



white paper

may 2002

hp virtualvault

**trusted and secure deployment of  
Internet-enabled business services**

**spotlight on the financial services industry**



## table of contents

executive summary .....	3
transitioning to a Web-enabled business world .....	4
<b>building a bridge to next-generation computing</b> .....	4
<b>key benefits of an Internet-enabled infrastructure</b> .....	5
addressing the risks of Web-enabled business services.....	6
<b>a virtual menu of e-business vulnerabilities</b> .....	7
<b>a thin line of defense</b> .....	7
specific challenges facing financial services firms.....	8
<b>recent industry-changing events and trends</b> .....	8
<b>corresponding technical challenges</b> .....	9
<b>security issues raise the competitive stakes</b> .....	9
the firewall fallacy .....	10
<b>delivering solid protection under specific circumstances</b> .....	11
<b>a wish list of security goals</b> .....	11
hp virtualvault: raising the security bar.....	12
<b>brief description of virtualvault</b> .....	14
<b>key benefits</b> .....	14
<b>alignment with security goals</b> .....	14
looking forward.....	15
for more information.....	16

**Businesses are rapidly shifting to service-centric computing models that allow them to offer Web-enabled applications to customers, suppliers, and partners over the Internet. By leveraging the ubiquitous, platform-independent, and “always-on” qualities of the Internet, companies today can respond quickly to shifting market dynamics and create new business services based on internal stores of proprietary information, transaction data, and other high-value digital resources. Recent examples of successful commercial Web-enabled business services include home banking, online travel transactions, and just-in-time inventory replenishment, to name just a few.**

**Financial services firms in particular have long been on the leading edge of deploying Web-enabled services for both consumer and business-to-business (B2B) customers. Making a strategic commitment to Web-based services enables banks, brokerage houses, insurance companies, and other financial firms to seize new revenue opportunities while simultaneously reducing operational costs.**

**But “opening up” internal data and program resources to external users via the Internet raises significant security issues. For example, customer account transactions, PIN codes, credit card numbers, and other financial information are high-value corporate assets in their own right and, as such, are uniquely vulnerable to theft, corruption, or loss. Although the strategic benefits of deploying Web-enabled business services are real, so are the accompanying risks. Given the patchwork nature of IT infrastructures currently in place, even those businesses that already deploy standard security mechanisms such as firewalls, Secure Sockets Layer (SSL) encryption, and digital certificates are vulnerable to attacks.**

**This white paper focuses on the security challenges that inevitably arise when businesses try to reap the financial and operational advantages of Web-enabled e-business services. Increasingly, such firms seek holistic and multi-pronged security strategies that deploy functionally overlapping deterrents and thus “raise the bar” on overall protection across all vulnerable operations. Although focused primarily on the financial services industry, the information in this paper is applicable to other business sectors as well.**

**The paper includes a concise introduction to HP Virtualvault, the leading application security product in the financial services industry today. By incorporating a commercial version of a military-grade operating system—and coordinating multiple security strategies within a single, standards-based integrated product—Virtualvault has also garnered a significant and growing share of the global security applications market. Widely viewed as the most secure run-time e-business platform available today, Virtualvault continues to expand its installed base of blue-chip enterprise, government, and technology vendor customers.**

## **transitioning to a Web-enabled business world**

**Most members of the business community initially perceived the Internet as an arcane academic research tool completely lacking in commercial value. Today, of course, the Internet serves not only as a cost-effective way to disseminate business information—its first commercial use—but also as an extraordinarily rich environment for designing, building, and implementing a widening array of innovative business services.**

**Many businesses are currently in the process of transitioning their legacy application infrastructures into platforms that support emerging Internet-based e-commerce services. However, significant existing investments in host/ and client/server technologies mean most enterprises cannot afford to immediately switch to this new computing model, even when the benefits are compelling. Along with cost considerations, security concerns are also slowing businesses' transition to IT infrastructures that are fully Web enabled.**

