WHITE PAPER

August 1997

Prepared By
Internet Solutions
Business Unit

Compaq Computer
Corporation

CONTENTS

Compaq Enterprise Security Framework

In the highly competitive world of enterprise computing, security has become an intricate and critical element. The Compaq Enterprise Security Framework incorporates the latest technology, a balanced hardware/software solution, and interoperablity with current security at multiple platform levels to clarify security solutions. Through use of The Compaq Enterprise Security Framework, you can develop solutions that do not compromise performance yet are still pragmatic and easy to use. In so doing, you can help to determine a practical roadmap for the deployment of enterprise security.

COMPAQ
248A/0897ECG

NOTICE

The information in this publication is subject to change without notice.

COMPAQ COMPUTER CORPORATION SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

This publication does not constitute an endorsement of the product or products that were tested. The configuration or configurations tested or described may or may not be the only available solution. This test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state or local requirements. Compaq does not warrant products other than its own strictly as stated in Compaq product warranties.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Compaq Enterprise Security Framework

First Edition (August 1997)
Document Number 248A/0897ECG

INTRODUCTION

Computing security is one of the fastest changing and most complicated areas in the information technology industry today. Each day seems to bring another threat to the security of the world's computing resources. Recently, the Social Security Administration took its operations off line because of privacy fears. In addition, Microsoft has had to re-tool its Explorer browser due to security concerns, and companies have reported a threefold increase in virus incidents over the last year. These items follow the spectacular stories of hackers who broke into and modified the content of the CIA's and Justice Department's web sites, and of computing thief Kevin Mitnick, who gained access to thousands of consumers' credit card numbers. These incidents represent only a subset of the wide variety of threats computer users and administrators must defend against. Making this area even more complex is the confusing array of technologies and solutions, including encryption, firewalls, smartcards, and digital certificates, which are offered to solve these problems.

With the overall growth of computing, particularly networked and inter-networked computing, more resources and information are at risk than ever before, with new threats emerging daily. Independent research estimates potential losses from lack of security at between $40-80 billion in the year 2000. Enterprises abilities to protect their resources and capitalize on opportunities will depend on the level of security they enforce.

Computing security breaches as well as the concerns of IT managers are rising, yet the deployment of security solutions lags. Over 75% of organizations responding to a recent poll reported a significant computer breach over the last year: the subset of these organizations, which could quantify their losses (249 institutions), reported losses of over $100 million. While most security problems remain basic, such as viruses, password exposure, and physical theft, to date most enterprises have employed only limited or point solutions for security.

IT managers must design a practical roadmap to guide their enterprises through this tangle of information, threats, and solutions. In charting a course, they must incorporate the latest technologies, adapt to new threats, and ensure that their solutions do not compromise performance.

The Compaq Enterprise Security Framework addresses enterprise security in terms of computing platforms, secure computing technology, and the objectives required of a strong enterprise security policy. The framework also describes solution sets for each platform in terms of "levels" of security. Using the easy-to-understand framework and levels, enterprises can plan a security solution roadmap that meets their business requirements. Compaq's Enterprise Security Framework delivers the critical needs of IT managers and makes the process of securing enterprise computing as easy as possible.

SECURITY ENVIRONMENT

Computing security has always been critical to enterprises. However, in today's environment the components of the computing world have changed in ways that make computing security more critical and complex. In the past, computing security focused on protecting assets in a mainframe-oriented system. In the current, inter-networked environment, enterprises view security as crucial for two reasons: first, computing security measures protect against potentially devastating losses; and second, security enables businesses and opportunities to generate new revenue and reduce costs. Facing a growing variety of threats, losses, and intense market pressures, IT managers will propel the demand for practical, sound security solutions in the near future.

Security Environment: Importance and Trends

Several computing environment trends have changed the nature and challenges of computing security (see Figure 1).

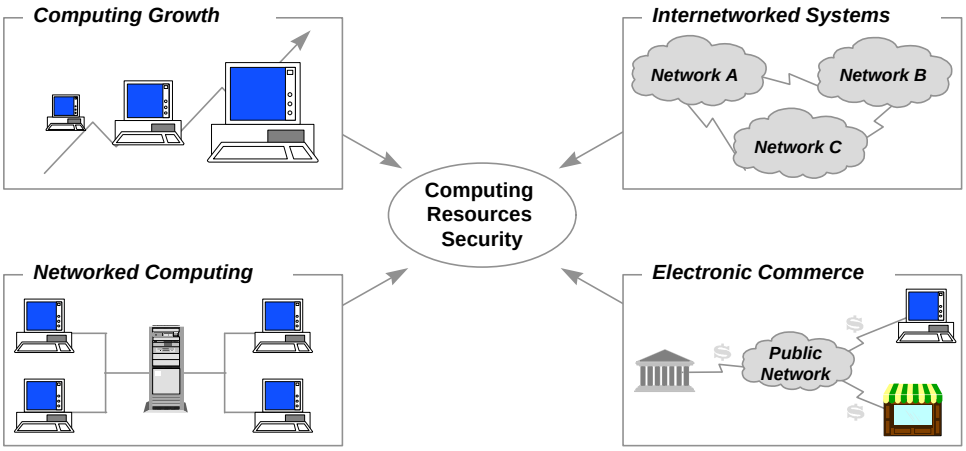

Figure 1

- The most obvious computing trend affecting security concerns is the dramatic growth in the installed base of desktops, workstations, laptops, and PDAs in both the consumer and business markets. The simple impact of this growth has been to place more valuable enterprise, personal information, applications, and hardware assets in the hands of numerous people.
- The next trend is the importance of networked (client/server) computing, primarily in enterprises and small businesses. As this type of computing has become the dominant architecture, more people have networked access to significant enterprise information and applications than ever before. Some analysts estimate that 50% of the world's computers are networked in some way (LAN, WAN, etc.).
- The third trend is the emergence of inter-networked computing. In the last 2-3 years, more enterprises and institutions have connected from their internal networks to the greater networks of other businesses and consumers on the Internet. Inter-connected networks now enable more parties (business partners, customers, and employees) to gain access to crucial systems' resources across public, traditionally unsecured networks.
- Finally, the promise of Electronic Commerce is pressing businesses and computing vendors to find ways to securely conduct commercial and private transactions over public networks. In many cases, these transactions involve parties with whom they have no previous affiliation.

Together, these trends have created a significantly different and more difficult computing environment for IT managers to secure. Previously, they could control the enterprise's information

residing on mainframes and mid-range systems in a closely monitored and physically secure environment – the glass house. In this setting, businesses deployed private, leased lines for external data transactions with known partners and used e-mail for internal communication only.

