

**White Paper Library:
Information Security for Small and
Medium-Sized Businesses**

Choosing Anti-Virus Software

A Guide to Selecting the Right Solution for Your
Business



If your data isn't secure, it isn't your data®

www.SoftwareSecuritySolutions.com

Table of contents

Executive summary	3
The current state of the anti-virus market	4
McAfee.....	4
Symantec	4
Trend Micro	4
Alternative approaches	5
Selection criteria	6
Anti-virus attributes	6
Performance	7
Scan on boot.....	8
Open document scan	8
Scan email before receiving or sending	9
Full system scan	9
So what does anti-virus really cost?	10
Protection	10
Viral malware	10
Non-viral malware.....	11
Trojan horses.....	11
Rootkits.....	11
So what kind of protection do you need?.....	11
Detection.....	12
Threat vector test parameters.....	12
False alarms and missed detections – the hidden cost of anti-virus	12
Transparency	13
The cost of not using what you’ve already paid for	14
What about security suites?	14
Suites are sweet for the manufacturer	14
Putting your action plan together	15
Conclusion	16
About Software Security Solutions	16

Choosing Anti-Virus Software

Executive summary

This white paper, the first in a series on different aspects of the Layered Security Solutions approach advocated by Software Security Solutions, is designed for the small to mid-sized businesses with little or no in-house information security expertise. Its intent is to clarify some issues around how anti-virus software should be evaluated, and where to look for advice, in order to find the right fit. Just because a particular solution has sold more than any other solution doesn't mean it's the right one for your business. We've been in and around the information security business – and small businesses - for a long time and we'd like to think we have enough experience under our belt to help you.

As part of this experiential approach, we surveyed a number of our customers in the small and medium business sector about various aspects of their anti-virus use and their attitudes towards the products they are currently using in order to calculate both the obvious and hidden costs of anti-virus use. Our primary goal in undertaking this research has been to determine whether “bloatware” products are costing companies real money, and data collected thus far would indicate that this is true.

We're not promoting any specific product in this paper; our goal is simply to help you through the minefield that information security solution selection has become. If anything is unclear in this document, or you have more questions than we've had space to answer here, please don't hesitate to contact us. You'll find our contact information on the last page of the paper.

The current state of the anti-virus market

The anti-virus market today is a mature market – it's somewhat depressing to realize that the software industry has been attempting to deal with the problem of viruses and other malware for almost 20 years now. Three vendors dominate the market, and all of them have been active in this business for almost all of those 20 years – Symantec, McAfee, and Trend Micro. Some might say that's a sign that the big guys don't have a solution and it's time to look at some different choices.

Let's take a quick look at those 'top three' vendors:

McAfee

McAfee has been many different companies during the course of its life, but seems to be refocusing itself back on pure security these days; it'll be interesting to see how they integrate their latest acquisitions.

Symantec

Symantec is a huge company these days, and since the acquisition of Veritas is no longer solely focused on its security business. Smaller businesses might wonder how much attention they can really expect from a behemoth.

Trend Micro

Trend has historically been strongest in Asia, its home market, but it has gained strength in the US and other markets by focusing on its server-centric solutions, particularly integration with enterprise infrastructures.

With two decades of experience under their respective belts and huge R & D budgets and marketing funds at their disposal, one might be tempted to assume that these vendors would have bullet-proof solutions by now. So it's not surprising that many people feel confident that, when they buy from a top-three vendor, they are getting the best product.

One of the more interesting factors that has affected all three is that all have had publicly-reported issues with code vulnerabilities and/or untested updates causing incompatibility problems at client sites, which could be a cause for concern for smaller businesses without their own in-house testing facilities.

Choosing Anti-Virus Software

It is no secret that malware writers are targeting the market leaders – specific malware programs have been and are being developed to elude detection, even to disable anti-virus and other security software products.

The big fourth?

Microsoft has of course also moved into the security market through various acquisitions and redirection of some aspects of its business, but it's probably going to be a while before many businesses are prepared to trust their security needs to a company that's seen by many as the source of many vulnerability problems in the first place.

When we talk with our customers, it's clear there is pent-up frustration with incumbent vendors – they're slow to respond to new threats, and it seems they're always trying to sell you something new to deal with the latest problem or threat. And because small businesses don't generate big revenues, if you're not a Fortune 500 company, customer service and tech support response can be patchy at best.

