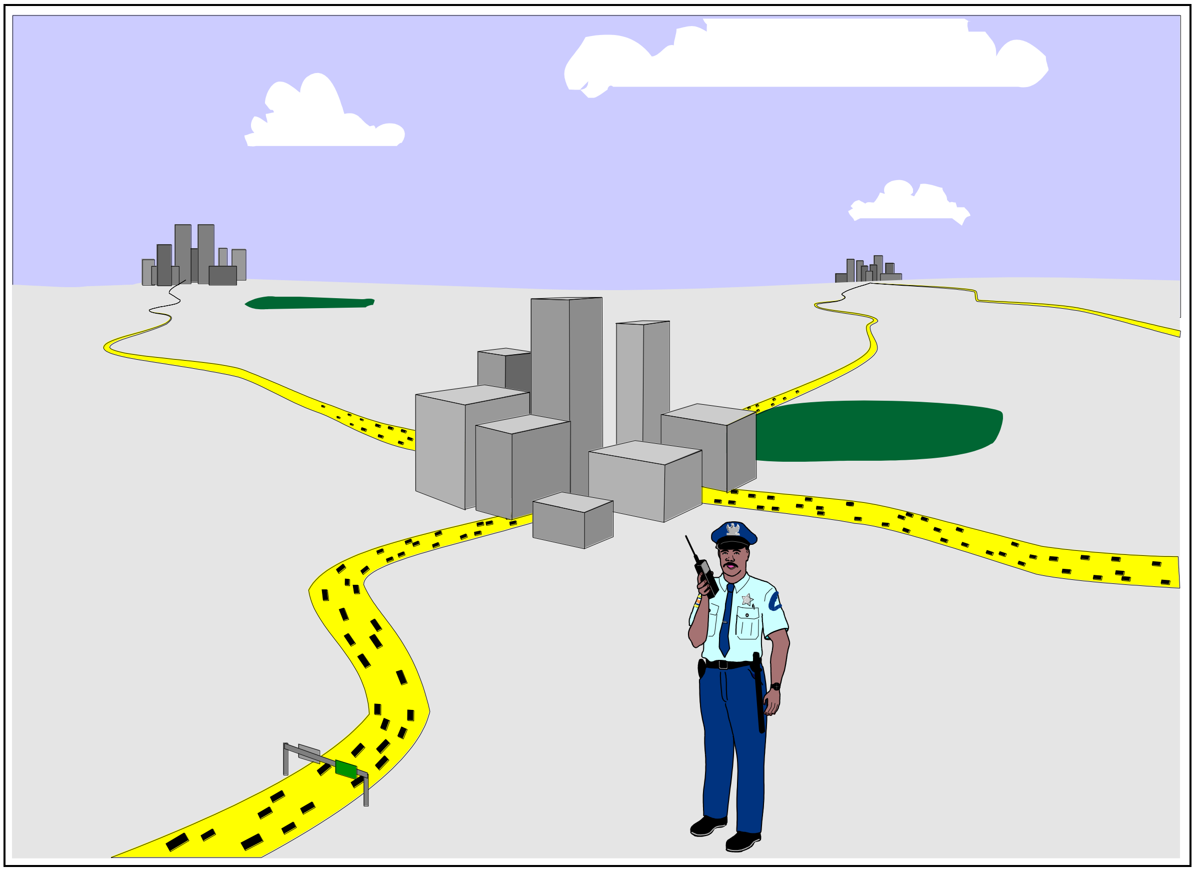
AXENT TECHNOLOGIES

Business Plan



Security for the Information Superhighway

Executive Summary

Client/server computing is having a profound effect on the way corporations protect and secure their information resources. A recent survey in *Computerworld* ranks client/server security as one of the most important issues facing computing professionals today. The conflict between client/server's easy access to data and the need to protect and secure corporate information assets creates an opportunity for new, innovative software products that can protect and safeguard distributed systems. Raxco intends to focus on this emerging need with a new product division called **Axent Technologies**.

Axent's vision is to provide the security solution for the new information superhighway. To achieve this goal, Axent Technologies will develop and market a comprehensive suite of client/server security products and services called **OmniGuard**. OmniGuard is a combination of Raxco's existing desktop security and storage management products, products under development, product acquisitions, and a new consulting services organization. In order to differentiate OmniGuard from the competition, the OmniGuard solution will emphasize both systems and data security. This means that we will position our storage management products as part of an overall security solution, rather than stand-alone data management tools. Axent will integrate these products and add consulting services in order to deliver a complete solution which will support all aspects of client/server security including:

- Enterprise-wide security management
- User administration
- Systems and data access control
- User identification and authentication
- Systems monitoring/intrusion detection
- Data security and availability
- Enterprise-wide storage management

Although the overall demand for client/server products is exploding, the market for client/server security products is still nascent. As yet, no real dominant player has emerged. Of the niche vendors concentrating on client/server security, none can currently match OmniGuard's breadth of function and cross-platform availability. Axent's goal is to focus solely on client/server security and become the dominant vendor in this emerging market. Since the market for client/server security software will ultimately be larger than the market for mainframe security software, Axent should enjoy rapid growth and success.

Table of Contents

Introduction

Computer-based information systems are moving away from the centralized, monolithic computing model typified by large mainframes, towards a distributed computing paradigm where processing and data can be located on multiple, heterogeneous hardware platforms dispersed throughout the enterprise. This trend, known as *client/server* computing, is having a profound effect on the way corporations protect and secure their information resources. The use of small yet powerful networked processors offer better price performance, increased ease of use, and greater flexibility. In addition, emerging client/server standards allow applications to run in an "open systems" environment, interconnected with computing resources all over the planet.

However, this new found freedom and flexibility are not without significant drawbacks. Open client/server computing, by its very nature, leaves corporate systems and data vulnerable to unauthorized access, modification and destruction. Bill Gates at Microsoft describes how client/server technology can empower workers by putting “information at their fingertips.” While this is a laudable goal, allowing easy access to systems and data may not always be desired, especially when dealing with highly sensitive applications.

A December 6, 1993, *ComputerWorld* survey[1] ranks systems and data security as one of the most important distributed computing issues facing information system (IS) professionals today. As more and more corporate information systems become connected to the emerging “information superhighway,” the threat of unauthorized access to a corporation’s information assets increases dramatically. There are already over two million systems connected to the Internet (the current backbone of the information superhighway) and thousands of new systems are being added every day. When Robert T. Morris launched his infamous “worm” through the Internet in 1988, only 2,600 of the 60,000 Internet systems were affected. Today the same rate of infection could seriously damage many hundreds of thousands of systems.

A study conducted at the University of Texas[2] suggests that most companies that lose a major portion of their critical business information do not survive longer than a couple of years. Catastrophes such as the World Trade Center bombing or the 1993 flooding in the Midwest serve as reminders of just how quickly our computing resources could be lost or seriously damaged. The security and integrity of corporate systems and data are not just matters of good business practice anymore, but matters of corporate survival.

Not all security threats are from such external “hackers” as Robert T. Morris, international terrorists, or natural disasters. A study in the August 11, 1993, *Computerworld Client/Server Journal*[3] found that most IS managers fear unauthorized access and data tampering from employees (intentional or accidental) far more then they do threats from outside the company. A hospital in the UK discovered a nurse who had gained access to the hospital’s computer system and intentionally altered patients’ prescriptions. A few years ago it was discovered that engineers at the Department of Energy’s Rocky Flats nuclear site had by-passed security measures in order to make their work easier. Of course, in doing so, they exposed our nuclear weapon secrets to any one who dialed into the computer. (Fortunately, the breach was discovered before this happened.)

The conflict between client/server’s easy access to data and the need to protect and secure corporate information assets creates a growing opportunity for software-based solutions to help resolve the problem. Corporations have spent decades developing workable security policies for their centralized mainframe platforms only to discover that these policies are either difficult to implement or unenforceable in the client/server world. While 83% of large organizations have a security policy in place,[4] these policies are only as good as their implementations. Security software designed for the mainframe environment is wholly inadequate for protecting distributed systems. The market needs a new breed of security solutions designed and built to implement security policies in a distributed client/server environment.

Axent's vision is to provide security for client/server systems. Axent's security solutions, comprised of software and services, can protect and safeguard an enterprise's distributed systems and data assets from unauthorized access, modification or destruction. Axent's client/server security solution, **OmniGuard**, consists of a set of integrated modules which cover all aspects of client/server security including:

- Enterprise-wide security management
- User administration
- Systems and data access control
- User identification and authentication
- Systems monitoring/intrusion detection
- Data security and availability
- Enterprise-wide storage management

OmniGuard is not a mainframe security package ported to the desktop. OmniGuard was designed specifically for distributed computing environments and is itself a client/server application. OmniGuard is available on multiple UNIX platforms, Microsoft Windows, and soon, Windows NT. OmniGuard's easy to use graphical interface (Motif or Windows) provides security and data availability across a wide range of distributed multi-vendor systems including UNIX TCP/IP, Novell Netware, Windows NT Advanced Server, and DECnet. OmniGuard provides a comprehensive way to ensure the safety and integrity of client/server systems without giving up the easy access to information that client/server was designed to provide.

Axent Product & Market Strategy

Product Requirements

Information security consists of meeting the following goals: **Confidentiality, Integrity and Availability**.[5] Most operating systems (other than certain PC operating systems such as MS-DOS) contain basic access controls, user identification and authentication, and audit trails to provide security. These basic functions are required for commercial grade or C2-level security as defined in the U.S. Department of Defense's Trusted Computer Systems Evaluation Criteria (DOD 5200.28.STD), commonly known as the "Orange Book." However, since most client/server systems are made up of a combination of hardware and software technologies from multiple vendors, security capabilities above and beyond vendor-supplied functions are needed. Add-on security software augments operating system level functions in order to provide effective security management, network-wide operation, and increased protection of systems and data. In most cases the security capability supplied by the operating system (or network operating system) is inadequate for handling the complexities of a heterogeneous, multi-vendor environment. Most organizations establish security policies and procedures and expect employees to follow them. However, the fact that operating systems have security functions built in doesn't necessarily mean that corporate security policies can or will be followed. The greatest threat to corporate systems and data is the circumvention (intentional or accidental) of established security practices. A vendor-independent, cross-platform security solution is necessary to enhance security features supplied by the operating system and to insure that security policies and procedures are indeed being followed.

Security requirements for client/server computing can be grouped into the following categories:

1. **Enterprise-wide security management**
   - Manages and ensures conformance with security policies
   - Checks all systems for vulnerabilities such as trap doors, logic bombs, or unauthorized privileges
   - Provides integrity checks, including anti-viral protection
   - Detects changes to security settings or files
2. **Administration**
   - Sets up user profiles for authentication and access controls

- Allows templates to quickly create certain types of user accounts
- Safely delegates pieces of administration to non-privileged users

3. **Access Controls**

- Controls system access or log-in
- Controls file and object access
- Controls database access, including records and fields within database
- Controls network access (firewalls, filters, wrappers)
- Protects unattended workstations

4. **Monitoring/Intrusion Detection**

- Keeps audit trail of failed and successful accesses
- Audits use of security system
- Logs user sessions
- Analyzes and reduces audit trail
- Detects intruders and escalates or responds automatically to break-in attempts

5. **Identification and Authentication**

- Ensures that user must enter a proper password to access system or network
- Provides identification and authentication beyond passwords (i.e., smart cards, biometrics, call-back security for dial-ups, etc.)
- Provides authentication across a network
- Provides single sign-on for multiple hosts in a network

6. **Data Availability**

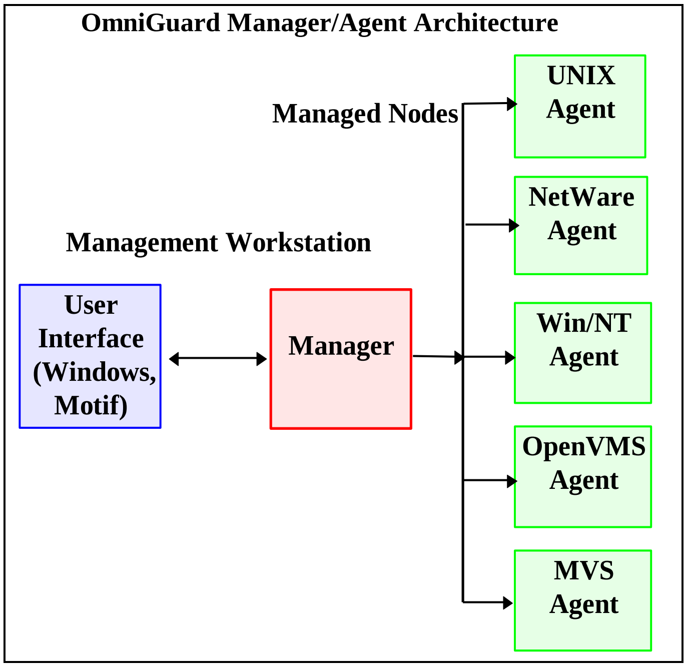
- Safely backs-up and restores data
- Provides hierarchical storage management (automatic file shelving and retrieval)
- Provides media management

The OmniGuard Solution

OmniGuard is a suite of integrated software tools which manages and controls systems and data security across multiple types of client/server environments. These environments include heterogeneous UNIX platforms, Microsoft Windows, Novell Netware, Windows NT, as well as mid-range and mainframe processors. OmniGuard is made up of six modules that collectively manage, secure and protect enterprise-wide client/server systems and data. OmniGuard enables security and data managers to establish security policies and manages conformance with those policies by user, by organization, and even across an entire enterprise.

