need high-throughput devices.

The core, possibly controversial part of this argument is that **protection is becoming much more processing-intensive.** This increased processing-power need is being driven by three primary factors:

- Harder-to-identify attacks
- An increase in application-layer attacks
- The move to real-time *intrusion protection,* rather than after-the-fact IDS

What's more, even current-generation IDS is subject to performance bottlenecks.

Attacks will get trickier

The basic idea of viruses and many other kinds of attack is to sneak some executable code onto the target's computer, and then of course execute it. The safest way to protect against this kind of attack is not to let any executable code through at all, except perhaps from utterly trustworthy sources. But that's not realistic today; else we wouldn't need virus scanners. And it's not going to get realistic any time soon; if nothing else, consider how many new complications will be introduced by the growth in *Web services* technology.

So, ultimately, you need protection of the form:

> Examine a string of bits, and see if they contain malicious code.

In full generality, that's an extremely hard problem. In practice, therefore, virus scanners (let's just focus on those for moment) examine code to see if it matches *known* malicious patterns.

In response, virus writers have long produced *polymorphic viruses,* which change the details of how they appear even as they're spreading. That innovation made the pattern recognition problem harder. But antivirus vendors kept up by scanning entire files for telltale snippets of functional virus code.

Then somebody came up with the bright idea of encrypting or otherwise utterly obscuring the nasty bits of the virus code itself, so that the only visible executable was, say, a decryption routine. So antivirus vendors started blocking files containing decryption routines known to be used in actual viruses. And in some cases they even extended their software engines to include the same decryption logic used in the viruses themselves.

So far, so good. But all these virus-fighting tactics have an element in common -- *heuristics.* The antivirus programmer has an impression of what pattern is being sought, and communicates that impression to the computer. However, humans have a much deeper ability to create and recognize patterns than they have to program pattern recognition into computers. The only known workaround is to apply lots and lots of raw processing power. That's why it was impossible to build a computer that could defeat the world chess champion until there was enough speed available for massive brute-force calculations. For the same reason, some day it will probably be impossible to write a program that outthinks a top hacker unless you can run it on a blindingly fast processor (or bank of processors).

I don't know which virus strategy AV vendors fear most (it's not exactly information they're eager to publicize). But I think they don't yet have great answers yet for compressed virus files, nor for viruses delivered in two separate (randomly broken up payloads) that can recombine on the client machine. At some point hackers will make one of these strategies work, and when they do, the AV vendors will cope. But the way they cope could well rely on vastly more processing power than their software previously required. And when that day comes, **AV performance will suddenly become a major technological issue.**

The Layer 7 burden

Some observers point out that the mere fact that attacks are moving to the application layer boosts the processing requirement. After all, you have to look at the whole packet to do Layer 7 inspection, while for other kinds of protection you might just have to look at packet headers.

Frankly, I think that the Layer 7 point taken alone is the least of the issues. After all, antivirus software defends against Layer 7 attacks today, usually while running on general-purpose computers. Even so, it's yet **another point in support of my overall thesis that security processing power requirements are exploding.**

The IDS/IPS mess

The increased-complexity argument I laid out for antivirus applies equally well to IDS. But the IDS market is also in turmoil due to more immediate problems:

- Conventional IDS don't work well; the *false positives* problem is ridiculous.
- Even if they did, they wouldn't be good for much; what's needed is prevention, not just detection.
- Their performance is already broken, as per the recent Network World review that seemingly proved no available IDS could meet real-world requirements.
- To make an IDS work at all requires immense amounts of skilled labor both at setup time and -- because of the false positives issue -- on an ongoing basis as well. And Total Cost of Ownership is of supreme importance to enterprise technology buyers.

In addition to these product problems, there are business issues as well:

- The leading IDS vendor, ISS (Internet Security Systems), is -- to put it tactfully -- not greatly adored by customers or other industry participants.
- Enterasys, another leading IDS vendor, is a seriously troubled company for reasons including accounting fraud.
- There are dozens of IDS/IPS startups, vastly more than could ever survive as independent companies, and M&A activity is accordingly fierce.

Actually, certain aspects of IDS work pretty well, including some basic attack signatures and some DOS (Denial of Service) attack detection. These are being turned into IPS and integrated directly into firewall appliances by such vendors as Sonicwall, Symantec, and Netscreen.

It should be noted that what Symantec and Netscreen are really putting into their firewall/integrated-security appliances in the near future is just a small subset of their overall functionality. It seems that these are the parts of the functionality that A. Are useful and B. Don't deliver a lot of false positives. That said, Netscreen has promised complete integration of OneSecure (its recently acquired IPS) into its firewall/VPN appliance by the end of 2003 (they'll also still be available separately).

While it's hard to predict exactly how much functionality will work how well on which appliances when, the most likely path is a continuation of what I suggested above. Any part of intrusion detection technology that works well (i.e., useful protection, low level of false positives) will be integrated into firewalls and called "intrusion protection". What's left over will be the part that doesn't work well, or else works only with a very high cost of ownership, and hence will only appeal to the highest-budget or most security-conscious enterprises. Thus, going forward, I expect that **only the most extreme users of security technology will invest in standalone IDS/IPS products to any significant degree**.

Integrating IDS with Network Management

Yet one more factor will change the shape of the IDS market. What's the best way to determine whether your network has been hacked? Well, if it's behaving differently than it used to, and no good reason can be identified, that's a clue that it might be behaving differently for a *bad* reason.

Indeed, if you look at the advances being proposed in IDS by a variety of vendors, many of them are "behavioral" in nature. If overall network traffic goes up inexplicably, or if a specific computer accesses specific resources it never used to, or if certain files (especially executables) are modified for no known reasons, these might be signs of unauthorized activity.

But of course there's already a large market for software to monitor network goings-on. In particular, companies such as Computer Associates, IBM/Tivoli, and BMC Software sell a whole lot of it. These and similar vendors are adding security-specific functions as quickly as they can, and **a significant class of security software in the future will consist simply of general network management software extended to deal specifically with security problems.**

This document is part of the Monash Technology Report continuous information service, and is meant to be used in conjunction with our personal consulting services. Although we send it to certain professional investors, some of whom are our clients, it is not an investment research report and should not be relied upon to make investment decisions as if it were. Opinions are our best judgment at the time of publication.