Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Regaining Control over your Mobile Users

No matter how much time or money some corporations spend on securing their network, once they allow mobile (laptop) users to connect to their internal network they are exposing that network to a wide variety of security risks. Their once-secure network has now potentially become a hacker's playground. This problem arises because mobile users will connect their corporate laptops to an un-trusted network while away from the office. When they return, they frequently do not have their mobile systems scanned before re-conne...

Copyright SANS Institute
Author Retains Full Rights

AD
Take control of vulnerability threats Now!
Request a Free Trial
Secunia
Stay Secure

Regaining Control over your Mobile Users

Shelly R Biller

GIAC Security Essentials Certification (GSEC)
Version 1.4c
Option 1
20 February 2005

© SANS Institute 2005 Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Table of Contents

Abstract	**Page 3**
Introduction	**Page 3**
Software Standardization	**Page 5**
Security Policies	**Page 8**
Security Awareness Training	**Page 11**
Commercial Products	**Page 15**
Summary	**Page 17**
List of References	**Page 18**

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Abstract
Security conscious corporations have taken a defense in depth approach to securing their network perimeter. This includes but is not limited to implementing firewalls, intrusion detection systems, properly configured routers, virtual private networks, and network policies to include anti-virus, patch management, and configuration management. No matter how much time or money some corporations spend on securing their network, once they allow mobile (laptop) users to connect to their internal network; they are exposing that network to a wide variety of security risks. Their once-secure network has now potentially become a hacker's playground. This problem arises because mobile users will connect their corporate laptops to an un-trusted network (i.e., hotel, home, dial-up or wireless) while away from the office. When they return, they frequently do not have their mobile systems scanned before re-connecting to the corporate network to ensure they still meet the current security posture of the corporation. Unless administrators are able to manage these mobile users' access to the corporate network, the networks risk to malware is greatly increased. In this paper, I will discuss the industry's recommendation for a secure environment for mobile users. Some areas of concern that I will cover will include software standardization, security policies, and security awareness training. I will briefly discuss two vendor's products that can help administrators gain control of their mobile systems and reduce the risk of malware on their network.

Introduction
With all of the advanced technology that is available today, network security is becoming more and more complicated for system administrators. Just when we thought that our network was secure, another exploit or malware is released into the Internet community, and the cycle of defense begins all over again. Network security has no definitive boundary. We must constantly review the security of our network at every access point. One point of access that many organizations have failed to secure is their mobile users, specifically laptop users.

In our organization approximately one-quarter of our users gain access to network resources on a daily basis using laptops. Each mobile user has local administrative privileges on their laptops. Each user has some form of Internet Service Provider (ISP) software loaded to gain access to network resources. Finally, these users have several avenues to access the internal, corporate network such as:

- Direct dial-in to our network via a Remote Authentication Dial-In User Service (RADIUS) Server
- Connection via a foreign local area network (LAN) that will assign them an Internet Protocol (IP) address (e.g. hotels and other government agencies)
- Dial-into their ISP and access via that Internet connection (web mail).

When looking at the overall security of our network and the vulnerabilities created by our mobile users; I conclude that the main security risk in our organization is our mobile users.

© SANS Institute 2005 Author retains full rights.

Mobile users take their laptops on the road and expect to work in much the same way they would if they were in the office. Once they leave the physical perimeter of the corporate network, they are no longer protected by firewalls, intrusion detection systems, patch management and virus definition updates. Upon returning to the office, there is no official policy regarding reconnection to the internal network. The effect is that the laptops are never scanned to see if they still meet the current corporate security posture before physically re-connecting to the network. With a lack of security controls in place for these laptops, they are at risk of attack by hackers and, even worse, may become the conduit for introducing malicious code into the corporate environment. [1]

This paper introduces a baseline (software standardization, security policies, and security awareness training) system administrators may implement to regain control of their mobile users. I will briefly discuss two commercial products that address how to secure the mobile users. This paper does not serve as an endorsement of any of the products mentioned, as there are many similar, competing products that would perform the same function. The products mentioned are merely representative of their respective technologies.