In the new environment, a wide variety of enterprise computers either contain or connect to critical business information. In addition, these devices can be portable (laptops, PDAs) and are rarely physically secured. Servers are corporally distributed throughout an enterprise, and each sever can be connected to hundreds of clients. These servers are also frequently networked to outside parties through the Internet or to remote access modems. Furthermore, businesses are now using the public networks as a platform for conducting commerce and exchanging sensitive information with consumers and business partners.

Security Environment: Threats and Pressures

With these trends, a variety of threats have increased in importance and proliferated across the computing landscape. The following examples provide an idea of the confusing issues with which IT managers must contend (see Figure 2).

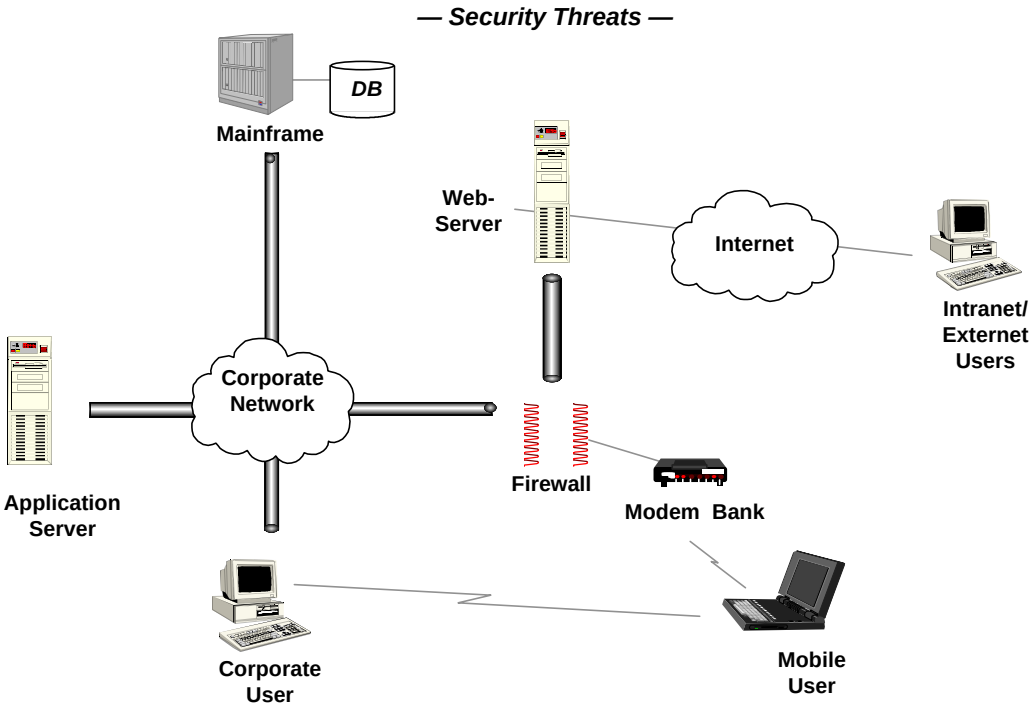

Figure 2

- Saboteurs and thieves (either internal or external) can access, steal, and change the content of crucial information.
- Hackers can launch viruses and other attacks that crash important systems.
- Disgruntled employees can either steal or guess passwords to gain access to information and applications they are not authorized to use (e.g. payroll, HR).
- Outsiders can dial-in directly to the network or PCs and use this as a launching point for internal network attacks.
- Attackers can use various tactics to crash web servers or change their content; web servers can also be used as access points to the internal network.

- Thieves can steal corporate laptops for their information and hardware value and sell assets to third parties (i.e. competitors).
- Physical security of home PCs is at risk from theft, and data stored on disks is at risk from viral attack.

In addition to their responsibility to protect hardware, software, and information assets from these threats, IT managers also face pressures to deploy advanced security to their networks. These pressures can be roughly grouped into "friendly" and "unfriendly" forces (see Figure 3).

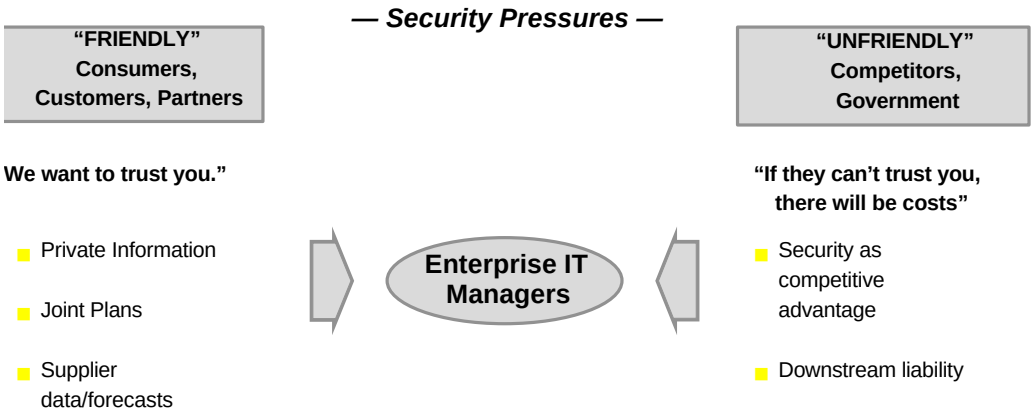

Figure 3

The "friendly" pressures primarily come from customers, consumers, and business partners. Both customers and consumers are concerned with the protection of the private information they share with companies (i.e., medical records, credit card numbers, joint plans). In addition, they are unwilling to participate in E-Commerce with companies until they feel the transactions are completely secure. Business partners' concerns are focused on two areas: first, on achieving a comfortable level of security for companies exchanging information over open "Externets"(meaning the Internet, when it is used for business to business commerce) and secondly, on the question of legal liability, which is brought into focus by the security issue.

Recent court cases suggest that there is an emerging precedent of "downstream liability." This precedent requires companies to employ "reasonable measures" of security or face potential liability for computer attacks launched on other parties from within their network (e.g. a criminal breaks into the inadequate security of Company B and uses this trusted position to hack into Business Partner C's more robust security system).

When enterprises do not adequately secure their networks, "unfriendly" forces such as competitors and government either take advantage of that deficiency or demand retribution. The first of these forces is competitors. Competitors can turn a company's security weaknesses into an advantage in one or both of two ways: initially, through the competitor-organized theft of information or hindrance of internal systems (i.e. attacks which crash strategic company systems such as call centers, web servers, etc.), and secondly if a competitor accesses or copies private information, they can quickly counter a business' strategies (e.g. beat their competitive bid for work, under-price their product in the market). By the same token, crashing a rival's critical systems can hurt their reputation for customer service or on-time performance. Competitors can also create a competitive advantage through the impact of a publicized breach on the market position and perception of a company. In many security-sensitive industries (e.g. health care, banking), the security of a company's network is a crucial part of the trust formed between business and customer. If this trust is in question, the relationship is compromised and may cease (e.g., if a private bank loses funds or account information electronically through a publicized security breach, they will probably lose clients as well).

