

Market Drivers For E-business Defense Technology

Rebecca Wetzel

Everyone knows websites need better protection, but not much is being done to harden them. Will a carrot work, or will it take a stick?

Prospects for technologies that protect online businesses from external attack have ignited high hopes, but this nascent market has been slow to develop. E-business defense technology developed mainly to resolve problems stemming from Web protocols

exposing e-business sites and their back-end information systems to the Internet. These “firewall friendly” Web protocols—HTTP (carried over TCP port 80), and HTTPS (carried over TCP port 443), as well as derivatives such as SOAP and WebDAV, are transparent to firewalls, thus subjecting any application vulnerabilities to exploitation.

The list of product vendors tackling this problem from a variety of angles is long and lengthening. It includes, among others, (see “Technology Choices—A Primer,” for category descriptions):

■ **Application firewall technology** from companies like eEye, Kavado, MagniFire, NetContinuum, Sanctum, Stratum8 and Ubizen.

Technology Choices—A Primer

■ **Application Firewall:** A proxy device typically located between the network firewall and the Web server(s), which inspects incoming Web traffic and blocks user behavior that is not allowed.

■ **Intrusion Detection System (IDS):** A software-based system that detects suspicious behavior and reports it to a central management console or security information management (SIM) system. Host-based IDSs monitor event logs or system-level application programming interface (API) calls to detect suspected activity. Network-based IDSs typically identify suspicious behavior by traffic-pattern anomalies (compared to some baseline activity), or by comparing traffic patterns to signatures of known attacks.

■ **Intrusion Prevention System (IPS):** A network-based system that can block suspicious network activity—often using a firewall or a router to perform the actual blocking. Some systems use software on the server platform to intercept and block API calls to the Web server software, the operating system or the underlying database or application servers. Some systems also

compare activity to defined policies and/or attack signatures and behavior heuristics, and protect applications from system calls that are not allowed.

■ **Trusted Operating System:** Host-based software which protects the operating system by preventing operating system kernel modifications, and blocks low-level system call intercepts.

■ **Air Gap Appliance:** A reverse proxy device that physically isolates application servers from insecure networks, and controls application layer access to application servers by scanning data to ensure that known, but not unrecognized, commands are allowed through.

■ **Exit Controller:** Software that monitors content leaving a website and prevents unauthorized alterations to content (such as site defacement) from being displayed by replacing it with the original content or an alternative form of approved content if the original content is not available.

■ **Application Vulnerability Assessment Scanner:** Software that uses Web attack techniques to emulate hacker behavior, and then reports on application vulnerabilities □

Rebecca Wetzel is an Internet industry analyst, consultant and writer. She is president of Wetzel Consulting LLC, and is an associate with NetForecast, an Internet technology and market analysis firm. She can be reached at rwetzel@rwetzel.com.

■ **Intrusion prevention products** from the likes of Enterscept, ForeScout, IntruVert, Okena, TopLayer Networks and TripWire.

■ **Intrusion detection systems** from such vendors as Enterasys Networks, Internet Security Systems and SourceFire.

■ **Trusted operating systems** from Argus, HP, Secuve and Sun Microsystems.

■ **Air gap products** from SpearHead and Whale Communications.

■ **Application vulnerability assessment tools** from Kavado, Sanctum and SPI Dynamics.

■ **Exit control products** from Gilian and Lockstep.

Strong Intentions, Weak Follow-Through

According to IDC, the market for e-business defense products will grow at a 60 percent compound annual rate from \$113 million in 2002 to nearly \$700 million in 2006 (Figure 1). Bear Stearns foresees the broader market for “application security products,” a combination of e-business defense products and authorization products from companies like Netegrity, Entrust and RSA, swelling to \$4 billion in 2006 from \$1.8 billion in 2002 (see Figure 2).

