

the Web Security report

A MESSAGING MEDIA PUBLICATION • DECEMBER 2006 EDITION • WWW.WEBSECURITYREPORT.COM

ABOUT THIS PUBLICATION

The Web Security Report acts as a publishing partner for Internet security solutions providers, testing labs, research entities and trade organizations. Published monthly by Messaging Media, LLC, the Web Security Report has an online and print audience of over 120,000 readers
publish@websecurityreport.com

12 06

What Have We Done?

The Internet As Global Critical Infrastructure

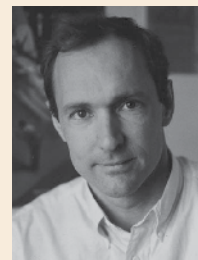
By **Melisa LaBancz-Bleasdale**

Without a doubt, the Internet has had a profound effect on almost every aspect of our lives. The formation of the Internet has changed the way we do business, communicate, entertain, retrieve information and even educate ourselves. Many have claimed credit for "inventing" or "creating" the Internet (insert your favorite Al Gore joke here), but it didn't spring fully-formed out of some scientists' heads – nor did it simply grow, powered by the mysterious magic of the marketplace.

Although ARPANET is said to have fathered the Internet back in 1969, the actual birth of the network as we know it happened in 1984 when 1000 networked computers converted, en masse, to the Transmission Control Protocol/Internet Protocol (TCP/IP) – a suite of protocols designed specifically to support multiple simultaneous communications.

In the beginning, there was Berners-Lee...

Tim Berners-Lee, inventor of the World Wide Web, is credited as one of the key constituents for the growth and success of the Internet. He currently heads up the World Wide Web Consortium (W3C) at the Massachusetts Institute of Technology – which oversees and coordinates Web development, worldwide.



> *continued on page 2*

TABLE OF CONTENTS

What Have We Done?	1
The Internet As Global Critical Infrastructure	
Web Security News	8
Sponsor Profile	10
In This Edition	12

in the next issue

SPONSORED BY
IRONPORT SYSTEMS



Special RSA Issue The Web Security Report will present special previews of technology innovations in Web security as well as a review of the best and brightest vendor solutions at this industry-leading conference.

Regular features include: Web Security News, Company Spotlight and Sponsor Profile.

In 1989, while contracting at CERN (the European Particle Physics Laboratory), Tim Berners-Lee set to work on an Internet-based hypermedia initiative for global information sharing and developed the foundation for what he called “the World Wide Web”. However, according to the Cooperative Association for Internet Data Analysis (CAIDA), it was the United States government which gave the Internet its first evolutionary push. In 1995 – under significant federal pressure and with little consideration given to economics or security – the National Science Foundation (NSF) transitioned the backbone of the Internet to the competitive market. Almost immediately came the dawn of “e-commerce” – with Internet pioneers viewing the online frontier as a new way to conduct business.

Building upon a complex (and at times confusing) origin, today’s Internet continues to evolve at breakneck speed – lending itself to the successes and failures of innumerable marketing campaigns and business ventures. Enabling global accessibility, it has completely redefined traditional business and communication models as a universal source of truth. The Internet’s unlimited potential has delivered equal opportunity for both utilization and exploitation. Its economic possibilities offer the promise of enormous financial gain – for both businesses and criminals alike.

Dr. Vinton Cerf, co-founder of the TCP/IP protocol, once defined the Internet as, “The largest network of networks in the world, capable of running on any communications substrate.” While this definition describes the technical core of the Internet, in less than a decade it has gone from being the world’s largest network to the backbone of the world’s business economy.

If We Build It, They Will Come

The success of the Internet has, by all measures, surpassed any other invention in the history of humankind. Internet uptake increases exponentially as developing nations implement the necessary

infrastructure to support its use. The first measurements in Internet usage statistics began in 1995. According to the Internet Society:

- In 2001, there were 150-175 million Internet hosts.
- The number of Internet hosts increased to over 200 million in 2002.
- By 2010, about 80 percent of the world’s population will be on the Internet.