The other potential "unfriendly" force is government. Government regulation of computing security is still evolving; however, it is possible that both the state and federal governments may begin to hold enterprises responsible for the privacy of consumer information.

Security Environment: Enterprise Opportunities/Risks

The business reasons for deploying enterprise security can be examined from an opportunity/cost perspective. Though these opportunities/costs have not yet been fully explored, and quantifying them is difficult, some estimates have placed potential worldwide enterprise computing losses at $40 billion by the year 2000. In the denominator of the opportunity/cost perspective are the costs of inadequate computing security. In the numerator are both the revenue-enhancing and cost-reducing opportunities enabled by sound computing security.

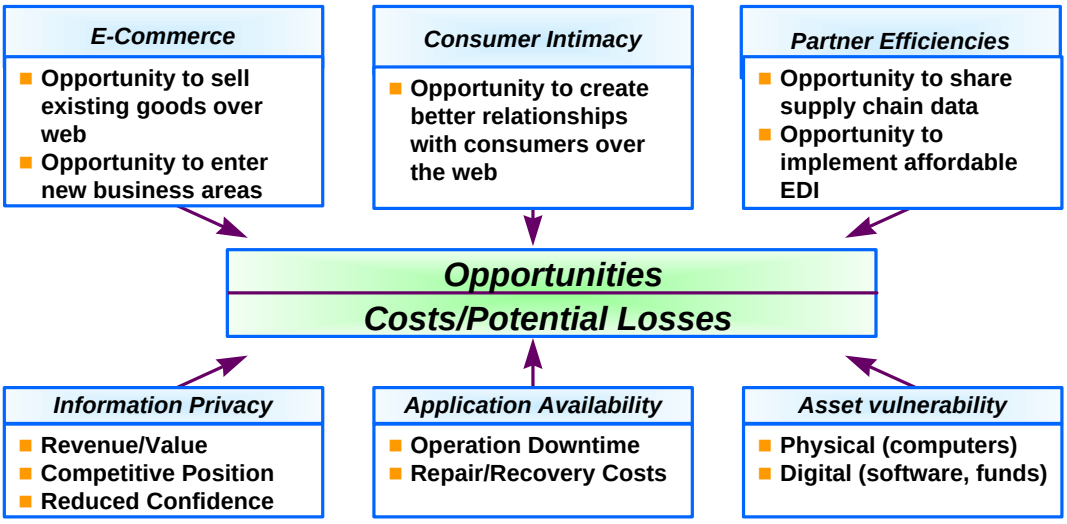

Figure 4

The first risk category (see Figure 4) in the denominator is the potential loss of information privacy. When sensitive information is compromised and falls into unfriendly hands, enterprises can face several types of losses:

- They can lose revenue/value when merger and acquisition plans or contract bid information is compromised.
- They can also lose their competitive position when product plans or designs are stolen or pricing strategies are spread to a competitor.
- Additionally, there is the reduced confidence in a company that results from a breach of security such as the early release of an SEC report, the compromising of medical records, or the theft of employee HR information.

Another area of risk well known to IT managers is application availability. A virus or other attack can create significant costs for an enterprise in the areas of operational downtime and repair or recovery. The final area of potential loss is the actual assets under enterprise control. Obviously, there are the losses associated with the value of the hardware (RSA reports that 200,000 laptops were stolen in 1996), but many businesses must also vigorously protect their digital assets. The entire business model of companies whose products largely reside in the digital domain (software companies, banks, etc.) is dependent upon the security of their assets; they must deploy the most advanced measures to protect them.

On the opportunity side of the security equation, IT managers must consider the possibilities that can be pursued with robust security in place. These items could be revenue-enhancing and/or cost-reducing to business' bottom line. The first category of opportunity is Electronic Commerce. Here, with adequate security, companies have the potential to sell their goods directly to their customers and potentially branch into new businesses. For example, a supermarket could set up a virtual store/web site for customers to purchase specific food bundles that could be packaged and delivered regularly. Businesses could also sell this information to food suppliers so that these vendors could effectively target their advertising mail and coupon efforts. In addition, businesses can foster closer relationships with customers and consumers. By creating and maintaining communities of interest over the web, businesses can strengthen their value to customers.

Finally, there are significant cost-saving opportunities for businesses with adequate public network security. Businesses can reduce their leased line expenses by setting up encrypted virtual private networks (VPNs) with their business partners to exchange information. By granting partners access to internal parts databases and allowing them to order parts directly, manufacturers and suppliers reduce their customer service costs.

Security Environment: Current Situation

Over the past several years, computing security breaches have become a regular issue for enterprise IT managers. The exact size of the issue is an open question. However, industry surveys identify a few important facts:

- Computer security breaches are a common, widespread, and growing problem.
- The most prevalent threats to computing security are well known.
- The insider remains the primary threat to computing security, but outsider attacks are quickly rising.
- To date, enterprises have deployed only simple solutions to address these issues.

The traditional threat to enterprise security has always been the insider. This menace remains prevalent in today's computing environment. However, the growth of the Internet has brought the insider and outsider threats to near parity in terms of the number of attacks and breaches reported this past year. Recent surveys report that this growing equality is due to the fact that corporations have established network links with outside sources (e.g. remote employees, consumers, business partners), and greater numbers of people have the requisite skills and tools to break into these networks.

While these external "hacker" attacks are rising, the most prevalent and damaging breaches remain the most basic ones. Most business surveys cite virus outbreaks as the most common computer security incident, affecting 75% of enterprises. The frequency of these attacks also seems to be rising. A recent study cited a threefold increase in virus attacks on corporate PCs over the past 12 months. The two most common, reported means of asset theft (digital and physical) are simple password exposure and equipment theft. RSA reports 200,000 laptops and 100,000 PCs were stolen in 1996. Although the theft of hardware represents a huge loss, the information and applications on these devices are far more valuable.

The problem is widespread. As mentioned earlier, over 75% of the businesses surveyed reported suffering a financial loss due to a breach in computing security. At least 32% of those recounted experiencing five or more significant breaches in 1996. Some surveys have stated that as many as 98% of businesses have been attacked at least once, and as many as 43% of large operations have been breached 25 times or more in the last year.