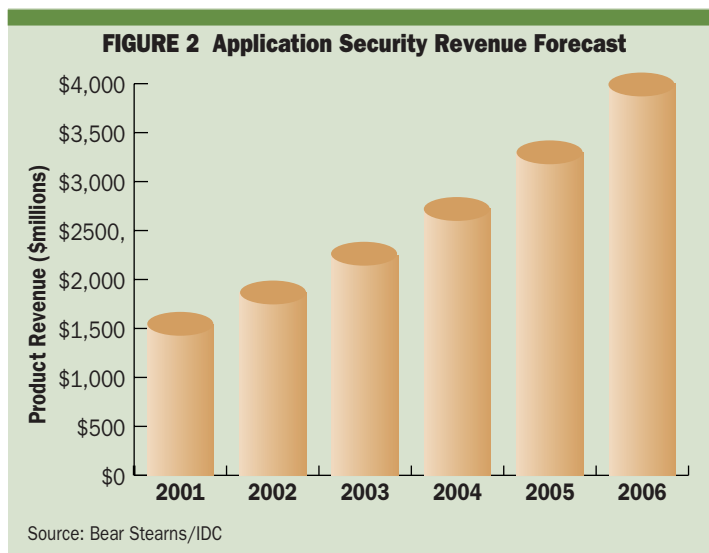
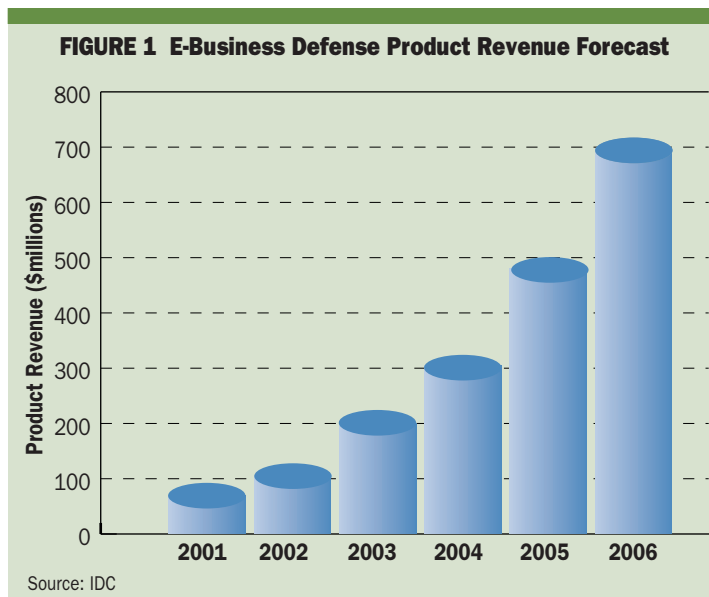
Buying intentions for the complete set of IT security offerings ran high through 2002. In survey after survey of enterprise buyers by Morgan Stanley, IDC, SG Cowen, *InformationWeek* and others, security consistently topped the list of high-priority IT projects (Figure 3) in 2002. But despite stated buying intentions and post-9/11 awareness of the need for better e-business protection, wallets failed to open as many had hoped for e-business defense products in 2002.

Chris Darby, CEO of security consulting company @Stake blames the economy for the slow market growth: “There is a disconnect between what is being said in the marketplace and what is being committed in terms of resources. We are in a tech recession. Security is being viewed in some camps as discretionary. A lot of people are making tough business decisions to take on more risk than they otherwise would if the economy were better.”

But a hamstrung economy isn’t the only thing holding the market back. According to Darby, enterprises are not yet ready to act. “People don’t fully understand how to mitigate their risk. There are a lot of firms that want to sell silver bullets. But risk mitigation is a very complex thing. It’s not just about a single product or service....[it] involves many functions and departments. There’s a paralysis about what to do. It’s problematic. You have to make decisions about how much risk you’re willing to bear and how much you’re willing to invest.”

One frustrated application firewall sales manager who asked not to be identified put it this way. “We expected 2002 to be the year that the market bit the bullet and bought solutions to protect their online business applications. But it has been a tough slog. The need is clear, interest is there, people want to learn more, but they’re just not willing to commit. The economic downturn certainly plays a role, but it’s not just that. Most companies

There are no silver bullets that will eliminate risk



Some vendors are trying to create ROI cases for security technology

are banking on the hope that they won't be hit. That's dangerous when you consider the losses sustained by so many to date. Hopefully 2003 will be different."