OmniGuard applications can work individually to solve specific problems or they can be combined to provide a comprehensive security solution. OmniGuard applications are designed to be open. They work well by themselves or in combination with other OmniGuard products or even products from other vendors. They are integrated with major systems and network management frameworks, including HP's OpenView, IBM's NetView/6000, Sun's Net Manager, Tivoli's TME, Bull's ISM, etc.

OmniGuard security applications never lock you in. Instead, they provide an open plug-and-play approach to add-on systems and data security.



Not only does OmniGuard ensure conformance with corporate security policy, OmniGuard applications can help organizations implement security and data management procedures. OmniGuard applications can control access to multi-platform client/server networks, detect and prevent attempted break-ins, monitor and analyze log-on attempts, lock unattended workstations or terminals, enable users to log-on once to multiple servers or hosts, back-up and restore clients and servers, and automatically migrate data files to optical or tape storage.

OmniGuard uses a *manager/agent* architecture. Functions that are common to all managed platforms are implemented on the *Management Workstation* and are accessed from an easy to use graphical user interface (GUI). Functions that are specific to a particular platform are implemented as *Agents* which execute on the managed nodes.

The user interface, manager and agent software can reside on different platforms. For example, the user interface can be placed on a Windows or UNIX workstation. The manager may be on a NetWare server, a UNIX server, or an OpenVMS server. Axent developers use cross-platform GUI development tools to build OmniGuard applications in order to support the widest possible range of management platforms from a single code base. This means that new applications can be developed faster and made available on all supported platforms simultaneously. Operating systems' specific functions are isolated to the agent modules which may reside on an even wider range of supported operating platforms.

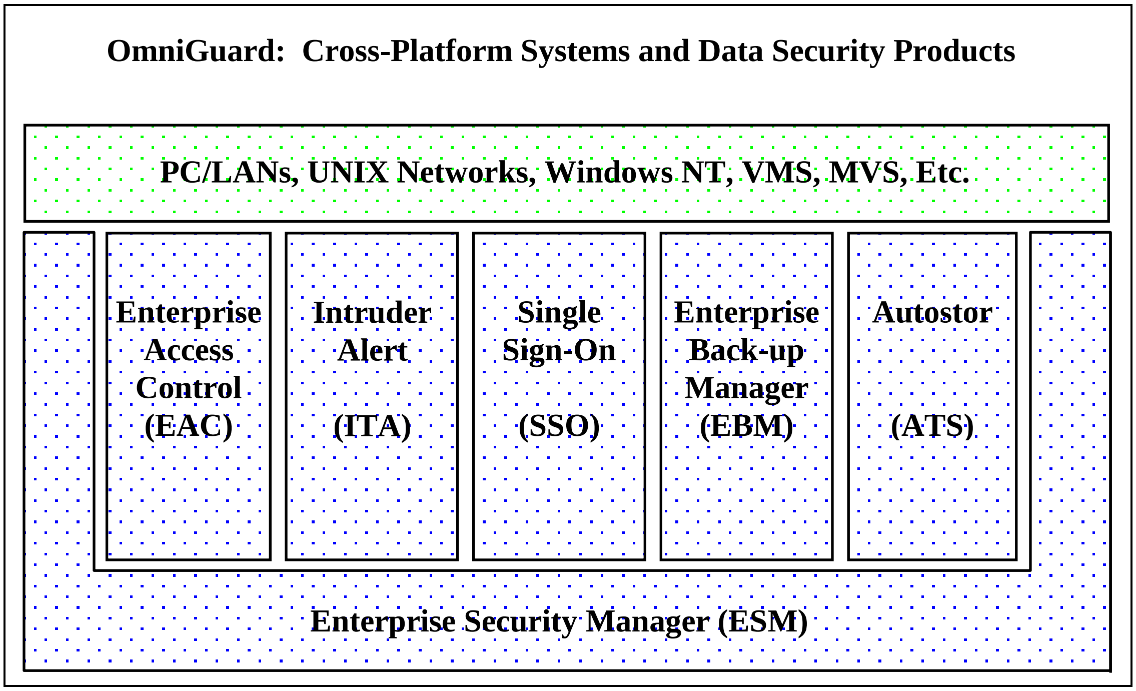
From the GUI on the OmniGuard management workstation you can manage systems and data security functions across a wide range of client/server environments. OmniGuard gives you a choice of management platforms including Microsoft Windows 3.x, Motif (AIX, HP-UX, Sun OS, Sunsoft Solaris, Digital Ultrix, Digital OSF/1, and several other UNIX environments), and soon, Microsoft Windows NT.

OmniGuard agents run on a wide range of personal computer (PC), UNIX and mid-range platforms including Novell Netware (3.x or 4.x), HP-UX, IBM AIX, Sun OS, Sunsoft Solaris, Digital Ultrix, Digital OSF1, OpenVMS (on Vax or Alpha), and others. We will soon add support for Microsoft Windows NT advanced server and Axent's plans include agent interfaces to mainframe (IBM MVS) security packages such as RACF or ACF2.

OmniGuard supports TCP/IP, Novell NetWare, and DECnet as underlying network protocols. These protocols account for 47.2% of the network traffic today with the fastest growth in TCP/IP. TCP/IP, is projected to increase 15% to 23% of network traffic in 1994. In the future, we will add SNA and Microsoft LAN Manager. SNA still accounts for 27.5% of all networks, although its relative market share is decreasing.[6] Microsoft is expected to make inroads into the network operating systems market through Windows NT Advanced Server by late 1995.

A November 1993 survey revealed that only 5% of NetWare users are running version 4.x in a production environment and 9% are using it in a test environment.[7] By the end of 1994, 40% are expecting to be running NetWare 4.x. and 29% are expected to remain on 3.x and never adopt 4.x.[8] Because of these statistics, OmniGuard will support both NetWare 3.x and 4.x for the foreseeable future.

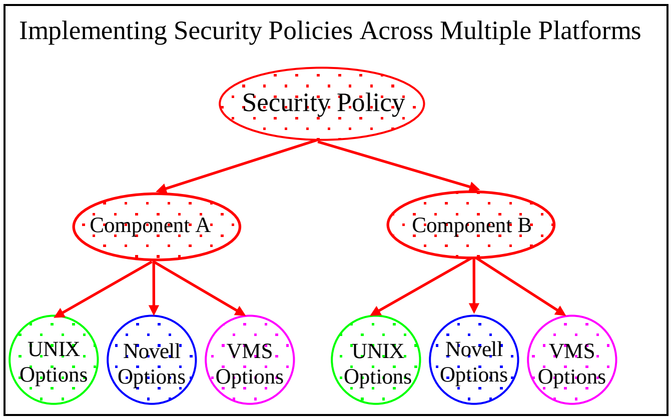
OmniGuard Product Modules and Functions


OmniGuard: Cross-Platform Systems and Data Security Products
PC/LANs, UNIX Networks, Windows NT, VMS, MVS, Etc.
Enterprise Access Control (EAC)
Intruder Alert (ITA)
Single Sign-On (SSO)
Enterprise Back-up Manager (EBM)
Autostor (ATS)
Enterprise Security Manager (ESM)

1. **OmniGuard/Enterprise Security Manager (OmniGuard/ESM)** [note: new name for STK/U & *stk/i*]

Enterprise Security Manager is the foundation of the OmniGuard security solution. ESM enables security administrators to manage their entire network of client/server systems from a single MS/Windows or UNIX Motif desktop. Security and data managers use ESM to establish systems and data security *policies*. Policies are made up of policy components and can be applied to a single individual, a group of individuals, an organization, a group of organizations, or the entire enterprise. Policies reflect the security standards and guidelines for that group and are checked seperately for each type of hardware and software in use by the respective group.

ESM checks each group of users for conformance with established systems and data security policy. ESM analyzes this information and provides security managers with summarized and detailed information about which groups and, if desired, which nodes within a group, are not conforming to policy. ESM enables the security manager to ensure that end users are using the security functions available in the operating system or from add-on security tools.



In addition to security management, ESM checks the network for potential security threats such as viruses, easily guessed passwords, trap doors, logic bombs, viruses, default accounts, unauthorized privileges, etc. If ESM detects a security threat, it can notify the security manager who can use ESM to automatically correct the problem or initiate a manual action.

2. **OmniGuard/Enterprise Access Control (OmniGuard/EAC)** [technology acquired from third party combined with existing WSLock product]

   Enterprise Access Control is an add-on security module that augments native systems and data access control functions. Using EAC's easy-to-use GUI, a security administrator can create a detailed profile for each authorized user in a client/server network. Profiles define the user's security privileges, including when they can log-on to the network, the number of authorized log-on attempts, the location(s) they can log-on from, what files they can access, what systems or applications they are authorized to use, etc.

   Enterprise Access Control uses these user profiles to enforce additional access controls beyond what client/server operating systems normally offer. These add-on security controls enable a security administrator to control when a user can access a system, what type of access a user can have, and the location(s) from which a user can access the system. Enterprise Access Control provides additional password controls like password history, password checking upon password selection, password format policy, and the ability to specify longer passwords. An audit trail is kept of all security administration activity which can be used for future analysis.

   In addition, certain aspects of user administration for particular types of users can be delegated to non-privileged users. This allows department managers to add new users to the systems without being granted systems administrator privileges.

   One of the biggest security threats is a workstation or terminal where an authorized user is logged in, but not at their desk. Obviously any unauthorized person who can gain access to this workstation or terminal will be able to access any systems or data the authorized user had access to. Enterprise Access Control eliminates this problem by automatically locking an unattended workstation or terminal after a specified period of time. The authorized user can set the time-out parameters. If Enterprise Access Control locks the terminal or workstation, the user simply enters his/her user ID and password, and the terminal or workstation returns to the same state in which it was left.

3. **OmniGuard/Intruder Alert (OmniGuard/ITA)** [new product under development]

   Most of a security administrator's time is spent ensuring that access controls are in place and maintained. But, what happens when security breaks down? What happens when an unauthorized user enters the system? And what happens when users begin probing into system areas in which they do not belong? The answer is that data security professionals are left with a violated system. They must use whatever audit trails or back-ups exist to repair the damage of a security breach.

   ITA allows security managers to be more proactive with system security. It addresses security problems as they occur, minimizing the impact of security breaches. ITA monitors multiples streams of security audit trail information in real-time, analyzes the data using site-specified rules, and reports critical events to the security administrator. Optionally, certain events may cause ITA to take action such as calling a pager, terminating a process, or disabling a user account.

   The various UNIX variants are capable of creating audit trails that detail security events. These audit trails are in proprietary formats, none of which are easy to decipher by the average administrator. In particular, many audit trail records must be tied together in order to reconstruct the details of a single event. By Q1 95, Axent plans to add network-wide, audit trail analysis and summarization which can pinpoint security violations and intrusions across a heterogenous UNIX network.

4. **OmniGuard/Single Sign-on (OmniGuard/SSO)** [new product from acquisiton or internal development]

   Today's users log into many systems throughout the network. Each time a user logs into a new system, the user is required to log in again. As a result, each user has to keep track of a multitude of user IDs and passwords. The purpose of single sign-on is to allow a user to log-in only once to the network. As the user accesses services from different systems, the authentication process to each new server will be automatic.