## **building a bridge to next-generation computing**

**A direct result of the large installed base of traditional system infrastructure components is that many businesses today deploy a diverse range of applications in various stages of Internet readiness. Businesses typically upgrade and strengthen their security efforts incrementally to support their increased deployment of Web-based services.**

**The following are three basic categories of Internet-enabled applications as defined by degree of openness to external requests for data or services:**

- **outbound access to the Internet—Early commercial adopters of the Internet began building limited connections between internal applications and external (Internet) resources in the late 1980s and early 1990s. Although these early efforts typically gave employees some degree of outbound access to the Internet, inbound traffic—including access to internal data and applications by external Internet users—was usually blocked. Efforts to make this sort of application secure consisted largely of constructing elementary firewalls that acted as one-way mirrors onto the Internet. A significant number of businesses today still maintain applications in this category.**
- **limited two-way connectivity with the Internet—The emergence of the World Wide Web and the debut of graphical interfaces, or browsers, spurred businesses to take advantage of the Internet to deliver business information to external users—usually static content in the form of Web pages. Because granting even the most limited requests for internal data from Internet-based (external) users raised significant security risks, businesses began placing content on Web servers that were separated from internal systems by one or more firewalls. This practice kept internal information safe by giving external users access only to limited amounts of data stored outside the firewall(s).**
- **dynamic interactions between external Internet users and internal data and applications—The most sophisticated e-business initiatives today use Web servers as front ends for delivering dynamic data and services to external Internet users. Although opening up internal data and applications to the Internet in this way increases vulnerability to hacker attacks and other security breaches, most businesses still depend primarily on firewalls to prevent unauthorized access to their internal networks.**

## **key benefits of an Internet-enabled infrastructure**

**Despite the increased risks associated with implementation of Web-enabled services, many businesses—particularly in the financial sector—are aggressively moving toward offering such services because of the significant competitive advantages involved.**

**Among other benefits, Web-enabled e-services allow businesses of all sizes and types to accomplish the following:**

- **expand business opportunities by enabling enterprises to offer new types of products and services**
- **reduce time-to-market and development costs of such products and services**
- **deliver personalized versions of products and services to individual customers**
- **identify the most profitable customers and create one-to-one marketing programs targeting their needs**
- **reduce operating costs and increase return on investment (ROI)**
- **establish electronic partnerships with other businesses that transparently deliver additional value to customers**
- **offer multiple integrated channels for customer transactions and communication so customers can interact with a business via telephone, e-mail, Web site, brick-and-mortar store, or any combination of the above**

**In the financial services industry, the ability to offer services such as online mortgage closings (utilizing electronic signatures) and real-time global access to investment portfolios can be a key differentiator for businesses experiencing erosion of customer loyalty because of deregulation and consolidation. As a result, increasingly complex transaction-oriented services that employ Java™, Common Gateway Interface (CGI), dynamic HTML, and Common Object Request Broker Architecture (CORBA) to enable Web access to active content are rapidly replacing legacy host/ and client/server architectures throughout the global financial services arena.**

**addressing  
the risks of  
Web-enabled  
business  
services**

**In their most recent *Computer Crime and Security Survey*, the Computer Security Institute (CSI) and the FBI's newly established Computer Intrusion Squad published the following figures:<sup>1</sup>**

- **85 percent of respondents in the 2001 survey detected computer security breaches within the previous 12 months**
- **64 percent acknowledged financial losses as a result of those breaches**
- **90 percent of those attacked reported vandalism**
- **78 percent of those attacked reported denial of service**
- **13 percent reported theft of transaction information**
- **8 percent reported financial fraud**

**CSI attributes 55 percent of security breaches to human error and 20 percent to physical security problems such as natural disasters and power outages. Remaining causes include insider attacks with the intent of profiting (10%), disgruntled employees seeking revenge (9%), viruses (4%), and "outsider" attacks (1%).**

---

<sup>1</sup> Computer Security Institute, *2001 Computer Crime and Security Survey*, [www.gocsi.com/prelea/000321.html](http://www.gocsi.com/prelea/000321.html).