Alternative approaches

In a somewhat belated response to the changing threat landscape, many antivirus vendors have embarked on product road maps that combine signature-based antivirus with anti-spyware, personal firewall, policy enforcement, and host intrusion prevention system (IPS) technology into a single solution. To date, these suite solutions have generally been disappointing – too great a trade-off between security and convenience seems to be the biggest issue – but there is reason to assume that this balance will be reset over time.

Changes in the way antivirus solutions are being delivered to consumers will ultimately impact the way anti-virus is priced and sold in the business market. The larger vendors' slow reaction to e-mail and web threats has given smaller, more agile vendors an avenue into the market. Interestingly, many of these so-called “second tier” vendors are European in origin – vendors like ESET, Grisoft, Panda, Sophos, and Kaspersky – and all now have solid operations in the US.

While these smaller vendors are not always able to compete effectively in the Fortune 500-level market, their ability to move quickly to respond to threats, and to deliver more personalized service and support, makes them well worthy of consideration by smaller businesses. Perhaps coming from Southern and Eastern Europe – where businesses tend to be smaller – gives them an advantage in understanding how small businesses in the US work.

Choosing Anti-Virus Software

Validating smaller vendors

A quick tour around the websites of some of these smaller vendors turns up a surprising fact. Independent testing labs are giving many smaller vendors' products higher marks than the big-name brands in both detection and clean-up of viruses.

These more engineering-driven firms are applying advanced techniques such as heuristics and predictive algorithms to increase detection rates and speed scanning times. In the next section, we'll take a more detailed look at how these techniques are providing a strong defense against the newer threats and show you where you can find good independent test reports on the web.

Selection criteria

Many anti-virus products have become overly large and complex, slow computers down, are difficult to manage and even miss threats. But users aren't changing vendors because they erroneously believe:

- Anti-virus solutions and technology are mostly the same.
- The biggest companies have the most resources, so their security solutions must be best.
- There's no way beyond trial and error (which no small business has time for) to tell the difference between them anyway.

It is critical that those charged with protecting digital information have access to different options and resources. This section looks at some hidden TCO (total cost of ownership) considerations, as well as providing some insight into the levels of protection professed by different vendors. Understanding the issues, the options and resources available will help users find the solutions that are the best fit for their environments.

Anti-virus attributes

Every anti-virus solution should offer **Performance, Protection and Transparency**. These are fundamental requirements and should not be subject to compromise.

- **Performance** – The solution must not impact the computer's performance in any way, otherwise it is quite simply getting in the way of business. Performance degradation adds significantly to the total cost of any solution, and many users unknowingly tolerate this degradation.

Choosing Anti-Virus Software

- **Protection** – The solution must not allow a system to become infected – period. The whole point of having anti-virus installed and making that yearly investment in keeping it updated is to be protected, not infected.
- **Transparency** – if the solution is difficult to use or manage, it becomes a liability and company resources are wasted on maintaining an existing installation when they could be spent on building a competitive edge for the business. If it's not transparent (i.e. invisible) to users, they start looking for ways to turn it off; when that happens, all security bets are off.

Finding all of these attributes in a single product is difficult at best, but there are steps both vendors and end users alike can take towards making it happen.

Performance

Performance issues begin when the anti-virus program demands a significant amount of system resources to run in either on-access (real-time or continuous scanning) or on-demand (you demand, it scans) mode. The resources an application requires to run is called the “footprint” and is primarily a measurement of the delta in system memory used when the machine is idle and when it is running a deep scan.

The size of the footprint is directly related to the system's ability to provide resources to *other* programs. A large footprint is especially hard on computers with limited memory. The larger the footprint, the fewer resources are available for other programs, slowing them down and impacting productivity.

The total cost of performance can be calculated from the time users must wait for resources to be freed up to enable them to work normally. The sheer volume of threats to check for and the resources available mean that scanning takes time, depending on security level settings, (lower settings are faster, but thoroughness is compromised). We asked users of a number of different anti-virus products to document performance hits in the following scenarios:

- Scan during boot
- Open document scan

TIP:

For the most respected independent lab tests of anti-virus software, consult these resources:

Virus Bulletin:

www.virusbtn.com

ICSA Labs

www.icsalabs.com

West Coast Labs

www.westcoastlabs.com

AV Comparatives

www.av-comparatives.org

AV-Test

www.av-test.org

Choosing Anti-Virus Software

- Check email before sending or receiving scan
- Full file system scan

Using these areas of scanning we can work towards finding how performance affects the bottom line. The results of these tests are provided on page 10.