Three different methodologies can be found in single sign-on products today: synchronization, scripting, and authentication server. Synchronization means that the same password is used on every system. The single sign-on software is responsible for ensuring synchronization among the various password files. In some cases, it automatically takes care of sign-on to each server once a user has given the password during initial sign-on to the desktop. The problem with synchronized passwords is that if a user's password is stolen, the intruder has universal access to everything the user has access to.

Scripting allows different passwords to be used for various servers. A user ID and password database is kept on the desktop and the single sign-on software is capable of detecting log-on and other password related screens or prompts, and automating the sign-on process through the use of pre-defined scripts. Both synchronization and scripting share the danger that passwords are transmitted in clear text through the network which makes them vulnerable to eavesdropping through sniffers such as were used in the well-publicized recent Internet break-ins *(Washington Post*, February 4, 1994). Also, if the desktop where the scripted passwords are stored is penetrated, the password database is likely to be compromised.

An authentication server (such as Kerberos or DCE) provides a means for the most secure single sign-on. A user must identify themselves to the authentication server which then issues cryptographic tickets for use with applications. While more secure, the cost of implementation is high as each system needs special software, and server applications may have to be modified as well. Also, in order to prevent transmission of clear text passwords, one-time passwords should be used. This implies the use of biometrics, smart cards, or one-time password desktop software.

Axent's approach to single sign-on is to provide a near-term solution using scripting and synchronization, and then to integrate this with DCE authentication services in '95. In addition, Axent plans to integrate with one or more smart card or biometric devices.

Encryption is an important enabling technology. Encryption can be used to provide authentication through cryptographic signatures and privacy by encoding data. It is a valuable tool for access control and authentication. It can also be used to ensure the privacy of backed up data that is stored off-line. Unfortunately, encryption is considered a weapon by the United States and is subject to onerous export controls. Any algorithm which is approved for general export for the purpose of encrypting either transmitted or stored data is likely to very weak. On the other hand, encryption can be easily exported if it is solely used for authenticating users.

We will make use of encryption for message and user authentication. This means that we will probably use DCE security or Kerberos. Where needed, we will use weaker encryption algorithms to scramble data for privacy purposes. As export controls ease, we will make use of standard, strong encryption algorithms such as RSA and DES (the Data Encryption Standard).

5. OmniGuard/Enterprise Backup Manager (OmniGuard/EBM) [new name for Backup.Unet]

No amount of built-in or add-on security can completely protect important data from unintentional loss or damage. For data to be secure, it must be *safely* backed-up to another location, preferably on a different machine and in a secure media. While back-up software is fairly common, most network-oriented products back-up data from multiple clients to a single server. In order to speed up the process, they store the backed-up data in a proprietary format. This works fine if you always restore the data with the same software you backed it up with and if nothing happens to the back-up record or catalog.

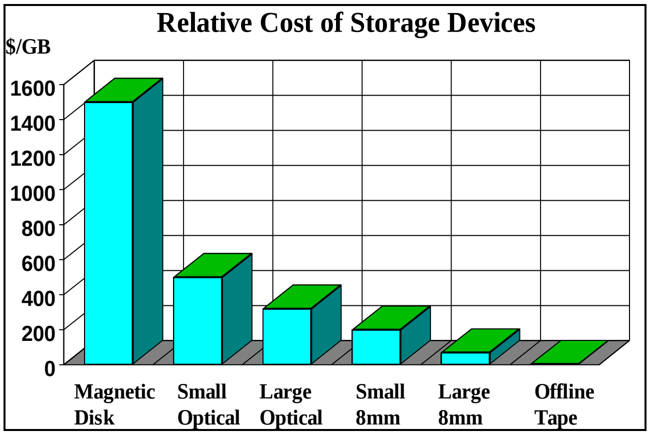
However, sometimes part of the backed-up data is lost or the back-up record or catalog itself is damaged or destroyed. In this case, the data will be lost since the remaining data on the server cannot be interpreted by standard utilities. Data is not secure unless it is backed-up (preferably in multiple locations) and stored in a format which can be read by standard UNIX or PC utilities.

Enterprise Backup Manager solves this problem by using a different approach to backup. Instead of multiplexing multiple streams of data onto a single tape, EBM backs-up multiple clients in parallel. EBM back-ups are stored in standard UNIX formats such as CPIO or TAR.

6. OmniGuard/AutoStor (OmniGuard/AST) [Lachman HSM]

Over 30,000,000 disk units were shipped in 1993. Peripheral Strategies of California estimates that the volume of data is growing at a compound rate of 60% per year, with large contributions from both existing as well as new applications. As new technologies, such as imaging and multi-media, become widely deployed, this trend will accelerate. What is startling is that as the price of a gigabyte of storage drops towards the $1000 mark, the number of individual data files which are stored on that media remains fairly constant -- in the 300,000 to 400,000 range. Thus, the physical number of files is becoming truly huge. Yesterday's manual methods for management of on-line storage are simply too costly to use in this environment. Only an automated, fully distributed hierarchical storage managment (HSM) solution can cope with the problem.

Why HSM? Why not more disks? Simple economics, as shown in the graphic on the left, answers these questions. Even though the unit cost of an on-line disk is low, when you start to deploy the vast number of disks necessary to hold the exploding data volume, the cost begins to rise. Consider not only the cost of the disk itself, but also the controllers, bus slots, server capacity, and other resources necessary to allow the disk to run. The cost curve shown in the graph illustrates that if infrequently used data can be moved to optical storage, the price drops to between 20% and 30% of the cost of on-line disk. If data which is not accessed from the optical media is further moved to a tape robot, the cost drops to 5% to 10%. Finally, very old data moves to off-line tape for less than 1% of the cost of on-line storage. Robotic devices can manage this progression of data movement with little or no operator intervention.



OmniGuard/Autostor allows you to install an HSM function on any system in a network which has disk storage, and migrate the files elsewhere in the network into a "mass store" composed of one or more levels of Robotic devices. This allows the flexibility to leverage your investment in optical and tape robotics across the entire network, and to provide the multi-level migration paths necessary to achieve the economic advantages shown in the graph. Like the Enterprise Backup Manager, Autostor stores data using standards based on open systems formats, thus avoiding the inherent disadvantages of proprietary file formats while ensuring that you have the best choice for data availability.

OmniGuard Cross Platform Availability

OmniGuard Application/Platform Matrix (Agents)

Functionality	**OpenVMS**	**UNIX**	**NetWare**	**Windows 3.x**	**Windows NT**	**IBM MVS**
Assessment/Conformance						
Manage systems & data security	**ESM**	**ESM**	ESM (Q3 '94)	ESM (2H '95)	ESM (Q1 '95)	ESM (Q2 '95)
Check integrity/viruses	**ESM**	**ESM**	ESM (Q3 '94)	ESM (2H '95)	ESM (Q1 '95)	ESM (Q2 '95)
Check vulnerabilities	**ESM**	**ESM**	ESM (Q3 '94)	ESM (2H '95)	ESM (Q1 '95)	ESM (Q2 '95)
Ensure policy conformance	**ESM**	**ESM**	ESM (Q3 '94)	ESM (2H '95)	ESM (Q1 '95)	ESM (Q2 '95)
Administration						
User profile management		EAC (Q3 94)	*	EAC (2H '95)	*	*
Profile templates		EAC (Q3 94)	EAC (2H '95)	EAC (2H '95)	EAC (2H '95)	*
Delegation to non-privileged		EAC (Q3 94)	EAC (2H '95)	EAC (2H '95)	EAC (2H '95)	*
Access Controls						
System access	*	EAC (Q3 '94)	*	EAC (2H '95)	*	*
File access	*	*	*	EAC (2H '95)	*	*
Database access						*
Network access		EAC (Q3 '94)	*	N/A	EAC (2H '95)	
Unattended workstations	**KBLock**	**EAC**	EAC (Q4 '94)	EAC (1H '95)	EAC (1H '95)	*
Monitoring/Intrusion Detection						
Audit trail of access	*	*	*	EAC (2H '95)	*	*
Audit security activity	*	ITA (Q3 94)	ITA (2H '95)	EAC (2H '95)	*	*
User session logs	**ITA**	ITA (Q3 94)	ITA (2H '95)	N/A	ITA (2H '95)	
Audit trail analysis	**ITA**	ITA (Q4 94)	ITA (2H '95)	N/A	ITA (2H '95)	
Intrusion detection	**ITA**	ITA (Q3 94)	ITA (Q1 '95)	N/A	ITA (2H '95)	
Identification and Authentication						
Password requirements	*	*	*	EAC (2H '95)	*	*
Smart cards and biometrics						
Call-back						
Network authentication	*	SSO (1H '95)	*	SSO (2H '95)	SSO ('96)	
Single sign-on	*	SSO (1H '95)	SSO (1H '95)	SSO (2H '95)	SSO ('96)	
Data Availability						
Backup		**EBM**	EBM (1H '95)	EBM (1H '95)	EBM ('96)	
HSM		**AST**	AST (1H '95)	N/A	ATS ('96)	
Library management		ATS (1H '95)	ATS (1H '95)	N/A	ATS ('96)	

* Basic functionality is included in the operating system or available from established mainframe security packages

Integration with Systems Management Frameworks

Each OmniGuard application is designed to function as a stand-alone product, or in combination with other products from Axent or another vendor, to create an integrated security solution. For example, OmniGuard/Enterprise Security Manager may discover that a certain group is not backing up their data according to company policy. The security manager may use OmniGuard/Enterprise Backup Manager or another back-up tool to correct the problem.

OmniGuard uses industry standard systems management frameworks as our integration platform. Rather than supply our own proprietary framework, OmniGuard instead works with open frameworks such as IBM NetView/6000, HP OpenView, Sun Net Manger, Tivoli, Microsoft Hermes, NCR Star Sentry, Bull ISM, etc. By using frameworks like these which are moving towards open systems standards such as X/Open's XMP (X/Open Management Protocol) or the Object Management Group's CORBA (Common Object Request Broker Architecture), we can ensure that our customer's investment is protected for the future.

Systems and data security is a big problem and no single vendor can possibly satisfy all requirements. By using open frameworks that work with many different vendors' products, customers can 'plug-and-play' multiple solutions from a variety of sources. Open solutions such as OmniGuard are far more practical than solutions which attempt to lock you into only one vendor's products.

Axent Consulting Services

Securing systems and data is a complex issue and software solutions alone are not the entire answer. Each organization has unique security requirements that may require a particular combination of education, training, advice, and technology. The March/April 1994 issue of *Infosecurity News* indicates that 59% of those surveyed plan to purchase training products and services in 1994, up from 32% the previous year (84% growth). Lack of end-user awareness was cited as the number one obstacle to achieving an appropriate level of security, and the number one concern among information security professionals. That is why Axent will offer a variety of professional services to complement our security products and enable customers to analyze and solve their most difficult security problems.

Security services will both lead and follow product sales. Axent Consulting Services will be available in pre-packaged modules covering:

1. **Training**
    - Security for end-users
    - Security for system administrators and EDP auditors
    - Product related training
2. **Implementation**
    - General Security
    - Security management
    - Secure access
    - Intrusion detection
    - Data protection
    - Enterprise storage management
3. **Security analysis**
    - Site assessment
    - Enterprise security assessment
    - Systems and data security planning
4. **Policy development**
    - Systems security
    - Data security
5. **Disaster recovery planning**

In addition to standardized consulting packages, Axent Consulting Services will offer fee paid consulting services on general systems and data security topics. This could include developing application-specific checks for policy conformance. For example, a bank may wish to ensure that the security in its funds transfer application is properly set up at all sites within a network.

Education and training packages will be priced per person, and will be available on-or off-site. Other consulting services will be priced between $1500 and $3000 per day depending on the seniority of the consultants. This is in keeping with security consulting fees charged by other consulting organizations in the industry. According to Dan Webb (President, OCSG) and Stosh Jarocki (Corporate Audit, Citibank), fees for senior security consultants currently range between $1500 and $3000 per day. These fees can be further leveraged for certain projects, such as developing a security policy, by reusing work previously completed and charging a set fee for deliverables.

Product Positioning

Axent will position OmniGuard as the premier, vendor independent, cross-platform, enterprise-wide add-on client-server security solution. While security software and services are available from a wide variety of sources, **Axent is the only vendor specifically focused on client/server security with products that cover the complete range of add-on security functions and are available across VMS, UNIX, PC/LANs, and Windows NT along with planned extensions into the mainframe environment**.