**a virtual menu of  
e-business  
vulnerabilities**

**The following common types of attacks used against businesses running Internet-enabled transaction systems or providing external access to active content are possible because of the bugs, errors, and design flaws routinely found in commercial operating systems and applications. Replacement code, patches, and interim software releases usually become available after a problem in a particular product is identified. The sheer volume of such incidents, however, makes security a moving target.**

- **root attacks—Many operating systems, in particular UNIX® and Windows NT®, have “superuser” or “root” accounts that give designated administrators unlimited system access. The most common method of penetrating a system is to somehow obtain the password to one of these root accounts.**
- **Trojan horses—Another common way hackers gain control of traditional operating systems and applications is by overwriting existing program files with malicious code disguised as authentic commands from root users or administrators.**
- **buffer overflows—Some Internet-enabled applications contain design flaws that make them uniquely vulnerable to hackers. One common application error called buffer overflow allows attackers to plant Trojan horses that give intruders free access to system data and applications.**
- **denial of service—Excessive network traffic or unexpectedly high volumes of service requests can overwhelm even the largest and most robust Internet sites. Hackers have been successful at using this method to cripple or shut down selected targets.**
- **application design flaws—Another common hacker trick is to gain access to all network interfaces by exploiting a security flaw in one component of an application.**

**Recent information released by CERT, the nonprofit security research organization located at Carnegie Mellon’s Software Engineering Institute, indicates that more than one-half of all computer system attacks originate within organizations. Revenge, greed, espionage, and even blackmail are among the possible motivations underlying the substantial annual increase in incidents directly reported to CERT’s computer-crime hotline.<sup>2</sup>**

**a thin line of  
defense**

**Most businesses try to repel computer system attacks by deploying various combinations of relatively simple security products and mechanisms such as SSL, firewalls, external encryption devices, and virtual private networks (VPNs). Yet these common security mechanisms simply restrict traffic to a specific application. Once an intruder gains access to an internal application—a feat easily accomplished if one of any number of exploitable software errors exist—the intruder has free rein over network resources.**

---

<sup>2</sup> CERT/CC Statistics 1988–2001, [www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html).

## specific challenges facing financial services firms

Technology is dramatically changing the face of today's financial services marketplace. Recognizing that their profits depend on the timely and accurate exchange of information, financial services firms are frequently early adopters of new technologies that promise to help manage the flow, accuracy, and security of high-value transaction data. Although affected by the same economic and political factors that triggered revenue slowdowns in most industry sectors, financial services increased its IT spending in 2001 and 2002 by approximately 5 percent annually, according to the *IT Spending Confidence Survey* conducted by Gartner Inc. and SoundView Technology Group in November 2001.

## recent industry-changing events and trends

Financial services companies are in the process of responding to a number of recent business, regulatory, and political events, including the following:

- **deregulation**—The Glass-Steagall Act, passed by the U.S. Congress in 1933 to partition the financial services industry into separate and mutually exclusive service niches such as savings and loans, insurance, and trading, was repealed in 1999. For the first time in more than 75 years, firms can compete across multiple financial markets. As a result, an industry previously consisting of many small specialty businesses has rapidly become one in which a few large firms provide a broad spectrum of products and services.
- **consolidation**—Managing the effects of widespread consolidation through mergers and acquisitions is currently one of the industry's top challenges. The world's largest financial services firms are struggling with decentralized and disparate systems, data redundancies, multiple and complex contractual agreements with multiple technology vendors and service providers, and dozens of proprietary and home-built applications stretching across multinational networks.
- **commodity status**—As a result of consolidation, products and services in the financial services industry have been reduced to simple commodities differentiated primarily by price. Savvy consumer and B2B customers are not only aware of their ability to pick and choose among vendors, they also realize that digital financial records are substantially easier to transfer to a new financial institution than paper files.
- **security legislation**—The Patriot Act, passed by the U.S. Congress in 2001 after the events of September 11, requires financial institutions to disclose and/or share customer information with law enforcement agencies and with other financial institutions. Although the specific implications of these new regulations are still being studied, financial firms will at the very least face significant new record-keeping and reporting responsibilities. (Under these regulations, federal law enforcement agencies would supply financial services firms with the names of individuals, entities, or organizations "reasonably suspected based on credible evidence" of engaging in illegal money-laundering or terrorist activities. Financial institutions would then need to search their records for matching accounts or transactions and, when appropriate, share those records with other financial firms as well as law enforcement agencies.)