Most analysts believe these surveys understate the threats to enterprise computing security. The FBI estimates that almost 95% of computer intrusions are undetected. This is due to the advanced

nature of some attacks, and because digital material can be copied without any evidence of access or theft. In addition, most computer crimes and security incidents go unreported because businesses are unwilling to reveal the weaknesses of their computer systems to outsiders.

Vulnerability stems from the implementation of only basic security measures. The most commonly used of these are log-in passwords and anti-virus software. These solutions, however, are easily defeated by a sophisticated virus attack. Unfortunately, the more advanced security solutions such as firewalls, token-based (two-factor) authentication, and data encryption have earned only limited acceptance and installation so far.

While these factors have left IT managers gravely concerned about security issues, their implementation of security solutions and technologies has lagged these concerns. Although three-quarters of IT managers reported that their senior management viewed security as a critical priority, two-thirds of technology managers stated that they are not confident that their networks are protected from attack. Despite these concerns, 55% of companies spend 5% or less of their IT budget on security, and the percentage of companies with an information security officer has actually declined over the past year.

These facts point to several conclusions:

- The need for enterprise-level security is increasing rapidly due to the growth in the networked and inter-networked computing environment, the vulnerability of corporate information and assets, and the variety of threats that have emerged in this environment.
- IT security expenditures are minute in comparison with the total losses caused by poor computing security.
- While the new threats to enterprise computing security are complex and diverse, the primary causes (insiders, viruses, and passwords) are well known.
- Demand for computing security will increase dramatically within the next 10-18 months. Enterprises will require device, internal network, and external network security solutions that carry minimal costs and administrative overhead.

UNDERSTANDING SECURITY

Compaq has laid out a security framework that provides a common set of easily understood terms with which to discuss security and to plan the deployment of security solutions. Computing security can be understood in terms of three inter-related dimensions (see Figure 5).

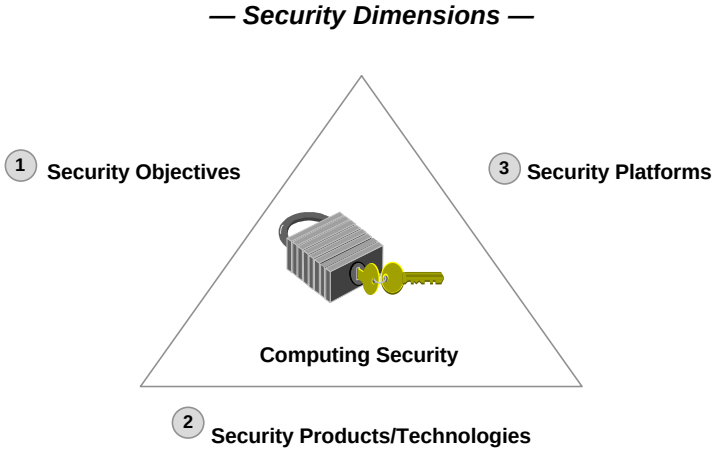

Figure 5

First, a complete security solution is defined by a set of security objectives. Second, products and technologies divide security solutions into categories that make it easy for enterprises to understand the types of solutions they are deploying. Lastly, platforms define the types of resources the solution is attempting to protect (those serving single users on the device, those serving groups of internal network users, or those serving users across the Externet). Using these terms, Compaq's enterprise customers can better understand the market for security products and easily map out the solutions they require.

Defining the objectives of security (see Table 1) is a critical step for IT managers because these objectives clarify the boundaries of a complete solution and enable managers to classify the diverse performance of today's security products. A complete enterprise security solution will integrate products that meet these objectives across all platforms.

TABLE 1: DEFINING THE OBJECTIVES OF SECURITY

Objective	Definitions
Identifications & Authentication	Ensuring true identity equals apparent identity; users and systems are protected from parties who impersonate other users and systems
Authorization/Access Control	Ensuring parties have access to only those resources they are authorized to use; information, applications, and other system resources are protected from unauthorized access, use or distribution
Privacy	Ensuring sensitive data is understandable only to appropriate parties; information is protected from unauthorized monitoring, access distribution, use, and name association
Integrity	Ensuring data/resources, information, and computing environment is protected from unauthorized manipulation and alteration
Accountability	Ensuring accurate, verifiable activity and transaction information is monitored and recorded; companies and individuals are protected from repudiation, or misrepresentation of actions or transactions

The product and technology categories for security solutions are hardware, software, and services (see figure 6). This initial categorization reveals the variety and complexity of solutions available in the security market.

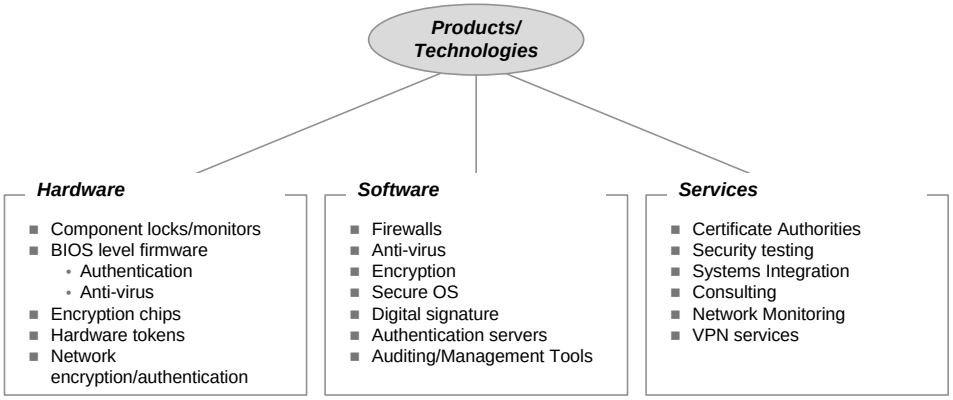

Figure 6

The hardware category features a variety of implementations, ranging from component locks that physically secure devices through high-speed encryption to chips that improve server performance of cryptographic operations. One of the most significant categories in hardware is portable tokens (including smartcards), which provide a high-performance identification and authentication solution for security environments.

Software is the most dynamic category in the security market. Firewalls and anti-virus software are the best understood and furthest developed stand alone solutions on the market, although they are hardly mature product categories. Recently, several notable new software approaches that provide for secure environments have begun to emerge. These approaches range from secure OS and secure APIs to corporate infrastructure software such as certificate servers, single-sign-on solutions, and middleware. In addition, many of the recent innovations in cryptography have been focused on the software category.

Security services form an essential part of the security market. In this confusing environment, the expertise of security professionals in consulting and security testing firms is crucial to large enterprises; these services are projected to grow into a $5 billion market by the year 2000. In addition, these companies have crucial ties to the other product categories as installers of solutions (system integrators) or as infrastructure providers (Certificate Authorities).

