<special_advertising_section>

< e_security >

Managing Your Risk: Complex Threats, Proactive Solutions

<e_security>

Managing Your Risk: Complex Threats, Proactive Solutions

(N)ot so long ago, information security was a matter of implementing the right products—technologies that would allow "good" users access to the network and keep "bad" people out.

Today, e-security is nowhere near as simple as that.

E-business applications allow—and even encourage—unknown users to access corporate Web sites. An extended supply chain, which can include employees, partners, distributors, and customers, means that a company's network no longer has definable perimeters. And the current generation of hackers is more skilled, determined, and professional than ever before. Whereas most of the hackers once were bored or disgruntled teenagers, cyber-criminals now breach corporate security in the name of profit, political activism, or sheer malice.

"There is no question that the world of electronic security is getting more complicated," says Bob Bush, chief security consultant for AOL Time Warner. "The number of hacking attempts is increasing dramatically, and vulnerabilities surface almost daily."

The effect on those targeted can range from mere inconvenience to major destruction. In May, hackers gained control of three international Microsoft home pages, changing company information into a taunting message. Recent denial of service (DOS) attacks on companies such as Compaq, Hewlett-Packard, Gateway, Disney, and Yahoo! disabled corporate Web sites, doubtlessly causing serious amounts of lost revenue.

When intruders penetrated Western Union's Web site last year, the company reported that more than 15,000 credit card numbers had been stolen. Visa U.S.A. lost at least $48 million in 2000 to online credit card scams. And cyber-criminals have made off with top-secret U.S. computer system codes that guide space ships, rockets, and satellites.

"The question is no longer whether you have enough security," says Phil Mellinger, chief information security officer for First Data Corp. "The question is when you will be hit. Companies put their sites on the Internet and expose their corporate data assets to the world, including thousands of hackers worldwide. The threat is so overwhelming that it's impossible to ignore."

Countering this risk is not a matter of fortress-building, it is a matter of instituting a measured risk management program. As with physical security, e-security requires a balance between the cost and inconvenience of strong security measures and the amount of protection you get. "Every part of e-security is a business risk management balancing act," says Steve Katz, a first vice president in technology infrastructure services for Merrill Lynch.

<special_advertising_section>

Fundamental Questions

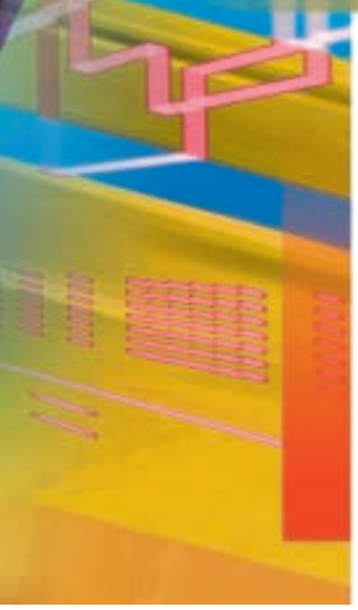
Katz specifies seven fundamental issues that a comprehensive e-security strategy should address: identity, proof, access, transaction confidentiality, message integrity, nonrepudiation, and responsiveness to problems.

Identity establishes who the user is who wants access to the data resources. Proof requires presentation of information that only the user knows. ID and proof technology must be complex enough to protect the business, but not so complicated and challenging that it discourages users.

Access determines which tasks a user is permitted to perform; it can be set up in a profile that specifies limits on the data available, purchase values, or transaction frequency available to a user. Because e-mail transmissions can be intercepted and read if not protected, the e-security strategy must also address transaction confidentiality.

"Every part of e-security is a business risk management balancing act."

– Steve Katz, First Vice President in Technology Infrastructure Services, Merrill Lynch



Message integrity is also critical. Instance: If a person sends a message ordering his or her broker to sell 100 shares of stock, the e-security technology must ensure that the data is not corrupted intentionally or otherwise. Nonrepudiation locks both the message sender and recipient into a situation in which neither party can deny sending or receiving the message.