According to *Information Week*[9], 83% of large corporations have a formal security policy in place. When their systems were all on the mainframe, they could use RACF, ACF 2, or Top Secret to ensure that their security policies were being followed. However, as Chevron points out in an interview with *Information Week*, "Security in the client/server environment is where mainframe security was more than 15 years ago...."[10] Axent is the only vendor to approach client/server systems and data security from the stand-point of implementing corporate security policy.

The OmniGuard solution is based on creating, managing and implementing organizational systems and data security policies. Managing and implementing corporate security policies is the common denominator across all the OmniGuard applications. OmniGuard implements systems access policies, policies intended to prevent break-ins, identification and authentication policies, and data management policies. Not only does OmniGuard implement system and data security policies, it verifies that policies implemented by other software, such as the operating systems, are being implemented. In addition, the OmniGuard architecture makes it possible to add application or database specific checks, such as checking the Oracle database security settings. Only OmniGuard tracks how client/server security policy is implemented, no matter how it is accomplished.

CA and OpenVision also have broad-based security solutions. However, they are both trying to be one-stop-shop systems management vendors. Not only are they attempting to be a complete systems management solution, they are also attempting to be in the network and systems management framework business with proprietary framework technology. Whereas they are spread across security, storage management, performance, scheduling, operations, and frameworks, Axent's focus on implementing systems and data security policies gives us a precise focus which differentiates us from the "be all things to all people" vendors.

There are several well positioned players in the desktop storage management market. To go head-to-head with such vendors as Epoch, Legato, and Cheyenne would be playing the game by their rules. Instead, we will position storage management as an integral part of a total security solution. For corporate data to be secure, the data must be backed-up in a standard format to safe locations. OmniGuard/ESM security checks will be extended to include checks for data security. For instance, OmniGuard/ESM will check clients and servers to see if data is being backed-up according to corporate policy.

Not only will we check to see if the data is backed-up, we will also ensure that the backed-up data is stored in a standard format. Data stored in a proprietary format is not safe and should not be allowed. (What is the sense of backing-up your data if it is not completely safe?) The loss of the back-up catalog (often stored on the machine that was backed-up) would result in the inability to decipher the backed-up data, even if it were on a different machine. Damage to the hard drive on the backed-up machine would result in the loss of the back-up record and the consequential loss of the data. Therefore, OmniGuard/ESM will check to make sure the data is backed-up in a standard format (TAR or CPIO in the UNIX environment) so that it can always be recovered regardless of what happens to the catalog.

Since most of our competitors use a proprietary data format in their back-ups, OmniGuard/ESM will report that their back-ups are not entirely safe. The customer will then have to decide on continuing to use a competitor's product or switch to a product that doesn't use a proprietary format, such as Axent's OmniGuard/Enterprise Backup Manager which uses TAR or CPIO.

We will position OmniGuard/Autostor as part of systems and data security. OmniGuard/AST is a second generation hierarchical storage manager and provides an automated way to move data to safe, near-line and off-line storage based on **corporate data management policy**. The best means for protecting valuable data is to move it to multiple locations. However, manually moving the data is tedious and error prone. OmniGuard/AST will automatically move the data without user intervention. It will also automatically restore the data anytime it is accessed by the user. OmniGuard/AST goes beyond back-up and recovery by automatically migrating files by policy, which is based on file type and user.

OmniGuard/AST will also be integrated with OmniGuard/EBM for a complete data security solution. Most back-up products are incompatible with an HSM. When a back-up is executed, it triggers the HSM to retrieve migrated files, which lengthens back-up times considerably. Retrieving migrated files during a back-up is unnecessary because the files are already protected by being in another location. OmniGuard/AST is designed to prevent this problem. OmniGuard/AST leaves a “stub” file as a place-holder for a migrated file, so that when a back-up is run, only the “stub” files are backed up, not the migrated file. Therefore, OmniGuard/AST not only works well with OmniGuard/EBM, but it will work with any other vendor’s back-up product.

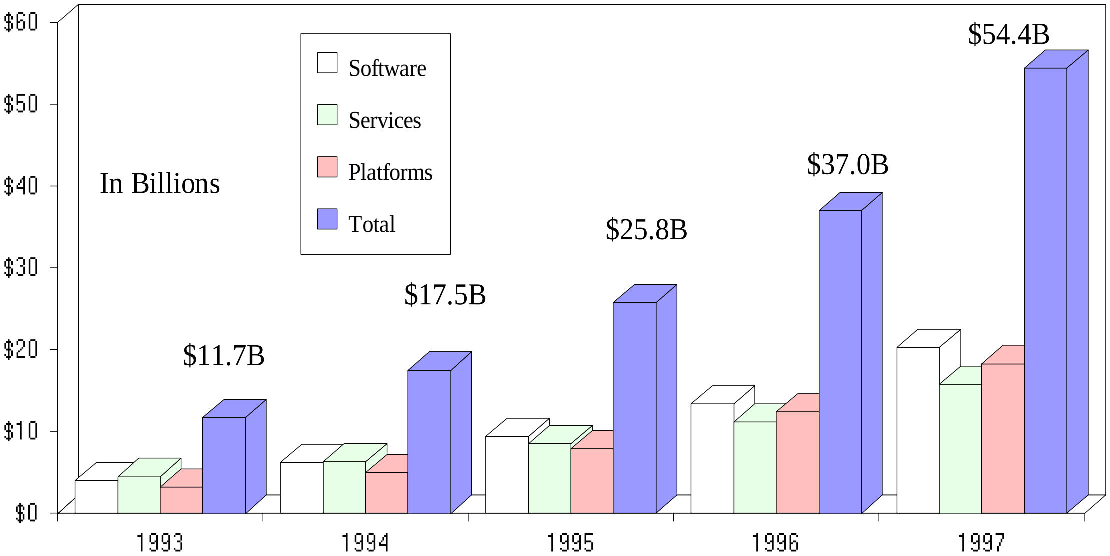
For those customers who want a complete security solution, as well as the means to ensure that the security solutions are being used, the inclusion of OmniGuard/EBM and OmniGuard/Autostor in the OmniGuard security solution will be an attractive offering. Since the major back-up software vendors do not have security software, positioning our storage management products as part of security will put those vendors on the defensive.

The Client/Server Security Market

The target customers for Axent's OmniGuard solution are large Fortune 1000 sites that have implemented, or are in the process of implementing, distributed client/server information systems. We are primarily interested in organizations that are deploying commercial, MIS applications. Engineering, scientific, or real time applications will be of secondary interest to us. Therefore, our market tracks closely with the overall client/server market.

The market for client/server software and services has been growing rapidly for the last several years. Sentry Market Research's 1993-94 survey[11] of the client/server market estimates that sales of client/server software, hardware platforms, and related services will grow from $12 billion in 1993 to $54 billion by 1998. The average site in the survey has more than $7.1 million budgeted in 1994 for client/server hardware, software, and services.

Projected Growth in the Client/Server Market



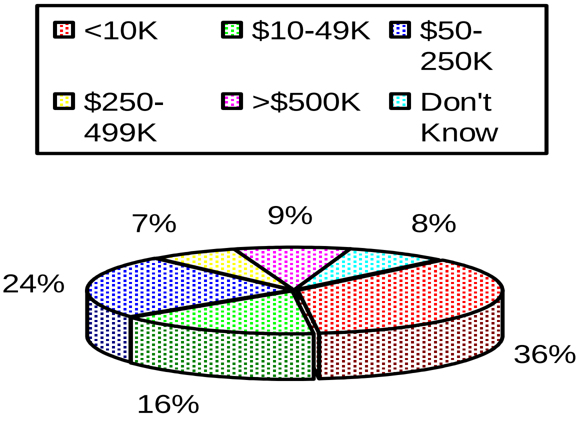
Source: Sentry Market Research 1993-94 Survey on Client Server Computing

As more and more client/server applications are deployed, the market for client/server systems and data security software is beginning to explode. The Sentry Market Research survey points out that the lack of systems and data security tools is one of the most serious inhibitors to implementing large-scale client/server systems. As more and more corporate data is stored on mid-range, UNIX, and PC-LAN servers, IS professionals are becoming increasingly concerned about the lack of available software products to help them manage, control and protect this data.

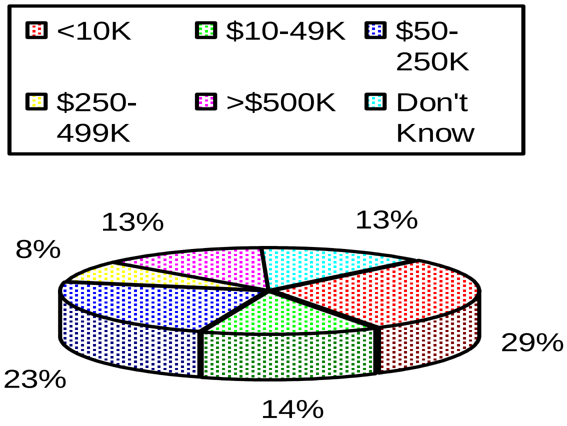
In response to this market need, software vendors are beginning to deliver an increasing number of client/server systems and data management tools. Even though most products today have limited capability, the average site in the Sentry Market Research has over $142K budgeted in 1994 for client/server systems and data management products. The overall market for systems administration and management software is estimated at $240 million in 1993. If spending patterns hold, systems management software expenditures could exceed $1 billion by 1998.[12]

In addition, Sentry Market Research found that while 38% of the sites surveyed had already implemented client/server backup/recovery software, an additional 58% are planning to implement this software in the next 24 months. Only 27% of the sites had implemented systems and data security software for client/server, but over 80% of the sites planned to do so in the next 24 months.

A survey of information security professionals in the March/April 1994 issue of *Infosecurity News* projects the annual budget for systems and data security products will increase significantly in 1994 over 1993 (see charts below).[13] Nearly 60% of the sites in this survey have in excess of $50K budgeted for client/server security software in 1994, up from 48% the year before. There are a growing number of sites that have in excess of $200K budgeted. The survey shows that nearly 21% of the sites have more than $250K budgeted for client/server security products in 1994, which is up from 16% in 1993.

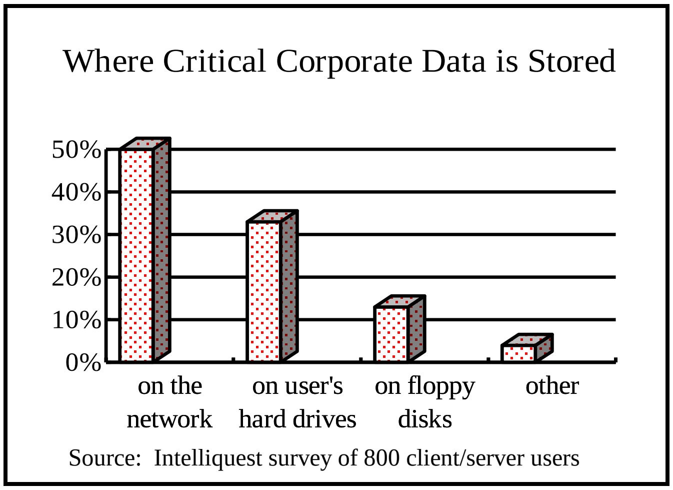


1993 security products & services budgets



1994 security products & services budgets

This is quite remarkable spending growth considering that a few years ago there was virtually no money budgeted for client/server security. Until recently, corporate security policy didn't even cover distributed computing environments and instead focused primarily on mainframe and mid-range systems. While 83% of large corporations have a security policy in place according to *Information Week*, *Infosecurity News'* survey reports that 79% of the sites they surved have recently extended their security policies to include client/server. Although they now have a policy in place, few of these sites have the means to implement these policies or track conformance with the policy. OmniGuard Enterprise Security Manager, Enterprise Access Control, Intruder Alert, and Single Sign-On will give organizations the means to manage and implement client/server security policies.


Where Critical Corporate Data is Stored

Source: Intelliquest survey of 800 client/server users

This explosive growth in the demand for client/server security solutions is also due to the increasing importance of data accessed by client/server systems. As more and more corporate data moves off of centralized mainframe processors, client/server protection and data availability becomes increasingly important. As the chart to the left shows, over 80% of critical corporate data used by client/server applications is stored either on the network or on the user's hard disks.[14]

Critical data stored on the network or on individual machines must be managed just as carefully as data stored in centralized mainframe environments. While the infrastructure for managing mainframe computing is quite mature, a corresponding infrastructure for client/server computing is just beginning to emerge.