The platform category groups solutions according to the types of attacks they defend against, as well as the types of resources they protect (see Figure 7):

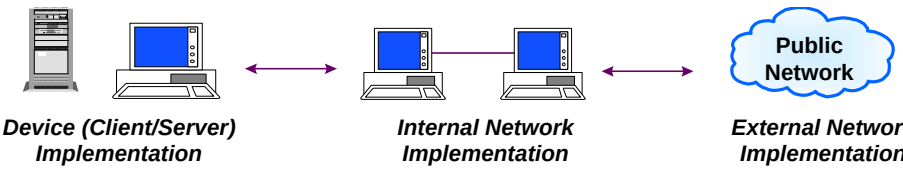

Figure 7

As a result of the diverse threats and vulnerabilities enterprises face, IT managers will need to deploy solutions that serve each security objective on every platform in order to form a complete security solution. For example, if a device does not have robust local authentication measures, parties may use this station as a launching pad for attacks on local network services that trust the identity of individual devices. Similarly, a client that trusts the identity of networked services is vulnerable to attacks from the network. Some solutions, however, can protect different platform levels, depending on how they are implemented. For example, smartcards can act as an identification and authentication solution for a device or as a tool that signs a digital certificate that identifies a user across an external network.

Enterprises can use these terms to understand and clarify the purpose and usefulness of various security solutions. A view of the security marketplace using these classifications is shown in Figure 8.

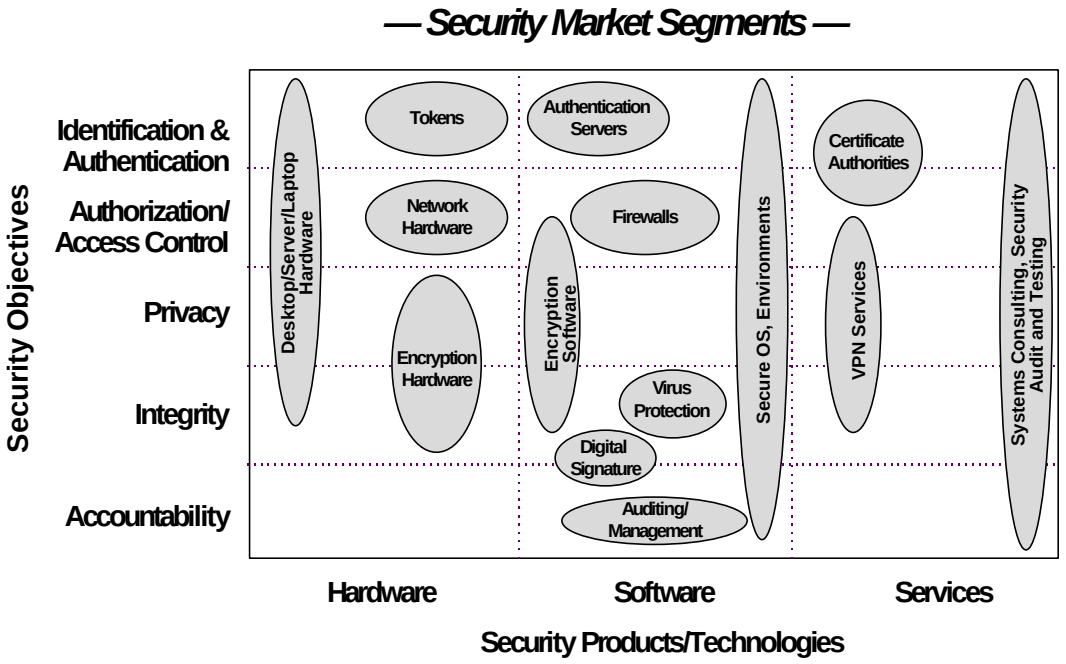

Figure 8

SECURITY MARKET

With a clearer picture of the computing security solution marketplace, enterprise decision-makers can identify and understand the implications of critical market trends on their purchasing decisions. Compaq has identified four key computing security trends that have important repercussions for enterprise customers and Compaq's own security strategy:

- the expansion of firewall functionality
- the developing need for strong identification and authentication measures
- the importance of balancing hardware and software in one's security approach
- the rapidly growing, but immature security marketplace

Security Market: Firewall Expansion

Over the past 12-18 months, firewall vendors have been aggressively expanding their security solutions to meet the multiple objectives of security (see Figure 9). To accomplish quick growth and diversification, most vendors have announced partnerships or acquisitions in order to embed their functionality and technologies, such as authentication and encryption (VPN), in the firewall and/or establish interoperability with other leading solutions. In addition, several firewall vendors have attempted to establish a common, open platform and a security middleware standard to define architecture for enterprise's complete security solution. In effect, these vendors intend for the firewall to become the management console for enterprise's security infrastructure.

As one of the most validated security solutions, a firewall's functionality was traditionally limited to network boundary access control, allowing only certain types of packets of information and applications to travel into and out of a defined network. In the early years of development, firewall vendors focused on refining their technology. They developed firewalls for multiple platforms, building their installed base by educating users about firewalls, and finding VAR or OEM partners.

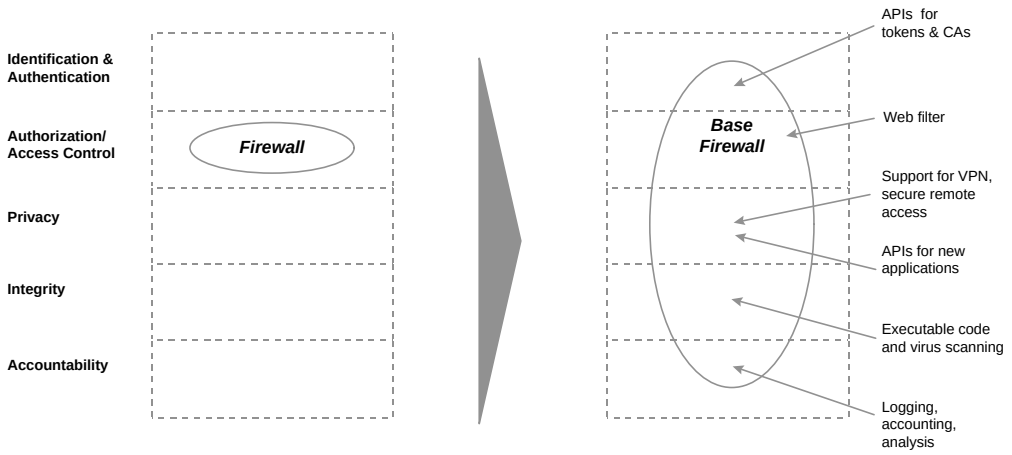

Figure 9

This past year, firewalls have finally gained significant market acceptance. Leading enterprises have recognized the necessity of firewalls and have begun to install them. Market forecasts predict triple-digit unit sales growth of firewalls through the year 2000.