Scan on boot

Today's boot times are fairly long, due in part to the size and number of applications loaded at startup. Of course, anti-virus is one of these, and tends to be one of the most resource-hungry; the larger the program's footprint, the longer its loading time during the boot. If the program is configured to perform an "on-demand" file scan at boot, which many do as part of security best practices, an additional load is placed on the system.

TIP:

Configure the initial or boot-up scan to perform a minimal scan – choose the "QuickScan" option, which only scans commonly-used areas such as the system startup files, memory, and applications loaded and/or run as part of the startup process. A weekly full system scan is sufficient for most situations.

Our customers report boot scan times anywhere from 30 seconds to 15 minutes. For the purposes of calculating the baseline cost of ownership, we've used the conservative 30 seconds per day figure, assuming one boot-up at the beginning of each work day.

Open document scan

Anti-virus products can be configured to scan certain document types before opening them – this usually impacts Microsoft Office data file formats - .doc, .xls, .ppt files – as these have been vectors for viruses in the past. This is especially helpful when working with older files which might contain macro viruses that avoided detection when the document was first created and used.

TIP:

Implement a policy in which all documents opened and saved to the network are scanned before and after each use.

Our customers report times of between five and 15 seconds to scan a document on open, depending on file size and type. For the open document calculation we've used five seconds as a baseline number, and taken 20 as the number of documents opened and closed each day. The open document scan is something we have found many companies disable because of performance issues. By doing so they are acknowledging that their anti-virus is getting in the way of business.

Choosing Anti-Virus Software

Scan email before receiving or sending

Email has been one of the most common vectors for virus transmission, in no small part because spam continues to succeed in getting into our inboxes far too often. So vigilance in this area is critical, as the threats from email change in form, function and presentation. As with document scanning, it is prudent to scan all incoming and outgoing messages; it's especially critical to scan general-purpose mailboxes like info@, which are frequently targets for "virus by spammer" attacks. Sending a virus-infected email (or document attached to an email) can also have serious liability issues for your business.

Again, feedback from customers indicates an average scan time for an email message of between five and 10 seconds, depending on size and content (graphics, html code, etc). For consistency, we've used the more conservative five-second timing for our TCO calculations, along with a total number of emails sent and received each day of 25.

Full system scan

A full system scan should be completed every week on every machine. Because updates can identify threats not known to previous versions of the anti-virus signature database, it's only common sense to check the entire machine whenever the signature database is updated. As we become less dependent on signatures and use more intelligent behavior-analysis techniques in future, the need for regular full-system scans should lessen, but for now, safe computing should be on everyone's agenda.

TIP:

Schedule deep system scans on end-user machines out-of-hours or when computing resources are not being heavily used, for example over the lunch break. Run server scans overnight or on weekends.

The full system scan is the second most common area of protection to be disabled by survey respondents.

As you can imagine, this is where things can really slow down if the anti-virus isn't optimized for your needs. Waiting for these in-depth scans to be completed is frustrating for users, who will turn it off if they can find a way to do so (and in our survey, approximately 50% did find a way). Then IT gets frustrated because their security policies and procedures are being breached and the network is being put at risk. It's difficult to put a hard number on the cost of this frustration, but you can just imagine the cost to the business if a virus got onto the network via an unscanned client and destroyed your customer database.

Choosing Anti-Virus Software

So what does anti-virus really cost?

The chart below is derived from data collected during our survey of companies using a variety of legacy anti-virus solutions. For each category, we used the most conservative numbers. The average wage of \$17.77 per hour used to calculate costs is taken from the National Wage index Figures for 2005. Index figures for 2006 were not available at time of publication. You can easily calculate your own costs by visiting our website and using the Anti-Virus TCO Calculator at www.SoftwareSecuritySolutions.com/anti-virus-cost-calculator.php

All scan times are shown in total seconds. Cost per year assumes a 50-week working year with the computer switched off during the two-week assumed vacation period.

# of PCs	Boot Scan (sec)	Open/Close Doc Scan (sec)	Email Scan (sec)	Total Time (min)	Cost per workday	Cost per year
10	300	1000	1,250	42.50	\$12.59	\$3,147.50
25	750	2,500	3,125	106.25	\$31.47	\$7,867.50
50	1,500	5,000	6,250	212.50	\$62.94	\$15,735.00
150	4,500	15,000	18,750	637.50	\$188.81	\$47,202.50
500	15,000	50,000	62,500	2125.00	\$629.35	\$157,337.50

Table 1: The true cost of anti-virus

Protection

Following is a quick overview of the major different types of malicious code (malware) that's in circulation. While it's not essential to understand the nature of the threats, it will help in formulating policies and determining the protection that's most appropriate to your needs.

TIP:

You wouldn't hire an electrician to fix a leaky roof, so you shouldn't expect an anti-virus product to fix a rootkit problem. Always look for the best tool for each individual job.

Viral malware

Viral malware is code that replicates from machine to machine. It usually appears in the form of a virus or worm, and these days, tends to exploit vulnerabilities in applications to move from computer to computer over the Internet or via email. In order to replicate, viral malware must travel with executable code (applications, macros, java scripts, etc).

Choosing Anti-Virus Software

Non-viral malware

Non-viral malware doesn't need to piggyback on another program; it is instead a standalone program that is distributed directly from its source point (frequently a spammer) to the user. In other words, they rely on user behavior (sometimes called social engineering) to trick users into downloading the program, which then inflicts damage. Most non-viral malware is some form of spyware, designed to capture confidential information.

Trojan horses

Trojan horses exist in the gray zone between viral and non-viral malware – they can be either or both. Trojans are created by hackers who want to get access to a particular machine or particular content on machines in general, and can take the form of password crackers, keyloggers, remote access programs or pretty much anything the hacker wants.

Rootkits

Rootkits are the latest and most serious threat of all. Rootkits are packages of many different types of malware that are designed to embed themselves so deeply onto a PC that they cannot be rooted out. When a rootkit is installed on the machine, it can hide all of its malicious actions and make it almost impossible to detect. When you read about computers being recruited into 'botnet armies' by the bad guys, this is frequently the result of a rootkit infection.

So what kind of protection do you need?

Our focus here is on anti-virus, a necessary element of any Layered Security Solution. The starting point for almost every anti-virus solution on the market is reactive – detecting known viruses and removing them; this is what the signature file updates deal with. Computer users today are pretty well protected against what's known. Once a threat is known ("in the wild"), signatures can be written and updates can be sent out. Of course by then it may be too late. Reactive protection is often too little too late in today's dynamic threat environment. Although it remains an important element, reactive technology means that the vendors are always playing catch-up with the bad guys.

Because of this, many anti-virus vendors today are incorporating proactive detection techniques (sometimes called 'heuristics') to deal with the increasing tide of new threats.

Choosing Anti-Virus Software

Detection

Identification of malware is getting harder every day. Since accurate detection and removal is the single most important function of anti-anything software, in order to be effective, solutions are must be agile and proactive - like the threats they face. Our customers are telling us that those “second-tier” anti-virus products we mentioned earlier regularly find threats missed by “the big three”.

Anti-virus solutions should be judged primarily on the basis of how well they detect viral threats. Choosing an anti-virus product based on its ability to detect spyware or rootkits is asking for disappointment. The following threat vectors are those you should consider first when considering an anti-virus solution.

Threat vector test parameters

An effective anti-virus solution must be able to handle three distinct types of scanning activity. All the major certification bodies (Virus Bulletin, ICSA, West Coast Labs) all require candidate products to pass tests in all three categories.

On-Demand Scans - The on-demand scan test uses similar settings for each product and tests the product’s ability to perform regular file system scans against a known set of test threats.

On-Access Scans - The on-access scan test uses similar settings for each product and tests the product’s ability to perform real-time or live scans against a known set of threats.

Proactive Detection Scans – The proactive detection scan test assesses the ability of anti-virus products to detect unknown threats using different criteria such as pattern analysis, behavioral analysis, fuzzy logic, heuristics, and other advanced mathematical techniques. Implemented correctly, it significantly enhances a product’s ability to defend a PC; however, a poorly-implemented proactive solution will result in time-wasting false alarms, so this is the area in which most products are now attempting to differentiate themselves.

False alarms and missed detections – the hidden cost of anti-virus

As noted above, false alarms can cost businesses a lot of wasted time hunting down non-existent threats. But the single largest known-unknown threat today comes from missed detections. Today’s malware authors, unlike those in earlier times, want to remain hidden so they can do their dirty work and get out before anyone notices them.

Choosing Anti-Virus Software

It used to be that the cost to recover from an attack event was measurable. You could add the employee down time, cost of new equipment and solutions to fix the vulnerability that allowed the infection to occur, and so on. Today, the cost to recover may not be known until it is too late. Your data may have been slowly leaking over time until there's nothing left and the company is in big trouble.

Transparency

As of this writing, 42 % of survey participants admitted to disabling some function(s) in their anti-virus. But it seems they are willing to accept the risk, and pay for more anti-virus than they actually use. If a security solution is not transparent to both user and business, it's not a solution - and it's not secure.

TIP:

Know what every function in your anti-virus actually does, and make sure you understand the trade-off if you decide to turn off one function because users are complaining. Better yet, find a different anti-virus that doesn't get in the way of business.

While only a few companies in our survey were able and willing to provide meaningful data on which functions tended to be disabled, we thought it was worth including that data. One respondent disabled email scanning as they felt that outsourcing their email relieved them of any need to scan the end user PCs (a feeling we would beg to disagree with, but that's a topic for another time).

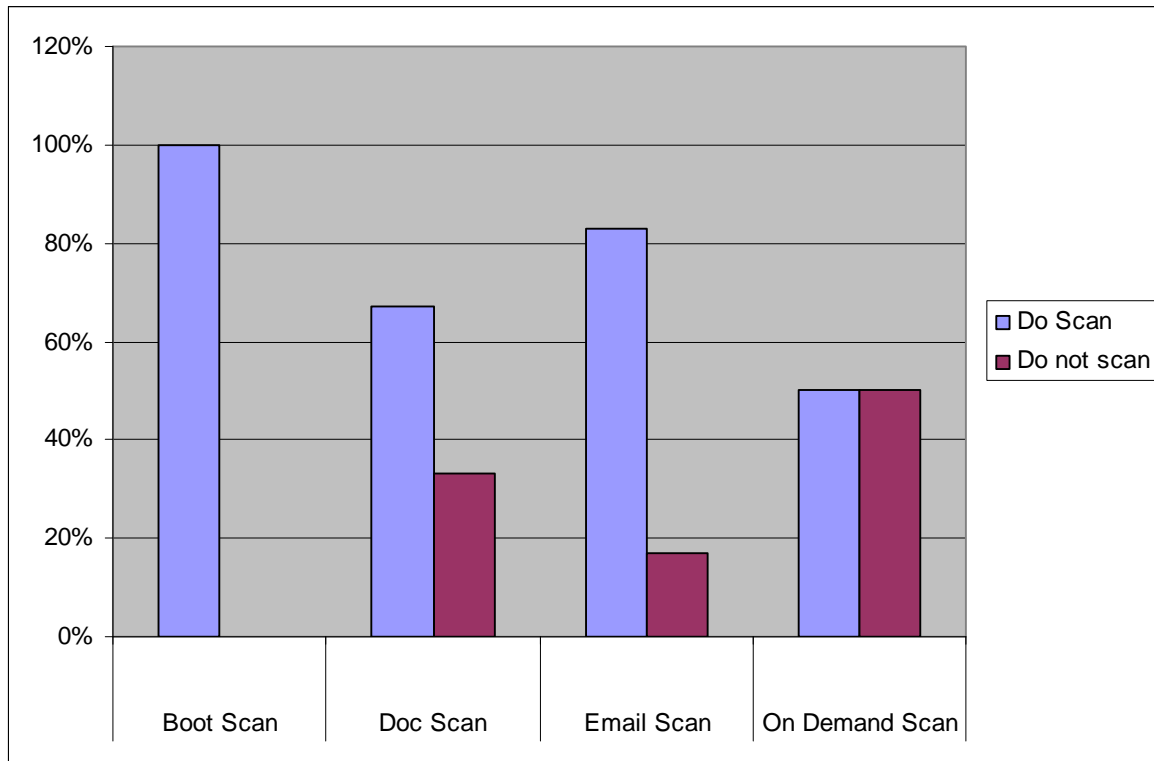


Table 2: How anti-virus is *really* used (or not used)

Choosing Anti-Virus Software

The cost of not using what you've already paid for

Unfortunately, the cost of not using all the functionality in your anti-virus solution could be equal to the cost of having no anti-virus at all – that function that you turned off because users were complaining about it might just be the one that was protecting your network against the latest worm.

What about security suites?

To want our anti-virus to deal with every type of threat doesn't make sense, as we noted earlier. Threats mutate quickly, and no software manufacturer can keep up with all of the threats all of the time. But in order to try to keep their customers happy (and support fewer products themselves) the anti-virus companies have been going out and acquiring technologies that deal with other threats and shoe-horning these frequently-incompatible technologies into their existing product lines. Or they created "security suites" that try to be all things to all people – usually unsuccessfully.

Suites are sweet for the manufacturer

Anti-virus companies typically create suites by acquiring technologies and then attempting to integrate those technologies into the anti-virus way of doing things. Not only does this not solve the security problem, but it creates huge, unwieldy applications (aka bloatware).

We believe that this approach is the consequence of a knee-jerk reaction and a resistance to change by the vendors concerned. It also is a highly inappropriate solution for business to load up the client with these mega-applications that only cause more performance problems and get turned off more often, thus letting in not only viruses but every other threat the suite supposedly protects against as well.

The common rationalization is "bigger is better" and "all-in one is convenient" but the reality in the security business is that those that specialize will be the ones that succeed.

Those independent tests we mentioned earlier will verify the strength of individual anti-virus, anti-spyware, firewall and other specialized solutions. But it is yet to be seen whether the suites can stand up to the rigors of independent threat category testing.

Putting your action plan together

First, you're going to need to do some legwork (or rather webwork). Visit the independent test sites and see how your solution stacks up against the rest of the offerings on the market, or ask a consultant to do it for you. It will be time or money well invested whichever you choose.

Start with your anti-virus software. The solutions are more mature and the market is more stable than for the anti-spyware and firewall categories, and the process will serve you well for future exercises in choosing the right products in those arenas. Find the solution that works for your environment, your network, and your budget. We have customers who report boot times and scan times being cut by more than half simply by changing their anti-virus solution.

Once you've made a short list of candidate products that meet your criteria, download a trial version from the vendor's website and put it to the test in your environment. And while you're doing this, test out the vendor's tech support and customer service response times – it's all well and good if the technology works, but you want to be sure the vendor will be responsive if something goes wrong. Also consider whether you would benefit from working with a reseller who has experience working with businesses like yours and understands the need for a multi-dimensional or layered approach to security

Once you've deployed the solution, make sure you have a security policy to back it up. An effective policy includes employee training that ensures your users are clear on the do's and don'ts of computer security. This is the largest area of risk and work done here can help tremendously if your users adhere to the rules.

Your research will have shown you that different solutions are good at different things. The best protection you can get is having a layered solution, with each layer addressing a specific problem area. Software Security Solutions is preparing guides similar to this one to cover choosing anti-spyware, firewall, and other specialist security solutions, so please contact us for more information on availability.

One final piece of advice – trust the experts. We've provided a few independent resources here, but security is one of those areas in which experience and knowledge really do pay off. And we're always happy to provide advice and guidance on where to go to get the most reliable independent information on security threats and security solutions.

Choosing Anti-Virus Software

Conclusion

No solution is perfect. Different tools are good at tackling different problems. Some are better at one or two than others. Some have better overall detection records than others. Some are faster than others. Footprints are different sizes. Some cost less up front but more in the long run when the total cost of ownership is considered. Some have good service and support; others would rather sell you another product.

Choose your advisors carefully. And make sure you do your homework, so you know who to trust. The most complex solution can become your worst nightmare with the wrong advisor – or simplicity itself with the right one.

About Software Security Solutions

Software Security Solutions is a privately held company founded in October of 2001. By focusing on computer security threats and products, we are able to provide insight and best-in-class solutions to the public. We advocate a Layered Security Solution because no one product or technique can efficiently and effectively provide all layers of computer security. We acknowledge that different users require different solutions. With Software Security Solutions, you can find the solution set and information that is the best fit for your user type.

Software Security Solutions

P.O. Box 150528

Lakewood, Colorado 80215

Phone: 303.232.9070

Fax: 303.232.9071

Email: info@SoftwareSecuritySolutions.com

Find us on the web at www.SoftwareSecuritySolutions.com