Whitelisting for Cyber Security: What It Means for Consumers

Written By: Janet Lo
Public Interest Advocacy Centre
1204 – ONE Nicholas St
Ottawa, Ontario
K1N 7B7

November 2010

With Funding from the Industry Canada's Contributions Program for Non-profit Consumer and Voluntary Organisations

The Public Interest Advocacy Centre
(PIAC)
Suite 1204
ONE Nicholas Street
Ottawa, Ontario
K1N 7B7

Canadian Cataloguing and Publication Data

Whitelisting for Cyber Security: What It Means For Consumers

ISBN
1-895-060-94-X

Acknowledgment

The Public Interest Advocacy Centre received funding from Industry Canada's Contributions Program for Non-profit Consumer and Voluntary Organisations. The views expressed in the report are not necessarily those of Industry Canada or the Government of Canada.

EXECUTIVE SUMMARY

The internet is a popular platform for electronic commerce and communications. As the internet is increasingly relied upon by the government, in workplaces and at home, cyber threats continue to increase exponentially, targeting both consumer information, valuable corporate informational assets and critical infrastructure. As cyber threats continue to increase, traditional cyber security protections such as anti-virus are challenged to keep up.

The Public Interest Advocacy Centre set out to examine the new technique of whitelisting and to provide examples of how whitelisting is being deployed in Canada by security companies. We attempted to understand how widespread whitelisting is being used and how it could be deployed to protect consumers. To this end, we conducted interviews with industry and government stakeholders.

From this research emerged a definition of whitelisting, which uses a different principle to secure computers and networks. Whitelisting defines a set of parameters to set out "safe" applications, email addresses and websites for a given system and enforces a set of accesses in order to control the computer system.

In our study of whitelisting, PIAC found three types of whitelisting solutions. Application whitelisting only allows approved applications on the whitelist to be installed on the computer or network, usually to prevent malware from being installed on the computer or network. Application whitelisting can also be used to prevent unlicensed or undesired programs from being installed, such as inappropriate content for children in a parental control context or gaming or file sharing programs that would reduce worker productivity or inappropriately use network bandwidth in a workplace environment. There are several application whitelisting solutions offered by pure-play vendors and by security vendors and operating systems as part of their holistic security solutions.

Email whitelisting defines a list of "safe" senders and recipients to prevent spam from reaching the targeted email address. Whitelisting in this context can be used to enhance the deliverability of email.

Finally, and less commonly used, whitelisting can be used to manage internet browsing and traffic. A whitelist could be set up by parents so that children could only access approved whitelisted websites. Similarly, internet service providers could employ whitelisting to prioritize certain types of internet traffic, such as gaming or streaming.

PIAC found whitelisting to have advantages for cyber security, such as preventative protection against zero day attacks. Whitelisting lends itself well to deployment in the enterprise environment, particularly closed environments where network resources and assets need to be protected. However, whitelisting is not a holistic cyber security solution and is particularly ineffective at dealing with grey areas such as spyware and adware. As well, a centralized whitelist can slow efficiency and stifle innovation.

Whitelisting is best used as one defense in a holistic approach using layered defenses for cyber security. At the moment, whitelisting technology is not efficient for consumers because it requires a level of technical sophistication and time to set up and manage that most consumers do not have.

Whitelisting is a pure form of internet control used to control and manage applications, email or internet traffic. Whitelisting could be used by governments or ISPs to completely control the internet network either for censorship or to restrict consumer internet freedoms. Deployment of whitelisting in this manner would compromise the historical values of the internet such as openness and network neutrality and stifle its generative qualities to the detriment of the public interest.

As whitelisting continues to develop in the enterprise space, pure-play vendors and holistic security vendors will likely look to innovate for deployment in the consumer space. The successful adoption of whitelisting will depend on innovation that makes it easier for consumers to implement and administer whitelisting. Consumer education about cyber security will help consumers understand the benefits that whitelisting has to offer and how to properly use whitelisting in conjunction with other mechanisms such as blacklisting and firewalls. As well, greater government leadership in cyber security is needed to protect critical infrastructure and help consumers deal with online safety challenges.

TABLE OF CONTENTS

INTRODUCTION

As the internet becomes increasingly popular as a platform for electronic commerce and daily communications, it is increasingly relied upon in the workplace and at home by Canadian citizens. With increased use, users store a greater wealth of information on their personal computers and on network servers, making their computers and servers a greater value target for cyber criminals. Users are also storing increasing amount of information online "in the cloud". However, the cyber threats of today are considerably more sophisticated and frequent than the cyber threats of a decade ago.

Security companies and network administrators have joined together in various cyber security initiatives to address emerging cyber threat issues. In 2007, whitelisting was referred to as "the future of security technology" by experts in the internet security industry who believed that a whitelist system would replace the current blacklist system.[1] This paper explores the whitelisting for computer and network security and its advantages and disadvantages. The paper discusses consumer uses for whitelisting technology and future trends for whitelisting technology in the consumer market.

METHODOLOGY

PIAC conducted detailed research, scanning cyber security documents and white papers published by security companies that discussed whitelisting. As well, we furthered our understanding of whitelisting through computer and technology magazine reviews of whitelisting products and techniques.

PIAC conducted interviews with industry players, such as security companies, application developers and internet service providers. PIAC also interviewed other interested stakeholder groups such as government agencies and public interest groups. Nineteen interviews were conducted in order to gather more comprehensive information about the cyber security industry and more specific information about the advantages and concerns with whitelisting with a view to learning how whitelisting cyber security techniques will protect virtual consumers. Appendix A lists the stakeholder organizations interviewed.

While this paper discusses various whitelisting products on the market provided by the various companies interviewed, the discussion cannot and is not intended to be a comprehensive discussion of all whitelisting products, as not all industry players could be reached for interviews. As well, the product market is constantly and rapidly evolving and innovating. Discussion of the whitelisting product market is merely meant to be descriptive of the types of whitelisting products currently available. This paper does not

[1] Michael Murphy, Vice President & General Manager of Symantec Canada, cited in Peter Nowak, "Internet security moving toward 'white list'" CBC News (17 September 2007), online: http://www.cbc.ca/news/background/tech/privacy/white-list.html.

review whitelisting products and as such, the contents of this paper should not be construed to rank or recommend individual products or companies.

The findings of the interviews will be drawn on throughout this report to explain how whitelisting solutions have been deployed in the market, especially in the consumer market, explore the advantages and disadvantages of whitelisting solutions and to survey future trends for whitelisting.

WHAT IS WHITELISTING?

Whitelisting is one method to secure computers and computer networks from a variety of threats, different from the traditional antivirus software that is commonly used to secure computers. The earliest form of whitelisting was used in firewalls. An enterprise network firewall served as a gatekeeper, loaded with a list of approved programs. Some consumer internet security suites included a firewall component with a whitelist feature for programs seeking outgoing internet access.

The traditional prevention method for dealing with malware is the process known as "blacklisting". Antivirus software employs a list of known threats facing computer and computer network users, compiling signatures of known viruses, Trojans, malware, spyware and similarly malicious code. This list of known threats is commonly called a "blacklist". An antivirus program will scan a computer or network, checking files against this blacklist of known threats. The blacklist must be regularly and frequently updated to include the latest known threats facing computer users and networks. However, the software is only as effective as the list it relies upon. Many news threats and forms of malicious code are released every hour of every day onto the internet and keeping track of them all is a nearly impossible task. Antivirus software is thus reactive protection, not preventative protection, for this very reason.

An example of an advanced blacklisting solution is heuristic software. Heuristics is the application of experience-derived knowledge to a problem.[2] Heuristics solutions look for known sources, commonly used text phrases, and transmission or content patterns that the user or company's history has shown to be associated with email containing viruses. The analysis looks at the email or program's structure, behaviour and other attributes instead of analyzing its signatures. However, heuristics makes a number of assumptions about the problem it is trying to solve and does not necessarily yield accurate results. This can result in "false positives", thus delaying the delivery of valid email, for example.[3]

Whitelisting is a newly emerging technique to address cyber threats that operates contrary to blacklisting principles. The premise of whitelisting is to lock down email, internet websites or applications on computers and allow only authorized ones to run.

---

[2] Faronics, "Blacklist Versus Whitelist Software Solutions" White Paper (August 2005), online: http://www.faronics.com/Faronics/Documents/Blacklist_vs_Whitelist.pdf at p. 4.
[3] Faronics, "Blacklist Versus Whitelist Software Solutions" at p. 4.

Definition of whitelisting

Whitelisting relies upon a different principle to secure computers and networks. Instead of checking every file against a list of known threats, whitelisting is the practice of defining a set of applications, email addresses or websites as "safe" for a given system and enforcing a set of accesses in order to control the computer system. All other parameters that fall outside of the parameters of what is "safe" are automatically blocked from the computer or network. A recent whitepaper by Faronics defined whitelisting as follows:

> Whitelist technology is the opposite of blacklist technology; the list of entities, whether domain names, email addresses, or executables, is a list of what is allowed to penetrate a system. For example, a whitelist of domain names is a list of URLs that are authorized to display, despite any rules of an email spam blocker program. The most common examples of whitelist solutions are email based, with users creating a list of authorized addresses that they can receive mail from, again despite the rules of an anti-spam program.[4]

The state of cyber security today

A "cyber threat" is defined as all malicious activity that exploits, harasses, disrupts, destroys or divulges confidential data. Cyber threats target virtual consumers for money, intellectual property and information. For example, in the first six months of 2007, Symantec reported that the incidence of malicious code was up, with findings of more than 212,000 new malicious code threats, up 185 per cent from the last six months of 2006.[5] In 2008, the number of unique malicious programs and variants that were created outstripped all the legitimate software published in the world.[6] One only need look at new Symantec intelligence reports to note the exponential growth of malicious code. For example, Symantec created 457,641 new malicious codes in the most recent quarter spanning from April to June 2010.[7] McAfee found that production of malware reached a new high in the first six months of 2010, cataloguing ten million new pieces of malicious code.[8]