In a 1998 Information Infrastructure Task Force (IITF) report, titled *The Emerging Digital Economy* (www.ecommerce.gov/emerging.htm), the Internet’s explosive growth rate was put into perspective by noting that it took radio 38 years and television 13 years for each to obtain a market of 50 million users. In comparison, the Internet took a mere *four* years to reach the same number of participants.

The *Internet Domain Survey* (www.isc.org/index.pl?/ops/ds), sponsored by Internet Systems Consortium, Inc., attempts twice each year to discover every host on the Internet by doing a complete search of the Domain Name System (DNS). This survey illustrates massive growth in the Internet population, in just a few months:

- In January 2006, 394,991,609 hosts were located on the Internet.
- The study noted 439,286,364 hosts in the July of the same year.

“Put yourself in the place of an enterprise IT department, trying to keep up with the speed of Internet evolution. What these people have had to go through is absolutely amazing. Look at the vendors who were on client/server architectures or host-based architectures. They had to immediately adapt their solutions or die,” says **Brian Breton**, Senior Product Marketing Manager at RSA, the security division of EMC. “How quickly have we gone from a million users of the Internet to hundreds of millions of users? Has there been anything in the history of mankind that has taken off so quickly?”

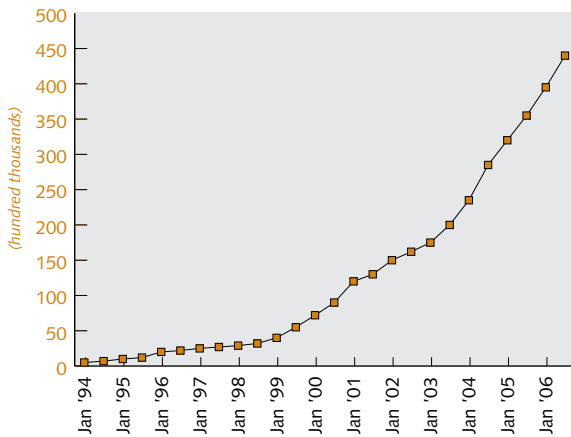


Figure 1: Internet Domain Survey Host Count
(Source: Internet Software Consortium)

When defining Internet scalability, vendors are generally speaking to an organization's ability to anticipate and support the growing demand for website accessibility, an increase in online transactions (both internally and externally) as well as the ability to add more applications in support of better internal process and external customer satisfaction. When industry experts talk about scalability, they variously describe the growth of actual Internet users, the ability to add more hosts, IP addresses, domain names and websites – as well as the hundreds of millions of networked systems that create the physical makeup of the Internet.

The Internet has always been scaling and its growth is continuously affected by a number of complex challenges – ranging from the security of interconnected networks, to the nature of individual users, to the globalization of the Internet framework. In theory, the Internet can handle an unlimited number of users, so long as ISPs continue to add server space and support. However, the necessity to upgrade the underlying framework of the Internet is the topic of discussion among numerous industry experts and Internet consortiums.

Larry Clinton, Chief Operating Officer of the Internet Security Alliance (ISA) explains, "What we're finding is that the Internet is becoming overloaded by a variety of different factors. First of all, there's a

massive amount of traffic. Back in 2000, at the height of the Internet bubble, there were maybe 250 million users. When the bubble burst, people thought that Internet usage would decrease but it didn't. In fact it grew to nearly a billion users."

Dr. KC Claffy, principal investigator for CAIDA, and resident research scientist at the University of California's San Diego Supercomputer Center, has published a list of the top 16 most critical current operational Internet issues. She states that the top unsolved problems in Internet operations and engineering are rooted in a triangle of economics, ownership and trust – dubbing it 'EOT'. Dr. Claffy explains, "The above issues do not mean there aren't useful technical problems to study (with regards to the Internet), but there will be no technical solutions to problems that don't first solve the EOT issues."

Dr. Claffy also notes that by making the Internet such an inherent part of our economic core, we have replaced a critical infrastructure with something not designed to be critical infrastructure, and therein lies the problem.

The Need for Internet Security

The Internet has become an enterprise utility, an expectation of living – much like gas, water and electricity. It is a checkbox in a long list of set up

activities for new businesses springing to life.