[1] Foster, Brian. "The Security of Remote Workers." Industry Views. July 2004. http://www.computeruser.com/articles/daily/8,10,2,0719,04.html (February 20, 2005).

© SANS Institute 2005 Author retains full rights.

Software Standardization

The risk of network infections introduced by nonstandard applications, mis-configuration of standard applications or failure to update the latest versions in mobile computing cannot be understated. With the explosion of mobile devices, how do you avoid leaving large holes in an IT network that intruders can exploit?[2]

Establishing and maintaining a software standard for mobile users can become a complicated task for administrators. There are several factors you must consider when migrating your users to one standard. I will discuss a few key elements that you may want to consider in the development of an effective standard. There may be more factors that you will want to consider depending on your users and your corporate mission, but this will give you a good starting point.

There are many approaches in developing and implementing a software standard for your organization's mobile users. So where should you begin? Before you begin to develop a software standard, you need to know what current software is running on your mobile users systems. Next, you will need to determine the skill set of your users and administrators. Finally, you will need to determine your organizations current and future software needs.

Conducting a software audit will help determine what operating systems, applications and versions your mobile users are currently utilizing. There are several products on the market today like PCProfile, Centennial Software, and LANauditor that will provide you with this type of inventory quickly and automatically. When selecting audit software you should be aware that there are companies out there that will not only provide you with the tools to inventory your current software, but also identify any changes in the software. Your software management tool will assist you in maintaining your software standard throughout your mobile workforce.

Once the audit is completed, you will need to assess the skill set of your users and administrators. This information becomes important when you are ready to rollout your software standard. Because the audit is based on the skill set of your users and administrators, you will be able to determine the amount of training they will require to use the new software. Knowing the current skill set of your users and administrators will ease the deployment of the new standard. If the need for training is considerably increased due to the new standard, you may want to consider implementing the standard in phases to ensure its success.

The next step is to assess your organizations current and future software needs. You may find that building a standards working group will assist you in this process. This working group can be made up from a number of representatives from each department. You may want to look at having a representative from

[2] Boston, Brad. "Trends for 2004: Managing and Securing your mobile workforce." December 19, 2003. http://www.computerworld.com/mobiletopics/mobile/story/0,10801,88098,00.html?source=NLT_&nid=88098 (February 20, 2005).

© SANS Institute 2005 Author retains full rights.

each department that has sufficient knowledge of their systems and their mobile users' needs. You may also want to include the budget personnel that are responsible for supporting such changes in the network. The working group will be able to look at the new technologies that are being released and determine their need for those technologies based on the budget and operational need of their department. The working group will be able to come to a consensus as to what direction they will take to update the standards.

Below is an example of the Department of Energy's Desktop Software Guidance Profile that was developed by a workgroup. They were able to identify the software packages and versions most widely used throughout the department. This chart can be used as a starting point for your organization to determine where your mobile systems are now in terms of software and where you would like your mobile systems to be in the future. With the use of this model or similar models you will be able to target all your mobile users' needs and maintain a manageable standard.

Department of Energy Desktop Software Guidance Profile

***As of February 28, 2001*

Status: / Software:	RETIREMENT	CONTAINMENT	CURRENT PRODUCTS	**TARGET by 2002-03	*Suite*
Presentation	Lotus	Corel Presentations 6 Harvard Graphics PowerPoint 97	**PowerPoint 97*** PowerPoint 97/98 PowerPoint 2000 Corel Presentations 8	**PowerPoint 2000*** Corel Graphics 2000	**Office 2000*** **Hardware Requirements
Spreadsheet	Lotus Excel 4,3	Excel 5.0 Lotus 123	**Excel 97*** Excel 98 Lotus	**Excel 2000***	
Word Processing		WordPerfect 6.1	**Word 97*** Word 98 Word 2000 WordPerfect 8	**Word 2000*** WordPerfect 9	
Email	ccMail	Groupwise ccMail	Outlook 97/98 Notes Eudora Groupwise	Outlook 2000 Notes R5 Eudora x	
Browser	Internet Explorer 3.2	Internet Explorer 4 x	Netscape Internet Explorer 5.x	Netscape Internet Explorer 5.5	
Operating System	Macs & Win 3.1 DOS	Windows 95 NT 3.1 Win 98	Windows 98 NT 4 Win 95 Mac 8.6, 9	**Windows 2000*** Mac OS X Linux	