Potential Market Drivers

Virtually all new technologies endure a period where interest vastly exceeds orders. So it's a good time to speculate about what factors are likely to propel the e-business defense technology market into the mainstream.

An obvious driver is the "ouch" factor—i.e., enterprises experiencing first hand pain, or unacceptably high risk of being next in line to feel the pain. The business case showing return on investment in the form of increased productivity, revenue and/or reduced operating costs is another potential driver, as are the stick of legal penalties and the carrot of transferring risk through insurance carriers.

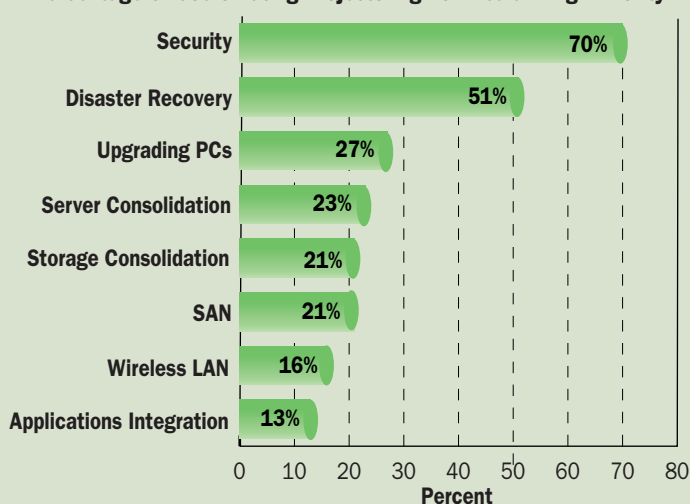
■ **The "Ouch" Factor (Risk):** With mounting numbers of companies suffering serious attacks (see *BCR*, December 2002, pp. 32–37), the "ouch" factor is likely to nudge at least some enterprises to install defensive technology. In a 2002 study by Symantec of a sample population of hundreds of online businesses, the average annualized probability of severe attack was 46 percent, but the risk was unevenly distributed by industry—for example, power and energy companies faced a 100 percent chance of severe attack in 2002, financial services firms faced a 92 percent probability of serious attack.

Once a firm tallies up damages from such an attack, it may well cry "ouch." A 2002 study by the Computer Security Institute and the FBI pegs the average loss from theft of proprietary information, financial fraud, denial of service, data network sabotage and system penetration from outside the enterprise at approximately \$1.7 million. Average loss from theft of proprietary information was more than \$6.5 million, and average loss from financial fraud topped \$4.6 million.

According to Jon David, an independent security consultant who was formerly responsible for online security at Lehman Brothers and Merrill Lynch, pain is a powerful teacher. "People will put up with risks because they haven't had damage yet. Once the damage is there, then they will take steps," he said.

■ **Return on Investment:** E-business defense technology vendors are busy writing return on investment case studies to show prospective customers how their products can reduce operating expenses. The idea is to drive adoption by show-

FIGURE 3 IT Spending Plans
Percentage Of Users Rating Projects High Or Medium-High Priority



Source: SG Cowen

ing that the technology actually saves money currently spent on operations. (Note, this is different from the case to lower risk, which aims to prevent losses caused by attacks rather than lower current operating costs.)

The ROI business cases are constructed around points like the ability of e-business defense technologies to protect even buggy business applications from attack. The cases highlight cost savings and efficiencies in such areas as reducing time spent reactively implementing security patches and updates, reducing cost through less frequent security audits and application vulnerability testing, and accelerating time-to-production for new/improved Web server applications.

As these business cases become more sophisticated, they may hold sway. Said @Stake's CEO Darby: "At the top line it's still a tough sell. The actual return from a revenue perspective is somewhat tenuous. You can create operating efficiencies and that can justify investments. You can certainly spend your security dollar wisely. There's a reasonably good body of knowledge about that. But ROI is an emerging discipline. We'll see more work on that area over the coming year."

■ **Legislation (The Stick):** Two pieces of legislation on the books, the Gramm-Leach-Bliley Act (GLBA) for the financial services industry, and Health Information Portability and Accountability Act (HIPAA) for the health care industry, mandate security and privacy for what is known as "personally identifiable information." The stick wielded by this legislation is in the form of stiff penalties for infractions, and according to Peggy Weigle, CEO of Sanctum, it's getting results.