Explosive growth forecasts, coupled with recognized leadership in the computing security market, have allowed firewall vendors to expand beyond traditional access control functionality to

encompass a broader range of security objectives. Leading vendors have entered into acquisitions and partnerships in order to offer new functionality. New functionality includes web filtering, limiting the web locations employees may visit, VPN abilities allowing encrypted communications between firewalls, networks or remote clients, screening capabilities for Java and ActiveX code, and logging software to audit network traffic. In addition, these vendors have made moves to improve the interoperability of disparate firewalls with other security solutions. For example, Raptor Systems' firewall has built-in interoperability with tokens and authorization servers from Security Dynamics.

The broadest effort of firewall vendors is to establish architecture and an API standard. This would allow firewalls to become the security management console for enterprise, capable of integrating and controlling the security operations of multiple third party solutions. The most aggressive effort to date is from CheckPoint, whose OPSEC architecture supports major existing standards such as IPSEC, LDAP, etc., and offers API support for multiple solutions such as access control, address translation, virus scanning, and activity monitoring.

The most important implication of these firewall developments is that security solution providers will need to interoperate with the APIs of dominant firewalls, or incorporate the latest firewall products into their systems.

Security Market: Identification and Authentication Importance

Identification and authentication measures are enterprises' first and most important line of defense. If a device is able to identify users reliably, and bind users to that device for the period of use, the task of providing overall authorization, privacy, integrity, and accountability protection is much easier.

Since client devices (PCs, NetPCs, laptops, PDAs) are now distributed further from physically secure environments, networked to increasingly critical enterprise resources, and carry crucial information, local device security has become an important concern for companies of all sizes. As a result, superior device and local-level solutions will experience fast market development. Markets for network-level, certificate-based solutions are developing more slowly due to lack of acceptance and emerging standards. Eventually, integrated local-level and certificate-based identification systems will emerge to provide stalwart identification and authentication security across the Internet.

Since individual laptops and corporate PCs are vulnerable to theft and unauthorized use, local identification controls are of immediate importance. Currently, most computer systems utilize only basic passwords to identify users to PCs. Resourceful users easily defeat these measures; passwords can be overheard, electronically intercepted, guessed, and bypassed during the boot process.

If local identification measures are tied strongly to local access control, vulnerable laptops and PCs are useless to criminals except for their hardware value. In addition, by reliably identifying users locally, it becomes easier for the network servers to authorize users to access a variety of information and application resources.

There is a much broader and more powerful variety of mechanisms available to identify users. These mechanisms might serve as solutions, and can be categorized into three groups based on the following:

- What you know (passwords).
- What you have (tokens, smartcards).
- Who you are (fingerprint biometrics).

In addition, many solution implementations combine two solutions, commonly labeled two-factor identification, to provide additional security. The technologies in each of these areas are mature

enough to be implemented immediately at the local level, without coordination with other network devices.

Digital certificates are paving the way for interoperable, secure identification across the Internet. Digital certificates are small pieces of software that use public-key cryptography to create a unique digital signature (or ID), reliably identifying a party across a network. These certificates enable previously unaffiliated parties, such as E-Commerce transactors, to identify one another with the aid of a trusted third party known as a certificate authority. Once digital certificates have been fully implemented, they allow for enterprise-wide single-sign-on, secure E-Commerce, easy establishment of VPNs, and many other applications.

The certificate infrastructure and technology is still developing. Certificate server products are still in development and Certificate Authority services are in their infancy. For example, Secure Electronic Transactions (SET), the new E-Commerce credit card protocol, will depend heavily on digital certificates but has been delayed because of procedural and performance issues. As a result, applications using SET have been delayed as well. Therefore, certificate-based security will develop more slowly over the near-term. These vendors will need to focus on setting standards, marketing, and partnering to extend this solution.

Over the long term, local access control and certificate-based security will eventually merge (see Figure 10).

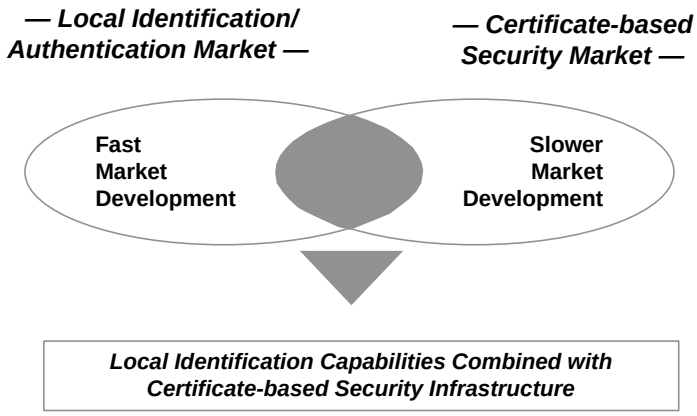

Figure 10

Certificates contained and coordinated between smart-cards and browsers could become the universal ID for a variety of identification and access control functions. In another scenario, biometric identification software could become an additional identification factor integrated into a certificate-based security architecture. For example, a server or PC can require that a user submit his/her fingerprint description, which will be matched with the fingerprint description on a corresponding certificate.

Security Market: Balanced Hardware/Software Solutions

Complete security solutions will need to provide products that balance hardware and software. Individually, neither provides an adequate solution.

A number of issues are driving the emphasis on software in security. Each of these factors increases the importance of software in the security market. As a result, enterprises will more likely invest in software solutions (see Figure 11). Analysts are recognizing this trend, and network software is projected to grow rapidly over the next several years, bringing with it a significant security component. IDC projects the Internet/Intranet Web server market will grow from $40 million in

1995 to $1.4 billion in 2000. In order to provide a total solution, systems companies will need to develop or acquire software expertise.