Finally, any e-security breaches that occur must be addressed quickly. Alarms should immediately notify appropriate personnel of breaches so that damage can be limited or controlled.

New Devices, New Vulnerabilities

Many of the standard security issues raised by wired networks are complicated when corporate wireless LANs and devices such as PDAs are involved. Paul S. Raines, global head of information risk management for Barclays Capital, says that many corporations using wireless LANs lack even basic authentication techniques.

PDAs present an opportunity for catastrophic virus or security vulnerability. "In an extreme case, hackers could use the infrared connections to install a virus on your PDA while you sit in a meeting, without you even knowing," Raines says. "Users want to be more mobile than ever, and 'mobile' means wireless. Wireless is where most of the security work will take place in the next few years."

Obstacles and Solutions

Mellinger of First Data says that simple measures could go a long way toward protecting electronic transactions. He says companies should institute policies to keep the amount of data stored online to a minimum (keeping close track of where that information is stored). He also advises corporations to take the initiative and test for their own vulnerabilities.

Some corporations have begun looking into e-business insurance for financial protection against cyber-crime. But Bob Bush of AOL Time Warner says underwriters must struggle to craft effective policies, because not only can it be difficult to quantify the statistical probability of electronic penetration, but weighing the value of the breach or the liability of the corporation is not easy.

But whichever way a company chooses to go in addressing security, the bottom line is that executives must take action. To ignore the problem borders on abdication of responsibility. As Steve Katz says: "CEOs must understand that e-security is not about pleasing industry regulators or stockholders. E-security is the foundation for trust and privacy, which is absolutely critical to customers. Companies must implement e-security because it allows customers to trust them, and customer trust is the name of the game."

Web Directory >

Computer Associates > www.computerassociates.com
Check Point Software Technologies > www.checkpoint.com
Gemplus > www.gemplus.com
Intel > www.intel.com

If you are interested in advertising in the next e-security section, contact Kathleen Matts, Associate Director/FORTUNE Custom Projects at kathleen.matts@timeinc.com or call 212-522-4420.

Produced by Eric Green • Written by CMK Communications Group, contact Cheryl Krivda at 215.257.3874 • Edited by James S. Harrison • Designed by Segal Savad

Reprints of this section are available in quantities of 100 or more; custom reprints can also be created. To obtain a reprint order form, please fax your request to Randi Bergman at 212-522-0999 or send an e-mail to randi.bergman@timeinc.com.

FOR MORE INFORMATION ABOUT THE ADVERTISERS IN THIS SECTION, PLEASE SEE THE READER RESPONSE PAGE IN THIS ISSUE.

Check Point Secures the Internet >

The Internet is rapidly becoming the communications backbone of corporations everywhere. Ubiquitous, less costly than other communications technologies, and eminently scalable, the Net offers real benefits for companies that are supporting voice and data communications among employees, customers, and business partners.

Yet the Internet is understood to be less secure than traditional communications technologies. And, traditional communications lines are surprisingly insecure to begin with. Security breaches, stolen data, and altered communications make executives ask: How can I make the Internet safe and manageable for my company's communications? The answer: comprehensive, integrated virtual private networks (VPNs).

"Working collaboratively demands new levels of security and integrity," says Ungerman. "Only VPNs deliver the power of the Internet made secure."