**corresponding  
technical challenges**

**New information-processing challenges that arise from these market changes are requiring financial services firms to perform the following actions:**

- **integrate disparate applications and systems after a merger or acquisition**
- **consolidate dispersed databases or other unnecessarily decentralized systems that suffer from poor performance**
- **seek strategies for streamlining operations and business processes throughout expanded and diverse operations**
- **implement customer relationship management (CRM) systems and other technologies specifically designed to track customer preferences and behavior**
- **leverage detailed customer knowledge to deliver high-quality customer services that improve satisfaction, loyalty, and retention as well as differentiate a firm's services from those of competitors**
- **protect current investments in legacy systems while also beginning to deploy new Web-enabled business services**

**security issues raise  
the competitive  
stakes**

**The same market forces that continue to drive investments in technology are increasingly balanced by concerns about information security, as banks, securities firms, investment houses, insurance companies, and other financial services firms grow more dependent on online transactions and other e-business initiatives each year.<sup>3</sup> A Jupiter Media Metrix report released in September 2001 predicts that the number of U.S. households participating in online banking initiatives will increase from 25 million in 2002 to 43.5 million in 2005; and the number of households using online investing services will rise from 19.6 million in 2002 to 34.2 million in 2005.<sup>4</sup>**

**Due to the sheer magnitude of its value, transaction data carries significant responsibility. With the possible exception of healthcare, no other industry has a stronger mandate to protect customers' interests and privacy rights than the financial services sector. A single high-profile hacker attack could instantly destroy the reputation of a major bank or insurance company. Although the Internet enables financial firms to react immediately to market opportunities, bring new products and services to market more swiftly, and take advantage of cross-selling opportunities, the potential risks of building an open Internet-enabled infrastructure are significant as well. Insurance firms will also be affected by the most significant medical legislation passed in decades. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) governs all healthcare entities that maintain or transmit "protected health information" (PHI) in paper or electronic form, including physician practices, hospitals, payers, and clearinghouses.<sup>5</sup>**

---

<sup>3</sup> **Gartner Dataquest Says U.S. External Services Market to Reach \$276 Billion in 2002,** [http://biz.yahoo.com/bw/020115/152025\\_1.html](http://biz.yahoo.com/bw/020115/152025_1.html); [www.gartner.com](http://www.gartner.com)

<sup>4</sup> **The State of Financial Services Online 2001,** Jupiter Media Metrix, [www.jmm.com/xp/jmm/press/reports/featuredDataAndResearch\\_09242001.xml](http://www.jmm.com/xp/jmm/press/reports/featuredDataAndResearch_09242001.xml).

<sup>5</sup> **Overview of Health Insurance Portability and Accountability Act of 1996 (HIPAA),** [www.medscout.com/hipaa/overview/index.htm](http://www.medscout.com/hipaa/overview/index.htm)

**Yet the potential for business growth is substantial enough to drive development in a host of Internet-enabled products and services. These include the following e-business initiatives currently underway:**

- **automating order management at buy-side brokerage firms by implementing Web-enabled straight-through processing (STP) of complex transactions that require the participation of multiple parties for successful completion**
- **allowing customers to complete mortgage transaction applications online using electronic signatures**
- **streamlining transaction processing for private-label credit cards via the Web**
- **providing high-net-worth banking customers with real-time access to their assets, coupled with Web-based data mining and analysis tools that allow them to “drill down” into complex portfolios of investments from anywhere in the world**
- **creating intelligent asset-management tools to help portfolio managers at private banks manage multiple accounts simultaneously**
- **improving Web-based trading tools that bring live markets to customers in real time**
- **developing Web-based customer-care programs—including intuitive online self-service options—that help customers perform a broad range of financial transactions**
- **continuing to improve online payment and fund-transfer services that enable customers to register, transfer, execute, and manage online payments 24 hours a day, 7 days a week from any location and using any type of computing device, including mobile devices**