**Changes from February 28, 2001 Videoconference.

The products in bold text with an asterisk (*) indicate the DOE Desktop Software Guidance Group's consensus on de facto Departmental desktop software standards.

Category Definitions	
Retirement	Obsolete or unsupportable software. Actively expend funds to get rid of it.
Containment	Do not purchase or promote use. Allow to be phased out.
Current Products	The current baseline of software organizations have in place and are supporting.
Target	Consensus direction the Department needs to take to establish desktop software standardization.

[3]

Software standardization may not be right for every corporation. There are many benefits as well as barriers to standardization. IDC's John Gantz and Vernon

[3] Blackston, Carol. "Department of Energy Desktop Software Guidance Profile." ITReform. February 2001.
http://cio.doe.gov/ITReform/desktop_workgroup/mtg_aug2-4_2000/desktop_guidance_profile_final.htm (February 20, 2005).

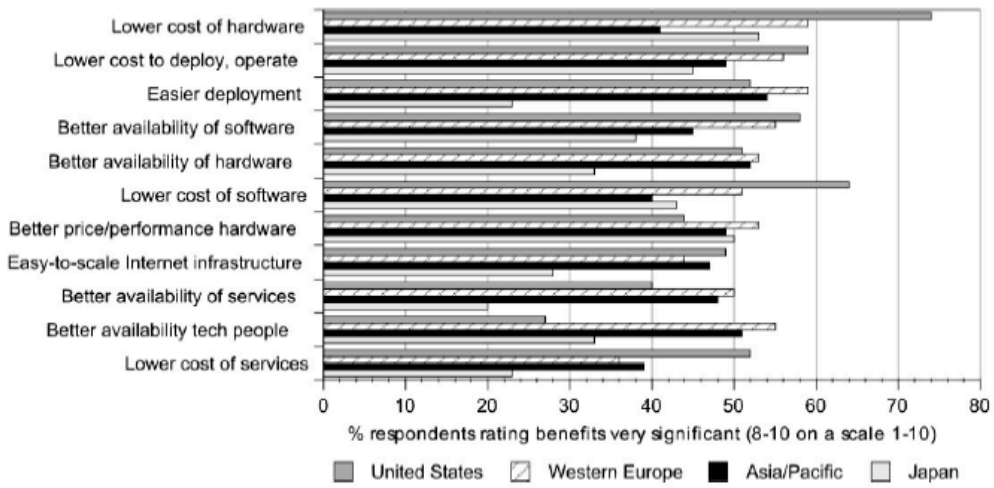
© SANS Institute 2005 Author retains full rights.

Turner conducted a research study on standardization in technology. From the 340 organizations that responded to the survey, the benefits outweighed the barriers 3 to 2. The most significant benefits were:

- Lower software costs
- Easier deployment
- Lower costs and services

The overall benefits of using standardized products are shown below:

Figure 2: Benefits of Using Standardized Products



Source: IDC, 2002 [4]

Although many benefits were found there were a few barriers noted. The leading barriers reported were:

- Perception that there would be performance and power issues
- Incompatibility with existing non-standard products

Overall, based on the feedback from the respondents, IDC determined the momentum is in favor of Industry standardization.

[4] Gantz, John and Vernon Turner. "Standardization, The Secret to IT Leverage." IDC. March 2002. http://www.dell.com/downloads/global/solutions/idc_standard.pdf (February 20, 2005).

© SANS Institute 2005 Author retains full rights.