"We are seeing GLBA and HIPAA as major drivers," she said. "Once companies learn they are exposed, they have to do something. So far, 31 percent of our customers are financial services

firms, and 12 percent are health care and insurance companies. That 12 percent has doubled over last year. As the HIPAA deadlines are coming, we are seeing more adoption from the insurance sector. Government mandates are driving purchases.”

Not everyone agrees, however, that legislation is necessarily a strong motivator for the adoption of e-business defense technology. Said @Stake’s Darby: “It’s industry specific. You may see legislation that comes into play for industries that are critical to the infrastructure of the nation. But you won’t see legislation that will drive general spending in the security market. The threat models are so dynamic and changing, that you couldn’t craft legislation that’s universal in any methodical way.”

David goes further, and argues that the government should not be in the business of legislating e-business security. In his opinion, legislation can do more harm than good, because it is written by people who don’t fully understand the problems. If the government legislates security—such as in the case of HIPAA and GBLA—David believes enforcement will be lax, and enterprises are likely to defer compliance.

“There are workarounds to obeying the law,” he pointed out. “If someone holds up a bank, the bank must report it, but if someone breaks into a computer and walks off with 100 times that amount, there are ways around reporting it. Things get misfiled all the time. Computers are far from perfect. Until there’s a complete investigation by the FCC, etc., things don’t get reported.” He added that many companies are unlikely to comply unless their competitors do so first.

■ **Insurance Incentives (The Carrot):** Insurance is a wild card. Historically, it has helped drive the adoption of technologies that prevent and mitigate risks—e.g., smoke detectors, sprinkler systems and air bags—and relative to the adoption of e-business defense technology, there are two ways in which insurance is likely to play a role.

The first is through the new cyber-insurance policies, and the second is through more traditional policies such as D&O (directors and officers) liability insurance, and E&O (errors and omissions) liability insurance, which will be touched by risks due to e-business openness to the Internet.

The jury is divided about the future of cyber-insurance. Companies like AIG, Chubb, St. Paul and Lloyd’s offer insurance policies to cover risks to online businesses from external attacks. Ty

Sagalow, Chief Operating Officer of AIG eBusiness Risk Solutions, believes nay-sayers are not fully informed about the role of insurance. “There are three legs to the risk management stool. There’s risk protection, risk mitigation and risk transfer. You need all three. If you’re not doing all three, then the stool falls over because you’re creating unnecessary financial liability.”

Security consultant David, however, doesn’t think insurance is a tenable solution for covering the risk of Internet-borne e-business attacks. “The risk involved is tremendous and it’s not actuarially determinable. I don’t see actuarial tables applying to computer crap. If nothing happens, they [the insurer] wins. The first time something major happens, they are out of business. If they charge too much, not many people will go for it...And technology is advancing at such a rate that no information they get will ever be adequately current. What if they spent the last three years identifying risks for Internet security, and new worms appear—then the work they did is now worthless.”

Sagalow, however, maintains that not only does his company know what its doing, he points to the fact that AIG has been selling cyber-insurance for three years and has 2,500 clients. “There are tech-

nologists who don’t understand the notion of risk management,” he said. “Their view is that you list all things that can go wrong and you eliminate them one by one and then, when you run out of money, you give up.

“AIG has been taking on these types of risks for 75 years,” he continued. “We were one of the first companies to offer directors and officers insurance in the case of shareholder

suits, and employment practices liability insurance in cases of class-action discrimination suits, and we were among the first to create environmental liability insurance. For these types of insurance in the beginning, there wasn’t enough actuarial data, but we just began. You gather the information as quickly as you can and you adjust terms, conditions and rates. These programs are now mature, multi-billion dollar premium industries. They didn’t start out that way, but this is where cyber-insurance is today.”