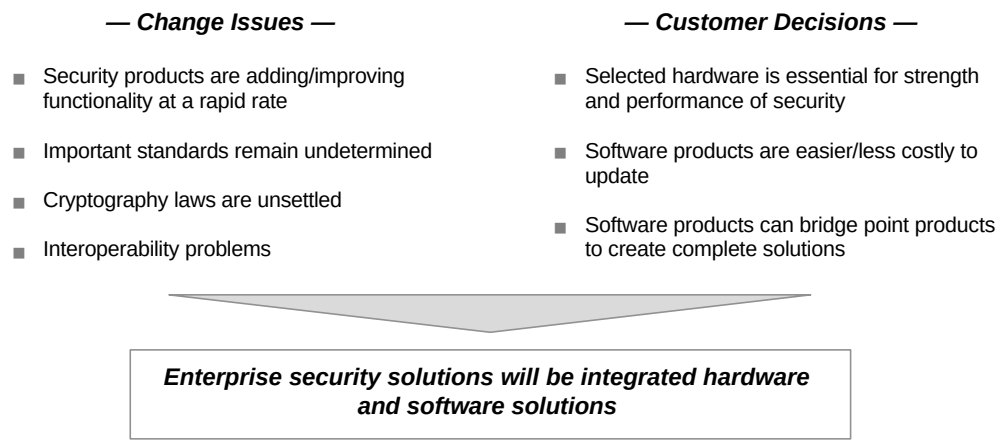

Figure 11

Hardware will also remain a critical element in resolving security issues. For example, E-Commerce applications using SET will require multiple public-key encryption operations per transaction, potentially slowing existing servers to a crawl. Specialized hardware will be necessary to alleviate this problem. In addition, smartcards and tokens can provide robust, high-performance encryption solutions on the desktop, and can be used as a tool for secure transactions with a multitude of new (inter-) networked applications. As a result, enterprises will require integrated solutions.

Security Market: Proliferation/Limitation of Security Offerings

As the networked computing environment has grown, there has been a corresponding explosion in the number and variety of security offerings from a diverse array of companies. While these solutions aim to provide a comprehensive security solution for enterprises, they have, for the most part, lacked a practical orientation. Additionally, they have substantial interoperability and ease-of-use issues.

In the last 12 months, we have witnessed the rapid growth of security offerings. Vendors are now producing products in all of the major market segments and expanding the functionality of their offerings to encompass other product categories. Figure 12 shows a small sample of the companies offering solutions in various segments.

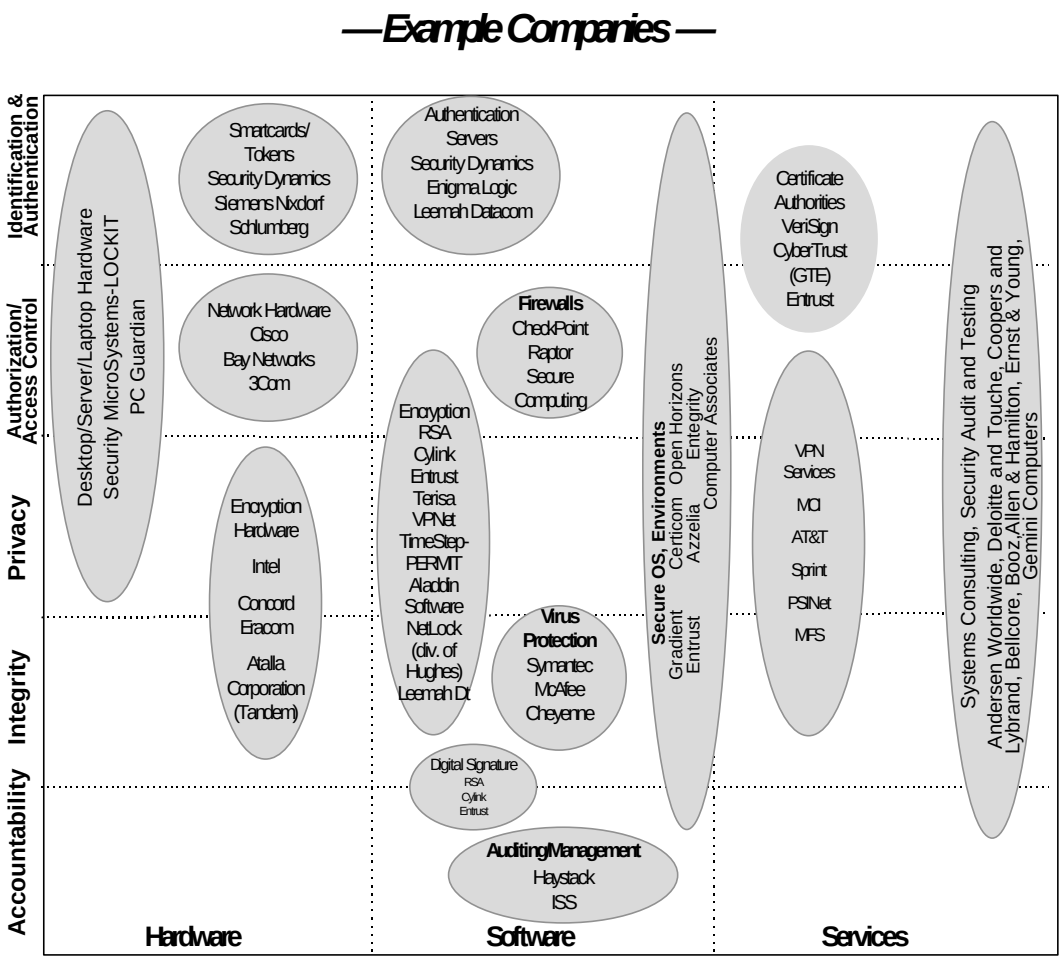

Figure 12

Cross-vendor usage, ease of use, interoperability, and practical applicability remain crucial issues. Firewalls provide some examples of the problems around ease of use and interoperability. While the industry has recently made strides in its interfaces and simplicity, configuring and managing firewalls remains a complex task for most IT managers. Similarly, very few firewalls interoperate with each other, specifically in the areas of virtual private networking (VPN).

The final limitation in many security offerings is their lack of focus on the practical security concerns of enterprises. While many vendors have pieced together point solutions or introduced broad, far-reaching frameworks, they have ignored the real requirements of and constraints placed upon enterprise IT managers, such as:

- In an enterprise with multiple platforms and the eventuality of working with other enterprises over public networks, IT managers security solutions must be based on open, interoperable standards, not proprietary systems.
- Enterprises need a clear migration path from their currently limited security solutions to the most comprehensive solutions possible, with stops along the way depending on their various levels of need.

The current offerings of most system vendors do not address these concerns.

ENTERPRISE SECURITY FRAMEWORK

To clarify security solutions and determine a practical roadmap for the deployment of enterprise security, Compaq has developed the Enterprise Security Framework. Using this framework, Compaq's enterprise customers can get a birds-eye view of the security market, judge the suitability of a solution set, and develop both short- and long-term deployment strategies for their enterprise security requirements.

The foundation of the security framework is the criteria set it uses to classify security solutions (see Table 2). The framework gauges these solutions relative to:

- Robustness.
- Comprehensiveness.
- Performance.
- Manageability.