Security Policies
The primary purpose of a security policy is to inform users, staff and managers of those essential requirements for protecting various assets including people, hardware, software resources, and data assets.[5] A security policy should be treated as a living document. A policy that is never updated is not worth implementing. Developing an effective security policy will take a lot of time and thought. Some key questions you may want to ask yourself when creating or reviewing your security policy are:

Is your security policy:
- Clear and simple
- Realistic
- Consistent
- Enforceable
- Communicated
- Reviewed and updated regularly

Clear and simple
Creating policies that contain a lot of technical jargon, leaves them open to interpretation by the users. If the policy has room for interpretation it becomes difficult to enforce that policy down the road. You will need to ensure the policy is straightforward and easily understood by all users. One way to make sure your policies are clear and simple is to get the users input. Have users at all levels review the policy and provide feedback. The feedback you receive will tell you if your policy is being understood or interpreted.

Realistic
Are the policies you are implementing realistic? Creating policies that are too restrictive hinder the productivity of your users and impede on business practices. A realistic policy will need to incorporate a perfect balance between your business, technological and security needs.

Consistent
Maintaining consistency in your policy will ensure user compliance. Once a policy is implemented you need to ensure there are no exceptions to the policy. Permitting users to deviate from the policy will cause discord among the users community, in turn nullifying your policy. An inconsistent policy is an unenforceable policy.

Enforceable
Ensuring that everyone adheres to your restrictions will require more than just a written rule set. It also needs strong management capabilities to ensure compliance with the rules. [6] Involving users and multiple levels of management

[5] Weise, Joel and Charles R. Martin "Developing a Security Policy." Sun Blue Prints Online. December 2001. http://www.sun.com/blueprints/1201/secpolicy.pdf (February 20, 2005).
[6] Parkhouse, Jayne. "Policy Management." SC Magazine. March 2003. (2003): 62.

© SANS Institute 2005 Author retains full rights.

in the development of policies will ensure buy-in when enforcing these policies. Users need to understand that it does not matter if they are a regular user or in a position of authority (management), they will be held to the policy and the consequences for violating such policies. Once the policies are in place you must continuously monitor the systems to ensure that the controls remain in place and are effective. Make it known that you are monitoring for policy violations and the consequences for non-compliance. If a violation occurs you must ensure the set consequence is carried out.

Communicated

Once security policies have been developed and before they are implemented; they will need to be disseminated. It is important that all users, staff, management, contractors, outside customers, and any other entity that may require access to your network receive a copy of the security policies. In addition to disseminating the policies, it is best to have a formal record stating they have read, understood, and agreed to adhere to the policies. It is advantageous to ensure everyone reviews the policies at a minimum of twice a year; at that time have them sign a new record stating they have reviewed the policies. Below is an example of what happened to a New York financial services firm that failed to effectively communicate their security policy.

> The consequences can be dire. Remnitz says a case in point is a New York financial services firm that had a security policy for encrypting code, but did not communicate that policy to the troops in the trenches. Unaware of the policy, an in-house software developer building a financial app for electronic commerce failed to encrypt code to protect credit card numbers. The result: Thousands of credit card numbers were stolen. [7]

Well-written security policies are useless if you are not able to communicate them to the users. Training users on the current security policies is the most important part of this process. Users not only need to understand the policies and the consequences for non-compliance, they need to know why they exist in the first place. Many times users have read the policy but do not realize the true harm that can come from not complying with the policy. There are a variety of ways to train your organization such as: annual mandatory security training, weekly bulletins emailed to users, involvement on security policy teams, and external security agency briefings just to name a few. Policies can be implemented in your security awareness training, which will be covered in the latter part of this paper.

[7] Yasin, Rutrell. "Management Strategies: Security Blanket." Internet Week. August 17, 1998. http://www.internetweek.com/trends/trends081798.htm (February 20, 2005).

© SANS Institute 2005 Author retains full rights.