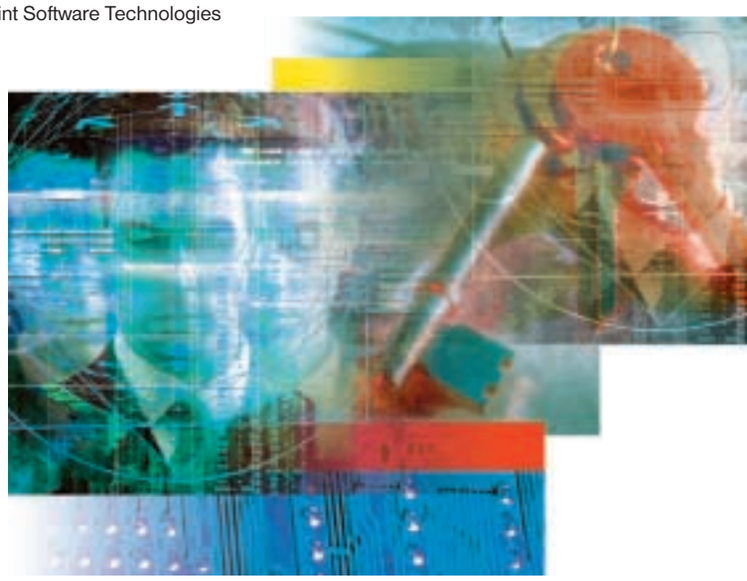
But not all VPNs offer the same degree of security. How should business leaders choose from among the available VPN solutions? Consider the integration, manageability, and scalability of the technology.

VPNs should be integrated with the overall Internet security of the business. While some products separate VPN security from other protection, this approach can be dangerous. "Stand-alone VPNs with discrete security technologies can compromise the integrity of the entire show," Ungerman says. "Corporations require VPN technology that's fully integrated into the corporate security strategy."

Comprehensive VPN security must reach from end to end—including client laptops, which can otherwise create significant risks. For example, clients who use DSL or cable modem Internet access are essentially wide open to breaches. And clients should be managed centrally to ensure that they don't violate corporate security policy by acting as Web servers or engaging in peer-to-peer transmission.

"VPNs have a tremendous ROI and offer cost-savings that are impossible to ignore."

– Jerry Ungerman, President, Check Point Software Technologies



By funneling communications through a protected "tunnel" and integrating them with the company's network security, VPNs help businesses cost-effectively harness the power of the Internet. A secure tunnel is not enough. Both ends and all networks have to be secured. The key is a comprehensive, integrated security infrastructure, such as Check Point's Secure Virtual Network (SVN) architecture. Stand-alone VPNs cannot offer the security and management needed for today's corporations.

Companies using VPNs commonly save upwards of 80 percent of their telecommunication costs. By replacing remote dial-up access with VPN connectivity, businesses can reduce the number of lines maintained for communicating with remote employees. Charges for toll-free access numbers or toll charges using calling cards for domestic or international communications can also be slashed.

"VPNs have tremendous ROI and offer cost savings that are impossible to ignore," says Jerry Ungerman, president of Check Point Software Technologies. Check Point's VPN-1 Next Generation product family offers comprehensive, integrated VPNs that are easy to use, manage, and scale with the highest levels of integrated security and performance. "The typical payback period for a VPN's installation is one month," Ungerman adds. "Companies can easily save hundreds of thousands of dollars a year in communication costs."

The greater benefit of VPN technology may lie in the strategic advantage it can deliver. By providing secure, nearly instant communications between offices, employees, customers, and partners, VPNs can deliver unprecedented access to data, applications, and information.

Finally, with new branch offices, remote employees, and merger and acquisition activity, executives need VPN technology that can be scaled without compromising effective centralized management. "The last thing you want," says Ungerman, "is to have to update individual VPN gateway servers each and every time your organization grows."

Under the framework of its SVN architecture, Check Point's Next Generation VPN infrastructure cost-effectively and manageably protects all aspects of enterprise security. Ungerman says: "Check Point Next Generation enables VPNs to be broadly used by every corporation. By securing the Internet, Check Point provides businesses with a secure path to the future."

Gemplus® Smart Cards: Meeting Diverse Customer Needs >

The slowing economy—along with recent declines in the stock market—is forcing many CIOs to reevaluate their IT spending plans. As a result, many CIOs find themselves forced to cut IT expenses and generate new opportunities for a wide variety of customers.