"Personally I am still in awe of the Internet, but it has become a utility," says RSA's Breton, "The biggest concern that

businesses have, as with any other utility, is making sure that the utility is available, that it's up. The Internet needs to be transmitting bits. And, if it is down, what kind of disruption is that? That's taking a utility infrastructure view, but the fact is that we're all leveraging that infrastructure to run business."

...by making the Internet such an inherent part of our economic core, we have replaced a critical infrastructure with something not designed to be critical infrastructure, and therein lies the problem.

Similarly, Larry Clinton reports that the ISA views the explosive growth of Internet users as one small part of a much larger security problem. Citing the integration of technologies as a more worrisome component, he points out, "The number of Internet users has grown 300 percent since 2000. But the amount of traffic has grown 2000 percent. It is the tentacles of growth such as PDAs, cell phones, AJAX-driven office suites, and the sheer increase of Web-enabled applications that are adding to the problem – inadequate Internet security."

Many experts point to the fact that the core Internet protocols are over thirty years old and, despite never receiving any significant updates or enhancements, they are still being used today. Adding to this concern is the understanding that these protocols are widely known to be unsecured. However, as CAIDA's Dr. Claffy pointed out, the Internet was unleashed to the public domain without thought to this important operational component.

Clinton views Internet security as a complex issue with no clear cut answers. "We have a tremendous amount of growth in the number of users. In addition, there is a disconnect between the functionality of devices, especially consumer devices and their security. We also have the fact that the Internet is built on a foundation that was not really designed with security in mind – at all – and hasn't been significantly enhanced. All of this is creating bigger and bigger problems with respect to Internet security."

There are schools of thought that point to the sheer number of users as a focal point for the introduction of vulnerabilities and other security issues. **Robert Richardson**, Director of the Computer Security Institute (CSI) offers this viewpoint, "I don't know that the scalability of the Internet necessarily figures into the security discussion, except for the important worry that any wholesale security solutions we come up with have to scale to match the size of tomorrow's Internet. At present, I'd say the current Internet architecture has fundamental security flaws that really weren't a product of the Internet scaling up. Not, at least, past the point where all the network

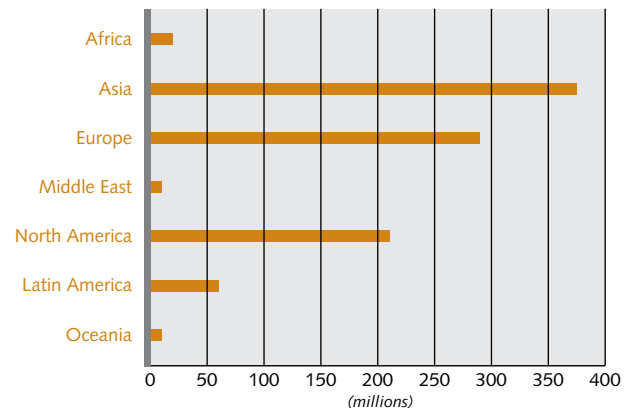


Figure 2: Internet Users by Geographical Region
(Source: www.internetworldstats.com, November 2006)

host administrators knew each other – and that's so far back, it's not really worth worrying about."

Despite inherent flaws in Internet security and a general dose of enterprise naiveté, the enormous desire to jump on the online bandwagon far outweighed any short or long-term consequences. "What's the first thing that a business tells their IT department? 'Get me a connection and get me online by March 1st come hell or high water!' What we originally saw with the Internet was that security was not necessarily an afterthought, but it was something that was put on the back burner on purpose. Simply because it didn't fit in the time-to-market needs of the business," RSA's Breton explains.

It didn't take long before Internet security concerns became a topic that could no longer be ignored. As businesses clamored to gain market share by putting themselves on the Web, they simultaneously exposed themselves to the intellectual wherewithal and creativity of computer hackers.

"If you're a large financial institution and you're scaling to allow four million customers to have access to your systems, what is your biggest concern for your customers? What access am I allowing those people to have to my information?" Breton continues, stating, "You have to do it securely, but if you make it too difficult for them, they're not going to be happy and they're going to go somewhere else. Convenience of security that fits to the scale of

information that these people are trying to access is what a lot of people are grappling with these days.”