Reviewed and updated regularly

Policies should be treated as living documents that must be reviewed on a regular basis and updated as necessary. Depending on how frequently your organization changes; will determine how often you will need to review and update your policies. If policies are neglected, the effectiveness of the policy will diminish. Best practice is to review your security policies at least twice a year and update as needed.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Security Awareness Training

Along with policies must come the training that will ensure the policies are adhered to once users return to their normal working environment. PentaSafe's 2002 Security Awareness Index revealed a serious failure on the part of most companies to adequately educate and train their employees in proper security awareness and workplace habits. [8] To ensure that security awareness becomes second nature to your users it must be part of their daily routine. With the amount of time mobile users spend connecting to foreign networks; it is imperative they understand the impact they may have on the network upon reconnecting.

Operating outside the internal network, users become more susceptible to theft, hackers, malware, and viruses, it is imperative they receive adequate training to protect themselves as well as the corporate network. Topics of discussion may include physical security, social engineering, passwords, Internet surfing, spam emails, antivirus and windows updates. There are several approaches your corporation may take to increase the user's awareness in security. The more popular methods are: emailing weekly newsletters, bulletins, alerts, monthly training sessions, and security awareness weeks. You may find it necessary to use more than one method when training your users. Developing an award system has proven to be successful for some organizations. Those users that have excelled in the corporations awareness program were awarded for their performance. Awards ranged from free lunches, gift cards, designated parking spot, time-off awards, and bonuses. Re-enforcing positive behaviors through the use of awards will not only display your commitment to the security program, but it will motivate users to succeed in your program.

Developing an effective security awareness program takes time and dedication. Three key elements I have found that increase the overall effectiveness of your security awareness program are:

- Begin with the basics
- Make training realistic and interesting
- Training should be hands-on and interactive

Begin with the Basics

Hardware and software familiarization is one key to security awareness training. Many times you will find that mobile users know just enough about their system to perform their day-to-day operations. What they don't always know is why their laptop performs abnormal processes. For example, why their laptop reboots automatically, constantly receiving pop-ups, or why their home page has changed. Educating users on the basics of system security will prove to be beneficial in the long run. Although it is impossible to fully prepare every user on what they may encounter once outside the network, you can make sure they are aware of the basic threats and how to prevent them. Users may have heard of

[8] "PentaSafe Security Awareness Index Report." NetIQ February 18, 2002. http://www.netiq.com/news/releases/release.asp?cid=20021213144711QDNH (February 20, 2005).

© SANS Institute 2005 Author retains full rights.

the terms viruses, Trojans, spam, and spyware, but they do not fully understand the impact they can have on a system or network. Educating users on the most prevalent forms of malware and the proper reporting procedures will reduce the number of compromises on your network. By creating this level of awareness with your users, they will begin to develop skills that will assist administrators in detecting anomalies on their systems and reporting such anomalies immediately.

Realistic and Interesting

Security awareness is not one of the easiest topics to teach. If you expect your users to gain useful information from your security awareness program you need to make it realistic and interesting. Most security training that is provided within organizations is too complex or boring. One rationale for inadequate training is that the security staffs are highly trained in their fields, but are not able to effectively communicate that experience to the users. If you're current staff cannot provide this level of training required, it may be to your advantage to outsource your security awareness needs to an outside security professional organization. These organizations are staffed with security professionals that can not only effectively communicate your policies, but they make the training interesting and fun for the users. Some of the training techniques that are used by such organizations are hands-on training, web-based training and seminar or small group discussions. Security professionals will assist you in determining the most effective training approach based on the needs of your users and organization. Several of the security professionals will expose your users to real security breaches. They will not only walk them through a case based scenario of how the attack occurred, but how it could have been prevented through properly practiced procedures. Presenting real cases of security breaches increases the user's awareness and demonstrates how easy it is to penetrate a network. It will also show the users the extent of the damage that could result from such a penetration. For the users to get the most out of the training you may find that the initial security awareness training should be hands-on and interactive.

Hands-on and Interactive

"Death by Power Point." We have all had this kind of training at some point in our careers, but how many of us actually took that training and were able to effectively apply that knowledge to our current jobs? Many times users attend the mandatory training but are not able to apply the training when returning to their normal work environment. Providing hands on training can help drive network security home to all users and make them think twice before they hand out their passwords, leave their mobile systems unsecured or unattended, or sending proprietary information over an unsecured network.