TABLE 2: SECURITY SOLUTION CLASSIFICATION

	Security Level Criteria
Robustness	*How sophisticated an attack can the security solutions withstand?* This criterion gauges a solution's effectiveness in determining/repelling the efforts of different levels of security attacks (i.e., those ranging from casual to planned). It can also measure the technological advancement of a solution set.
Comprehensiveness/ Interoperability	*How complete a solution does the security measure offer?* This criterion rates a solution set's ability to provide a security solution that extends from the local client/server platform to external network interactions. A solution's relative comprehensiveness can be judged by the variety of attacks it protects against (e.g., impersonation, denial of service, theft) and the security objectives served (inter-enterprise communications).
Availability/Performance	*How "available" will the solution be and how will it affect system performance?* These criteria measure how transparent the execution of the technology is (e.g., how fast is it in operation?).
Ease of Use/Integration	*How easy to install, use, modify, and manage is the solution within a platform or enterprise environment?* This criterion gauges whether a solution provides security in a way that users and administrators will actually use, as well as the centralized administration tools they need to manage the solution over the long term. It also measures whether enterprises can integrate a solution seamlessly with the existing product set.

Each of these criteria is a critical determinant of how effective or appropriate a solution may be to an individual enterprise.

The Enterprise Security Framework establishes "levels" of security based on these criteria, which begin to shape a conceptual roadmap for enterprise security (see Table 3). Each level describes a solution based on how it performs against the above criteria. As solutions move up levels, from A to B to C, these solution sets become sounder and more comprehensive, perform more consistently, and are easier to use. Enterprises may choose the level of security (and thereby the solutions) appropriate to their needs.

TABLE 3: LEVELS OF SECURITY

	Level A	Level B	Level C
Robustness	Capable of deterring basic, unsophisticated attacks: • Colleagues attempting to log-on as different/higher level users • Employees who unwittingly introduce viruses	Capable of repelling more sophisticated attacks by those with some level of computing power/expertise: • Attacker with sophisticated hacking utilities and ability to break encryption	Capable of defeating sophisticated/organized attacks uniformly across the enterprise by those with significant computing power/expertise: • Organizations with the ability to break strong encryption, targeting competitive data
Comprehensiveness/ Interoperability	Offers measures addressed to a single point (e.g., log-in, data storage) and/or security objective (e.g., identification access control) typically on a device.	Offers measures addressed to multiple points and objectives. These measures are to some degree interoperable with other solutions and work across many (but not all) platforms (e.g., single sign on for segment of enterprise).	Offers pervasive package that functions across all the heterogeneous platforms/environments within a large enterprise and/or across Externet environment, seamlessly. These solutions may only address a single objective, but offer a complete solution (Externet/large enterprise single sign-on).
Availability/ Performance	Solution is generally available with some periodic maintenance and set-up required. Overall performance is acceptable.	Solution has high availability, but sometimes requires scheduled maintenance. Security feature performance is strong and has no impact on other operations.	Solution is available 24x7 with limited maintenance time required. Solution performs transparently to user.
Ease of Use/Integration	Offers a solution which is not well integrated with other security solutions. Limited flexibility and management tools for enterprise security administrators.	Offers more integrated solutions for enterprises which make many security measures transparent to appropriate users. Offers easy to use administration tools.	Offers centralized, seamless administration for internal network, and Externet security services. Easy to manage; Enterprise can flexibly build/change solutions to meet their needs. Based on open standards.

In practice, several solution sets fit into each level and across devices and networks. However, certain types of solutions characterize each security level. For example:

- Level A solutions are primarily concerned with achieving basic security through stringent access control to local devices, and basic boundary protection for the network.
- Level B solutions require greater levels of authentication and authorization control locally, and centralized security services for the internal network.
- Level C solutions enable secure Externet applications and communications with advanced external network functionality. Level C also contains robust security at the boundary of and inside the corporate network.

Higher security levels primarily operate as network services. Table 4 details at what platforms and levels specific solutions operate**:**

TABLE 4: PLATFORM AND LEVEL-SPECIFIC SOLUTIONS

	Level A	Level B	Level C
Client/Server Device	• Local information privacy-basic encryption (selective file, drive). • Basic integrity protection (standalone anti-virus software) • Physical security measures • Robust access passwords	• Robust privacy using strong encryption (long key, dedicated encryption engine) • Strong two faction local identification and access control solution, using software (password) and hardware (tokens/smartcards)	• Strongest identification: biometric devices coupled with digital certificates • Very strong file and drive privacy protection/encryption
Internal Network	• Network operating system password • Basic ACLs, embedded in network operating system	• Secure e-mail and Web • Software enabling multiple robust security services • Centralized access control/authorization with flexible rules and scaleable infrastructure (enabling single sign on) • Auditing/Management tools	• Enterprise-wide replication of security services with centralized management • Standard-based/interoperable public key infrastructure offering which covers key recovery, certificate creation/management, signatures, and hashing algorhythms
External Network	• Basic boundary control (firewall) • Access and integrity protection (secure Web server/browser)	• VPN abilities (I.D., privacy, integrity) with known partners using public key technologies (certificate servers) and transmission encryption (firewalls) • Secure E-commerce application • Accountability software (logging and tracking) • Intrusion detection/investigation tools • Network integrity protection	• Robust infrastructure enabling VPN abilities even with unknown parties based on interoperable certificate servers and firewalls • Single sign-on across internal and external networks enabled by interoperable access control and authorization servers

CONCLUSION

Compaq believes that in the next 18 months, enterprise will be able to partner with technology providers to strengthen basic solutions. In the short term, client and server device-level solutions will remain the focus of enterprise, enabling completion of the implementation of Level A solutions. In addition, within an 18-month window, we will be able to focus on enhancing Level A security functions. We will achieve this by using newer technology with an integrated approach, and will begin deploying these solutions as the building blocks for Internet/Externet compatible solutions that incorporate computer devices, operating systems, networking equipment, and firewall products. Additionally, within the next 24 months, we should be able to install enterprise-wide security solutions that operate across client, server, and networking equipment and provide vigorous and seamless security solutions for the Internet, Intranet, and Externet.

Compaq's goal is to simplify the choices, standardize the offerings, integrate the solutions, and provide a manageable, secure computing environment. Guided by our customers' requirements, our strategy is as follows:

- Integrate the best of security technologies with our platforms/products.
- Provide performance and attune technical information to our customers.
- Supply our customers with capacity planning information.
- Explore the opportunity for Compaq to build hardware and software security solutions that address both specific and generic enterprise security requirements.

By using the Compaq Enterprise Security Framework, enterprise IT managers can plan a security solution roadmap which meets all the objectives of security at every point in the IT infrastructure.