The 2006, CSI/FBI Computer Crime and Security Survey shows that computer viruses have been a top organizational concern from as far back as 1999 – the only year it doesn't top insider abuse of Internet access as the number one challenge. From the year 2000 onward, viruses have continuously topped the list as the biggest security concern (with access abuse following closely behind).

The ISA's Clinton adds, “Just as the Internet has become increasingly easy-to-use, attacking the Internet has also become user friendly. A few years ago, only the ‘big-brained geeks’ knew how to hack into a system. Now you have websites all over the place that basically give you ‘hacking in ten easy lessons’, and this has been discovered by really bad people.”

But it took more than worms and viruses to build security line items into the operational budget for enterprise infrastructure. The threatscape started changing in parallel to the economic viability of the Web as a portal for business.

Dan Hubbard, Vice President of Security Research at Websense, explains, “It really wasn't until late 2003 and into 2004, with the advent of and the widespread use of phishing and spyware, that people were really all that concerned about the Web as an attack vector for infecting individuals, employees or organizations in some way. Prior to that, people were really more worried about email and Windows-based worms.”

From the enterprise perspective, IT departments scrambled to address the snowballing wave of security concerns – website defacement, unauthorized access to internal networks, unintentional introduction of viruses into the system, self-propagating and mutating worms, DoS attacks – with every new threat there stood a vendor with a product. But limited funds and internal resources, coupled with vendor solutions that could not respond quickly enough

to evolving attack mechanisms, soon created an enormous security conundrum.

“Every time you buy a computer security product, it's because you're trying to make up for the shortcomings of the products you currently have,” said **Bruce Schneier**, industry expert on new and emerging IT threats and the founder and CTO of managed security provider, BT Counterpane.

Evolution of the Threatscape

“Crime used to be based on proximity, but the Internet changed that. I would get next to you, hit you over the head and take your wallet. On the Internet there's no conscription to place, every place is ubiquitous to every other place. So you have more things like identity theft being perpetrated by organized crime syndicates from Eastern Europe and sub-Saharan Africa, because the criminals feel safer there,” says Schneier, “You, sitting in whatever happy town you are in the United States are usually protected by oceans from South East Asian criminals. But on the Net, you aren't. Globalization is extremely important. It makes it harder to track and prosecute criminals, and it makes it harder to defend yourself.”

“At the ISA, we've certainly seen a dramatic increase in computer crime throughout the industry. A few years ago hacking was done for show-off reasons, and ‘hacktivism’. Now it's serious, organized crime generating billions and billions of dollars. There's an economic incentive to become a computer attacker, which broadens the field,” notes Clinton.

Computer crime has become a full time income generator for savvy organized crime families. The exact cost of global loss due to fraud, targeted attacks and other types of computer crime may never be known as many organizations do not know

As online criminals continue to up the ante, targeted threats have become the challenge du jour. These attacks are especially insidious because they are designed to outsmart even the most sophisticated security solutions.

————— > *continued on page 6*

that they've been attacked or, if they do, prefer to keep the incidents under wraps rather than report their findings. However, the United States Federal Bureau of Investigation (FBI) estimates that computer crime, as a whole, costs U.S. industry \$400 billion dollars per year – topping drugs as the number one illicit pursuit of organized crime. The collaboration between “computer geeks” and traditional criminals has created a sort of blended attacker. The black hat community isn't known for their money laundering skills just as the Mob lacks a background in C++ programming. But the coming together of the two groups has yielded a powerful enemy, which has been very difficult to outwit.

“2005 is what I'd consider the year of the Internet criminal,” remarks Websense's Hubbard, “The criminal underground got significantly more involved in making money on the Internet through a number of different means. Techniques, such as phishing and targeted attacks, Trojan creation, stealing information from companies and their users, and creating large numbers of computers (bot networks) all allowed them to sell attack space, if you will. They could attempt to sell a certain type of attack or a certain set of machines to somebody that wanted to send spam,

conduct a DoS attack on a customer or extort a company.”