Hands-on

Using hands-on techniques have proven to be effective in many corporations. Providing hands-on training affords the users the opportunity to actually walk through scenario-based training and how to properly respond.

© SANS Institute 2005 Author retains full rights.

There are a number of training exercises you could provide to the users to help them understand how important network security has become. Below is an example of a possible training scenario. First, start up a network monitor and begin monitoring the traffic from the users in the lab environment. Next, have the users perform some of their normal surfing activities as they would at their workstation. Have them check personal email accounts, bank accounts, retirement accounts and any other Internet surfing they may do during a normal workday. At this point have each user run a spyware program like Adaware or Spybot. Adaware and Spybot are signature-based programs that detect spyware that was loaded on their systems during their time on the Internet. Demonstrate in the limited amount of time they were on the Internet how many instances of spyware were loaded to their system and the type of information that can be gained through the use of spyware. Finally, show them the results from the network monitor that was running during this exercise. Present all the information you were able to capture just by monitoring the traffic. For instance, the types of information they were disclosing (i.e. account numbers, user names or passwords) that they thought were personal. This will enable them to see how much information can be gathered by innocent internet surfing, emails, or even instant messaging, and how that information is out there for anyone to readily own or compromise. "Seeing is believing." If you can make your users see how easy it is to gain personal and corporate information they will take the extra time and precautions to protect such information in the future.

Interactive

You may find that conducting mock exercises can be quite an effective training method when developing interactive training. I will use the example of social engineering to explain how this technique can be deployed in your organization. Social engineering is a commonly used technique used by hackers to gain personal information about a user or company. This information can be used at a later date to gain access to personal or corporate accounts or data. One of the hardest concepts about social engineering is getting users to realize when they are actually being socially engineered. Generally speaking most users want to be helpful, even when it comes to revealing proprietary information about themselves or their company.

During a mock exercise you will have a security professional come into the organization acting as part of the company. The main reason for using an outside company for the exercise is that they have no prior knowledge of the corporation. The data that they gather will strictly come from users and possibly from gaining physical access to areas within your organization. You will be able to prove that every little bit of information in your organization can be part of a bigger puzzle and if enough information is gathered the corporate data is no longer secure. The first part of the exercise should be unannounced to avoid persuading user's actions. If the users are unaware of the exercise, it will prepare them for real world situations and how easy it is for a hacker to gain

© SANS Institute 2005 Author retains full rights.

information. Given a specified amount of time and through the use of phone calls, emails and casual conversations determine how much and the type of proprietary information the security professional was able to gain. Once the exercise is complete, the next step is to compile the information that was gained through social engineering and/or physical access, and determine the usefulness of the data that was revealed. The final phase of the exercise is presenting the data gathered to the users in a security training session. The purpose of the exercise is not to embarrass or single users out, but to make them realize no matter how official a person or email message sounds it can lead to a potential compromise in the network. It is important for users to understand that security is everyone's responsibility. Users need to realize that any information pertaining to themselves and the corporation has some meaning to someone, even if the user cannot see the importance of the data at the time. The smallest amount of information such as a phone number, user name, or any other information can be enough for a hacker to put the rest of the puzzle together and compromise the network.

There are many training techniques to help develop interactive training. For instance, mock exercise, role-play, and distance learning to name a few. You may need to examine a few techniques to determine which one will work best for your organization. Through the use of these hands-on and interactive training techniques you may begin to see a change in attitude toward mandatory security awareness training.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Commercial Products

Scan and Block technology is considered to be on the cutting edge of technology. Currently, many enterprises are looking to deploy some form of a "scan & block" technology to regain control over their mobile users. Although there are many companies offering similar types of technology each of them have their own unique advantages and disadvantages. The concept of scan and block technology is based on a set of predefined access policies. These policies can be set to test for operating systems and versions, updated patches and hot fixes, latest anti-virus updates, and applications. Once the predefined access policies are in place then each system or device that accesses the network are scanned against these policies. If a system or device is found to be non-compliant with the policies they will either be forced to update their system prior to access to the network or their system will be routed to a quarantined part of the network. Whether the systems or devices are located internally or externally to the network they are consistently being scanned for host integrity.