According to a Peripheral Strategies study on enterprise data management, the market for storage management products in a client/server environment will grow from a 1993 level of $120 million to over $1.2 billion by 1998.[15] Storage management software includes network back-up and automated storage management (also called hierarchical storage management). Peripheral Strategies concludes that the largest class of data management software will be automated storage management products that span PC/LANs, UNIX networks and mid-range processors. They estimate that the market for cross platform storage management products will grow at a much faster rate than stand-alone LAN or UNIX backup products. This represents a huge opportunity for Axent's cross-platform data security products, OmniGuard/Enterprise Back-up Manager and OmniGuard/Autostor.

To size the overall market for security software, we consulted William Malik of the Gartner Group. Bill is an analyst specializing in computer systems security and is one of the recognized authorities on the security software market. He has produced many research notes on computer systems security and is often quoted by the trade press on computer systems security issues. Bill used his knowledge of the overall market and internal Gartner research to produce the following estimates:

	Type of System	Installed Base	ASP Security Software	Current Penetration	Maximum Penetration	Potential Market Value	Current Market Value	Opportunity	Growth Rate
IBM Systems									
	MVS	11,400	$100,000	95%	97%	$1,105,800,000	$1,083,000,000	$22,800,000	-8%
	VM	21,800	$12,000	10%	25%	$65,400,000	$26,160,000	$39,240,000	3%
	DOS-VSE	26,400	$9,500	5%	10%	$25,080,000	$12,540,000	$12,540,000	5%
	SNA networks	31,000	$2,500	5%	85%	$65,875,000	$3,875,000	$62,000,000	-5%
	AS/400	200,000	$1,500	0%	50%	$150,000,000	$0	$150,000,000	-13%
Total IBM Market						$1,412,155,000	$1,125,575,000	$286,580,000	
Digital Systems									
	DECnet	65,000	$750	15%	75%	$36,562,500	$7,312,500	$29,250,000	-7%
	VAX	500,000	$5,000	5%	50%	$1,250,000,000	$125,000,000	$1,125,000,000	-7%
Total Digital Market						$1,286,562,500	$132,312,500	$1,154,250,000	
Client/Server Systems									
	PC Server	3,200,000	$500	1%	75%	$1,200,000,000	$16,000,000	$1,184,000,000	3%
	UNIX Server	148,000	$500	1%	75%	$55,500,000	$740,000	$54,760,000	23%
	PC/UNIX Client	115,000,000	$100	0.75%	50%	$5,750,000,000	$86,250,000	$5,663,750,000	25%
	Portables	21,000,000	$75	0.10%	60%	$945,000,000	$1,575,000	$943,425,000	40%
Total Client/Server Market						$7,950,500,000	$104,565,000	$7,845,935,000	
Total combined market		140,203,600				$10,649,217,500	$1,362,452,500	$9,286,765,000	

According to the Gartner Group's figures, the market for security software for client/server computing dwarfs both the historical IBM and Digital markets. Security software has barely penetrated the client/server market and there is a nearly $8 billion in revenue opportunity to be had. The opportunity for client/server security tools is eight times greater then the IBM mainframe security software market and is growing between 25 and 40% a year. When you keep in mind that mainframe security software such as ACF 2 and TOP SECRET were the products that fueled much of Computer Associates' growth in the early '80s, there is unquestionably a huge potential in client/server security software.

The data cited above, in addition to our own customer experiences, clearly indicates that there is an emerging market for client/server security. There can be little doubt that this market will grow to be quite sizable. But the real question is whether or not the client/server security market is larger then other categories of systems management which Axent could exploit. After all, systems management is a broad discipline and other software vendors seem to be concentrating in other areas.

Sentry Market Research's 1994 Software Market Survey would seem to indicate that Axent's product strategy is on the right track. Sentry interviewed over 1,600 IS professionals involved in evaluation, recommending, and purchasing software for large corporations. A portion of the interviews concentrated on the anticipated growth in systems and network management software for 1994. Sentry evaluated several categories of systems and network management software for current penetration, expected penetration at the end of 1994, the percentage of sites that were planning to purchase the software , and the over all rate at which the penetration rate is expected to grow. The software categories were ranked by anticipated growth rate in 1994[16]. As the results listed in the following table show, five of the top six growth categories are addressed by the Axent product plan. Based on the data in this survey, Axent is focused on the fastest growing components of systems management, and is addressing customers' most critical needs.

Current and Planned Systems and Network Management Software

Platform	Product Catagory	Current Penetration	Expected Penetration YE 1994	Sites Planning	Penetration Growth
PC	LAN Security/Data Access Control	34%	77%	42%	123%
UNIX	Security	34%	74%	39%	115%
UNIX	Utilities/Disk Management (backup)	51%	91%	40%	78%
PC	LAN/Network O/S	71%	86%	55%	77%
PC	Utilities/Disk Management (backup)	70%	85%	45%	64%
PC	Security (data/virus)	69%	90%	41%	59%
UNIX	Operating Systems	100%	100%	48%	48%
AS/400	Capacity Planning	23%	31%	08%	37%
AS/400	Systems Utilities	53%	68%	15%	27%
Mainframe	Network Management	52%	66%	14%	27%
DEC VAX	Systems Management	56%	71%	14%	25%
Mainframe	Automated Operations	41%	52%	10%	25%
DEC VAX	Network Management	56%	69%	14%	24%
AS/400	Performance Tuning	47%	58%	11%	23%
Mainframe	DASD Management	62%	73%	11%	18%
Mainframe	Capacity Planning	31%	36%	05%	16%
Dec VAX	Security	44%	50%	06%	15%
Mainframe	Security	65%	73%	08%	12%
Mainframe	Performance Monitors	67%	74%	07%	10%

Based on all the data that we have reviewed and our own experiences with our current customers, Axent believes that there is a significant market for client/server systems and data security products. While this market is still emerging, the rapid growth in client/server computing ensures that those applications which manage, control and protect client/server systems and data will be in high demand for some time to come. We also believe that client/server systems and data security represent the best market niche in systems management for Axent to focus on.

Competition/Potential Partners

Befitting an emerging market, there are a large number of relatively small vendors offering products that would compete with the Axent product line. While most of these vendors offer UNIX products, there are a few emerging companies with PC-LAN (mostly Novell) applications. Most of the small ISVs client/server products are less than three years old, and many products have been on the market less than one year.

Only one established independent software vendor (ISV) is a contender in the client/server security market: Computer Associates (CA). CA is a logical competitor in client/server security since they market two of the three leading mainframe security packages: ACF 2 and TOP SECRET (the third product, RACF is sold by IBM). However, CA's entry into client/server security, Unicenter, has barely been on the market for one year.

The following matrix compares the product functionality and platform coverage of the larger players in the client/server security market. While there are many vendors offering competitive client/server security products, most can be characterized as niche players.

Functionality	Axent	OpenVision	Computer Associates	IBM	HP	Sun	Digital	Bull	ICL	BrainTree	Symark	Woodside Technologies	Bellcore	Los Altos	DynaSoft	DataLynx	OCS	Tivoli	Mergent	Fischer International	Datamedia	Engima Logic	Security Dynamics	Blue Lance	The Lan Support Group	Epoch	Legato	Cheyenne	Emerald	QStar	Netstor
Assessment/Conformance																															
Checks vulnerabilities	⬛	⬛					⬛			🟦		🟩	🟩		🟩										🟥						
Checks integrity/viruses	⬛	⬛								🟦		🟩	🟩															🟥			
Checks security changes	⬛	⬛								🟦																					
Ensures policy conformance	⬛	⬛					⬛			🟦			🟩																		
Administration																															
User profile management	⬛	🟩	⬛	⬛				🟩	🟩		🟦				🟩	🟩		🟩	🟪	🟪	🟪										
Profile templates	⬛		⬛					🟩	🟩	🟦	🟦				🟩	🟩			🟪	🟪	🟪										
Delegation to non-privileged	🟩		⬛																												
Access Controls																															
System access	🟩	🟩	⬛					🟩	🟩					🟩	🟩	🟩			🟪	🟪	🟪										
File access			⬛					🟩											🟪	🟪	🟪										
Database access	🟩	🟩																													
Network access	🟩	🟩					⬛								🟩		🟩														
Unattended workstations	⬛	🟦								🟦					🟩				🟪	🟪	🟪										
Monitoring/Intrusion Detection																															
Audit trail of access			⬛																🟪	🟪	🟪			🟥							
Audit security activity	🟩		⬛					🟩	🟩						🟩	🟩			🟪	🟪	🟪			🟥							
User session logs	🟦	🟦									🟦																				
Audit trail analysis	🟦									🟦														🟥							
Intrusion detection	🟦	🟦					⬛				🟦																				
Identification and Authentication																															
Password requirements	🟩	🟩	⬛					🟩	🟩					🟩	🟩	🟩			🟪	🟪	🟪										
Smart cards and biometrics									🟩						🟩						⬛	⬛	⬛								
Call-back	🟦													🟩																	
Network authentication		🟩		⬛	⬛	⬛	🟩	🟩	🟩								🟩				🟪										
Single sign-on				⬛					⬛										🟪	🟪	🟪										
Data Availability																															
Backup	🟩	🟩	⬛				🟦																			🟩	⬛	🟥	🟥	🟩	🟩
HSM	🟩	🟩																								🟩				🟩	
Library management			⬛				🟦																								

🟦 OpenVMS 🟩 UNIX 🟥 PC-LAN 🟪 PC ⬛ Mixed

Most of these companies only provide security products for a single platform or environment. Axent's strategy is to offer systems and data security across multiple platforms. In addition, our strength in managing security across PC, UNIX, mid-range and mainframe networks gives us a unique advantage.

Of the competitors mentioned above, only OpenVision, CA, DynaSoft, Mergent, and Fischer are major players in the client/server security market. OpenVison, Epoch, Legato, Cheyenne, and Emerald are major players in the data security/storage management market. The following table shows the relative sizes (based on Axent estimates or readily available industry data) of some of the key players in the client/server security market:

Relative size of client/server systems security ISVs (software only)

Company	Speciality	Platforms	1993	1994	1995
Axent	Cross platform security	UNIX, VMS, NetWare	$7.0	$10.0	$15.0
OpenVision	Cross platform security	UNIX, VMS	$5.0	$8.0	$11.0
BrainTree	Assessment	VMS	$3.0	$3.0	$3.0
Computer Associates	10% of CA-Unicenter	UNIX	$5.0	$8.0	$11.0
Woodside Technologies	Assessment	UNIX	$1.0	$1.0	$1.0
Dynasoft	Access Control, Admin	UNIX	$3.0	$4.0	$5.0
Mergent	Access Control, SSO	PC, PC-LAN	$5.0	$7.0	$9.0
Datamedia	Access Control, SSO, Smart Cards	PC, PC-LAN	$2.0	$4.0	$6.0
Fischer International	Access Control, SSO	PC, PC-LAN	$4.0	$6.0	$8.0
The LAN Support Group	Assessment	NetWare	$2.0	$3.0	$4.0
Tivoli	Admin (uses ISVs) 5% rev	UNIX	$1.0	$1.0	$1.0
Los Altos	Access Control, Call-back	UNIX	$1.0	$1.0	$1.0
DataLynx	Access Control, Admin	UNIX	$0.0	$0.0	$0.0
OCS	Authentication (Kerberos)	UNIX	$1.0	$2.0	$3.0
Bellcore	Assessment	UNIX	$1.0	$1.0	$1.0
Enigma Logic	Authentication, Smart Card	PC, UNIX, VMS	$2.0	$4.0	$6.0
Security Dynamics	Authentication, Smart Card	PC, UNIX, VMS	$3.0	$4.0	$5.0
Haystack	Audit trail analysis	UNIX	$1.0	$1.0	$1.0
Network-1	Anti-virus, monitoring	VMS	$1.0	$1.0	$1.0
CIS	Assessment, monitoring	VMS	$1.0	$1.0	$1.0
Symark	Monitoring, Admin	VMS	$1.0	$1.0	$1.0
Blue Lance	Monitoring	NetWare	$1.0	$1.0	$1.0
Total (in $millions)			$51.0	$72.0	$95.0
		Axent market share:	13.7%	13.9%	15.8%

Relative size of client/server storage management ISVs (software only)

Axent	Network back-up, HSM	UNIX	$1.0	$2.0	$3.5
OpenVision	Network back-up, HSM	UNIX	$3.5	$5.0	$6.5
Epoch	Network back-up, HSM	UNIX	$29.0	$32.0	$35.0
Legato	Network back-up	UNIX, PC-LAN	$12.0	$19.0	$26.0
Cheyenne	Netware server back-up	NetWare	$60.0	$80.0	$100.0
Emerald	Netware server back-up	NetWare	$4.0	$6.0	$8.0
Qstar	Network back-up, HSM	UNIX	$5.0	$6.0	$7.0
Total (in $millions)			$114.5	$150.0	$186.0
		Axent market share:	0.9%	1.3%	1.9%

Data in shaded areas is based on Raxco's Estimates

As the data indicates, Axent has a dominant position in the systems security market and can be considered one of the leading vendors of client/server security software. In addition to Axent's market share, Axent also enjoys strong market recognition and significant "mind-share" in the systems security world. While Axent is not a dominant player in the data security arena, the positioning of storage management as part of our security solution should enable us to gain market share relative to the other players.

Computer Associates

CA-Unicenter, CA's client/server systems management solution, will be one of Axent's primary competitors. However, because CA does not currently sell the security functionality unbundled from CA-Unicenter, we have not experienced much head-to-head competition to date. CA-Unicenter costs about

$8000 per system node (a node is an end-user's workstation, server or management workstation), while the OmniGuard products represent a fraction of this cost. Customers trying to solve a security problem balk at the high cost of CA-Unicenter. However, we expect CA to unbundle various components of Unicenter, including security, sometime in 1994. When this occurs we expect to see more head-to-head competition.

As a bundled product, CA-Unicenter competes more with HP's Operations Center and Tivoli. We are already partners with IBM, HP and Tivoli and plan to have our security products bundled with their system management frameworks. CA-Unicenter is a proprietary, closed architecture. This means that CA-Unicenter products are integrated through the CA-Unicenter framework, but other vendor products cannot easily be added. While the CA approach will appeal to some mainframe sites who are downsizing to UNIX networks, most customers are looking for a more open approach to solve their client/server systems management needs. Since it is unlikely that any one vendor (including CA) will be able to offer a complete solution to distributed systems management problems, best-of-breed products will dominate the market for the foreseeable future.

In the area of security, CA-Unicenter offers user administration, password management and some additional access controls. Although single sign-on was originally planned, it has not yet been delivered. .CA-Unicenter does not include security management and assessment, policy conformance, workstation locking, or intrusion detection. CA-Unicenter's additional access controls include the ability to restrict root access as well as enhanced file access controls such as date and time restrictions. Many of the enhanced access controls require significant changes to the UNIX operating system. This increases the level of difficulty in implementing CA-Unicenter or porting it to other platforms.

CA-Unicenter currently supports HP-UX. Other ports such as Solaris and AIX are nearing completion. Additional ports are planned for Windows NT, NetWare, OS/2, AS/400, MVS, and other flavors of UNIX. CA has not announced plans to port CA-Unicenter to the PC, although it does have the CA-Cortana product which offers password protection and file protection for DOS and Windows.

Axent rarely loses today to CA. Customers looking for client/server security software are unwilling to take the entire CA-Unicenter package in order to get a security solution. Even if we assume that at some point in the future they will unbundle their security offerings from CA-Unicenter, the OmniGuard product line still has superior depth and breadth of function. The current OmniGuard solution includes the basic functionality of CA-Unicenter's security, but does so without requiring significant operating system changes. In addition, we have security management, assessment/policy conformance, workstation locking, and intrusion detection functionality which CA lacks. OmniGuard/ESM provides complete cross-platform security management and ensures that systems and data security policies are implemented. CA has no equivalent functions. In addition, Axent believes it will beat CA to market with a secure single sign-on and additional platform support such as NetWare and Windows/NT.

OpenVision

Currently, OpenVision is our primary competitor in the security market. OpenVision was founded in 1993 as a startup funded with $35M in venture capital by Warburg Pincus. They later received an additional $10M from the same source. The capital was used to acquire 10-12 small companies with UNIX system management products. The remainder of the capital was burned in operational expenses. In March of 1994, OpenVision raised another $28M in a private placement through Alex Brown. FY '93 revenues were at $12M and revenues for the first half of FY '94 (July - December '93) were $8M with $1.3M of that coming from consulting.

One of OpenVision's principal acquisitions was Demax of San Mateo, California. Demax had been doing about $5.2M in security sales when they were acquired, which was down slightly from the year before. Only about $1M came from a single UNIX product, the balance from OpenVMS products. Demax has been our primary competitor with their SecureMax and SystemDetective products. OpenV*SecureMax, an assessment/policy conformance product, runs on OpenVMS, HP-UX, SunOS, Solaris, AIX, and Ultrix. OpenV*Detective, a monitoring/intrusion detection product only runs on OpenVMS.

OpenVision also acquired Geer-Zolot, an MIT Kerberos product and network security consulting company. Geer-Zolot's primary competition was the Open Computing Security Group (OCS). The product has been named OpenV*Secure and provides Kerberos network authentication services. OpenVision has recently added OpenV*GateKeeper, a UNIX access control and user administration product. They also acquired the DMS of Salt Lake City, which gave them DBR, a second tier UNIX backup product. DBR was probably doing about $3M in revenue, $2M of which was for DG AOS rather than UNIX. We understand that they have subsequently dropped the DMS products from their offerings.

Desktop Product Functionality	Axent OmniGuard/	OpenVision OpenV*
Assessment/Policy Compliance	ESM	SecureMax
Access Control/Administration	EAC	GateKeeper
Monitoring/Intrusion Detection	ITA	
Station Locking	EAC	
Authentication	SSO (planned)	Secure
Back-up	EBM	Backup
Storage Management	AST	HSM

OpenVision has announced that all its products will be integrated into its OpenV*OPSS framework, but they have significantly missed their delivery date (*Network World*, January 10, 1994; page 3). Recently, OpenVision has been less adamant about having its own proprietary framework and instead has emphasized a “best-in-breed” strategy.

Because of the Geer-Zolot acquisition, OpenVision has a small security consulting organization. They have two standard consulting packages OpenV*Tiger for $10,000, a simple network security vulnerability test, and OpenV*Network Security Threat Analysis for $75,000, a more in-depth network security assessment.

At this time OpenVision has no PC or PC/LAN security products, nor have they indicated any intent to add PC or PC/LAN products. Also, no plans have been announced to extend the OpenV*SecureMax product in order to provide a foundation for policy-driven, cross-platform security management for the network. This should give us at least a one-year window of opportunity with our OmniGuard/Enterprise Security Manager product.

Though we must not underestimate OpenVision, in most competitive situations to date we have been able to beat them. We recently closed a $200K security deal with Motorola, a $250K deal with SGS Thompson, and a $100K deal with Mobil Oil in head-to-head competition. At EDS, Demax/OpenVision was the incumbent vendor, and we managed to beat them on a $300K plus deal. OpenVision’s strength is a cosmetically appealing user interface, but it is far weaker than OmniGuard products in several key areas. Our Enterprise Security Manager handles more than twice the number of security checks as OpenV*SecureMax. We cover more platforms and, with the addition of Netware support, we will be able to manage UNIX, NetWare, and VMS from a single UNIX management workstation or Windows 3.x PC. OpenV*SecureMax is limited to VMS and UNIX. *Network Computing* magazine states in an October 1993 review that Axent’s OmniGuard/ESM provides more security checks and is more diligent than OpenVision’s product.[17]

Platform Vendors (IBM, HP, Digital, Sun, AT&T, etc.)

As can be seen in the competitive/partner matrix, the platform players are not focusing on add-on security. HP and Sun have a stated direction of focusing on core operating system functionality and basic C2-level systems security. IBM has add-on mainframe security in the RACF product and has NetSP for single sign-on between MVS, AIX, OS/2 and PC-DOS. IBM also bundles SMIT, a user administration tool, with its RS/6000 AIX systems. Digital has the PolyCenter Compliance Manager, Intrusion Detection and Security Reporting Facility for OpenVMS and UNIX. Digital has not done well with these products and, in fact, asked Axent to make an offer to purchase them in early 1993. Since that time its security market presence has declined rapidly.

Bull and ICL have the richest security offerings as shown in the matrix. ICL has a single-sign-on product based on an authentication server which uses scripting or DCE, if available. Bull’s product is just being released, but will suffer from lack of a focused channel. ICL’s product, AccessManager, has had no impact outside of the U.K.

Building cross-platform security products is at odds with a platform vendor’s primary mission, which is to sell more boxes. Of the large platform vendors, only Digital has attempted to address cross-platform security. IBM, on the other hand, has the RACF mainframe security product. The NetSP single sign-on product currently addresses mainframes with RACF, the RS/6000, OS/2 and PC-DOS--all platforms that IBM sells. IBM also bundles the SMIT user administration software with the RS/6000, but it does not address other UNIX platforms.

Platform vendors are likely to continue to focus on core technology and basic operating system security and frameworks (NetView/6000, HP OpenView, Sun NetManger). Rather than build the necessary additional security controls and management products, platform vendors are likely to continue to rely on third party partners to provide product. As a result, our strategy will be more along the lines of partnering than competing with the platform vendors. We have already had good results with HP and IBM with this strategy.

Tivoli

Tivoli is an emerging leader in the distributed systems management market. While the platform vendors have concentrated on network management, Tivoli has focused exclusively on systems management. As a result, Tivoli’s solution is far more robust and functional then the platform vendor’s frameworks (IBM Netview/6000, HP OpenView, etc.).

They have developed an integration framework called the Tivoli Management Environment (TME), which is designed exclusively for systems management applications. On top of this framework they have delivered several applications that primarily address what they call “configuration”. These applications include user administration, change management, software distribution, mail management, and print queue services. Applications that address what they call “automated operations” will be provided by third party strategic partners. Automated operations applications by their definition include workload management, problem tracking, performance monitoring, storage management and security. Tivoli’s strategy is to partner with a few key vendors who will enable their products to TME.

At the present time Tivoli has partnerships in place with Epoch for storage management, Autosys for workload management, and Remedy for problem tracking. Axent is their designated partner for security products. We are presently working with their CEO to solidify this relationship. Under the terms of this proposed partnership Axent would enable the OmniGuard solution to TME. Tivoli would then OEM OmniGuard as part of its overall systems management offerings. In the mean time Tivoli sales representatives have been referencing our products and have worked closely with Axent sales representatives.

Security is a critical area for Tivoli since their primary competitor is OpenVision. OpenVision claims to have a systems management framework that competes with Tivoli (The fact that they haven’t delivered it yet doesn’t stop OpenVision from talking about it). They also have several applications, such as event management, workload management and storage management, that compete directly with Tivoli applications. While Tivoli has the superior framework and some key applications, OpenVision has greater breadth of function. One key area that OpenVision has been pushing relative to Tivoli is security. Axent is the only viable security vendor capable of delivering a competitive product to OpenVision’s. Therefore Tivoli is highly incented to work with us.

For this reason we don’t regard Tivoli as a competitor at this time. However we must work to formalize our relationship and complete our integration efforts before other options become available to Tivoli. We are cautiously optimistic that we can conclude a deal to become Tivoli’s security solution in the near future.

Database Vendors

Database vendors such as Oracle, Informix, Sybase and Ingress all have built-in security capability in their databases. This security capability is akin to the security capability available from mainframe databases such as DB2. ANSI-standard Relational databases have three types of Structured Query Languages (SQL). Data Definition Language (DDL) defines tables and the relationships between tables. Data Manipulation Language (DML) defines how you access relational tables. Data Control Languages (DCL) defines who can access what.

The relational database vendors view security as a data access problem. They have multiple mechanisms, based on DCL, that allow database administrators to restrict access to certain tables, or even rows in a table, based on the user profile. However, there are many ways to circumvent DCL-based security. Often relational database applications ignore security concerns and sometime DCL isn't even enabled. Furthermore, relational database security only applies to the tables themselves, it doesn't prevent unauthorized access to the files that make up these tables or to the applications that access the tables.