Although organizations realize that the Internet introduces a number of serious security issues,

they just aren't sure what to do about it. The best and most frequently updated vendor solutions offer some defense against online criminals. But it is always a race of threat vs. response, with the criminals often ahead of the game. “Internet security is a serious problem and it's not getting better. In fact, I think it's getting much worse. Organized crime has taken over in a big way. It's a huge growth area for crime and that's not going to change as long as there's profit to be made,” explains Schneier.

As online criminals continue to up the ante, targeted threats have become the challenge du jour. These attacks are especially insidious because they are designed to outsmart even the most sophisticated security solutions. Pursuing specific pieces of enterprise information, they are well-thought and often highly lucrative business.

According to Hubbard, “At Websense, we're seeing an industry trend of much more corporate and network espionage, as well as attacks that are going after specific entities and pieces of information. These items can range from the obvious (credit card numbers, user names and passwords and access to certain machines), to the not so obvious (like marketing plans and PR strategy, schematics and even confidential government documents). There is a lot of underground activity that is being designed to attack specific sectors or companies, or particular government agencies. There is even a flourishing business to conduct targeted attacks on behalf of other people.”

Although the term “cyber terrorism” feels like a fall out cliché from the events of 9/11, the government has continued to monitor the Internet, mitigating serious threats to our national infrastructure. Says Clinton, “The ISA has seen a worrisome amount of attention paid to the Internet by the international terrorist community. Initially they were using the Net for communication and recruiting – then it grew to fundraising. Now there are people at senior levels of government who are very, very concerned about the physical damage that can be done through cyber means. Incoming Secretary of Defense, Robert Gates, was widely quoted as calling the Internet ‘the ultimate weapon of mass destruction’, in relation the amount of physical damage that could occur from its misuse.”

“Technology isn't enough to bring security and trust to electronic transactions. We need good global laws and regulations. Criminals need to know they can be extradited for prosecution from any country where they break the law. And for global e-commerce to flourish, we need to know that the availability and integrity of information provided by businesses and government agencies is maintained at the highest levels, no matter where it is created,” insists Clinton.

Internet security is an evolutionary process that requires a hearty combination of vigilance, budgetary and personnel resources, and a clear definition of an organization's acceptable levels of risk.

So...How Have We Done?

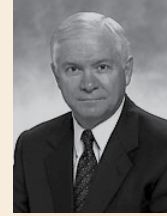
By all accounts, we have a long way to go as an industry in protecting ourselves against new and emerging Internet security threats. While nearly all of the individuals interviewed for this piece felt that the development of sophisticated anti-spam technology was the biggest industry success story, each noted that Internet crime remains the biggest threat to enterprise infrastructure. Internet security is an evolutionary process that requires a hearty combination of vigilance, budgetary and personnel resources, and a clear definition of an organization's acceptable levels of risk.

"The governmental structures that were built up over the last two centuries don't match up well with the problems of the 21st century because they don't really take into account the technology, globalization, or terrorism. So, we really need to rethink and restructure them, and that's a big job," says the ISA's Clinton. "On the corporate side, we find that organizational structures are not properly appreciating the actual values that they are receiving from security spending. As a result, they are not doing as good a job as they need to in terms of adopting best practices for security, making investment in security, or weaving security into their business plans."

"The level of protection we need for our modern economic infrastructure, and to gain high levels of trust in e-commerce and e-government, requires security to become in many ways, invisible. Because data is ubiquitous, and is increasingly being traded among agencies, citizens, partners and suppliers, simply keeping data secure within an application or a local area network is not enough. Security must become part of the entire fabric of modern communications and information exchange," said **Philippe Courtot**, Chairman and CEO of Qualys, Inc., "Security technology must be simplified and, for this to happen, it must become unified with the core infrastructure. When this happens, many aspects of information security will become 'invisible' as a result."

The new face of Internet security?

Incoming Secretary of Defense, Robert Gates, was widely quoted as calling the Internet "the ultimate weapon of mass destruction", in relation the amount of physical damage that could occur from its misuse.



RSA's Breton adds, "Before the Internet (in a world of closed, proprietary networks), you only worried about access control inside – you didn't worry about people from outside. Well, for the last ten years, we've been worried about the people outside. I think we've done a reasonable job of it, and we can always do better, but I think we took our eye off the ball a little bit inside because we had to build that 'Great Wall of China' out there to protect against the invading hordes that never used to come knocking at our door."

Dr. Claffy of CAIDA offers hope for the future of the Internet by explaining, "We made something so great that everyone wants it. In fact, many of us want it more than once!" She views the current industry as a historical artifact of technical, scientific and regulatory policy 'innovations' from the 60's, 70's, 80's, 90's, and today – pointing out, "While we were busy studying the interplay of people with the Internet, our economy and our future, it became global critical infrastructure. Oops." ■

About the Author

Melisa LaBancz-Bleasdale is a communications consultant and strategist specializing in the Internet security industry. Her focus is on emerging and innovative security technology, current events and market concerns.

Chinese Malware Seeks Online Passwords

If the malware originated in China, chances are it was designed to swipe your username and password. Industry-leading security firm, Sophos, reports that its analysis of viruses, spyware and spam (all of which was written in simplified Chinese) found that over 45 percent of them sought online gaming login information.

Another 7.5 percent of the studied malware was designed to grab usernames and passwords for the

Chinese QQ instant messaging client. While many may wonder what benefit grabbing an IM password holds, Sophos says that many people use the same password across multiple sites, including online banking.

To view the full press release about these findings, visit: <http://www.sophos.com/pressoffice/news/articles/2006/11/chinamalware.html>

All We Want for Christmas is the R&D Credit

Leaders from more than a dozen high-tech groups are urging Congress to renew the research and development (R&D) tax credit, during its post-election session. The United States was the innovator of the R&D tax credit in 1981. Now it has fallen behind other nations, and tech industry leaders warn that could make U.S. innovation fall behind, too.

According to William Archey, CEO of the tech group AeA, Australia now spends the most on R&D, and China offers generous benefits for companies increasing R&D spending by 10 percent each year. Archey compared that to the 20 percent R&D tax

credit the United States used to offer – which expired this year. “We used to be number one. We’re now sadly number 17,” said Rhett Dawson, CEO of the Information Technology Industry Council (ITIC). Industry officials agree that the R&D credit should be something the lame-duck Congress can pass – because it is a non-partisan issue with the potential to ensure that U.S. companies stay competitive in worldwide markets.

Additional information about the R&D tax credit can be found at: <http://www.investinamericasfuture.org/>

Gartner Reports: Web Security Fears Cause Online Commerce Loss

According to Gartner analysts, consumer anxiety about Internet security has caused a \$2 billion loss in e-commerce and banking transactions this year.

The study queried 5,000 U.S. adults about their e-commerce and banking decisions. Nearly half of those surveyed said their concerns about information theft, data breaches and Web-based attacks affected their purchasing payment, online transaction and email behavior.

To combat this backlash moving forward, Gartner notes that organizations will need to do more to actively regain consumer trust – not only by installing the right technology to improve security, but also visibly showing consumers what they are doing to secure information.

The full study, *Toolkit: E-Commerce Loses Big Because of Security Concerns*, is available at: www.gartner.com

McAfee Announces Security Risk Management Strategy

McAfee, Inc., the world's largest dedicated security company, recently outlined details of its security risk management strategy, providing enterprises with a more effective way to minimize risks from security threats and non-compliance. This strategy builds on McAfee's core strengths in threat prevention, by adding new compliance management capabilities including remediation, network access control and data loss prevention. With the acquisition and integration of organizations such as security policy

compliance firm, Citadel Security, and data protection technology provider, Onigma Ltd., McAfee becomes the first to integrate threat prevention with compliance management, providing enterprises with greater automation, operational efficiency and protection of their investments.

To learn more about McAfee's new strategy, visit: http://www.mcafee.com/us/about/press/corporate/2006/20061016_052000_1.html

SANS Top 20 Unveiled

The SANS Institute recently released the 2006 version of their annual "Top-20 Internet Security Attack Targets" list. The SANS Top-20 2006 gives organizations a starting point to address critical security issues. The list is compiled from recommendations by leading security researchers and companies around the world.