Two software solutions that provide this type of support are Sygate and StillSecures' - Safe Access. I will briefly explain each of these software products and their unique features.

Sygate's Solution for Mobile Users

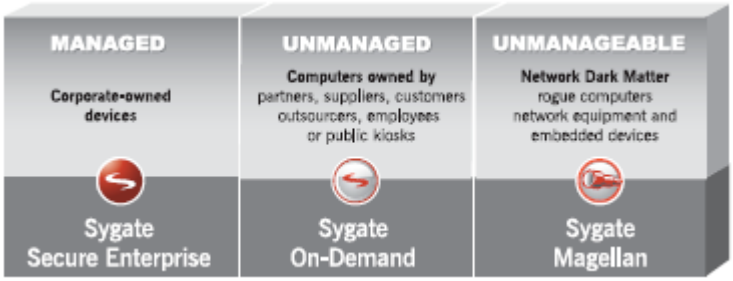
Sygate takes securing the mobile user to a whole new level. Sygate provides an automated process of detecting and eliminating rogue and compromised devices, applications and behaviors from their networks. Sygate has implemented a continuous compliance process consisting of four elements.

Within the discovery process it ensures that devices using the corporate network do not elude the protection process. The protection process blocks hackers and thieves from compromising endpoints. The enforcement process that ensures policies and protections are enforced on all devices, prior to allowing those devices to connect to the corporate network. Finally, the remediation process restores compromised devices to a protected and compliant state sufficient to maintain productivity. [9]

[9] "Sygate Products." 2004. http://www.sygate.com/products/index.htm (February 20, 2005).

© SANS Institute 2005 Author retains full rights.

The Sygate solution is comprised of managed, unmanaged and unmanageable devices. Sygate offers three powerful products to manage systems of these types. Each of the products mentioned below can run independently or together as a package. Running all three products in conjunction with one another is the most efficient and effective approach to cover all possible avenues of access to your network.



Sygate Secure Enterprise
Within this product a security agent runs on each endpoint, one or more policy management server is distributed across the enterprise, and one or more enforcement mechanisms. Enforcement mechanisms include enforcement servers on the local area network, remote network access points such as Wireless, VPN, and RAS concentrators. Enforcement utilities are also built into each endpoint. Remediation is provided through built-in software distribution and execution capabilities for delivery of patches, software updates, or self-running clean-up programs. [10]

Sygate On-Demand
This program provides continuous protection to endpoints the corporation doesn't own (unmanaged), yet allows on its network, such as employees or partners connecting from their own systems, airport kiosks, or hotel business center computers. Sygate On-Demand integrates with Web applications to ensure the compliance of endpoints and to protect the data that are transmitted to them through an On-Demand Agent that downloads to each endpoint at the time of connection.[11]

Sygate Magellan
Eliminates Network Dark Matter™, or unmanageable endpoints to ensure that all devices on the network are known and under security management. Multiple discovery and correlation engines run as network appliances. They identify devices and assets; they probe configurations

[10] "Sygate Secure Enterprise." Sygate. 2004. http://www.sygate.com/products/sygate-secure-enterprise.htm (February 20, 2005).
[11] "Sygate On-Demand." Sygate. 2004. http://www.sygate.com/products/sygate-on-demand.htm (February 20, 2005).

© SANS Institute 2005 Author retains full rights.

and services; they document de facto compliance with security policies; they enable administrators to bring newly discovered devices into compliance with Sygate Secure Enterprise or Sygate On-Demand. [12]

Implementing Sygate Secure Enterprise, Sygate On-Demand and Sygate Magellan proves to be the most effective way to protect your network from all types of systems and devices. There are many features and advantages to Sygate's solution that I have not covered in this paper. If you would like to find out more information on this product you can visit them at http://www.sygate.com/.

