

Attempts to Automate Client Security at Virginia Commonwealth University

Doug Stinnette
Virginia Commonwealth University
Sanger Hall B1-001
1101 East Marshall Street
804-828-9843
drstinne@vcu.edu

ABSTRACT

To enhance protection against Internet threats, Virginia Commonwealth University planned to implement Symantec Client Security for all faculty, staff and students. This product integrates antivirus, personal firewall and intrusion detection and allows centralized management of policy configurations, deployment and installation settings for multiple antivirus and security technologies. Presently implementation has been placed on hold while we attempt to address some implementation problems. This poster session will exhibit the problems we have encountered in our efforts to deploy this product as a managed client.

Categories and Subject Descriptors

K.6.5 [Security and Protection]: Invasive software – viruses, worms, Trojan horses. Unauthorized access – hacking.

General Terms

Security, Standardization, Management, Reliability.

Keywords

Antivirus software, Personal Firewall

1. INTRODUCTION

Virginia Commonwealth University has been using Symantec Antivirus Corporate Edition, which provides a centrally managed environment, for over a year. Due to the proliferation of worms and other malware that are not handled by antivirus software, it was decided that the university's network users needed another level of protection. The Symantec Client Security product appeared to be a good solution in that it provides integrated antivirus, personal firewall and intrusion detection. The package also allows a high level of customization for various firewall settings and client groupings. The plan was to manage these components through the same centrally managed system that the Symantec Antivirus Corporate Edition uses. The following

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SIGUCCS'04, October 10–13, 2004, Baltimore, Maryland, USA.
Copyright 2004 ACM 1-58113-869-5/04/0010...\$5.00.

sections explain what we encountered when we attempted to configure and test this product as a managed client.

2. PRODUCT CONFIGURATION TESTING

We tested the product with different configurations and researched problems and documented the solutions. We decided that one simple configuration was the best strategy since we planned on providing it to a large diverse group of users.

3. TEST PHASE

During our testing, it was discovered that Symantec Client Security does not allow upgrades to the various integrated components through the Symantec System Center. The only updates that we successfully pushed to client machines were antivirus signature file updates, which is the same capability offered by the Symantec Antivirus Corporate Edition managed client. In order to automate the distribution of signature file updates and security patches to the intrusion protection and firewall components, we would need to use a third party solution.

4. ADJUSTMENT OF PLANS

It was important to develop a plan for testing in a pilot deployment. We had a test plan and had identified several groups that were good candidates for providing useful feedback.

Once we discovered that we could not automate the distribution of signature file updates and security patches for all the components of the SCS, it was decided that we could not implement this product in its current state. We then began looking for a way that we could use this product with full automation and minimum hands-on maintenance. The goal was to automate the update process from beginning to end and avoid spending a lot of staff time managing the updates.

5. CONCLUSION

We are aware that there are some possible solutions to the problem of automating the update distribution to the SCS clients. However, some of these solutions are not viable in our current environment. We are now focused on a third party solution for patch management that we are hoping will integrate with SCS and allow us to achieve our goal of providing optimal security protection for university workstations with a reasonable amount of management by the technical support staff.