Cyber threats are also increasingly complex and evolve very quickly. Staying safe online is an increasingly complex challenge for virtual consumers who want to access websites for information about consumer products and services and participate in electronic commerce. Hackers are no longer perpetrating cyber threats for fun or to

---

[4] Faronics, "Blacklist versus Whitelist Software Solutions" at p. 5
[5] Peter Nowak, "Internet security moving towards 'white list'" CBC News (17 September 2007), online: http://www.cbc.ca/news/backgrounds/tech/privacy/white-list.html.
[6] Roger A. Grimes, "Test Center review: Whitelisting security offers salvation" InfoWorld (4 November 2009), online: http://www.infoworld.com/print/98835.
[7] Symantec, "Symantec Intelligence Quarterly" (April to June 2010), online: http://www.symantec.om/content/en/us/enterprise/other_resources/b-symc_intelligence_quarterly_apr-jun_2010_21072009.en-us.pdf at p. 1.
[8] Sakthi Prasad, "Malware threat at new high: McAfee" The Globe and Mail (10 August 2010), online: http://www.theglobeandmail.com/news/technology/malware-threat-at-new-high-mcafee/article1667792/.

boost their online reputation. Money is a large motive behind organized and sophisticated cyber threats and cyber criminals have access to software toolkits that help them create their own phishing attacks. Symantec reports that credit card information was the most common advertised item for sale on underground economy servers in the second quarter of 2010, accounting for 28 percent of all goods and services. Prices for the credit card information ranged from $1 to $30 depending on the type of card, the country of origin, and the amount of bundled personal information used for cardholder verification. Symantec observed bulk purchase offers of 1000 credit cards for $1,500.[9] The second most commonly advertised item for sale on underground economy servers during the same quarter was bank account information, accounting for 24 percent of all advertised goods. The advertised price for bank accounts ranged from $10 to $125 for bank balances from $373 to $1.5 million.[10]

One particular phenomenon targeting consumers is social engineering threats that are based on consumer behaviour on the internet. Coordinated attacks with the goal of harvesting personal information from systems are more frequent, and this collected information is combined in sophisticated databases with other information, public and semi-public, gleaned from Facebook and other social networking profiles.[11] As such, intelligent, targeted attacks on individuals and businesses are expected to increase in frequency and sophistication.

The shortcomings of anti-virus technology

With the number of malware specimens rising exponentially, traditional blacklisting methods that rely on signature-based defenses against known threats are widely regarded as inadequate on their own.[12] Though anti-virus technology has grown to become an industry in its own right with revenues just below $4 billion, the viruses continue to proliferate and organizations and individuals still have to bear the high costs of virus attacks.[13] Anti-virus programs have become less effective as new viruses are more frequent and existing viruses mutate faster. Keeping up with malware signatures is proving to be increasingly difficult, as demonstrated by Symantec who in 2008 put out more anti-virus signatures than it did in the company's previous 17 years of existence.[14] Anti-virus companies are constantly playing catch up to create signatures for new viruses, worms and Trojans, which is increasingly difficult with a number of threats

---

[9] Symantec, "Symantec Intelligence Quarterly", *supra* note 7 at p. 1 and 3.
[10] *Ibid.* at p. 4.
[11] Larry Seltzer, "What Security Will Look Like in 2010" PC Magazine (15 December 2009), online: http://www.pcmag.com/print_article2/0,1217,a%253D246903,00.asp.
[12] Many stakeholders interviewed reflected that anti-virus solutions are not keeping up with malware threats. Stakeholders who suggested this include Savant Protection, CoreTrace, SignaCert, and Immunet Corporation.
[13] Robin Bloor, "Anti-Virus is Dead: The Advent of the Graylist Approach to Computer Protection" Hurwitz & Associates (2006), online: http://www.zdnet.de/anti_virus_is_dead_the_advent_of_the_graylist_approach_to_computer_protection_download-399002355-88034318-1.htm.
[14] "Top 10 emerging enterprise technologies: 2009's up-and-coming technologies for business that will have the greatest impact in years to come" InfoWorld (17 November 2009), online: http://www.infoworld.com/print/100378.

having the ability to morph into variations to avoid signature detection or cloak themselves using encryption. Thus, signature-based anti-virus software will not protect the user when a new virus emerges and the signature has not yet been discovered and added to the detection program.[15]

As well, blacklisting and anti-virus solutions for computer security provide diminishing returns in effectiveness. Anti-virus solutions cannot provide 100% security. Symantec suggests that the traditional method of blacklisting helps computer performance and protection against malware, with about 90% of software usually scanning clean.[16] Moreover, some accounts argue that anti-virus solutions barely provide any computer security. For example, Australia's Computer Emergency Response Team, AusCERT, in 2006 found that the top-selling anti-virus solutions let in 80 percent of all malicious code.[17] In 2009, InfoWorld suggested that the best detection rates for anti-virus software are between 40 and 70 percent and most products do not achieve rates at the high end.[18] Other estimates suggest that anti-virus software is effective for only 25 to 40 percent of cyber threats.[19]

Anti-virus solutions also do not provide protection against spyware or adware that the user might have inadvertently agreed to install. Because very few users read the full terms and conditions of the user agreement before they install applications, they do not realize that they have volunteered to allow advertising on their computer and the collection of information about the software they use and which websites they visit to be sent back to the advertising company through their internet connection.[20]

In the consumer market, anti-virus solutions are often packaged and marketed to consumers as a "suite" or a holistic solution for their home PC. Big players such as Symantec and McAfee currently dominate the anti-virus market. Some small whitelisting solution companies suggested that even though traditional anti-virus solutions are becoming less effective, there is no incentive for these big players to offer better protection using whitelisting because they continue to earn most of their revenue

---

[15] Bruce Schneier, "Is Antivirus Dead?" Schneier on Security (10 November 2009), online: http://www.schneier.com/blog/archives/2009/11/is_antivirus_de.html.
[16] PIAC telephone interview with Vincent Weafer, Senior Director of Development, Symantec Security Response, Symantec Corporation, 4 December 2009.
[17] Robin Bloor, "Anti-Virus is Dead", *supra* note 13 at p. 6.
[18] Roger A. Grimes, "The killer app for mashing malware" InfoWorld (30 July 2007), online: http://www.infoworld.com/print/85750. See also Anti-Virus Comparative, "Proactive/retrospective test (on-demand detection of virus/malware)" (May 2009), online: http://www.av-comparatives.org/images/stories/test/ondret/avc_report22.pdf. The Anti-Virus Comparatives report tested 16 anti-virus products.
[19] Amit Yoran, security consultant and former director of the U.S. Department of Homeland Security's National Cyber Security Division, cited in Linda Musthaler, "Implicit whitelisting blocks malware instead of productivity" IT Best Practices Alert, Network World (5 March 2010), online: http://www.networkworld.com/newsletters/techexec/2010/030810bestpractices.html.
[20] Robin Bloor, "Anti-Virus is Dead", *supra* note 13 at p. 7.

from consumers through blacklisting.[21] These companies argue that there is no incentive for anti-virus vendors to change their business model. Consumers continue to renew their licenses for anti-virus security suites and these players will continue updating their blacklists.

As well, anti-virus solutions cannot be effective for consumers if consumers do not understand how to evaluate security risks against the consumer's desired functionality. Installation and execution warnings tend to be non-existent, overly generic or excessively enthusiastic, eventually prompting users to ignore them with a click to accept the security risk.[22]

With anti-virus software becoming a less holistic solution to the challenges of more frequent and complex malware, various newer types of malware defenses, such as cloud-based reputation analysis, took off in 2009. Whitelisting is one new cyber security defense technology that helps bridge the shortcomings of traditional anti-virus and endpoint security systems.

A SCAN OF CURRENT WHITELISTING SOLUTIONS

Application Whitelisting

Whitelisting is a technique that can be used in a variety of ways to protect computers and networks. The most obvious way it can be used is to prevent computers and networks from falling victim to malware. Whitelisting can be configured to expressly forbid the opening or installation of any malicious file on a computer or a network. Whitelisting only allows known, "good" executables to run on a system:

> Whitelisting starts with a clean, malware-free image of a desktop or server. Then whitelisting software is run to uniquely identify files using one or more cryptographic hashes. Thereafter, monitoring agents on managed systems flag the presence of any executables not on the hash list or prevent them from running. Most companies distribute standard system images across the enterprise, so whitelisting can be an extremely efficient way to lock down security. Some whitelisting software can fingerprint and block a wider range of files than executables, including scripts and macro modules, and even write-protect any text or configuration file. The latter is useful for noting unauthorized modifications, such as the changes that many malware programs make to the DNS Hosts file.[23]

Whitelisting can be used to control what kind of applications are being used and installed over a computer network, such as one that may be employed by a business.

---

[21] PIAC telephone interviews with Paul Paget, President & CEO and Bob Kamsler, VP Engineering of Savant Protection, 2 February 2009, and JT Keating, VP Marketing of CoreTrace Corporation, 2 March 2010.
[22] Roger A. Grimes, "The killer app for mashing malware" *supra* note 18.
[23] "Top 10 emerging enterprise technologies" InfoWorld, *supra* note 14.

This control is beneficial, as it can prevent the installation of undesired, outdated or unlicensed programs on a network. It can also increase worker productivity and reduce demand for network resources as applications such as games, instant messaging clients or media players can be prevented from being installed on corporate computers and networks.

There are several application whitelisting products on the market. There are various pure-play whitelisting vendors, such as Bit9 and CoreTrace, but whitelisting solutions are increasingly adopted and implemented with more holistic security solutions marketed by security vendors such as Symantec and McAfee. As well, Bit9 Parity, CoreTrace Bouncer, Faronics Anti-Executable, SignaCert's Enterprise Trust Server, and Solidcore S3 Control (now acquired by McAfee and called McAfee Application Control) have all scored good reviews, which indicates whitelisting product maturity.

Pure-Play Application Whitelisting Solutions

Bit9 Parity

Bit9 Parity is a whitelisting product that scored the highest in InfoWorld's competitive product review of the major application whitelisting solutions on the market.[24] Bit9 Parity provides IT professionals with a way to automatically whitelist authorized applications that meet certain established criteria such as publisher, repository, application and updater, or applications that are trusted by a specific user. Bit9 Parity's risk and trust ratings allow IT administrators to discriminate between the merely noncompliant and a security threat, reporting these issues to the administrator and letting the administrator define the policy and appropriate treatment.

Bit9 also provides software identification and analysis through the Bit9 Global Software Registry, an online cloud database of over six billion files and over nine million applications. System administrators can use this information to identify an unknown application or to research specific products, publishers, known vulnerabilities, security scan results, and much more. Bit9 Parity offers full integration with all software distribution and patch management systems.[25] This Software Registry is licensed by Kaspersky and Symantec.

Bit9 currently offers whitelisting solutions for enterprise and government agencies but does not offer its solutions for consumers. Bit9 sees the greatest need for whitelisting in the enterprise space and is developing a downloadable product.

Faronics Anti-Executable

Faronics Anti-Executable software is a commercial application whitelisting solution. Anti-Executable scans a workstation's hard drive and creates a whitelist of all authorized programs, thereby preventing unwelcome applications from executing or installing. Anti-Executable allows administrators to choose what applications will be

[24] Roger A. Grimes, "Bit9 Parity 5.0 shines brightest among whitelisting competitors with strong protection and useful risk metrics" InfoWorld (4 November 2009).
[25] Brien M. Posey, "Running a Controlled Windows Endpoint Environment".

authorized to run on a workstation. Any executable not authorized will not install or run. Anti-Executable also includes blacklisting in the application.

Anti-Executable is sold by the license so an individual user could purchase a license for home use. However, consumers are not the main targets for Faronics Anti-Executable yet, as product marketing continues to focus on corporate and enterprise users.

CoreTrace Bouncer

CoreTrace Bouncer automatically creates a whitelist from each computer and updates that whitelist whenever new and trusted applications are added. Bouncer enables IT departments to predefine multiple sources. If predefined by IT, users can safely install applications and have them automatically added to the whitelist without requiring any further IT involvement. Under the "Trusted Change" settings, Bouncer simultaneously stops bad applications and allows trusted users to perform their own installation or upgrade of safe programs. Bouncer provides enterprise endpoint security. At this time, marketing Bouncer as a whitelisting solution in the consumer market is not yet practical.

Savant Protection

Savant Protection focuses on automated application whitelisting and its product, with the same name as the company, is a business-driven application whitelisting solution that protects the operating system and software running on desktops, servers, process control systems and point-of-sale systems. Savant Protection uses an "implicit" whitelist to stop sophisticated malware attacks by creating a unique whitelist for each individual device, which becomes the ultimate authority of what is permitted to run on that specific device. This eliminates the need for complex policies and a centralized whitelist database.

Savant Protection focuses on the business marketplace, marketing its solution to government, educational, retail, distribution and large and small companies.

SignaCert

SignaCert developed one of the first whitelisting products available on the market, providing end-to-end and partner-based IT compliance solutions based on known-provenance whitelisting technology. Provenance means that SignaCert understands the origin of the product. SignaCert defines whitelisting differently from the rest of the application whitelisting developers, using whitelisting to determine if the IT system is built and deployed as intended by the people who built and deployed it. SignaCert continuously checks whether the computer or network is configured correctly and checks for vulnerabilities. Instead of blocking unauthorized applications, SignaCert focuses on identifying deviations from trusted, predefined baselines of files and security configuration settings, specializing in midsize to large environments such as financial services, government and health care institutions.

SignaCert has more than one billion predefined file signatures as part of its Global Trust Repository service. This repository is a collection of software measurements obtained through direct partnerships with software vendors covering a broad range of operating

systems, device drivers and applications. The repository is used to deploy its whitelisting solution.

SignaCert has an arrangement with Microsoft to share its whitelisting software-standardized data. Microsoft shares software measurements out of the supply chain to enhance SignaCert's precise image management.

Holistic security solutions incorporating whitelisting techniques

Some security vendors and operating systems have begun adding whitelisting techniques to their holistic security solution products.

Symantec

Symantec's Norton Internet Security 2010 and Norton Antivirus 2010 included other types of malware protection using techniques such as whitelisting and behavioural-based detection.

Symantec in June 2009 announced that they would introduce reputation-based security in the next version of its Norton Antivirus 2010 product. Gerry Egan, Symantec product management director, suggested that the old way of checking for viruses was inefficient: "There are two approaches: blacklisting works well with files that you know are bad, and whitelisting works well with files that are known to be good but these don't work so well in the middle – it was clear that we needed a new model."[26] The reputation-based security strategy is a hybrid approach that leverages blacklisting and whitelisting. This reputation-based approach works with an algorithm that takes data from the 30 million users that have signed up to Community Watch and calculates whether every individual program is safe or not. This reputation-based approach is intended for use in consumer products.

Symantec currently offers a Symantec Software White-List program. The program offers software developers and authors and Independent Software Vendors (ISVs) the opportunity to be added to a white list of known good software maintained by Symantec to reduce the possibility of false positives. Software developers and Independent Software Vendors can submit their new or updated software to Symantec to be whitelisted.[27] Symantec notes that its decisions are subject to change depending "on a variety of factors that include but are not limited to alterations in the software, distribution of the software, or vulnerabilities in the software to misuse by the publishers or others." Symantec may also change its classification criteria and policies over time to address the constantly evolving security landscape.

Windows 7 AppLocker and User Account Control

Since Windows 2000, a form of application whitelisting has existed through Software Restriction Policies (SRPs). However, SRPs do not offer a way to easily identify all the

[26] Maxwell Cooter, "Symantec culls user data to spot unsafe programs" Techworld (26 June 2009), online: http://www.networkworld.com/news/2009/062909-symantec-culls-user-data-to.html.
[27] Symantec Software White-List program, online: http://submit.symantec.com/whitelist.

programs the user wants to allow to run. Thus, entire directories must be manually whitelisted by the user, requiring them to carefully manage administrative rights, which may be too sophisticated, or time consuming for an average user. As well, the SRP whitelist requires constant maintenance as new applications are installed or applications are updated. In Windows 7, Microsoft changed SRPs into AppLocker, which attempts to address many of these limitations. AppLocker is only available in certain editions – Ultimate and Enterprise, thus not available to the average home user. AppLocker is turned off by default, requiring the administrator to opt in to use this feature.

AppLocker allows the user to apply an allow/deny set of criteria to applications running on their computer and is based on a number of criteria: software vendor, application name, certificate, hash or unique file identifiers, or application version. The primary uses of AppLocker are for controlling what applications can or cannot be run on a machine, application validation, version control and malware control. A wizard recommends preconfiguration by using Group Policy and recommends designating that all programs present be allowed to run, even if they are installed in the future without being added to the whitelist, effectively functioning as a blacklist. AppLocker still requires careful management of administrative rights.

At this time, AppLocker is mostly used by businesses and enterprise users, as AppLocker may be too complicated for consumers to set up at this time and is not available in the consumer version of Windows 7.[28]

The User Account Control (UAC) found in Windows 7 and Windows Vista serves the purpose of reducing the need for users to run as administrators and to force developers to consider when they are requesting more rights and privileges for an executable. User Account Control has garnered critical reception from users and administrators, who have found it frustrating because of the many pop-up warnings and prompts. In order to be effective as a security measure, the UAC settings had to be so restrictive that many people found it objectionable.[29]

Email Whitelisting

Whitelisting can be used to define a list of "safe" email senders and recipients to control spam and limit the risk of malicious code or hyperlinks being distributed over email networks. The most simplistic form of an email whitelist is an individual user's contact list, which is usually automatically registered as a whitelist. This means that any emails originating from email addresses on the user's contact list will be sent directly to the user's inbox.

Email clients often have built in spam filters that use both white and black lists of senders and keywords to look for in e-mails. If a spam filter keeps a whitelist, mail from

[28] PIAC interview with Bruce Cowper, Virtualization Lead, Microsoft Canada, 19 January 2010.
[29] Faronics, "Defense in Depth: How Application Whitelisting Can Increase Your Desktop Security" Whitepaper (16 November 2009), online: http://www.faronics.com/Faronics/Documents/AE_WP_ApplicationWhitelisting_EN.pdf at p. 5.

the whitelisted e-mail addresses, domains and/or IP address will almost always be allowed.

Some inbox providers and internet service providers offer a formal whitelisting program, but may not necessarily say that they perform whitelisting publicly. The goal is to whitelist email senders whose practices are so good that the user will accept all mail that they send, which helps save resources by bypassing filtering and testing.[30] Internet service providers receive several requests from legitimate companies to add them to the ISP whitelist of companies for email delivery. In some cases, the ISP may sanction an email whitelist, which then allows messages sent from these addresses to pass through their systems. Many ISPs hand over the management of their inbox processes to a third party that originates and maintains the whitelist.[31] Whitelists allow ISPs to easily identify legitimate emails amidst the glut of spam emails and give increased functionality to trusted senders. However, whitelists do not allow email senders to enroll and then put their sending practices on autopilot. Senders must continue to adhere to email best practices to stay on the whitelist.[32]

If an email sender is able to get on the inbox or ISP whitelist, the status will offer deliverability advantages, such as bypassing some spam filters and increasing allowable-per-hour or per-send volumes over non-whitelisted senders. Email sender whitelisting dramatically improves the changes so messages arrive in the inbox versus being blocked or routed to junk or spam folders and also arrive with images in tact.[33] However, whitelisting an email sender will not necessarily ensure that email is delivered. Most ISPs analyze message content and filter for bulk sender volume. Thus, emails could be blocked for trigger keywords such as “free”, names of prescription drugs, common URLs, attached programs or strange images.[34]

There are also noncommercial and commercial email whitelists. For noncommercial whitelists, rather than paying fees, the sender must pass a series of technical tests. The operator may remove a server from the list if complaints are received. Commercial whitelist providers, such as GoodMailSystems’ Certified Email and Return Path Certification, are systems by which an internet service provider allows email senders to bypass spam filters when sending email messages to its subscribers in return for a pre-paid fee, which can be either an annual fee or a per-message fee. A sender can have more confidence that their messages have reached their recipients without being blocked or having links or images stripped out of them by spam filters. The purpose of commercial whitelists is to allow companies to reliably reach their customers by email.