StillSecure Safe Access

Safe Access utilizes a five-step process that includes Define, Connect, Test, Enforce and Report. Within the definition stage is where the administrators define the access policies. In addition to the regular policies you would normally scan for you can scan for banned items such as file-sharing, peer-to-peer(P2P), instant messaging, or spyware. They provide an unlimited number of custom tests that can be created and integrated into Safe Access through an open application programming interface (API). As devices access the network, they are quickly tested for compliance with the designated policy. Test results trigger the appropriate enforcement; if the device meets policy requirements it is allowed entry to the network. Devices that fail can be denied access or quarantined to a specific part of the network. Safe Access ensures compliance while the device is on the network by continually checking for system changes that violate corporate policy. Real-time and historical reporting is provided to administrators, managers, executives and auditors. [13]

Summary

Regaining control of your mobile users will require time, persistence and money. I have presented some of the industry's suggested standards for securing your mobile workforce. This paper provides you with a good starting point to begin developing a secure environment not only for your internal users, but also for your mobile users. With the proper balance of software standardization, security policies and security awareness training, you will find the overall security of your network is more secure from hackers and malicious malware.

This paper provided you with two commercial products that will assist you in maintaining your secure network once you have established the software standard, security policies and security awareness training for your organization.

---

[12] "Sygate Magellan." Sygate. 2004. http://www.sygate.com/products/sygate-magellan.htm (February 20, 2005).

[13] "StillSecure enforces endpoint security compliance with industry's first agent-les solution." 2002. http://www.stillsecure.com/news_events/040504b.pnp (February 20, 2005).

© SANS Institute 2005 Author retains full rights.

List of References

Blackston, Carol. "Department of Energy Desktop Software Guidance Profile." ITReform. February 2001. http://cio.doe.gov/ITReform/desktop_workgroup/mtg_aug2-4_2000/desktop_guidance_profile_final.htm (February 20, 2005).

Boston, Brad. "Trends for 2004: Managing and Securing your mobile workforce." December 19, 2003. http://www.computerworld.com/mobiletopics/mobile/story/0,10801,88098,00.html?source=NLT_&nid=88098 (February 20, 2005).

Foster, Brian. "The Security of Remote Workers." Industry Views. July 2004. http://www.computeruser.com/articles/daily/8,10,2,0719,04.html (February 20, 2005).

Gantz, John and Turner, Vernon. "Standardization, The Secret to IT Leverage." IDC. March 2002. http://www.dell.com/downloads/global/solutions/idc_standard.pdf (February 20, 2005).

Parkhouse, Jayne. "Policy Management." SC Magazine. March 2003. (2003): 62.

"PentaSafe Security Awareness Index Report." NetIQ February 18, 2002. http://www.netiq.com/news/releases/release.asp?cid=20021213144711QDNH (February 20, 2005).

"StillSecure enforces endpoint security compliance with industry's first agent-les solution." 2002. http://www.stillsecure.com/news_events/040504b.pnp (February 20, 2005).

"Sygate On-Demand." Sygate. 2004. http://www.sygate.com/products/sygate-on-demand.htm (February 20, 2005).

"Sygate Magellan." Sygate. 2004. http://www.sygate.com/products/sygate-magellan.htm (February 20, 2005).

"Sygate Products." 2004. http://www.sygate.com/products/index.htm (February 20, 2005).

"Sygate Secure Enterprise." Sygate. 2004. http://www.sygate.com/products/sygate-secure-enterprise.htm (February 20, 2005).

Weise, Joel and Martin, Charles R. "Developing a Security Policy." Sun Blue Prints Online. December 2001. http://www.sun.com/blueprints/1201/secpolicy.pdf (February 20, 2005).

© SANS Institute 2005 Author retains full rights.

Yasin, Rutrell. "Management Strategies: Security Blanket." Internet Week. August 17, 1998. http://www.internetweek.com/trends/trends081798.htm (February 20, 2005).

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced