

End Point Security

White Paper: Protecting Access
to Corporate Information



- The purpose of this paper is to discuss the security issues associated with end points used for remote access.
- This paper looks at client side security tools that provide pre-login assurance, intra-session protection from spyware, as well as post-logout cleanup.

Introduction

Today's enterprises have evolved into open network environments where corporate data are accessed from third-party owned devices by a combination of employees, business partners, contractors, and customers. Many applications and services, such as email, virtual private networking (VPN), customer relationship management (CRM), enterprise resource planning (ERP), financial applications, and human resource applications, have transitioned from client-server to Web-enabled architectures. The security implications of this fundamental shift have changed the way employees, business partners, customers, and suppliers access and utilize corporate information. In this environment, enterprises have little or no control over the security of the end point accessing the Web application and the data that are transmitted to them. The results are high levels of exposure of corporate data and the associated risks to the enterprise.

SSL VPN

Business Driver

SSL VPNs have emerged as a popular alternative to the traditional client-server IPsec VPNs because they reduce the cost of remote access, eliminate the need to pre-install client software, and enable access from anywhere with a Web browser. These are easier to use and are ubiquitous.

Security Threats

SSL VPNs are often used to provide access to multiple services and applications, such as file sharing, client-server services, and Web applications. The same reasons that are making it popular also create some issues, since the end user access now could be from any system, anywhere in the world. It is possible to limit access from an SSL VPN similar to how IPsec is limited, but the benefits of SSL VPN are not taken advantage of. To get the best of both worlds, where the enterprise is assured that the remote computer at the end of the tunnel poses no risk, even when it is being used from a CyberCafe or somebody's virus infected home computer, a smart approach is required to limit the exposure caused by the following situations:

1. Unauthorized access to enterprise resources gained with a stolen SSL VPN account and
2. Confidential / proprietary data stolen when it is left behind on an end point used to access the internal network.

The same risk exists with IPsec VPN, but access is usually limited to systems where the clients are installed by IT, so there is a perception that they pose less risk. But, IPsec does not provide any enforcement of policies on the remote machine. Therefore, even IT issued machines tend to fall out of compliance fairly quickly.

Increasing Exposure: WebMail

Business Driver

Webmail enables employees to access their email, calendar, and contact information from any location, on any computer, and at any time of day. This application enables tremendous productivity improvement by enabling employees to work after hours from their homes or while traveling on business. Webmail often reduces an enterprise's need to purchase laptops for employees who want to work from home occasionally. With Webmail's integration into leading client-server email systems, such as Outlook and Lotus iNotes, the adoption of Webmail has emerged as a corporate standard in recent years.

Security Threat

Many enterprises have come to rely on email as their primary means of communication. As a result, extremely confidential information in the form of email text and attachments are commonly sent through the email system. While this practice is still a security risk in the client server world, it is an even more dangerous activity in the Webmail world. When a typical user accesses an email with a confidential attachment from a third-party owned computer, the user is asked to choose either to "open" or "save" the document. In both cases, the file is saved to the local hard drive and then opened by a local application. If this document is a business plan, customer information, or revenue projections, its confidentiality and integrity could be compromised by malicious code on the local system; or more commonly, the document could be simply left in the local system's temporary folder, on its desktop, or in its "My Documents" folder where the next person using the computer could view it. A simple search for "*.doc" or "*.xls" on a hotel business center, Kinko's, or other public-use computer amply demonstrates how confidential documents are commonly left behind for anyone to steal. This type of search can be either very amusing or scary, depending whether you are the thief or the victim.

Web-Based Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP)

Business Drivers

Like many other enterprise applications, CRM and ERP have evolved to be Web-based. As a result, sales and operations personnel have raised their productivity levels. Sales people can now access up-to-date customer information and place orders from anywhere in the world, and the operations team can now coordinate projects and resources from multiple locations.

Security Threats

While Web-based CRM and ERP have many benefits, they also put sensitive information at risk. Customer information, sales forecasts, and project timelines are information assets that organizations cannot afford to expose to their competitors and the public. Failure to protect this information in some industries can result in regulatory violations. Within many CRM applications, a sales person could save a sales forecast to an Excel file on any computer. The minute that Excel file is downloaded, the enterprise loses control over it.

Increasing Exposure: User Examples

With the variety of connection methods (SSL VPN, Webmail, Portal), users, and devices that access corporate information, crafting a one-size-fits-all set of policies is difficult, if not impossible. Attempts to create a single policy for all typically result in either opening security holes or reducing the productivity of users. Adapting security policies to the specific needs of different connection methods, users, and devices is critical to a successful security program.