Such cuts can translate into reduced operational support. To sustain profitability, corporations trimming IT investment budgets must generate more revenue with the same assets—that is, they must increase productivity. In support of this goal, companies also must more effectively retain profitable customers by delivering personalized services that breed loyalty.

For executives with vision, these changing economic conditions actually offer tremendous opportunity. But the challenge of converting the softening economy into real advantage is one that requires the assistance of forward-thinking solutions providers such as Gemplus®.

Gemplus, the world's leading provider of smart card-based solutions for security, wireless, and enterprise e-business applications, offers the next generation of productivity-enhancing information and privacy protection solutions. Gemplus provides key components of the technology value chain, such as reader infrastructures, wireless subscriber identification module (SIM) cards, and application management.

"Gemplus excels in providing total information and privacy protection solutions to wireless, financial services, and enterprise customers," says Gilles Michel, executive vice president for financial and e-business services. "With the next generation of smart card solutions, Gemplus helps companies make their client devices smarter, which can be critical to maintaining profitability and maximizing return on assets."

Because the new generation of smart card-based solutions is built on open Java®-based technology, the smart client empowers end users with new features and functions. The potential applications are virtually unlimited.

First USA/Bank One chose Gemplus to provide a smart card program to address a variety of customer needs. "As the largest Visa issuer, First USA continuously strives to improve our products and services to meet our cardmembers' changing needs," says Doug Filak, senior vice president for new product development and emerging technologies, First USA/Bank One. "We continually search for new technologies that will provide our customers with enhanced convenience, functionality, and security for navigating their way through the virtual world. Gemplus has been instrumental in helping us develop and enhance our products in order to solve many of the issues relating to the most complex technologies."

The computational intelligence of Gemplus smart cards allows customers to use one card to support many applications, thereby meeting consumers' extensive portfolio of payment needs. The smart card solution transforms the traditional payment card from a product into a service tool – a tool that enables consumers to fulfill multiple needs, based on which channel and medium they're using, where they are, and when they want to use it.

Offering best-in-class technology to corporations around the world, Gemplus is the only provider of smart card-based solutions to work with industry leaders such as IBM®, iPlanet™, and Sun Microsystems®. Gemplus leads the industry in wireless SIM cards and in the financial and security services market.

"Gemplus is the market leader," says Terfel Roberts, director of business development for Nextel Communications, Inc. "They brought their considerable technical expertise to bear in our vision for international roaming. Gemplus worked with us as partners to help us get to market first."

> "Gemplus has been instrumental in helping us develop and enhance our products."
>
> – Doug Filak, Senior Vice President for New Product Development and Emerging Technologies, First USA®/Bank One®

As one of the primary providers of technology to Visa U.S.A.'s Smart Visa program, Gemplus even worked with its own competitors to ensure that the ultimate product most effectively met Visa's needs. Says Patrick Gauthier, senior vice president of smart card applications and marketing development for VISA U.S.A.: "Gemplus was most willing to work hard at developing the markets in multiple ways. They put aside their short-term interests for the purpose of providing a superior solution in developing the market. We wouldn't be where we are today if it weren't for the contributions of Gemplus."

Computer Associates: Enabling Trusted E-Business >

For medium- to large-size companies, the challenge of security has never been greater. New technologies such as wireless and the Internet have opened unlimited avenues of e-business opportunity, enabling companies to conduct business and share information on a global basis. But as technology evolves, it's imperative that corporations keep pace with solutions that enable them to expand the borders of their enterprise—quickly, safely, and securely. Vendors have responded with a broad slate of new products, leaving executives scrambling to decide which to implement and how to make them all work together.

Many companies hire system implementers, hoping that experts can stitch point products into a unified solution. But the costs are staggering, and maintaining the system over time can become a true nightmare.

How can business leaders do it all—seeing to it that the corporate security solution addresses all potential vulnerabilities and that discrete products work together seamlessly—without busting the budget?

Introducing eTrust security software from Computer Associates. eTrust helps businesses defend against perimeter intrusions, enables Internet access, and manages access to enterprise IT assets. Designed to work together, this family of products reduces integration costs and ongoing maintenance expenses.

"CA offers products that are deeper and broader than anything else on the market today," says Barry Keyes, vice president eTrust Solutions, Computer Associates. "No matter which e-business asset you need to protect—Web sites, databases, enterprise servers, applications, data warehouses, or ERP/CRM solutions—Computer Associates' eTrust technology does the job."

Computer Associates has been developing security solutions for decades, delivering expertise unmatched by newer niche vendors. Business executives recognize this leadership: 99 percent of FORTUNE 500® companies use Computer Associates products. And with nearly 20 eTrust products, Computer Associates sells more security software than anyone else.

"Computer Associates offers a combination of greater convenience and reliability for buyers," says Jim Hurley, managing director of security for Aberdeen Group. "In addition to having security solutions in every space, Computer Associates has added the ability to configure, manage, and maintain security by business policy rather than by technology controls. They are ahead of the supplier market, but they're in step with what buyers want."

Key to the success of eTrust is the seamless integration across the entire product line. All eTrust products work together, exchanging data, optimizing security operations, and leveraging the efficiencies that can only occur when technologies are tightly integrated. When one eTrust product is enhanced or upgraded, the others in the suite transparently incorporate changes, eliminating the need for customized development and implementation common to best-of-breed solutions.

"A company with eTrust Web Access Control and eTrust Single Sign-On could have an internal or external user strongly authenticated with a certificate issued from eTrust PKI, have the certificate validated in real time by eTrust OCSPro, and provide personalized access to permitted applications," Keyes says. "And it would all work seamlessly. That's the primary difference between Computer Associates' solutions and everything else."

Companies need not buy the entire eTrust family of products; a business that needs only one or a few products can buy just those. Each eTrust solution can function independently or with whichever other eTrust products are installed. In addition, eTrust is an open solution that can interoperate with other security technologies. For companies that need assistance optimizing their overall security infrastructure, Computer Associates offers state-of-the-art implementation and integration services.

With a simplified new business model, service offering, and pricing structure, Computer Associates makes trusted eBusiness a painless experience. Says Keyes: "Larger businesses need many types of security technologies, but they don't want the time or expense that comes with integrating them. eTrust delivers precisely what they need."

"eTrust offers security products that are deeper and broader than anything else on the market today."

– Barry Keyes, Vice President eTrust Solutions, Computer Associates

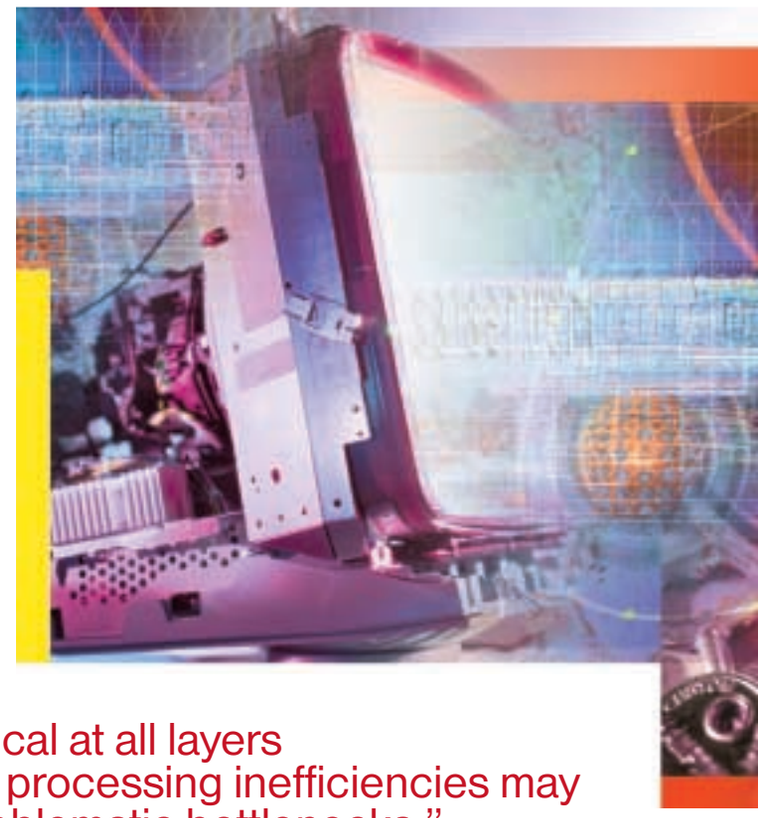
Intel Partners for New E-security Efficiencies >

(T)rusted e-business is impossible without e-security. Without comprehensive, well-planned protection, businesses imperil their success—to the point of risking the solvency of the corporation.

But the security technologies that address these risks rely on processing-intensive math operations. Some security products so negatively impact the performance of clients, servers, and the network that organizations opt to minimize or eliminate security entirely, choosing productivity over safety.

Now, there is no longer any need to have to make this choice. Business executives can see to it that maximum efficiencies have been built directly into companies' computing platforms by selecting the infrastructure building-block vendor that works to optimize system and application performance: Intel Corporation. Intel®, the industry's leading vendor of high-performance computing microprocessors, is also a leading force behind e-security efficiencies. By championing industry standards and initiatives, working closely with applications vendors, and developing innovative technology platforms powered by the Pentium™, Xeon™, and new Itanium™ processor families, Intel-based servers provide a solid foundation for today's corporate e-security strategies.

Intel developed the Wired for Management (WfM) specification, which is used by millions of users to strengthen authentication during PC start-up, thereby reducing vulnerability to so-called "Trojan horse" attacks. Furthermore, Intel supports Internet Protocol Security standard, which provides end-to-end encryption and authentication, protects data on both sides of firewalls, ensures data integrity and confidentiality, and is transparent to applications.



"As security becomes more critical at all layers of the enterprise, processing inefficiencies may create increasingly problematic bottlenecks."

– Mike Fister, Vice President and General Manager, Intel® Enterprise Platforms Group

Initiative Support

In a world with perfect security, all messages, transactions, and connections would be trusted, reliable, immediate, and protected. But companies that adopt technologies to address each of these needs must also worry about performance. "The lack of speed and reliability in security is one of the roadblocks to large-scale adoption of e-commerce," says Mike Fister, vice president and general manager for Intel's Enterprise Platforms Group. "As security becomes more critical at all layers of the enterprise, processing inefficiencies have the potential to create increasingly problematic bottlenecks."

Intel supports several significant industry initiatives designed to address various aspects of the security/performance issue. Intel recently joined with Compaq, Hewlett-Packard, IBM, and Microsoft to form the Trusted Computing Platform Alliance (TCPA). Through the collaboration of 150 partners, TCPA just released a specification to help vendors deliver enhanced hardware and operating system-based trusted computing platforms.

Intel's Common Data Security Architecture (CDSA) addresses operating systems (OSs) and middleware; CDSA helps developers create stable application programming interfaces, adopt best-of-breed security technologies faster, lowers development costs, and reduces application time to market. For IT departments, CDSA supports the use of interoperable applications in mixed OS environments, reduces cost and risk, and increases deployment flexibility.

Enabling Efficiencies through Partnerships

In addition to supporting and leading industry initiatives, Intel uses its optimization, tuning, and software development expertise to help IT vendors shorten their time to market for security products. Through developer services; solution services like integration, optimization, and solutions scaling; worldwide solutions centers; and software development products, Intel helps partner vendors maximize processing efficiency.

Intel also partners with leading software vendors to optimize both hardware processing and application code.

"Performance improvements we make in concert with Intel translate into real dollars for customers."

– Mike Vergara, Director of Product Marketing, RSA Security

Says Rick A. Smith, Intel solutions product manager: "Intel's success in security, a key e-business building block, is due to our strategic relationships with the industry's leading software and OS vendors. These solution providers have worked with us to deliver enhanced reliability, leading security and application performance, and scalability on Intel Pentium, Xeon, and Itanium systems."

For example, RSA Security, a leading e-security vendor, has worked with Intel since the mid-1990s. "Processing-intensive security technologies put a strain on many devices," says Mike Vergara, director of product marketing for RSA Security. "For e-commerce applications, the faster you can make connections, the faster you can process transactions, the more people you can serve, and the more money you can make. The performance improvements we make in concert with Intel translate into real dollars for customers."

Network Associates, whose McAfee division develops antivirus products, has also been a long-time Intel collaborator, with positive results. "Intel's early development programs, their willingness to provide early technology and engineering resources, and early documentation about that technology has been outstanding," says Christopher Bolin, senior vice president of product development for McAfee. "Their cooperativeness has been better than any other of our big partners by a long shot, which helps us to serve our customers."

Other collaborative efforts include examples like Intel's relationship with Covalent Technologies. Covalent maximized the performance of SSL-encrypted sessions in its Apache Web server product by building on the Intel Itanium processor-based platform and using RSA Security's BSAFE SSL-C product, which is also optimized for Itanium. Separately, Entrust Technologies recently worked with Intel to distribute its trust relationship management software on Intel architecture.

Numerous other vendors of security software products also work closely with Intel. Symantec Corporation, an Internet security vendor, and Intel have enjoyed a lengthy beneficial association. "Our relationship with Intel has been a key component of our overall strategy to provide our corporate customers with centrally managed, leading-edge security solutions," says Gary Ulaner, Symantec group product manager. "By working with Intel, we are continuing to provide our customers with a world-class antivirus solution."

By working so diligently with so many vendors, Intel ensures that enterprise solutions deliver high performance and maximal protection for all operating systems—including 64-bit HP-UX, AIX, Linux, and Windows, as well as existing versions of 32-bit Unix and Microsoft Windows. Says Intel's Rick Smith: "Customers can expect premier performance of Intel products and security solutions on every OS."

Building Blocks

Beyond supporting industry initiatives and enabling software enhancements, Intel's real strength lies in delivering building-block technology for high-performance security solutions. From the Intel PRO™ family of security-enabled network adapters to the NetStructure™ family of virtual private network (VPN) solutions, Intel technology helps corporations develop entrusted e-business practices.

Intel's comprehensive selection of processors enhances secure e-commerce transactions. The Xeon processor is more than twice as fast on secure transactions as its closest competitor, primarily because of features to speed up the large computations required for public key cryptography.

The new Itanium processor, based on Intel's unique EPIC 64-bit architecture, offers even more dramatic performance. In tests on preproduction hardware, the Itanium processor-based platform performed 11 times faster than the competition, processing more than 1,300 secure transactions each second.

And Intel relies on this technology to protect its own assets. "As Intel moves closer to its goal of becoming a 100 percent e-corporation, every aspect of our business becomes more and more reliant on secure computing and transactions," says Doug Busch, vice president and director of Intel Information Technology. "We rely on our own microprocessor-based products to deliver both the internal and external computing security necessary to run a multibillion-dollar corporation with very high confidence."

RSA's Mike Vergara says that Intel's practice of working with vendors to squeeze every drop of performance from its products and their solutions demonstrates Intel's commitment to corporations. "In the past, businesses haven't implemented security solutions because it was too much of a drag on their systems," he says. "Now with the new Intel hardware and RSA software, it doesn't have to be that way. Companies can run their security applications at the speed they need, and at the volume they want. It's available now, because vendors like RSA are making it work with Intel."