---

[30] PIAC telephone interview with John R. Levine, President, Coalition Against Unsolicited Commercial Email (CAUCE), 11 January 2010.
[31] silverPOP, “Unlocking the Secret World of Whitelisting: Insight for Enterprise Email Marketers” (2007), online: http://www.marketingscoop.com/Article_Tools/WhiteListing.pdf at p. 2.
[32] “Return Path’s Email Delivery Imperatives Report Advises Email Senders on Best Practices for Sending Email in 2010” BusinessWire (22 February 2010), online: http://www.returnpath.net/blog/2010/02/return-paths-email-delivery-im.php.
[33] silverPOP, “Unlocking the Secret World of Whitelisting” *supra* note 31 at p. 1.
[34] Ben Isaacson, “Whitelists and Filters” ClickZ (10 May 2004), online: http://www.clickz.com/clickz/column/1718078/whitelists-filter.

Email service providers, such as ExactTarget, provide a self-serve email solution for small businesses and work with Canadian businesses. Working with an email firm allows businesses to leverage the firm's existing whitelist relationship with ISPs like Sympatico and Rogers and ensure that their messages comply with current email marketing legislation.[35]

Email whitelisting solutions

Return Path

Return Path, a leading email deliverability and reputation management company, publishes Email Delivery Imperatives guide to outline best practices for email senders. Return Path helps commercial email senders get more email delivered to the targeted inbox by providing tools and services to diagnose and prevent email deliverability and rendering failures by improving and maintaining email sending reputations. Return Path boasts that the majority of clients see an increase of 15 to 20 percent deliverability.[36]

Return Path runs the internet's largest and most widely used third-party email whitelist, the Return Path Certification Program. Return Path has over 900 clients ranging from the largest senders on the internet, such as marketers, email technology providers, social networking sites, and internet service providers, to community and not-for-profit groups. It whitelists almost 6,000 IP addresses and its whitelist is used by large email providers such as hotmail and yahoo, as well as email services provided by internet service providers.

Goodmail Systems

Goodmail Systems in 2010 published a domain-based whitelist of good email senders called CertifiedDomain. CertifiedDomain assigns and tracks reputation at the internet domain level, as owners of the internet domains listed undergo an accreditation process, passing checks across a number of public and private databases. Goodmail cross-references a domain's reputation against this data, making sure the applicant adheres to email sending best practices.

Internet Website Whitelists

In Internet Explorer, the Content Advisor and Anti Phishing filter enable the user to filter the types of content viewable when browsing the internet. Content Advisor is a tool to control the types of content that the user's computer can access on the internet. Only rated content that meets or exceeds the user's set criteria can be viewed and settings can be adjusted to suit the user's preferences. Ratings are provided in the metadata for a site and filtering is applied based on the ICRA (the Internet Content Rating Association) V3 guidance. The anti phishing filter checks all websites for three criteria: sites listed on the "trusted site" list, which is the whitelist; sites listed on the phishing list

[35] Tessa Wegert, "Getting the message" The Globe & Mail (5 April 2009), online: http://www.theglobeandmail.com/report-on-business/article828206.ece.
[36] PIAC telephone interview with Neil Schwartzmann, Director, Certification Security & Standards, Return Path Inc, 25 January 2010.

through the smart screen filter and online site list; and heuristics which asks whether the site looks correct based on criteria such as valid certificates.

As well, Windows provides Live Parental Controls, which is a tool for parents to control how their children use computers at home. While parents demand control, they also require technology that is easy for the parent to use and to retain control of the multiple computers and devices that can access the internet. This parental control feature is disabled by default and requires a parent administrator to opt in and configure the settings in order to use this feature. The Live Parental Controls give parents the ability to control content across multiple computers based on login credentials and the profile of the user. Extensive logging is performed on things such as website activity, instant messaging conversations, emails and application usage.

The challenge in using whitelisting solutions for parental control lies in keeping the whitelist up to date, especially if the parent is managing the whitelist manually. Parents may struggle with keeping the whitelist up to date, as it requires monitoring new websites and communications technology. As well, parents should strive to seek a balanced whitelist, as a whitelist that is too restrictive may result in their children finding a way to access the internet elsewhere.[37]

Internet traffic whitelisting

Juniper Networks delivers network security solutions and network performance optimization technology. Juniper Networks uses traffic control methodologies that employ both whitelisting and blacklisting and policy management for web filtering. Juniper Networks caters to enterprise, service providers and the public sector. Juniper Networks applies whitelisting to traffic management, which allows the consumer to decide what traffic is most important to them.

Juniper Networks focuses on improving consumer functionality. It is not currently possible for consumers to prioritize applications. Juniper hopes to deliver its product with a service provider, which would give the end consumer control over which applications or traffic it would like to prioritize. This is a form of whitelisting. For example, a consumer might prefer to have World of Warcraft or XBox prioritized over email delivery and web surfing. This network performance optimization technology also helps service providers manage their finite network capacity and consumer demand.

Implementation of whitelisting solutions

Enterprise space

Application whitelisting has found good adoption in enterprise environments, particularly where the corporate network needs to be absolutely secure, such as banks. Before application whitelisting, enterprise spaces mostly relied on software restriction policies. However, these software restriction policies required substantial administrative overhead and were easily circumvented by knowledgeable users. Application

[37] PIAC interview with Microsoft Canada.

whitelisting provides a manageable solution without much overhead and prevents circumvention, allowing the technical team to fully control the desktop environment; to identify and control applications; to prevent users from installing unauthorized applications; to protect computers from malicious malware; and to prevent data leakage by controlling portable devices such as Flash drives.[38]

Initially, not all enterprises or small businesses rushed to adopt whitelisting, as some organizations viewed it as too restrictive. Whitelisting works well in static work environments where the computers and networks only need to be updated every six months or so, such as in call centers or retail, point-of-sale (POS) environments.[39] However, in more recent years, enterprise spaces have begun to adopt whitelisting as one prong of their infrastructure protection.

Corporate employees do not always welcome the implementation of whitelisting solutions in enterprise markets. For example, CoVantage Credit Union of Antigo, Wisconsin found that its employees strongly objected when the IT department tried locking down their computers using whitelisting technology from Faronics. The credit union found that whitelisting got in the way of immediate use of applications that employees legitimately needed and employees did not like having to contact the IT department when these kinds of new applications came along.[40] However, whitelisting products continue to improve their management systems and innovate in this space as the technology gains momentum in combating malware. As more enterprise spaces implement whitelisting solutions for better cyber security, a cultural shift may be seen as employees will have to give up some measure of control over what they run on their own desktop or laptop computers.

Brien Posey, a Microsoft Most Valuable Professional for his work with Security and with Microsoft Exchange Server, suggests that organizations considering investing in a third party product for application whitelisting should look for a product with the following capabilities:

- Software identification and analysis;
- Automated and adaptive whitelisting; and
- Open integration with existing systems.[41]

Whitelisting programs are beginning to prove themselves to be "mature, capable and manageable enough to provide significant protection while still giving trustworthy users room to breathe."[42] Indeed, in InfoWorld's test of six application enterprise-grade

---

[38] Brien M. Posey, "Running a Controlled Windows Endpoint Environment", *supra* note 25.
[39] Dr. Jim Anderson, "Application Whitelisting Only Works Sometimes – CIOs Need to Know the Facts" (9 November 2009), online: http://www.theaccidentalsuccessfulcio.com/security/application-whitelisting-only-works-sometimes-cios-need-to-know-the-facts.
[40] Ellen Messmer, "Whitelisting Made Strides in 2009" Network World (18 December 2009), online: http://www.cio.com/article/print/511379.
[41] Brien M. Posey, "Running a Controlled Windows Endpoint Environment" *supra* note 25.
[42] Roger A. Grimes, "Test Center review: Whitelisting security offers salvation" *supra* note 6.

whitelisting programs, all products fared well.[43] For enterprise spaces, whitelisting programs provide more than locking down desktops to prevent malware – they also provide software configuration and licensing compliance as well as regulatory auditing.

Internet service providers

Bell Canada offers whitelisting for enterprise clients, which establishes security policies according to the client's needs.[44] TELUS also offers whitelisting as part of its security solution for internal network operations and for private networks established for institutional and government clients. For example, only traffic from certain devices or port numbers may be allowed.[45] Rogers Communications Inc. has a small business enterprise and does not currently offer a whitelisting solution.[46]

The three major Canadian internet service providers interviewed are not currently using whitelisting techniques on the internet connections sold to retail customers.[47] At the retail service level, blacklisting is most common, with ISPs blocking certain known "bad" applications and traffic sent using certain ports. Blacklisting is implemented countrywide by internet service providers in conjunction with their security solutions for their networks. As well, signature-based blacklisting is usually deployed in conjunction with heuristics to clean the retail internet networks.

TELUS observed that consumers want control or at least the option to control the characteristics of their internet access. Thus, TELUS does not manage the network and it is up to the user to decide whether they wish to whitelist certain applications on their home computer or home network. Rogers similarly suggested that a sophisticated end user may want to set up a whitelist but most consumers would not want this option. Bell expressed a preference not to introduce whitelisting to the retail ISP network unless there is a third party establishing the whitelist. Bell does not want to be responsible for monitoring and making decisions about what content should or should not be on an approved whitelist.

Consumer Space

New business-oriented whitelisting tools are now practical and efficient for enterprises to implement. However, there are currently few consumer-oriented whitelisting products. Even where a consumer can purchase whitelisting products on an individual license basis, the product is usually designed with enterprise spaces in mind. As such, their design and set-up are not ideal for an average consumer with limited technical knowledge.

---

[43] InfoWorld tested Bit9 Parity, CoreTrace Bouncer, Lumension Application Control (formerly SecureWave Sanctuary), McAfee Application Control (formerly Solidcore S3 Control), SignaCert Enterprise Trust Services, and Microsoft AppLocker.

[44] PIAC interview with Dave McMahon, Director, National Security Strategy, Bell Canada, 17 December 2009.

[45] PIAC telephone interview with Craig McTaggart, Director, Broadband Policy, TELUS, 21 December 2009.

[46] PIAC telephone interview with Ken Englehart, VP Regulatory, Rogers Communications Inc, 19 March 2010.

[47] PIAC interviews with Bell Canada, TELUS and Rogers Communications Inc.

However, over time, consumers drive the use of business tools in the consumer space, a phenomenon that is called "cross-pollination" and has been previously observed with online safety.[48] An example of consumer-oriented whitelisting that may see the most take-up among consumers is child and parental controls on home computers.

The challenge in moving to the consumer space is that consumers are used to full access to the internet, with websites, content and applications available to them with a simple click. Consumers are also not used to paying for security solutions and are unlikely to take up whitelisting if the solution is costly. In a recent survey about anti-virus software, Microsoft found that nearly 100 percent of consumers have installed anti-virus software on their computer, but 70 percent of consumers have out-of-date anti-virus or their subscription has expired because they did not realize they have to pay or update their security suites.[49] Consumers may need to become aware of the gravity of the recent exponential increases in malware threats in order to see the need to better secure their home computer from cyber threats and contemplate whitelisting solutions. As well, consumers will most likely be exposed to whitelisting solutions that are packaged with anti-virus security suites sold by security vendors – this may be the easiest way to make it cost affordable for consumers and would serve the consumer market through channels that already serve consumers and have earned their trust.

Both Savant Protection and SignaCert estimate that whitelisting in the consumer market is approximately five years away.[50] The small whitelisting solution companies expressed a desire to move into the consumer marketplace. However, moving into the consumer marketplace at this time is not practical for small whitelisting developers, as they do not have the marketing resources to pursue consumers. Marketing to consumers will become more feasible once the technology is proven and the brand is built through the enterprise space.

TRENDS IN WHITELISTING

Advantages of whitelisting

Security Through Prevention and Protection Against Zero Day Attacks

Whitelisting offers a few advantages over the traditional blacklisting method of securing computers and networks. An important advantage is whitelisting's preventative quality. Since there is no central blacklist that needs to be consulted, such as with traditional antivirus software, users are protected the moment a new piece of malicious code is released without needing to update any databases.

[48] PIAC interview with Microsoft Canada.
[49] PIAC interview with Microsoft Canada.
[50] PIAC interviews with Savant Protection and Wyatt Starnes, CEO, Founder & President, SignaCert, 26 January 2010.

Whitelisting has been lauded for its ability to protect against zero-day attacks. A zero-day attack is a threat that tries to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developers. When the vulnerability is discovered, the developer races to close the hole before attackers discover it or the security hole becomes public. A "zero day" attack occurs before the developer gains awareness of the security hole, meaning that the developer has not had an opportunity to distribute a security patch to fix the software. Whitelisting solutions would prevent zero day attacks because if attackers became aware of a security vulnerability in a whitelisted application and dropped malicious code onto a machine, the code would not be allowed to execute because it was not on the approved list.

Whitelisting is also useful for defense against malicious code which may be specifically written and tailored to a particular target, such as a large corporate database.

Resource Efficiencies

Whitelisting can also reduce the load on computers and networks, sometimes to a dramatic effect. Traditional blacklisting techniques require regular and frequent updating and scanning of entire computers and networks, which can be very resource intensive. Bell noted that deploying an antivirus and firewall suite to protect a computer does slow down the performance of the computer with constant updates and scans.[51] Whitelisting frees up time and system resources by skipping evaluation and deep scanning of email and software.[52] Also, unauthorized applications will not be able to run, thus conserving the resources they would have consumed.

A corporate IT department could also whitelist applications that consume a reasonable amount of bandwidth to ensure that network bandwidth remains efficient. For example, if peer-to-peer programs are not approved for the whitelist, as they are known to consume the maximum amount of bandwidth available, these programs could not be installed by an employee.

Anti-virus software have also begun utilizing whitelisting technology not as a primary feature, but to determine what files or applications are already approved and thus can be skipped by the scanning process to check against the blacklist. Whitelisting is used then to free up the amount of resources the anti-virus scan requires and is a competitive way to increase the speed of the scan.

Reducing Technical Support

Whitelisting can also reduce the amount of technical support required by some less savvy users. Programs that are not permitted by the whitelist may not be installed on protected computers and networks. This prevents conflicts between programs or errors caused by unauthorized software installed on computers and networks. As Freeform Dynamics reports, the biggest security holes in any organization are caused by "users

[51] PIAC interview with Bell Canada.
[52] PIAC interviews with CAUCE and Max Weinstein, Stop Badware Project, Berkman Center, 18 December 2009.

doing stupid things", or at least "users not remembering what not to do".[53] A great deal of time, effort and money are spent to train corporate users to properly use computers and making them aware of threats and policies and what they can do personally to minimize the risk. This means that organizations that have implemented whitelisting security techniques will spend less money and time on computer and network maintenance as well as providing technical support to users.

Disadvantages of whitelisting

Whitelisting is not a foolproof solution

A computer must be clean before installing the whitelisting solution. If malware is already entrenched on the computer, the application will be whitelisted and will be allowed to continue running in its corrupted state. As well, many stakeholders commented that whitelisting would not be effective as a standalone security solution because it would be too restrictive and overly broad, infringing on the functionality of a computer and the network. Thus, it is not necessarily better or more effective than blacklisting. To be effective, whitelisting needs to be employed in conjunction with other security solutions.

To be effective, whitelisting needs to deal with change effectively

Vulnerabilities can develop over time. A website or email sender or application that has previously been deemed "safe" can become infected or compromised and its security state may change.

It is not uncommon for malware to use legitimate software to do its dirty business. For example, malware could be attached to a data file, such as a Word macro virus. Whitelisting would not be able to prevent this type of malware from executing. There has been some innovation in this area to improve whitelisting technology's ability to recognize changes in the system and highlight vulnerabilities in the software's configuration.

Whitelisting can also become vulnerable if an attacker gains the ability to modify the whitelist. In June 2010, a third party research reported a zero-day vulnerability affecting the Help and Support Center application in Windows Server 2003 and Windows XP. The Help and Support Center is the default application used for handling access to online Microsoft Windows documentation to assist users in troubleshooting their system's issues, which can be accessed directly through other applications such as web browsers. When the application receives a request through the user, the requested file is verified using a whitelist to restrict untrusted sites from accessing unauthorized data.[54] This vulnerability demonstrated a flaw in the way that the application handles errors while checking the whitelist. The flaw could be manipulated to successfully

[53] Jon Collins, "How bad are the bad guys: The changing nature of Web security threats" Freeform Dynamics in conjunction with Webroot (September 2009), online: http://www.webroot.com/shared/pdf/Freeform_Dynamics_How_Bad_Are_The_Bad_GuysWR.pdf.
[54] Symantec, "Symantec Intelligence Quarterly" *supra* note 7 at p. 5.

bypass the whitelist, as it was possible to add URLs to the whitelist. The attacker could exploit the vulnerability to gain unauthorized access to restricted help documents on the victim's computer. The attacker could then combine exploits of other vulnerabilities to execute malicious code on the target computer. This is especially problematic if the user represents a system's administrative account, as the attacker could gain control of target computers and carry out additional malicious activities, such as stealing confidential or personal information or using the computer to send spam.[55] At the time of writing this report, Microsoft is developing a security update to address the vulnerability and, in the interim, has implemented an automated workaround solution.[56]

As well, whitelisting programs can have difficulty blocking programs that run inside of virtual environments or in the cloud.[57] As Web 3.0 and users explore virtual worlds and innovative new technologies, whitelisting may not be able to help ensure security in these areas.[58]

Whitelisting is not helpful for grey areas such as spyware or adware

Like blacklisting, whitelisting is not a helpful cyber security technique to deal with grey areas such as spyware or adware, where policy decisions need to be made by the individual user. Various users have different definitions of spyware or adware, depending on their functional needs and their tolerance levels for these technologies. These grey areas need security technology that can handle a spectrum or sliding scale.

Symantec noted that several vendors could build grey area categories into their commercial product. Nonetheless, cyber security techniques such as whitelisting and blacklisting are pure techniques that are not ideal to address the grey area.[59]

A centralized whitelist may slow business efficiency and stifle innovation

Because all applications need to be checked against a whitelist, a whitelisting solution may end up slowing business efficiency and stifling innovation. For example, depending on who is managing the whitelist and vetting new or updated software, it may take several weeks for new or updated software to be added to the whitelist. In a corporate environment, the average corporate IT department does not have a good idea of what software is running on all the computers within the corporation and does not want the administrative overhead of managing all the change requests.[60] Some application whitelisting solutions are also innovating in this area by giving administrators the ability to create some parameters within which users can install or update software without the need to check it against admin first.

---

[55] David Murphy, "Google engineer releases details on XP exploit, hacks off internet" PC Magazine (13 June 2010), online: http://www.pcmag.com/article2/0,2817,2364988,00.asp.
[56] Symantec, "Symantec Intelligence Quarterly" *supra* note 7 at p. 6.
[57] Roger A. Grimes, "Test Center review: Whitelisting security offers salvation" *supra* note 6.
[58] PIAC interview with Bell Canada.
[59] PIAC interview with Symantec.
[60] Bruce Schneier, "Is Antivirus Dead?" *supra* note 15

Centralized whitelists are of particular concern for application whitelisting in the consumer market. Symantec Fellow Carey Nachenberg says: "Users install millions of legitimate applications every day from literally hundreds of thousands of software vendors. … Thus, it's all but impossible for the average company, or for that matter even most security vendors, to maintain a comprehensive, up-to-date list."[61]

Whitelists are not efficient for individual users

The initial step of creating whitelist is not efficient for individual users. While this step may be well worth the time and effort for system admin of a corporate or enterprise environment, it is likely not feasible for individual home users. For example, average users have neither the expertise to determine what is a safe application that should be whitelisted nor the time to sort through their junk mail to find email from senders who have not yet been added to their email whitelist. Different whitelisting solutions provide different mechanisms to create a whitelist. Some solutions create a starting whitelist based on what applications are already installed on your computer; others present a default whitelist, to which the user can add additional programs that should be on the whitelist. The initial set up may be time consuming and too complicated for the average user.

While whitelisting would considerably improve the security of individual users' computers, the average user will likely ignore the warning message of "the program you are trying to run is not on your whitelist". If the whitelisting solution frequently displays pop-up warnings, the user may habitualize adding unapproved programs to the whitelist to carry on with their use without fully investigating the security implications of adding the application to the whitelist. This may leave their computer open to vulnerabilities. Even worse, unsophisticated users may believe that their computer is broken when they try to run a new piece of software.

However, in recent years, some whitelisting products have added the ability to automatically whitelist updated files. As whitelisting companies continue to innovate in this area and start to look toward the consumer market, whitelisting solutions will likely become more automated so as to operate invisibly to consumers, lessening the administrative burden for individual users.[62]

Whitelisting cannot be successful on its own: A Layered Defense Is Needed

A number of defense mechanisms against cyber threats exist but no single technique offers a "magic bullet" solution. Each mechanism offers its own advantages. Users and networks must implement a layered approach that makes appropriate use of each one.

---

[61] Brian Prince, "Will the Antivirus Market Be Challenged or Complimented by Whitelisting?" eWeek.com (26 June 2009), online: http://www.eweek.com/c/a/Security/Will-the-Antivirus-Market-Be-Challenged-or-Complimented-By-Whitelisting-871340/.

[62] PIAC interviews with Savant Protection and Oliver Friedrichs, President, Immunet Corporation, 8 April 2010.

By using an entire arsenal of tools, each protecting a different area or specifically designed to counter a specific threat, more threats are protected against and if one defense is compromised, a second, third or fourth stands ready and must be overcome.[63]

> Security software developers need to take the best of all the various technologies (signature detection, heuristics/behavior detection, whitelisting, blacklisting, code signing, community groups, and so on) and make them work in concert to give end-users the best chance of escaping infection.[64]

As several stakeholders emphasized, whitelisting is an important part of a holistic cyber security solution.[65] Using whitelisting in conjunction with the various other security techniques can compound the power of the best whitelisting products on the market. Whitelisting complements and augments existing defenses.

Faronics refers to this layered approach as "defense in depth".[66] By layering defenses, computer security will be more effective. Symantec suggested that whitelisting is gaining momentum in the cyber security industry as major vendors are using whitelisting as a component of their whole security solution.[67]

Cooperation of industry players

In 2007, a CBC news article suggested that an effective whitelisting solution would likely require cooperation and funding from a majority of players in the technology industry.[68] Michael Murphy, Vice President & General Manager of Symantec Corporation, suggested that the trick of whitelisting would be to develop a "global seal of approval".

In PIAC's interviews with various stakeholders, there were varied views regarding the need for industry cooperation for whitelisting.

All stakeholders acknowledged that industry cooperation would be helpful, such as Symantec, Microsoft, SignaCert, Faronics, Savant Protection, CoreTrace, and Google Canada. Symantec suggested that software developers should allow their software to be scanned so that hashes and signatures could be catalogued for a whitelist. There could be some logistical issues as new software updates were deployed. As well, cooperation to develop trust and reputation standards would be helpful, as certification of every new piece of software is burdensome and time consuming. Some stakeholders suggested that industry cooperation helps establish standards, which provides greater certainty for application developers. As well, cooperation would create efficiencies and distribute resources across the industry, by helping smaller players that might not have

---

[63] Faronics, "Defense in Depth", *supra* note 29 at p. 3.
[64] Roger A. Grimes, "The killer app for mashing malware" *supra* note 18.
[65] PIAC interviews with Microsoft, Immunet, CAUCE, Berkman Center and Dmitry Shesterin, VP Marketing and Brent Bednar, Account Manager Sales, Faronics, 12 January 2010
[66] Faronics, "Defense in Depth" *supra* note 29 at p. 3.
[67] PIAC interview with Symantec.
[68] Peter Nowak, "Internet security moving toward 'white list'" *supra* note 5.

all the resources to create and manage a whitelist. However, all stakeholders recognized that industry cooperation in this regard would be extremely difficult, if not impossible.

Other stakeholders, such as Faronics and Savant Protection, believe that industry cooperation is not fundamental to whitelisting's success. Savant Protection suggested that industry cooperation would make whitelisting a very expensive solution. For most consumers, a default list maintained by a vendor will be large enough to include most of the applications they need to run. For more technically savvy consumers, they may need to maintain a greylist of applications not on an approved vendor whitelist but not on anti-virus software's blacklist. It would then be up to that individual consumer to find a whitelisting solution that worked for their needs.

Google Canada noted that cooperation between industry players might actually have negative effects. If a whitelist is created by consensus, the decision-making model may lead some players to feel as though certain applications or websites or emails have been approved, even though they would not have agreed to do so if they were managing their own whitelist.

There are already efforts within the industry towards some cooperation and sharing of information. For example, anti-virus vendors share samples of viruses to coordinate blacklisting efforts. Similarly, email security groups share samples of spam for research purposes.

In 2009, Comodo CEO and chief security architect, Melih Abdulhayoglu, set up an organization called the Common Computing Security Standards Forum (CCSS). Its purpose is to give ordinary internet users a list against which they can check programs and publishers before buying software on the internet. The CCSS was confident that the list comprised 95 percent of legitimate software security vendors. Abdulhayoglu stated that there was a need for an organization to get the industry together to solve security problems.[69]

The Anti-Spyware Coalition (ASC), convened by the Center for Democracy and Technology, brings together a mix of industry stakeholders, including anti-spyware software companies, academics and consumer groups, to build consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies. ASC has published documents about definitions of spyware and other potentially unwanted technologies, best practices suggestions, conflicts resolution, tips for consumers and corporations, and considerations for anti-spyware product testing.

Another group is the Anti Phishing Working Group (APWG), a global pan-industrial and law enforcement association focused on eliminating fraud and identity theft resulting

[69] John E. Dunn, "AV vendors fight 'scareware' with new whitelist: New list to check up on legitimate products" Techworld (16 July 2009), online: http://www.networkworld.com/news/2009/071609-av-vendors-fight-scareware-with.html.

from phishing, pharming and email spoofing of all types. APWG monitors the state of phishing threats in the world and provides tips on how to avoid phishing scams for consumers.

One form of cooperation in Canada is through the Information Technology Association of Canada, which hosts a Cyber Security Forum. This forum is an industry-government policy roundtable that brings stakeholders together every quarter to discuss issues such as cyber crime, cryptography policy, critical infrastructure protection, national security, network security, spyware and phishing. The forum receives updates from the private and public sector and will often discuss reports, bills and consult on legislation. On occasion, the Cyber Security Forum strikes a task force to study a particular issue.

Centralized whitelist

If industry cooperation were achieved, strides might be taken towards a centralized whitelist, which would raise some concerns.

If an oversight body were created to oversee a centralized whitelist, a model with a good vetting procedure for adding new applications to the whitelist would need to be employed.[70] Great care must be taken when designing the parameters of the whitelist, as standards must not be compromised, which may reduce its effectiveness in protecting against threats and result in loss of confidence in the centralized whitelist. As well, procedures may need to be put in place for dispute resolution and conflicts management.

As well, a centralized whitelist would require a speedy approval process, so as not to stifle innovation by application developers or block communications from new email senders. With blacklisting, there is already a latency issue with developers trying to close the zero-day gap. Managing a whitelist would not solve latency issues, but create a different latency issue by delaying the ability for users to install or open new applications and websites and email not yet approved by the whitelist. An oversight body for a centralized whitelist would have to be neutral and mindful of open-source software, which is often modified.

Some stakeholders interviewed noted that a centralized whitelist would be an authoritative approach that is not in line with the history of the internet, where openness and innovation at the fringes allow consumers to benefit from the long tail and produces generative qualities.[71] While a centralized whitelist would be effective and accomplish the goal of keeping the consumer safe, it would not address free speech, community and privacy concerns. Whitelisting would benefit form a plethora of viewpoints from the industry and consumer groups.[72] As well, a centralized whitelist may drive up the cost

[70] PIAC interview with CoreTrace.
[71] See Chris Anderson, *The Long Tail: Why the Future of Business is Selling Less of More* (New York: 2006) and Jonathan Zittrain, *The Future of the Internet and How To Stop It* (York University Press, 2008).
[72] PIAC interviews with Heather West, Policy Analyst, Center for Democracy & Technology, leading the Anti-Spyware Coalition, 12 January 2010 and Berkman Center.

of commercial software for consumers, as companies will need to seek approval for the whitelist and pass these costs on to consumers in the price of their products.

Future trends for whitelisting

Whitelisting can be most useful when it is used on computers such as application servers. It is also most useful when used in conjunction with other cyber security products, such as endpoint security and blacklisting techniques and other defenses.

The market for whitelisting products is still emerging. It seems that all the major security companies are beginning to plan and participate in this new strategy to combat cyber threats. While the market for whitelisting products in 2009 appeared to be confined to targeting enterprise environments, there is a desire by businesses to roll out the technology to consumers. However, there are diverging opinions on how this might be achieved. Some players suggest that whitelisting products may need to be marketed and sold in combination with existing anti-virus and endpoint system solutions, suggesting that there will be market consolidation in whitelisting products. This seems to be supported by Solidcore's acquisition by McAfee and SignaCert's purchase by Harris Inc.

As more computing moves into the cloud, whitelisting will be most useful in protecting virtualized applications in particular. McAfee's Director of Product Management for Systems Security, Kish Yerrapragada, says that "application control is the best way to put your foot forward" as traditional approaches for on-demand scanner put a lot of pressure on the system. Whitelisting technology is a turning point for virtualized application control.[73]

CONSUMER CONCERNS

Lack of understanding about security technology

Many industry stakeholders expressed concerns about the lack of consumer understanding about security technology and their ability to manage risk and properly deploy security technology on their home desktop computers.[74] Most consumers focus on keeping their computer running and operating and accessing the content that they wish to access. Few consumers follow developments in business technology and do not monitor the security threat level for their home computer. As Savant Protection noted, there is fear and doubt in the consumer market, as consumers do not know how to manage their own home security and often purchase holistic security suites offered by the large security vendors for endpoint security.[75]

[73] Ellen Messmer, "Whitelisting Made Strides in 2009" Network World (18 December 2009), online: http://www.cio.com/article/print/511379.
[74] PIAC interviews with Microsoft Canada and Faronics.
[75] PIAC interview with Savant Protection.

Stakeholders such as Microsoft and Bell Canada suggested that consumers do not understand security messages, particularly when they are presented with a choice of responses. For example, when the average unsophisticated consumer sees an error message with a "Yes" or "No" option, there is a 50/50 chance that they will click on either. In fact, many consumers will simply click on the "yes to all" option to stop the pop-up warnings, which they likely do not understand and view as annoying.

User technical ability to set up and control whitelist

Technology such as whitelisting may require too much administration. Because setting up a whitelist often requires the administrator to set up parameters of what to allow and how to deal with future changes, these choices may overwhelm and overly confuse consumers.

At this time, whitelisting technology may be best suited for parental control functions until technological innovations allow for easier set up and administration geared to consumer use. Setting up parental controls would require parents to make fewer choices and makes more sense, as the question is whether this application or website is appropriate for my child to use, instead of asking the parent to gauge the security risks and vulnerabilities of a particular application or website. As well, there are a number of resources for parents and third party rating lists that have established a level of confidence among parents.[76]

There is innovation in the area of user set up and administrative management of a whitelist. As whitelist technology advances, vendors are beginning to develop the ability to auto-generate whitelists from a computer and to set up ways to make easy changes to the whitelist for patch management and updates. As these mechanisms develop, whitelisting technology may become more appealing in the consumer market as consumers will not have to deal with too much management.[77]

Consumer expectations for computer security

Consumers expect that computer security will not interfere with the functioning of their computers. SignaCert suggests that security should be invisible to the end user. Computer security should be intrinsic and trusted, with safety and trust features already built-in and included in the computer.[78]

HOW MIGHT WHITELISTING AFFECT SOCIETY?

Despite the advantages offered by whitelisting, it is not a perfect system without controversy. The ability to block certain types of applications or content over computer networks can be used in certain ways to influence how citizens can access and use the internet.

[76] PIAC interview with Microsoft Canada.
[77] PIAC interview with CoreTrace.
[78] PIAC interview with SignaCert.

Internet Censorship

One major problem is that of internet censorship. Some governments have mandated internet filtering practices. Jonathan Zittrain and John Palfrey describe internet filtering:

> A filtering system is meant to stop ordinary citizens from accessing some parts of the internet deemed by the state to be too sensitive, for one reason or another. The information blocked ranges from politics to sexuality to culture to religion. As user-generated content has gained in popularity and new tools have made it easier to create and distribute it, filtering regimes have pivoted to stop citizens from publishing undesirable thoughts, images, and sounds, whether for a local or an international audience. The system that facilitates a state's internet filtering can also be configured to enable the state to track citizens' web surfing or to listen in on their conversations, whether lawful or unlawful.[79]

There are a myriad of principal motives and targets of filtering, from political speech to moral motives such as filtering pornography. These motives will not be discussed in great detail here.[80] The principal techniques used for internet filtering include IP blocking, DNS tampering and proxy-based blocking methods.

One recent example of political censorship occurred during the summer of 2009 when the government of Iran banned the use of Facebook[81] and Twitter,[82] for fear that users would propagate messages that might prove damaging to the regime in place.

Whitelisting techniques could make such censorship quite easy and difficult for users to circumvent. Politically sensitive content or dialog could be censored by excluding it from a whitelist used to protect a country's network infrastructure. China institutes the most extensive filtering regime in the world, with blocking occurring at multiple levels of the network and spanning a wide range of topics.[83] Prior to 2009, the Chinese government blacklisted sites that were considered bad or dangerous when they were discovered, using IP blocking to obstruct access to at least three hundred IP addresses. The blocking is done at the international gateway level, affecting all users of the network regardless of ISP.[84] China also filtered URLs by keywords that appear in the domain name or URL path.

---

[79] Jonathan Zittrain & John Palfrey, "Introduction" in Ronald Deibert, *et al.,* eds., *Access Denied: The Practice and Policy of Global Internet Filtering* (2008) The President and Fellows of Harvard College, United States of America 1 to 4 at pp. 1-2.

[80] For an excellent summary of the various motives and targets of internet filtering, see Robert Faris & Nart Villeneuve, "Measuring Global Internet Filtering" in *Access Denied* 5 to 27 at pp. 9-12.

[81] "Iranian government blocks Facebook access" Guardian UK (24 May 2009), online: http://www.guardian.co.uk/world/2009/may/24/facebook-banned-iran.

[82] Ali Sheikholeslami, "Iran Blocks Facebook, Twitter Sites Before Elections" Bloomberg (23 May 2009), online: http://www.bloomberg.com/apps/news?pid=20601087&sid=anh.uW3gNZp4.

[83] *Access Denied, supra* note 79 at p. 3. See also Ben Elgin & Bruce Einhorn, "The Great Firewall of China" Business Week (12 January 2006), online: http://www.businessweek.com/technology/content/jan2006/tc20060112_434051.htm.

[84] *Access Denied, supra* note 79 at p. 14.

In December 2009, the Chinese government went beyond the blacklist of banned websites with new internet regulations that institute a whitelist for approved sites as part of its ongoing anti-pornography campaign.[85] The Ministry of Industry and Information Technology introduced a plan that would require all websites to be registered and only allow Chinese citizens access to sites on the approved whitelist.[86] Rebecca MacKinnon, Hong Kong University's leading analyst on the Chinese internet, suggests that it appears that Beijing's officials want to impact what the internet looks like outside of Chinese borders. By requiring foreign sites to register, MIIT may be able to persuade outsiders to take down content it considers "hostile," "offensive" or "unwholesome".[87] The move to internet whitelisting by the Chinese government would mean that millions of completely innocuous sites would be banned.[88]

States have the sovereign right to carry out internet filtering as they see fit and thus this is a matter of concern for domestic policy. However, whitelisting technologies enable states to carry out internet filtering at a level that is very broad, impacting in particular the freedom of expression, freedom of association and individual privacy. Zittrain and Palfrey sum up the internet's potential force for democracy and productive citizenry as follows:

> The internet is a potential force for democracy by increasing means of citizen participation in the regimes in which they live. The internet is increasingly a way to let sunlight fall upon the actions of those in power – and providing an effective disinfectant in the process. The internet can give a megaphone to activitists or to dissidents who can make their case to the public, either on the record or anonymously or pseudonymously. The internet can help make new networks, within and across cultures, can be an important productivity tool for otherwise unfunded activitists, and can foster the development of new communities built around ideas. The internet can open the information environment to voices other than the organs of the state that have traditionally had a monopoly on the broadcast of important stories and facts, which in turn gives rise to what William Fisher refers to as "semiotic democracy." (footnote omitted) Put another away, the internet can place the control of cultural goods and the making of meaning in the hands of many rather than few. The

[85] Gordon G. Chang, "China Closes Down the Internet" Forbes.com (25 December 2009), online: http://www.forbes.com/2009/12/24/china-internet-blacklist-beijing-opinions-columnists-gordon-g-chang.html.

[86] Chris Nickson, "China creates 'whitelist' for approved sites: Yet more censorship for the Great Firewall" TechRadar UK (22 December 2009), online: http://www.techradar.com/news/internet/china-creates-whitelist-for-approved-sites-659757.

[87] "China Closes Down The Internet" Forbes.com, *supra* note 85.

[88] See Lucy Hornby & Yu Le, "China to Require Internet Domain Name Registration" Reuters (22 December 2009), online: http://ca.reuters.com/article/technologyNews/idCATRE5BL19620091222. Some analysts speculated that the domain name registration could constitute a barrier to trade if Chinese citizens are prevented from accessing legitimate overseas businesses. Other technology commentators suggested that these new rules might not be enforced, as has happened in previous cases when the Chinese government suddenly implemented internet rules without warnings.

> internet is increasingly an effective counterweight to the consolidation in big media, whether the internet is controlled by a few capitalists or the state itself.
>
> The internet also can be a force for economic development, which is most likely the factor holding back some states from filtering the internet more extensively or from imposing outright bans on related technologies. The internet is widely recognized as a tool that is helping to lead to the development of technologically sophisticated, empowered middle classes. Entrepreneurship in the information technology sector can lead to innovation, the growth of new firms and more jobs.
>
> This critique of internet filtering boils down to a belief in the value of a relatively open information environment because of the likelihood that it can lead to a beneficial combination of greater access to information, more transparency, better governance, and faster economic growth. The internet, in this sense, is a generative network in human terms. In the hands of the populace at large, the internet can give rise to a more empowered, productive citizenry.[89]

Net neutrality and internet freedom

Whitelisting technology could be employed by ISPs or network providers such that only certain content or applications are allowed to travel over their networks. The technology already exists today to stop some applications from operating over broadband or wireless networks. Companies such as Ellacoya and Sandvine produce devices that examine broadband internet traffic and can block some applications, such as peer-to-peer filesharing. Others, such as Nokia, produce wireless network equipment that can block other types of applications such as voice over IP telephony programs like Skype. On the flipside, companies such as Juniper Networks develop technology to optimize the performance of preferred applications. Currently, none of the Canada's largest internet service providers use whitelisting to regulate content or filter retail customer internet connections.[90]

Canada's largest ISPs launched Project Cleanfeed Canada in November 2006 in partnership with www.cybertip.ca, the nation's child sexual exploitation tipline. The project is intended to protect ISP customers "from inadvertently visiting foreign websites that contain images of children being sexually abused and that are beyond the jurisdiction of Canadian legal authorities." Complaints to cybertip.ca from Canadians about images found online are assessed by analysts who may forward potentially illegal material to the appropriate foreign jurisdiction. If a URL is approved for blocking by two analysts, it may be added to the Cleanfeed Canada distribution lists. Each of the participating ISPs voluntarily blocks this list without knowledge of the sites it contains.