According to Sagalow, established insurance policies, such as D&O and E&O coverage inevitably will be affected by risk from the exposure of corporate resources to access from the Internet. As payments on established insurance policies due to Internet-borne attacks increase, so will awareness of such risks. This, in turn, is

**If someone holds up a bank,
the bank must report it.
If a hacker breaks
into a computer and
steals 100 times
that amount,
it might not get
reported**



Insurance incentives are more likely than legislation to drive adoption of security technology

likely to prompt insurance companies to use incentives to encourage the adoption of e-business defense technologies to lower their risks.

Sanctum’s Weigle believes insurance is a red herring. She cites the example of network firewalls whose widespread adoption, in her opinion, was in no way influenced by insurance. She believes the same will hold true for the new e-business defense technology.

Sagalow, in contrast, predicts that insurance will be a carrot, which drives the adoption of new application security technology. “Throughout history, positive reinforcement in insurance has worked well. Car insurance premiums go down if you have airbags. Fire insurance premiums go down if you have sprinkler systems. Your boiler insurance goes down if you have proper equipment and maintenance. The insurance industry has modified the cost and availability of insurance to motivate good behavior. You need a way of communicating best practices and spreading out risk.”

Conclusion

The soaring percentage of the world’s economy mediated through the Internet will whet the appetites of hackers, “hacktivists” and hacker-terrorists to aim at companies that expose their internal systems to the external world. This spells opportunity for technologies that prevent and mitigate damage from such attacks. But what will drive the market to live up to its potential, and when? Will risk alone drive the market, or will some combination of risk, ROI, legislation and/or insurance prompt technology adoption?

Where there’s pain there’s gain; the risk of business damage will be a primary driver for the adoption of e-business defense technology, especially in high-risk industries such as financial services and power and energy firms. Within select vertical markets, the stick wielded by legislation, such as HIPAA and Gramm-Leach-Bliley will accelerate technology adoption.

But the carrot of insurance incentives is more likely than legislation to boost mainstream deployment of e-business defense technologies over time. With time, insurance and legislation are, however, likely to become intertwined, with legislative compliance becoming a prerequisite for some relevant insurance coverage. As for the final potential driver—return on investment—although it is helpful, and can add momentum, it’s unlikely to be a compelling purchase driver.

Given today’s outlook, the next two years are likely to see slow, steady adoption of e-business defense technology as financial services firms and other at-risk vertical markets overcome current paralysis and begin deploying the technologies in response to direct concerns of risk, and in response to legislation. Look for insurance to kick in as an incentive in three to five years, and for the market for e-business defense technology to enter the mainstream during that time.

Conscience dictates concluding with a caveat. The market drivers described here may be subject to counterbalancing market “dampers,” which will slow or even halt e-business defense technology adoption. These include the possibility that e-business defense technologies, in some way, wind up hampering transactions and applications—i.e., make them more difficult or unacceptably slow. If these dampers appear, they could stall the market and all bets are off□

Companies Mentioned In This Article
@Stake (www.atstake.com)
AIG eBusiness Risk Solutions (www.aignetadvantage.com)
Argus (www.argus-systems.com)
Chubb (www.chubb.com)
eEye (www.eeye.com)
Enterasys Networks (www.enterasys.com)
Entercept (www.entercept.com)
Entrust (www.entrust.com)
ForeScout (www.forescout.com)
Gilian (www.gilian.com)
Hewlett-Packard (www.hp.com)
Internet Security Systems (www.iss.net)
IntruVert (www.intruver.com)
Kavado (www.kavado.com)
Lloyd’s (www.lloydssoflondon.co.uk)
Lockstep (www.lockstep.com)
MagniFire (www.magnifire.com)
NetContinuum (www.netcontinuum.com)
Netegrity (www.netegrity.com)
Okena (www.okena.com)
RSA (www.rsasecurity.com)
St. Paul Companies (www.stpaul.com)
Sanctum (www.sanctuminc.com)
Secuve (www.secuve.com)
SourceFire (www.sourcefire.com)
SpearHead (www.spearheadsecurity.com)
SPI Dynamics (www.spidynamics.com)
Stratum8 (www.stratum8.com)
Sun Microsystems (www.sun.com)
Symantec (www.symantec.com)
TopLayer Networks (www.toplayer.com)
TripWire (www.tripwire.com)
Ubizen (www.ubizen.com)
Whale Communications (www.whalecommunications.com)