According to the Top-20 list, the shift from server-side to client-side vulnerabilities continues to be an increasing trend, as are attacks by cyber criminals for financial gain. Also highlighted, was a significant surge in the number of online criminals in Asian

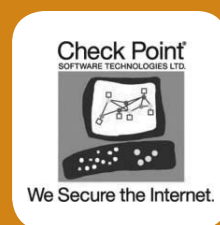
countries, as well as Eastern European initiated attacks. As a result, several banks have reported 400 to 500 percent increases in losses to cyber fraud from 2005 to 2006. The list showed a marked change from previous years – with technologies such as VoIP and factors like "human error" being included for the first time. Sections for cross-platform applications, network devices, policy and the overall issue of zero-day attacks were also added.

For the complete list of the SANS Top-20 vulnerabilities, and more details about each, visit: www.sans.org/top20

company spotlight

Check Point Software

Check Point Software Technologies Ltd. is a leader in securing the Internet. The company provides security software for corporate networks and service providers, spanning firewalls, intranets, and extranets. Check Point also offers products that enable companies to set up virtual private networks for added security and availability.



Making Internet communications secure, reliable and available everywhere has been and continues to be Check Point's ongoing vision. The company is committed to staying focused on real customer needs, developing new and innovative security solutions and continuing to redefine the security landscape. www.checkpoint.com

IRONPORT SYSTEMS, the leader in Internet Gateway Security, has recently introduced the IronPort S-Series Web Security Appliance. This enterprise class solution delivers the industry's most comprehensive malware protection by integrating processing at both the network layer and at the application proxy layer. Furthermore, the IronPort S-Series includes a heavily optimized, high-performance signature-based scanning engine as well as the first Web reputation system.

Network-Layer Protection

The IronPort S-Series™ has an integrated Layer (L4) traffic monitor. This wire-speed device can sit inline or on a network tap. It monitors all network activity looking for malicious traffic that is trying to “phone home” or connect to a rogue server. The L4 traffic monitor shares data with IronPort's Web reputation system, to identify and stop malware before it does harm. The L4 traffic monitor also does an excellent job of identifying the most infected PCs on the corporate network—allowing IT administrators to proactively and efficiently launch desktop clean up efforts.

Proxy-Layer Processing

The IronPort S-Series also includes an extremely high performance Web proxy. Built on IronPort's proprietary operating system, AsyncOS™, the IronPort S-Series proxy can support up to 100,000 simultaneous connections—as much as 10x more than traditional UNIX-based proxy servers.

Accelerated Signature Scanning

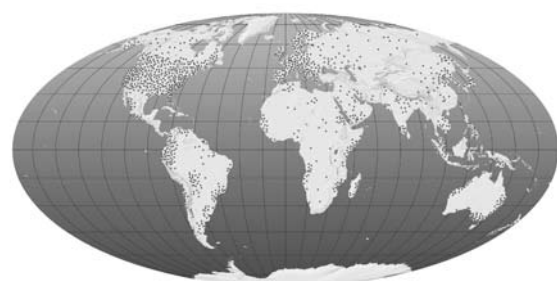
IronPort® developed its proprietary Dynamic Vectoring and Streaming™ (DVS) engine to accelerate the signature scanning of Web content and minimize latency. The DVS engine performs intelligent scanning and reputation-based caching to minimize the amount of scanning that actually needs to take place. When an object does need to be scanned, the DVS engine has a unique streaming capability. It can scan an object while simultaneously receiving the remainder of it and buffering it though to the end-user. The combination of intelligent scanning and streaming of data yields a decrease in latency that approaches 1/10th that of traditional signature-based systems. This makes the IronPort S-Series imperceptible to end-users.

The World's First Web Reputation System

IronPort invented the concept of reputation filtering more than three years ago. This capability is at the heart of the IronPort S-Series. For each Web request, IronPort makes an assessment of the reputation (or trustworthiness) of the URL requested. This reputation score is based on over 45 different parameters, including such factors as:

- How long has the domain been registered?
- What is the country of origin?
- What is the IP range of the hosting server?
- How does the name server infrastructure behave?
- How much traffic is the URL getting?