---

[89] Jonathan Zittrain & John Palfrey, "Internet Filtering: The Politics and Mechanisms of Control" in *Access Denied*, *supra* note 79, 29 to 56 at pp. 50-51.
[90] PIAC interviews with Rogers, TELUS, Bell Canada.

Blocked sites fail to load but attempts to access them are not monitored and users are not tracked.

Whitelisting can also be a useful tool for larger organizations to avoid legal problems regarding copyright infringement. Users who attempt to install applications that may facilitate copyright infringement (such as peer-to-peer software) or applications with expired licenses will be unable to do so. This may be useful for an organization, which could face a software audit, the result of which could include the risk of a lawsuit alleging copyright infringement or paying thousands of dollars in license fees for applications installed without a proper license.

Jonathan Zittrain describes the history of the PC as an example of a generative platform, which invites contributions from anyone who can make them. The recurrent pattern ensues:

> These contributions start among amateurs, who participate more for fun and whimsy than for profit. Their work, while previously unnoticed in the mainstream, begins to catch on and the power of the market kicks in to regularize their innovations and deploy them in markets far larger than the amateurs' domains. Finally, the generative features that invite contribution and that worked so well to propel the first stage of innovation begin to invite trouble and reconsideration, as the power of openness to third-party contribution destabilizes its first set of gains.[91]

Creating a "cleaner" version of the internet

Australia has recently discussed mandating internet filtering on the backbone of the country's network. Discussions are still underway, however most recently, the government backed down from its plan for a filtered internet. Australian software vendor, the Cyber Guardian, has created software that uses a "whitelist" as a guide to what websites children are allowed to access. Parents control the settings and can restrict access to any application, browser and downloads on a computer. Time limits on internet access can also be applied. As Cyber Guardian CEO Max Thomas boasts, "[w]e are creating a new version of the internet which is cleaner. … We host all the whitelisted URLs on our servers and protect that list."[92]

---

[91] Jonathan Zittrain, *The Future of the Internet and How To Stop It* (CREDITS) at p. 18.

[92] Spandas Lui, "Software vendor: Whitelist clean-feed better than blacklist filter: The Cyber Guardian claims to offer 'cleaner' internet access for children" ARN Net (18 May 2010), online: http://www.arnnet.com/au/article/346881/software_vendor_whitelist_clean-feed_better_than_blacklist_filter/.

RECOMMENDATIONS

Further study of application whitelisting in the wireless sector needed

Applications are currently certified for mobile phones, suggesting that the whitelisting model is used for application deployment in the wireless sector. The number of applications developed for mobile platforms are relatively small compared to the scale of applications and software developed for the internet. Phone developers heavily regulate the deployment of mobile applications. This is a walled garden model: consumers are free to choose applications for their phone as long as they are on the approved list. This issue is not a focus of this report, however, the process of approving applications for smartphones is controversial and further research should be explored to examine the anti-competitive and censorship implications of the practice.

Government leadership in cyber security

In December 2009, the US Government announced that Howard Schmidt was appointed to the Executive Office of the President of the United States to serve as the Cyber-Security Coordinator of the Obama Administration.[93] Commonly known as the "Cyber security Czar", Schmidt has the responsibility of orchestrating the many cyber security activities across the government and serve as an important piece of the President's National Security Staff. In March 2010, the United States government announced a $40 billion US Comprehensive National Cyber security Initiative, a plan outlining the powers of the government and how it will use the powers in the event of an emergency. This is an effort to combat potential cyber-attacks from foreign and domestic hackers due to fears of growing cyber-terrorism.

The federal government's speech from the throne in March 2010 promised to work with provinces, territories and the private sector to implement a cyber-security strategy to protect Canada's digital infrastructure.[94] Government officials have said that they are working to develop a framework to deal with cyber-attacks.[95] It appears that such a framework would be focused on cyber-attacks targeting underlying infrastructure such as banking and communications or sensitive documents such as national security data. On October 3rd, 2010, the Government of Canada launched Canada's Cyber Security Strategy.[96] The Strategy will invest in securing Government of Canada systems and partnering with other governments and with industry to ensure the safety of vital cyber systems outside the federal government. The 2010 budget allocated $90 million over five years and $18 million in ongoing funding for Canada's Cyber Security Strategy. This is an important step in government leadership on cyber security matters.

---

[93] The White House Blog, "Introducing the New Cybersecurity Coordinator" (22 December 2009), online: http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator.
[94] Speech from the Throne (3 March 2010), online: http://www.speech.gc.ca/eng/media.asp?id=1388.
[95] "Risk of cyber-attacks growing: CSIS memo" CBC News (18 May 2010) online: http://www.cbc.ca/canada/story/2010/05/17/cyber-security-hack-csis.html.
[96] Government of Canada "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada" 3 October 2010, online: http://www.publicsafety.gc.ca/prg/em/cbr/_fl/ccss-scc-eng.pdf.

Online safety contributes to the economy by making Canada a safer place to work, live and to do business. Greater government leadership on cyber security is needed not only to protect critical infrastructure but also to help consumers deal with online safety challenges.

Consumer education

The whitelisting approach needs more public awareness and consumer education before consumers will adopt it. Much of this public awareness will likely be taken on by individual vendors and internet service providers that begin to incorporate whitelisting techniques into their computer protection solutions.

Consumer education for the unsophisticated computer user is needed so consumers do not blindly trust operating systems or anti-virus suites that are provided free of charge to provide full protection for their home computer. If consumers are to understand how to deploy and use layered defenses, increased consumer awareness is needed. Consumers need comprehensible information on how to set up and manage a whitelist.

Some believe that a whitelist model may prompt consumers to become more responsible in the software they deploy: "… when you turn the situation on its head, and make individuals responsible for the decision to allow software that is 'new and unknown' to run or not, they begin to behave more responsibly. No matter how technically ignorant a user is, a user normally knows or can easily get to know what is and is not likely to be 'bad'. Users know the context in which they are using their software."[97]

The burden of educating users about security risks has typically fallen to security vendors through marketing materials for their products. Governments also provide some basic consumer education information. The Government of Canada's Cyber Security Strategy promises to "increase Canadians' awareness of common online crimes and [to] promote safe cyber security practices through the use of web sites, creative materials and outreach efforts."[98] Efforts at consumer education should focus on tools available to consumers to protect computer systems and how to best deploy and combine these tools in the face of cyber threats.[99] For example, Public Safety Canada provides basic cyber security information for Canadians, however does not provide more technical information about how to best utilize defenses such as firewalls and anti-virus and anti-spyware software to maximize effectiveness.[100]

---

[97] Robin Bloor, "Anti-Virus is Dead" *supra* note 13 at p. 13.
[98] *Supra* note 96 at pp. 8 and 13.
[99] Canada's Cyber Security Strategy on p. 8 suggests that Canadians must become aware of the tools to recognize and avoid threats. On p. 13, the Strategy suggests basic cyber security practices such as frequently changing passwords, updating antivirus protection and using only protected wireless networks but does not suggest how users could employ other defense layers.
[100] Public Safety Canada, "Protect your computer, your information, your family and yourself" online: http://www.publicsafety.gc.ca/prg/em/cbr/prtct-pc-eng.aspx#a1.

CONCLUSION

In our study of whitelisting, PIAC found three types of whitelisting solutions. Application whitelisting only allows approved applications on the whitelist to be installed on the computer or network. Application whitelisting is offered by pure-play vendors and by security vendors as part of their holistic security solutions. Email whitelisting defines a list of "safe" senders and recipients to control spam and whitelisting in this context can enhance the deliverability of email. Finally, and less commonly used, whitelisting can be used for managing internet browsing and traffic. This could be useful for parents looking to control the websites their children can surf or by internet service providers who may want to give consumers the ability to prioritize certain types of internet traffic, such as video streaming or gaming applications.

PIAC found whitelisting to have advantages for cyber security, such as preventative protection against zero day attacks. Whitelisting lends itself well to deployment in the enterprise environment, particularly closed environments where network resources and assets need to be protected. However, whitelisting is not a holistic cyber security solution and is particularly ineffective at dealing with grey areas such as spyware and adware. As well, a centralized whitelist can slow efficiency and stifle innovation. Whitelisting is best used as one defense in a holistic approach using layered defenses for cyber security. At the moment, whitelisting technology is not efficient for consumers because it requires a level of technical sophistication and time to set up and manage that most consumers do not have.

Whitelisting is a pure form of internet control used to control and manage applications, emails or internet traffic. Whitelisting could be used by governments or ISPs to completely control the internet network either for censorship or to restrict consumer internet freedoms. Deployment of whitelisting in this manner would compromise the historical values of the internet such as openness and network neutrality and stifle its generative qualities to the detriment of the public interest.

As whitelisting continues to develop in the enterprise space, pure-play vendors and holistic security vendors will likely look to innovate for deployment in the consumer space. The successful adoption of whitelisting will depend on innovation that makes it easier for consumers to implement and administer whitelisting. Consumer education about cyber security will help consumers understand the benefits that whitelisting has to offer and how to properly use whitelisting in conjunction with other mechanisms such as blacklisting and firewalls. As well, greater government leadership in cyber security is needed to protect critical infrastructure and help consumers deal with online safety challenges.

APPENDIX A – Stakeholders Interviewed

PIAC thanks the following stakeholders for their cooperation with this project and their time and insight.

Anti-Spyware Coalition (ASC)

Bell Canada

Berkman Center for Internet, Stop Badware Project

Bit9

Center for Democracy & Technology (CDT)

Coalition Against Unsolicited Commercial Email (CAUCE)

CoreTrace Corporation

Faronics

Google Canada

Information Technology Association of Canada (ITAC)

Immunet Corporation

Industry Canada Electronic Commerce Branch

Juniper Networks

Microsoft Canada

Return Path Inc.

Rogers Communications Inc.

Savant Protection

SignaCert, Inc.

Symantec

TELUS Communications Company