**In addition to these Web services, scores of new B2B information exchanges and procurement markets, trading and research sites, imaging archive services, and new financial products based on smart cards are currently under development.**

## **the firewall fallacy**

**For years, the popular press and the business publishing world have featured prominent articles documenting the significant risks and related costs of Internet-based system attacks and intrusions. Such reports continue to stress that many of the most egregious security breaches have occurred at some of the world’s most technically sophisticated and security-conscious organizations. Yet according to FBI computer crime specialists, many senior executives, including CIOs, CEOs, and CFOs, still fail to grasp the severity and complexity of the computer security problem.<sup>6</sup>**

**Indeed, security analysts believe that the single highest barrier to more universal implementation of effective security strategies—in financial services as well as in other industries—is simple denial. More specifically, a surprising number of businesses today persist in the belief that firewalls represent their best defense against intruders.**

---

<sup>6</sup> Bruce J. Gehardt, director, FBI, Northern California office, [www.gocsi.com/prelea/000321](http://www.gocsi.com/prelea/000321)

**delivering solid protection under specific circumstances**

**Firewalls are highly effective when used to guard a private network by analyzing data leaving and entering the network via an Internet application server. Firewalls can also provide network address translation so IP addresses of computers inside the firewall are hidden. Relatively new variations on firewall technology include packet-filtering firewalls that analyze the source, destination, and port of each incoming packet to determine whether it should be allowed into the network. More advanced packet-filtering firewalls and proxy firewalls deliver even more robust protection.**

**Yet firewalls cannot effectively manage all the security risks of Internet-enabled applications that perform transactions or access active content. Firewalls were designed to direct traffic between multiple external machines residing in the so-called hostile Internet environment. This activity does not include sufficient functionality to protect applications that perform transactions or access resources on the internal network.**

**For example, one common Internet-enabled architecture provides outside users with general access to those applications outside the firewall but only limited access to programs or data stored on the intranet. This method is a fairly secure way to provide Internet users with a “Webified” view of internal data. But security risks are substantially increased when an outside Web server is used to provide Internet users with access to active content. Such access is possible only if the network security administrator “pokes a hole” through the firewall to enable the necessary interaction between the Internet application and the internal intranet program or data.**

**a wish list of security goals**

**Because of the functional limitations of firewalls, businesses need to supplement this technology with more comprehensive and multifaceted security protection. Financial services firms, which place digital assets of high value online every day, seek security solutions that fulfill the following goals:**

- ensure file-system security—Some perpetrators attempt to gain access to the server’s file system in order to browse through system data contents, discover security holes, or exploit known program bugs. A security product should conceal as much of the file system as possible from users (authorized or unauthorized) and even from the system itself.**
- authenticate users—One of the most important functions of any security solution is to swiftly and correctly determine whether any given user is legitimate. All system transactions also need protection from eavesdroppers.**
- set and control granular levels of access—Many businesses want to be able to differentiate various classes of data and applications—usually on the basis of value or sensitivity—and ensure that users have access only to the systems for which they have been assigned clearance. One way to reach this goal is to implement a multilevel security strategy in which files and data are assigned labels, and programs and users are given clearance for specific labels.**
- maintain system integrity—Security products that immediately flag any unexplainable file errors or directory changes enable system administrators to determine if an intruder has tampered with data.**

- **enable trusted communications**—Because multi-tiered Internet architectures are increasingly common in the Web-driven business world, security products need to provide a range of options for allowing trusted communications between an application's front end and the varying number of tiers of functionality and data that can make up a total system. Specifically, a security program should support traditional CGI, monolithic, and split Internet architectures in order to accommodate the complex system migration required when transitioning to a Web-services architecture.
- **secure system services**—Unrestricted access to "system services," or system calls already built into a system, allows hackers to run malicious programs or introduce Trojan horses to bypass other security measures. A security product that can partition such services and assign privileges to each reduces the risk of such attacks.
- **protect root accounts**—Most systems have a superuser or root account that allows a designated administrator unlimited access to system programs and data. The most common method for unauthorized penetration of a system is to gain access to the root account password. Any viable security solution must find a way to prevent exploitation of this common operating system vulnerability.
- **detect intruders**—In addition to preventing unauthorized *virtual* access, security solutions must offer real-time intrusion detection that triggers alarms in case of physical penetration.
- **facilitate regular audits**—Because businesses are usually unaware that system penetration has taken place, many security breaches are unreported. As a result, hackers or other intruders can repeatedly visit the same system to steal, erase, or corrupt data. A security auditing system that reports details of attacks is essential in order to prevent breaches from recurring.
- **include easy-to-use administration tools**—Overly complex or difficult-to-use administration tools can compromise even the most robust and full-featured security product. Therefore, the ease of use of a particular solution—which includes the availability of detailed online help and/or 24x7 call-center assistance—is as important as all the other functions discussed in this paper.
- **eliminate unnecessary network traffic**—Extraneous network traffic that results from routine message routing as well as processing non-Web protocols such as File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and telnet can easily "distract" a server from its primary function. Because hackers exploit this operational reality when launching denial-of-service attacks on Web sites, security solutions must include some mechanism for eliminating unnecessary network traffic.

## hp virtualvault: raising the security bar

To date, the only application security product that supports all of the above goals is HP Virtualvault, a secure platform for Internet-enabled e-business applications. Unlike most other security products, which deploy fairly simple mechanisms for restricting unauthorized user access to data and applications, Virtualvault delivers military-grade protection by integrating multiple security strategies into the operating system of a single product. The only way to undermine the security of a Virtualvault system is to break into the operating system—a nearly impossible task. In the unlikely event that an intruder does achieve this penetration,

**Virtualvault automatically shuts down the system, immediately restricting access to both applications and data.**

## brief description of virtualvault

The Virtualvault operating system incorporates B-level U.S. Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) features. A binary-compatible version of the HP-UX 11.0 operating system, the Virtualvault operating system (VVOS) 11.04 has a 64-bit architecture and integrates security directly into the operating system and network layers. Virtualvault is a strictly partitioned run-time environment that supports threads and streams, and includes a number of vaulted application integration programs, including CGIs, application gateways, and a Java Virtual Machine.

Virtualvault filters external users via advanced authentication processes while keeping them outside the system. In other words, users never obtain direct access to systems or data because Virtualvault acts as a go-between. After authenticating a user, Virtualvault first processes a request for data or application access by verifying that the user has permission to access the requested resources, and then brings the resources from the back-end application or database to the front area where the authenticated user is waiting. The process is similar to the way a bank officer provides service from behind a glass barrier for a customer at a teller window by retrieving a lockbox from a vault and bringing it to the window.

## key benefits

The philosophy of protection behind Virtualvault assumes that a perpetrator who successfully penetrates a system despite an initial defense shield will be effectively stymied, or at least slowed down, by a second, third, or even fourth security deterrent. In other words, security is not based on a single mechanism, but on a multi-pronged overlapping array of multiple security techniques.

The following are some of the many benefits Virtualvault offers:

- reduces the risk of financial loss due to hacker attacks, employee theft, or organized fraud schemes
- decreases downtime arising from unauthorized intrusions or hackers
- enables delivery of the full range of benefits possible from deployment of Web-enabled business services, including increased customer satisfaction, lower operating costs, and increased revenues
- lowers financial and logistical barriers to implementing innovative e-business initiatives by integrating standard front-end infrastructure components with multi-pronged security strategies in a single product
- ensures credibility with customers, partners, and investors, especially in sensitive industries such as financial services, healthcare, and government

## alignment with security goals

Virtualvault meets all of the requirements discussed earlier for creating a secure Internet-enabled infrastructure. Virtualvault is currently the only run-time application security solution that simultaneously:

- conceals major portions of the file system from users, employees, programs, and even the system itself
- provides multilevel security, assigning labels to files and data and granting clearance to programs and users in accordance with these labels
- partitions data into tightly controlled compartments so that even if unauthorized users gain access to one program or database they cannot freely browse through all other programs or databases on the intranet

- uses SSL encryption to ensure that only valid hosts can access the system
- checks system integrity by comparing the current state of the file system against the file system original, and flags errors or suspicious changes to files and directories
- restricts program behavior through use of a “least privilege” model that assigns individual Web-enabled services a limited set of discrete privileges, denying access whenever any user without the required privilege attempts to access a service
- establishes a balance of power by dividing the superuser or root administrator privileges among multiple administrators
- enables regular real-time auditing of system events and user activities across a broad range of activities at the operating-system level
- includes real-time intrusion detection with alarms to protect common penetration points
- simplifies system administration and reduces errors with an intuitive and easy-to-use set of administration tools
- eliminates unnecessary network traffic by using a filtering router that reduces traffic not bound for the site and restricts traffic to HTTP Web protocols only

## looking forward

Gathering precise data on security incidents and associated costs is notoriously difficult, primarily because most businesses are reluctant to report computer-related crimes committed against them. Only 36 percent of the respondents from the most recent CSI/FBI security survey said they reported security intrusions to law enforcement agencies. Although this number represents a significant increase over previous years—in 2000, only 25 percent of respondents made official reports of such crimes—most businesses continue to believe, perhaps correctly, that any possibility of legal redress would be substantially outweighed by lost credibility.

Because of this history of underreporting, businesses tend to underestimate rather than exaggerate the probability that they will sustain measurable damage. Still, a growing number of enterprises are becoming aware of their potential vulnerability and are implementing security solutions that transcend the current practice of simply adding firewalls.

In summary, traditional operating systems such as UNIX and Windows NT and traditional security measures such as firewalls do not adequately protect the Web-enabled applications of financial services firms and other businesses that routinely process transactions involving high-value data. By integrating existing Internet infrastructure and application security features such as authentication, authorization, and access control into the network operating system itself, Virtualvault creates an integrated and multi-layered security architecture that significantly reduces overall risk.

In effect, products such as Virtualvault slow down the progress of would-be system intruders by combining a strategic number of overlapping security devices and detection sensors. Alarms and automatic system shutdowns are activated long before the intruder gains access to valuable data or programs.

**Virtualvault's design is based on the philosophy that the most effective computer security solutions attempt to minimize, not eliminate, overall security risk. Virtualvault implements this approach by deploying an array of proven technologies at a reasonable cost. Indeed, most security professionals today acknowledge that no perfect defense exists for protecting Internet-enabled businesses. Even if company security budgets were unlimited, creative and resourceful hackers would continue to pose security challenges. Likewise, operating system designs and application software codes will never be completely free of flaws for unscrupulous people to exploit.**

**Increasingly, enterprises are focusing on risk reduction rather than pursuit of the perfect defense. Businesses as well as government organizations are beginning to grasp the scope and complexity of the security risks that pervade business, societal, and political environments in today's world. The wisest course is to strive for realistic reductions of identifiable risks, while elevating strategic discussions about security to top organizational levels.**

**for more  
information**

**For more information about Virtualvault, please refer to the following link:**

<http://www.hp.com/security/products/virtualvault/>

**how virtualvault works:**

**See Virtualvault Concepts Guide:** <http://docs.hp.com/hpux/pdf/B5413-90051.pdf>

**See Virtualvault Philosophy of Protection:**

<http://docs.hp.com/hpux/pdf/B5413-90027.pdf>

**Web proxy information:**

**Visit [www.hp.com/security/press/releases/20010409-rsa/virtualvault.html](http://www.hp.com/security/press/releases/20010409-rsa/virtualvault.html)**

**Java is a U.S. trademark of Sun Microsystems, Inc. UNIX is a registered trademark of The Open Group. Windows NT is a U.S. registered trademark of Microsoft Corporation.**

**Technical information in this document is subject to change without notice.**

**© Copyright Hewlett-Packard Company 2002**

**Printed in U.S.A.**

**6/02**



**i n v e n t**