By analyzing these objective parameters the Web reputation system can make a very accurate determination about every active Web server on the Internet. Based on configurable thresholds, the IronPort S-Series will reject traffic that is clearly hostile—without wasting system resources on a full signature scan. Similarly, known good traffic with a sufficiently positive reputation score will bypass the DVS



Over 100,000 organizations participate in IronPort's SenderBase Network, enabling the world's largest email and Web traffic monitoring system.



The IronPort S-Series Web security appliance: Powerful malware protection enables the industry's most comprehensive perimeter defense.

scanning engine and move right through to the end-user. Traffic with a neutral or slightly negative score will be passed to the DVS engine for further analysis.

By creating a score for each individual URL, IronPort's Web reputation system can rectify an increasing problem. Legitimate websites (the most recent being myspace.com) will often host an ad through an advertising network. However, they do not control the content of the ad. Nefarious advertisers can come from a server that is two or three parties removed—an affiliate of an affiliate of the ad network. Sometimes these advertisers will use this mechanism to deliver malware to unsuspecting machines, even though the ad appeared on a legitimate, trusted site. Because IronPort's Web reputation system assigns individual URL scoring, the questionable ad would be given a neutral score and be sent to the DVS scanning engine—but the remaining objects on the page would be given a high score and be exempt from signature scanning.

This is an excellent example of how IronPort's Web reputation system maximizes system throughput, reduces latency and increases overall accuracy by as much as 20 percent.

Powered by IronPort's SenderBase

IronPort's SenderBase® is the world's first, biggest and best traffic monitoring network. SenderBase measures more than 25 percent of the world's messaging traffic, receiving over five billion queries per day. IronPort appliances are deployed at eight of the ten largest ISPs in the world, as well as more than 40 percent of the Global 100—the 100 largest corporations in the world. Having access to this type of traffic is a key differentiator for both SenderBase and IronPort. SenderBase is unique in that it even collects data from the

networks of organizations that are not IronPort customers. IronPort shares data with other large ISPs in a data peering relationship. Currently, there are over 100,000 different networks contributing data to SenderBase. This translates into the industry's most accurate reputation system. IronPort's Web reputation system can increase malware catch rates by more than 20 percent over signature-based scanning alone—an unprecedented increase in efficacy.

Enterprise Management Tools

Global corporations need powerful management and reporting systems to optimize their investment and minimize the required administration time. The IronPort S-Series is built on IronPort's proprietary AsyncOS operating system and thus it inherits the world class management and reporting capability that has made the IronPort C-Series™ the number one choice among enterprises for email security.

The IronPort Advantage

IronPort Systems is focused on building comprehensive gateway security for enterprise customers. IronPort is a clear leader in the industry, pioneering technical breakthroughs like reputation systems and very high performance proxy appliance designs. IronPort's industry-leading systems have a demonstrated record of unparalleled performance, accuracy and reliability. To secure greater protection for your company's messaging system, visit www.ironport.com or call 650-989-6530.



www.ironport.com

PAGE 1 What Have We Done?

The Internet As Global Critical Infrastructure

Provocative, insightful and educational commentary about the security and scalability of the Internet. Contributors to this feature include representatives from technology companies, trade associations, research groups and the Federal government.

PAGE 8 Web Security News

Your source for short takes on Web security tales, tools, tips and trends.

PAGE 10 Sponsor Profile

Web Security Report sponsor, IronPort Systems, is developing revolutionary technologies to help make the Internet safe.

THE WEB SECURITY REPORT

A Messaging Media Publication

BUSINESS OFFICES

Messaging Media, LLC
P.O. Box 643084
Los Angeles, CA 90064
Phone: 866-808-4200
Fax: 310-836-4067

ADVERTISING/SPONSORSHIP INFORMATION

Managing Partner: Tim Matteson
publish@websecurityreport.com
866-808-4200 (ext. 361)

the Web Security report

Messaging Media, LLC
10536 Putney Road
Los Angeles, CA 90064