Employee Access to Corporate Information

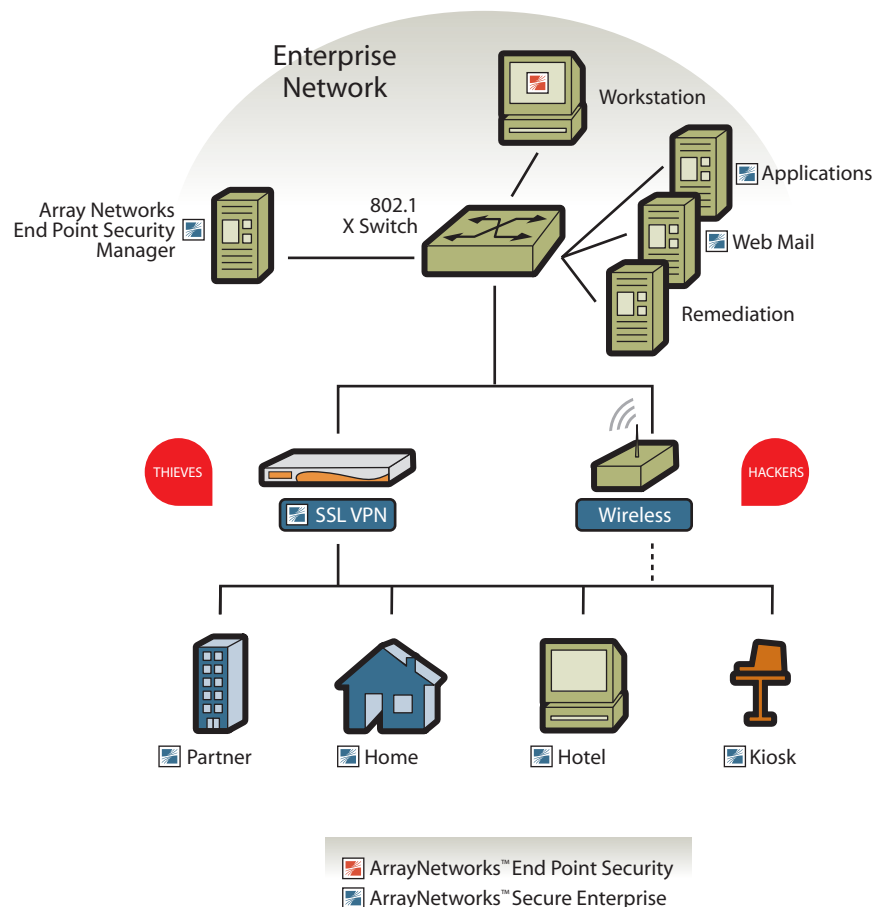
Different types of employees have different corporate data usage profiles based upon their work patterns and job descriptions. For example, Tele-workers access corporate information from home a majority of the time, while Traveling Workers access them primarily on the road; and Day Extenders and Campus Workers are at their desks most often when accessing corporate information. In addition, company employees use a variety of corporate-owned and third-party owned devices, such as laptops, workstations, kiosks, hotel business centers, customer, and partner computers, to access the information.

Third-Party Access to Corporate Information

Third-parties, such as consultants, contractors, outsourcers, company agents, and other partners, often require some type of access to proprietary corporate information. Typically, the corporation has little or no control over the endpoints used to connect to this corporate information. Despite this lack of control, these users are often given broad levels access to corporate resources either by connecting on campus or by using an IPsec or SSL VPN.

Array Solution

Array delivers the first integrated End Point Security solution for both corporate-owned and third-party owned devices that protects corporate networks by preventing intrusions, enforcing security policies, and safeguarding confidential data. Array End Point Security enables enterprises to secure access methods, such as SSL VPN, Webmail, extranets, and intranets, by ensuring the integrity of endpoints connecting to those portals and protecting the data that are transmitted to the endpoints.



How Array's End Point Security Works

Using the Array End-point Security Manager, an administrator creates a Web page for downloading the Array End-point Security Agent (AESA). This AESA download Web page is then configured to be the default page of a Web Application, such as mail.company.com, and placed on the Application's Web server. When a user connects to this Web page, typically via an SSL VPN, Web mail server, or Portal Web server, AESA is downloaded and launched on the endpoint. Once launched, AESA verifies the integrity of the endpoint, including antivirus software, personal firewall, service pack, and patch/hotfix policies.

After completing the host integrity verification process, AESA creates a Secure Desktop environment on the remote computer. From within that virtual environment, AESA launches the login process to the Web application through a Web browser in the Secure Desktop and enables the user to access corporate resources, such as e-mail or corporate servers. When the session to the enterprise is complete or times out after an administrator-defined interval, AESA can either automatically erase all proprietary data created or downloaded to the Secure Desktop during the session or preserve the environment in an encrypted and password-protected archive that remains on the computer.

Array End Point Security Modules

Adaptive Policies

The Array End-point Security Agent has the ability to adapt security policies by specific network locations and types of network devices (corporate owned vs. third-party owned) to ensure that all confidential data are protected without affecting user productivity. Adaptive Policies ensure that users accessing the portal have the appropriate level of security according to the type of device they are using to connect and the location from which they are connecting. Array End Point Security also enables administrators to designate trusted locations and devices from which users may access Web Applications without virtual security agent modules, such as secured network locations or a company-owned system with complete security software. For example, computers running the full Array Security Agent, located inside the corporate network or with the corporate image could be considered trusted and put immediately into a Web application login page.

Cache Cleaner

Array's Cache Cleaner ensures that Web browser information, such as cookies, history, autocomplete, stored passwords, and temporary files, is erased or disabled upon termination of a session, inactivity timeout, or closing of the browser. On Windows NT, 2000, 2003, and XP systems, Cache Cleaner can either work in conjunction with Array Secure Desktop or as a standalone module to clean browser cache. On other operating systems, such as Macintosh OS X, Linux, and Windows (98, ME), where Secure Desktop is not an option, Cache Cleaner can operate as a standalone module to protect browser information.

Secure Desktop

AESA creates and launches a Secure Desktop environment that enables users to download confidential data into an encrypted environment. They can be opened by local applications, modified, and uploaded back to the Web application, saved to a floppy disk, placed on a USB hard drive, or stored on some other removable media. The Secure Desktop environment enables employees, business partners, and customers to access confidential information securely from third-party owned devices.

AESA can either operate as a persistent desktop, or it can be automatically uninstalled after sanitizing all proprietary data after each session. When the Secure Desktop environment is configured to be persistent, it prompts the user to create a password prior to the entering the Secure Desktop for the first time. Then, each subsequent time the user wants to enter the Secure Desktop, that password must be entered. The persistent desktop eliminates the need for the user to download and re-install AESA each time the user connects to the enterprise portal, and it enables access to data stored in the encrypted environment regardless of whether a Web application session is active. Policies governing Secure Desktop persistence can be applied by location, making it possible to enable employee home computers to have a persistent desktop while uninstalling the AESA after the termination of any session originating from a kiosk.

The Secure Desktop can be closed by either the user manually closing the Secure Desktop or automatically by AESA after an administrator defined period of time. If configured for a single session (i.e. non-persistent), closing the Secure Desktop will sanitize all proprietary data downloaded or created in the Secure Desktop during the session. The Secure Desktop sanitizes data by deleting it and overwriting it multiple times, according to the United States Department of Defense standard for sanitizing data, to ensure that the data cannot be recovered from the device hard drive.

If configured to be persistent, the Secure Desktop will give the user the option to choose whether or not it will sanitize the data. Upon closing the Secure Desktop and after data sanitization, the Secure Desktop can either require that it be uninstalled, or recommend that it be uninstalled.

Host Integrity Checker

Host Integrity verifies that the devices providing access to Web applications are secured by anti-virus software, updated virus definitions, a personal firewall, critical service packs, patches, and other important security layers. This verification ensures that the corporate network will not be compromised by infected endpoints accessing protected corporate resources from unmanaged devices. Host Integrity policies are created with “and/or” logical functions that enable administrators to create sophisticated checks, such as each End Point must be verified to have:

Anti-Virus Rule:

((Norton running + Virus Definitions <=14 days old), (Mcafee running + Virus Definitions <=7 days old), or (PCcillin Virus Definitions <=10 days old))

AND

Personal Firewall Rule: (Array Personal Firewall, ZoneAlarm Pro, or Windows Internet Connection Firewall must be running)

AND

Service Pack Rule:

Windows 2000: Must have at least Service Pack 3 installed

OR

Windows XP; Must have at least Service Pack 1 installed

If any of the required Host Integrity checks fails, instead of launching the Web application login page, AESA will display a failure page and notify the user why access was denied and which security check (e.g.. not running Array Personal Firewall) was not met. Administrators may also customize this page to include additional information about why the end user is required to meet the stated security requirements and links to a remediation server.

Array' End Point Security in Practice

The Array End Point Security architecture is designed to work with any remote access situation. Using the Array management UI, an End Point Security Configuration Manager is installed on the administrator machine and is used to configure the security policies. Once configured, they are read by Array in to its memory and applied to new access. All of the necessary information needed to launch the client security modules is now enabled on the SSL VPN. Once this is completed, users accessing through the SSL VPN will receive the Array End Point Security Agent as a pre-authentication step to the normal login process.

Array Key Differentiators

Array End Point Security uniquely addresses the four critical requirements for safe access to the corporate network from third-party owned devices.

On-Demand Deployment in any Environment

The key to securing access from third-party owned devices is the ability to deliver the security solution to every end point that needs to access protected Web applications. Array End Point Security can be delivered with guest rights, when ActiveX is disabled, and even if the endpoint's browser security is set at high. No other solution today offers the ability to install on-demand security on locked-down systems, such as kiosks, partner computers, and at hotel business center computers.

Verifying the Security of Endpoints

To protect the corporate network and information from exploits that can use remote access methods to bypass hardened perimeter defenses, the Host Integrity of every end point seeking access must be checked for the presence and status of antivirus software, personal firewalls, service packs, and patches prior to allowing access. Without the ability to check for Host Integrity, compromised endpoints could be mistakenly used to access corporate resources, thereby infecting those resources. Array provides the ability to accurately determine the security level of a system, including ensuring that an antivirus product is running with up-to date virus definitions, a personal firewall is active, service pack levels are met, and critical patches are installed.

Preventing Information Leakage

Every day, corporate information such as business plans, financial projections, and customer information is accessed from third-party owned computers and left unencrypted on those devices for anyone to view and exploit. Array On-Demand provides comprehensive protection for corporate information, sanitizing data at the end of Web sessions, preventing information leakage, and protecting data privacy.

Adapting Protection to the End Point Environment

Endpoints present varying levels of risk to corporate networks and information, depending on the type of device (corporate-owned vs. third-party owned), the network environment (Office LAN vs. Internet Café), and the security protections in place on the end point (Host Integrity). Applying a uniform policy or security technology to every end point typically leads to either diminished productivity or an inadequately protected endpoint. For example, if a corporate owned desktop, running all mandated protection, were to connect from the office network and access a Web application, security policy need not apply the same protections to that application as it does when the accessed is sought from an airport kiosk. Array End Point Security automatically determines and applies the appropriate policies and security technologies necessary for a given end point environment always based on the enterprise's security policies. Array's ability to deploy On-Demand protection in any environment, verify the security of endpoints, prevent information leakage, and adapt its level of protection to the environment makes Array End Point Security uniquely capable of protecting the enterprises data and networks from the vulnerable end point when using Web applications.

Conclusion

The ways in which employees, customers, and partners access corporate information have shifted from client-server to Web-based applications. The results have included increased productivity, decreased costs, and tremendous exposure of corporate information and networks to external threats, such as malicious code, information leakage, and network attacks. These threats manifest every day in the form of passwords being stolen; business plans being left on hotel business center computers, and networks being attacked by malicious code. Array's End-point Security Agent can check the security of every system accessing a Web application, encrypt and protect the data inside the Secure Desktop environment, and then remove all confidential proprietary data at the termination of a Web application's session. The Array End Point Security solution provides a highly effective, low cost, and seamless approach to solving the End Point security problem for Web applications.

About Array Networks

Founded in 2000, Array Networks is a leading provider of high-performance, secure universal access solutions. Array delivers product lines that address the rapidly growing SSL VPN market as well as the application acceleration market. More than 500 customers including enterprises, service providers, government and vertical organizations in healthcare, finance and education rely on Array to provide anytime, anywhere secure and optimized access. Array provides the world's fastest and most scalable SSL VPN products on the market today. Array's technology performs 8 times faster and scales 12 times higher than its nearest competitor. As a result, no other company can deliver high-performance SSL VPN solutions at a comparable cost. Array has been recognized by industry leaders including Deloitte, Red Herring, and Synergy as a market and technology leader.

Array is headquartered in Milpitas, California with sales offices around the world. The company has approximately 60 resellers and VARs worldwide.

For more information, please visit www.arraynetworks.net or call **1-866-MY-ARRAY**.