Consequently Axent doesn't view relational database vendors as potential competitors, rather we see them as potential partners. The OmniGuard solution can be easily extended to manage database security in addition to system and file level security. This would give database administrators a way to ensure security controls are not circumvented or bypassed. Each of the major relational database vendors are on our list for potential strategic partnerships. We plan on approaching them as soon as we announce Axent.

Anti-viral Companies

The competitive matrix above does not include the following providers of anti-viral software in the PC and PC-LAN arena:

Alternative Computer Technologies Inc. - Sweep for NetWare
Central Point - Anti-virus, Anti-virus for NetWare, Anti-virus for Windows
Command Software Systems, Inc. - LANGUARD, F-PROT, NET-PROT, Security Guardian
Digital Dispatch - Data Physician Plus!
Datawatch, Tiangle Software Division - Virex
Diversified Computer Products and Services, Inc. - PC Doctor
Fifth Generation Systems - Disklock, SAFE, Untouchable
Fink Enterprises - Antivirus
Fora, Inc. - SafeGuard
G4 Software - Virotect Professional
Hilgraeve, Inc. - HyperACCESS, IBSMU, Intrity Plus
Intel - LANDesk Virus Protect
International Microcomputer Software, Inc. - VirusCure Plus
International Security Technology, Inc. - Virus Pro
JAS Technology of The Americas Ltd. - IDE Stealth
Leprechaun Software International, Ltd. - Network Security Organizer
McAfee - Clean-Up, NETShield, OS/2 Clean, OS/2 Scan, ViruScan, Vshield, Wscan
Ontrack Computer Systems, Inc. - Dr. Solomon's Anti-Virus Toolkit
Optimum Electronics, Inc. - PC PASSkey
Panda Systems - Panda Pro
PC Guardian Security Products - Data Security Plus
Qualtec Data Products, Inc. - Security Products
Reflex, Inc. - Disknet
RG Software Systems, Inc. - Vi-Spy
Safetynet, Inc. - StopLight, Stoplight/LAN
Silver Oak Systems - IronClad
Sophos - V-Sweep
Stiller Research - Integrity Master
Symantec Corp - Norton Desktop Network Menuing Admin Pack
System Security Technology - TNT Antivirus, Turbo CRC
Systemetrics - SENTRY Network Security Monitor

In the PC arena numerous companies provide anti-viral products. These products detect viruses and, in some cases, even remove viruses from infected software and diskettes. Some anti-viral products can only detect known viruses, while others use signatures of various kinds to detect viral changes to software. While most anti-viral software is designed for the PC, some products will run across a LAN.

The anti-viral market has been very lucrative ($100+M), but is crowded. Most PCs come bundled with anti-viral software. At volume discounts, the price per PC is under $10. Our plans are to make use of anti-viral software where appropriate (for example, Enterprise Security Manager includes anti-viral software and file integrity checks as part of its standard security management program), but Axent does not plan to offer stand-alone products.

We do not believe any of the anti-viral software vendors represent a credible player in the client/server security market.

Axent Marketing Channels

Axent will use a multi-channel approach to marketing and selling the OmniGuard product line. Multiple channels include dedicated direct sales people, telesales/telemarketing, value added resellers (VARs), original equipment manufacturers (OEMs.), distributors, and even catalogs. Since the OmniGuard products are technical solutions to complex issues, Axent channels will have to become versed in understanding and solving client/server security problems. OmniGuard will be a technical, solution-oriented sale which will require a technically-oriented, problem-solving sales force.

Direct sales personnel will be supported by well-trained and knowledgeable pre-sales representatives. Pre-sales will be augmented by consulting services when they are not being billed. This will leverage our investment in consulting services and give us a larger pool of qualified technical talent to assist in selling the products. Some of the pre-sales engagements may actually be billable, and consulting services will be employed in these situations.

Direct sales should employ consultative selling techniques by working to understand a customer’s requirements and recommend the best mix of products and services to solve their problems. Since the opportunity for OmniGuard products at a customer site can range from $20K to several hundred thousand dollars, it is expected that the direct sales organization will need to make on-site sales calls. In some situations Axent pre-sales support will be needed for on-site installation and set-up or to insure the success of a product trial. The telephone should be used to qualify opportunities and assess customer requirements. Telemarketing will be used to identify and qualify prospects which can then be passed on to the direct sales force for follow-up. Axent will also make use of customer briefings at Axent’s corporate headquarters to help close significant opportunities and expose existing and prospective customers to Axent’s strategy and direction.

Direct sales will be responsible for selling both products and services. Products will also be sold through value added resellers (VARs). In most situations, VARs will bundle an Axent product with a product or service of their own to create a more complete solution for the customer. VARs can augment the direct sales channel and should be seen as complementary to, not competitive, with the direct sales. It is also important to remember that VARs need a lot of help and support. They are not particularly good at marketing products, therefore Axent will need to provide much of the marketing and lead generation for them. They also need a great deal of technical support since they are likely to be involved in technically complex situations. A separate program to provide responsive technical support, outside of normal customer support, to the VARs must be established.

Since establishing direct operations in foreign countries is expensive, we will establish direct operations in the UK, and set up VARs and distributors in other countries. International distributors will follow a normal distributor model. That is, they will receive a distributor discount and they will in turn directly resell the products to the customer.

Perhaps our most lucrative channel will be OEMs. OEMs typically bundle Axent products with their own products and sell the combined solution. Examples of this type of channel include HP, IBM, Tivoli, Bull, AT&T, etc. HP’s Network and Systems Management Division (HP NSMD) is very interested in Axent becoming its security software supplier as part of the OpenView product line. The opportunity here is tremendous. If we can successfully conclude a deal with HP NSMD, HP would bundle most, if not all, of the OmniGuard products with OpenView (as part of the Operations Center component).

Direct Sales Channel: North America

In North America we will use a dedicated direct sales model with four districts: Northeast, Mid-States (including eastern Canada), Western (including western Canada), and Federal. The Western and Northeast districts will have 3-4 sales representatives with a $500-750K quota. The Western and Northeast districts will be managed by a working District Sales Manager (DSM). The Mid-States will have 4-5 sales representatives and the Federal district 3-4, all with a $500-750K quota. These districts will be managed by a single, full-time DSM. This gives Axent the equivalent of 14-18 commissioned sales reps in North America.

Direct sales will be supported by a separate technical pre-sales group (3-4) that will do demonstrations, walk-throughs, benchmarks, install trials (if necessary), and generally assist the sales representatives in closing business. Sales managers will be tasked with helping account representatives plan account strategy, forecast future business, and close deals (in addition to carrying a partial quota).

Sales representatives will each be assigned a $500-750K quota, and we anticipate that, on the average, the entire sales force will achieve at least 80% of quota.

Number of N.A. Reps	Quota	Total	Revenue @ 80% of Quota
18	$500,000	$9,000,000	$7,200,000

Alternative Channels

For a software company to be successful in the ‘90s it must take advantage of alternative sales channels. While our primary channel will be direct sales, we also intend to take advantage of VARs, systems integrators, and OEMs.

VARs by definition “add value” to the Axent products. Typically, this is done by offering products and services that complement Axent products. For instance, a VAR may sell a complete system to a customer including the computer, peripheral devices, and software. This VAR may bundle our software into this package, thereby giving the customer a complete solution. VARs allow us to sell products up-front, when the customer is actively involved in purchasing the computer systems rather than attempting to sell add-on products at a later date. VARs will enable Axent to broaden its channel while reducing overall cost of sales.

A common misconception is to think of VARs as distributors. VARs don’t actually sell the product as a distributor would, rather they sell a solution which includes the product. Since VARs typically have a large product portfolio, they cannot spend time marketing an individual product. They must rely on the vendor to create awareness for the product, and in many cases they depend on the vendor to actually generate the leads. Because they deal with so many different products, VARs cannot be experts in all of them. They must rely on the vendor for feature/function/benefit information, sales aids, and competitive analysis. Therefore, in order to have successful VAR relationships, Axent will have to put together a complete sales and marketing support program specifically for VARs.

This will involve a VAR relationship manager and several VAR support representatives. The relationship manager will set up and manage the business relationship with the VARs. He/she will be assigned quarterly targets for the VAR channel and will be goaled based on attainment of this target. He/she will make sure that the VARs are qualified to sell the product and that they have been adequately trained in both the sales and technical aspects of the product. The relationship manager will work with the corporate marketing group to put together marketing programs that attract and retain qualified VARs. In addition, he/she will also coordinate marketing programs that increase product awareness and generate leads for Axent VARs.

The VAR support representatives provide pre-sales technical and sales support for the VARs. This begins with product training and sales training, and involves help with marketing collateral, proposals, customer installations, competitive situations, configurations, and helping to resolve post sales problems. Each VAR support representative would be assigned a certain number of VARs, and it would be the representative’s priority to ensure that the VARs are successful with Axent products. VAR support representatives will receive incentive compensation based on successful retention of individual VARs as well as revenue attainment by their assigned VARs.

OEMs represent another large revenue opportunity. OEMs are large hardware or software vendors that would bundle our security solution with their products. Currently, we have four potential OEM opportunities: HP, Tivoli, NCR and IBM. Bull in France is already an OEM for two of Axent’s OmniGuard products.

We have worked directly with Robert Hoog, the General Manager of HP's Network and Systems Management Division (NSMD). Hoog is interested in having Axent supply the security component of Operations Center (the systems management component of their OpenView framework). If we are successful in concluding a relationship with NSMD, HP representatives will be able to sell Axent's security solution as part of OpenView and Operations Center. OpenView represents one of the more successful network and systems management frameworks and is available on HP and Sun platforms. Sales of OpenView are expected to grow dramatically over the next several years as customers look to integrate network and systems management applications. If we are successful in putting a deal together with HP we could expect revenue in the first twelve months from HP to be in the $500 to 1,000K range based on the current rate of OpenView sales.

We have a similar opportunity with Tivoli. The Tivoli Management Environment is an integration framework focused solely on systems management. They have integrated in several applications such as license management, software distribution, and user administration, but at this point in time they have no security products. Tivoli competes directly with OpenVision. Since OpenVision has a security solution and Tivoli does not, Tivoli is highly incented to work with us in order to beat OpenVision. Tivoli has experienced a great deal of success in recent months and has reportedly closed several $1+ million deals. Bundling our security solution with Tivoli's systems management solution would greatly increase our channel presence and give us immediate credibility. A successful relationship with Tivoli could net Axent another $500 to 1,000K in the first twelve months.

IBM has also expressed an interest in bundling our security solution as part of its network and systems management offering, NetView/6000. IBM has not licensed nearly as many products as HP and Tivoli. They, too, are feeling the pressure from their customers to offer a comprehensive security solution and view HP, Tivoli and OpenVision as competitors. While an OEM relationship with IBM will be more difficult than with HP or Tivoli, we believe one is possible.

We already have an OEM relationship with Bull in France. Bull markets our OmniGuard/Enterprise Backup Manager and is planning to include components of our systems security solution as part of their network and systems management framework, ISM. While Bull doesn't have a strong worldwide presence, they do have a loyal following in Europe, especially France.

Other OEM opportunities include vendors of such storage devices as Storage Tek or MTI, network operating systems vendors such as Novell, other hardware vendors such as Sun or AT&T Global Systems (NCR), or operating systems vendors such as Microsoft. We will be spending a considerable amount of effort to sign-up these vendors and close the current deals we have on the table. If we are successful in getting agreements with the large network and systems management vendors like HP, IBM, and Tivoli, we would be well on our way to establishing OmniGuard as the defacto systems and data security solution for the client/server market.

Other alternate channels we may employ include software distributors, catalogs, and systems integrators. Even though most of Axent's products involve a technical sell and are solution oriented, we expect client/server systems and data security to become more accepted and commonplace as time goes on. In this case, commodity style products can be easily sold through these types of indirect channels.

Tactical Marketing/Lead Generation

Marketing programs will be conceived and managed from the product marketing organization and implemented by corporate marketing. Product marketing will identify the target market, determine the best tools for reaching that market, establish the product positioning and the marketing message. Corporate marketing will provide product marketing with the necessary support to implement these programs.

We envision a mix of marketing programs which will be combined with an integrated marketing campaign. Integrated marketing means that all of our marketing tools -- corporate brochures, product brochures, product fact sheets, advertising, direct mail, sales seminars, and trade shows -- all complement and reinforce one other. For instance, the concept and image of our advertising will match and reinforce the messages contained in our direct mailings. Integrated marketing requires careful planning, as well as a clear sense of the audience we want to reach and the message we want to send them.

Advertising

Advertising in such general industry trade publications as *ComputerWorld*, *Open Systems Today*, *Software Magazine*, *Client/Server Computing*, *Information Week*, etc., will be aimed at building a corporate image for Axent. What we want to do with corporate advertising is to let prospective customers know what business we are in so that they will identify with us when they are ready to purchase. What we want to have happen is for customers to immediately think of us as the leading client/server security vendor when they hear the Axent name. We do not anticipate significant leads will be generated from corporate ads placed in this type of publication.

We will also run product specific ads in more targeted publications such as *Digital News and Review*, *Sys Admin*, *Infosecurity News*, *Network Computing*, etc. These publications have much smaller circulations and are focused toward a more technical audience of “recommenders” rather than decision-makers. We expect this type of advertising to generate some leads, but it will be designed primarily to increase product awareness.

Direct Mail

Our primary lead generation mechanism will be direct mail programs. We will use large (~20K) mailings to generate leads for the OmniGuard product line. However, we do not intend to rely on direct mail alone and we will follow up on the direct mailings with a telemarketing campaign. In other words, we will mail the information first, and then make phone calls to those on the mailing list. In our experience, direct mail response can be dramatically improved by using this method. Telemarketing will also accept all inbound calls and pre-qualify a prospect before the lead is sent to the sales organization for followed up.

Seminars

We will also use direct mail and telemarketing as a mechanism to populate Axent sponsored seminars. We will schedule a series of educational seminars on current topics related to client/server systems and data security. There is a tremendous amount of confusion in the marketplace and customers are looking for anyone who can help them understand the issues and learn about available solutions. We envision that these seminars will be run by the consulting services group and be educational in nature rather than sales oriented. Prospective customers are more likely to attend free educational seminars rather than those perceived to be simply a sales pitch. Of course, there will be an underlying marketing message and attendees will be able to learn how Axent addresses the problem of securing systems and data in a client/server environment. Attendees will become highly qualified prospects because they will be educated as to our vision. This will make them excellent candidates to be contacted by our direct sales organization after the seminars.

Trade Shows

Axent will attend a wide range of industry-related trade shows ranging from general client/server shows such as Uniforum, Client/Server World, DECUS, IS Expo, FED UNIX, CSI, and Distributed Computing World, to security specific trade shows such as NSWC, ISSA, NAVSEA, EDPAA/CACS, and OPSI. Trade shows will be staffed by product managers, pre-sales support, and consultants. We expect to give away premiums at these shows in return for filled-out questionnaires that can be used to qualify customers.

Lead Generation for the International Market

Since the international channel must deal with a variety of countries and languages, tactical marketing and lead generation for the international market will be run from Axent’s UK office. Product marketing will still determine the product positioning, target audience, and marketing message, but international marketing will use this information to develop appropriate programs for particular regional markets.

Targets for Lead Generation

Since an average Axent product transaction is expected to be between $15-50K, in order to generate $7 million in new business (see financial analysis section) we will need to generate the following number of qualified leads in the North American market:

$7,000,000/15,000 = 467 transactions
50,000 well qualified should lead to 500 transactions

Axent Organization Plan

Axent will be divided into three basic groups:

- North American Sales
- International Sales
- Product Operations

Raxco finance and administration will continue to supply financial accounting service to the Axent group, and the North American sales group will continue to report to the Senior VP of Sales and Marketing for Raxco. Axent International sales will also report to the Senior VP of International Operations.

The Product Operations organization will be divided into four groups with personnel focused on the following functions:

1. **Product Marketing:** Acts as the product champions and owns the Axent software product line from a marketing perspective. This group handles product management and pre-sales support activity.
    - Product Manager OmniGuard/Enterprise Security Manager product line. The person in this role is responsible for:
        - Working with development to ensure building the right product
        - Working with marketing communications to plan lead generation programs
        - Working with inside sales to ensure they have the right sales tools and programs
        - Working with alternate sales channels to ensure they have the right programs and support
        - Trade shows
    - Product Manager, OmniGuard/Enterprise Access Control, Enterprise Access Control, Intruder Alert, Station Lock, & Single Sign-On product lines. The person in this role is responsible for:
        - Working with development to ensure building the right product
        - Working with marketing communications to plan lead generation programs
        - Working with inside sales to ensure they have the right sales tools and programs
        - Working with alternate sales channels to ensure they have the right programs and support
        - Trade shows
    - Product Manager, OmniGuard/Enterprise Back-up Manager, Autostor, & Print Queue Manager. The person in this role is responsible for:
        - Working with development to ensure building the right product
        - Working with marketing communications to plan lead generation programs
        - Working with inside sales to ensure they have the right sales tools and programs
        - Working with alternate sales channels to ensure they have the right programs and support
        - Trade shows
    - Director of Technical Support (5 TSRs & 1 manager). The people in these roles are responsible for:
        - Technical pre-sales support for assigned products
        - Demonstrations of the assigned products
        - Trade shows
        - RFPs
        - Assisting with QA as needed
2. **VP of Engineering:** Responsible for the development of the Axent product line and the technical architecture of the products.
    - Director of Development, Reston Lab (9 programmers, 2 QA analysts/second level support, 1 manager). Primarily responsible for developing and maintaining the OmniGuard/Enterprise Backup Manager, Autostor, and Print Queue Manager product lines.

- Director of Development, Orem Lab (13 programmers, 3 QA analysts/second level support, 1 manager). Primarily responsible for developing and maintaining the OmniGuard/Enterprise Security Manager, Enterprise Access Control, Intruder Alert, Station Lock, & Single Sign-on.
- Manager of Technical Writing, (3 documentation writers, 1 manager all located in Orem)
- Manager of Corporate Systems (1 manager located at the headquarters). Responsible for acquisition, support, and maintenance of Axent hardware and software assets.

3. **Director of Customer Support**: Responsible for all level one post-sales support for Axent products. **(**6 support reps, 1 manager).

4. **Vice President of Consulting Services:** Responsible for Axent's consulting services business. This position has profit and loss responsibility for consulting products. This group will develop and deliver security and data management training and consulting in North America. (4 consultants & 1 VP all located at the headquarters).

The North American sales organization will employ personnel focused on the following functions:

1. **Director of Marketing:** Responsible for tactical marketing programs (lead generation) for the North American sales channel

   - Creative Services (1 person located at corporate headquarters) The person in this role is responsible for:
     - Creation and maintenance of product collateral
     - Internal & External newsletters
   - Marketing Events (1 person located at corporate headquarters). The person in this role is responsible for:
     - Scheduling and coordinating trade shows
     - Scheduling and coordinating sales seminars
   - Telemarketing (1 working manager, 2 telemarketing reps located at the corporate headquarters)
     - Lead generation
     - Lead qualification
     - Populate Seminars

2. **District Sales Manager, Northeast:** Responsible for product sales in the Northeast United States. (4 sales representatives, 1 manager located at the corporate headquarters).

3. **District Sales Manager, Mid-States:** Responsible for product sales in the mid-west, south east, and eastern Canada. (5 sales representatives, 1 manager located at the corporate headquarters).

4. **District Sales Manager, West:** Responsible for product sales in the western U.S. and western Canada (4 sales representatives, 1 working manager located in Orem).

5. **District Sales Manager, Federal:** Responsible for product sales to the U.S. Federal government and government contractors. (4 sales representatives, 1 manager located at the corporate headquarters).

6. **Director of Alternative Channels:**Responsible for product sales through VARs, OEM, and distributors (except international distributors)

The international sales organization will employee personnel focused on the following functions:

1. **Director of International Marketing:** Responsible for tatical marketing programs in support of the international direct sales organization.

2. **Director of Sales, U.K.:**

   - Direct sales representatives who are responsible for direct product sales in the U.K. territory

- Pre-sales support for the U.K. sales team.

3. **Director of Alternate Channels:** Responsible for establishing distributors in the rest of the world and setting up VARs where appropriate.

4. **Director of International customer support:** Provide support for all Axent products in Europe.

Axent Revenue Plan

Revenue in $ millions

	1993	1994	1995	1996	1997
Products	$8.00	$9.80	$13.00	$17.80	$25.00
Services	$0.25	$0.60	$1.00	$1.40	$2.20
Total Revenue	$8.25	$10.40	$14.00	$19.20	$27.20
Percent growth		26%	35%	37%	42%

Notes:

1) The services division will be in start-up mode in the second half of 1994.

2) Extended platform support into networks (beyond VMS & UNIX) occurs with produict releases in Q3 1994 into Q1 1995.

Axent Product Revenue (total billings) by Security Catagory
$ millions

Catagory	93 total product revenue	94 projected revenue	% Growth	95 projected revenue	% Growth	96 projected revenue	% Growth	97 projected revenue	% Growth
Enterprise-wide Security Managem	$3.90	$4.90	26%	$6.20	27%	$7.90	27%	$9.80	24%
User Administration & access contr	$1.70	$1.95	15%	$3.00	54%	$4.84	61%	$8.13	68%
Monitoring/Intrusion Detection	$1.16	$1.25	08%	$1.30	04%	$1.40	08%	$1.45	04%
Identification and Authentication	$0.00	$0.00		$0.20		$0.40	100%	$0.90	125%
Data Availability	$0.83	$1.35	63%	$2.20	63%	$3.20	45%	$4.70	47%
Other	$0.41	$0.35	-15%	$0.10	-71%	$0.06	-40%	$0.02	-67%
Consulting Services	$0.25	$0.60	140%	$1.00	67%	$1.40	40%	$2.20	57%
Total all Axent products	$8.25	$10.40	26%	$14.00	35%	$19.20	37%	$27.20	42%

Summary

The industry trend towards distributed computing has created a need for a systems and data management infrastructure equivalent to what has been available on the mainframe. But since most organizations tend to deploy less critical applications in client/server first, systems management requirements have evolved from basic needs to more sophisticated ones. The way in which organizations deploy client/server applications has resulted in the client/server security market developing from basic products like back-up and recovery to more advanced needs like automated storage management and systems security. Hence the market for storage management software is the most mature systems management discipline in the client/server arena.

As organizations move more and more of their critical systems to distributed platforms they will have increasingly complex systems and data security requirements. Axent believes that systems security will be the next major market to emerge from the client/server movement. We believe that its growth will parallel that of the storage management market (which has already begun to take off) and will eventually exceed the market size of mainframe security and data management products. There is a real potential to develop a $50-100 million business by 1998 with the right client/server security products and services. And because client/server is growing so fast, a market leader in the client/server will be able to grow along with the market.

Axent is well positioned to take advantage of the market's need for client/server systems and data security. Axent products are already well regarded in the security products market. With the new products scheduled to come on line later this year we will have the broadest product function across the largest number of platforms of any of our competitors. Our commitment to security consulting services will fuel our revenue growth while enabling us to ensure that customers are successful with our products. Increased customer success will lead to more product sales and more service revenue. Based on our revenue analysis, Axent is already as large, if not larger, then our nearest competitors in client/server security. If we successfully execute this marketing plan, Axent stands a strong chance of becoming the predominant player in the emerging client/server security market.

[1]End Notes

[1] Horwitt, Elisabeth. “DCE Integration: Anemic, but Available.” *ComputerWorld*, December 6, 1993: 12

[2] Cassidy, Peter, “Lines of Defense.” *CIO Magazine*, February 15, 1994: 47

[3] *ComputerWorld Client/Server Journal*, August 11, 1993

[4] Panettieri, Joseph C., “Tempting Fate.” *Information Week*, October 4, 1993: 44.

[5] National Research Council, *Computers at Risk* Washington, D.C: National Academy Press, 1991.

[6] *Open Systems Today*, Aug. 16, 1993, 38

[7] *LAN Times*, Feb. 28, 1994: 91

[8] Ibid.

[9] Panettieri Joseph C., “Tempting Fate.” *Information Week*, October 4, 1993: 52

[10] Ibid.

[11] Sentry Market Research. 1993-94 *Client/Server Market Report.*

[12] Ibid.

[13] *Infosecurity News* “Annual Infosecurity Industry Survey.” *Infosecurity News*, March/April 1994: 23

[14] Intelliquest Annual survey of client/server users, January, 1994

[15] Peripheral Strategies, Inc. February, 1994 report on Enterprise Data Management

[16] Sentry Market Research. March, 1994. 1994 Software Market Survey, 7-6