



โปรแกรมป้องกันไวรัส (Webroot) บนเครื่องคอมพิวเตอร์

เวอร์ชั้น 2.0

สารบัญ

•) 1	ไระวั	ติ	หน้า	3
•) f	າວາມ	ต้องการของระบบ	หน้า	3
•) }	าน้ำห	หลักโปรแกรมป้องกันไวรัส (Webroot) บนเครื่องคอมพิวเตอร์	หน้า	5
	0	สถา	นะการทำงาน	หน้า	6
	0	Stay	v informed Join the discussion	หน้า	7
	0	Adv	vanced settings	หน้า	7
		•	Install settings	หน้า	7
		•	Scheduler	หน้า	8
		•	System Optimizer	หน้า	9
		•	Scan Settings	หน้า	10
		•	Firwall	หน้า	11
		•	Access Control	หน้า	12
		•	Proxy	หน้า	13
		•	Heuristics	หน้า	14
		•	Import / Export	หน้า	14
		•	System Optimizer	หน้า	15
		•	Secure Erase	หน้า	15
	0	PC	Security	หน้า	16
		•	Scan & Shields	หน้า	16
		•	Quarantine	หน้า	18
		•	Block / Allow File	หน้า	19
	0	Ider	tity Protection	หน้า	20
		•	Online Protection	หน้า	20
		•	Application Protection	หน้า	21
	0	Util	ities	หน้า	21
		•	Antimalware Tools	หน้า	22
		•	Reports	หน้า	23
		•	System Control	หน้า	25
		•	System Optimizer	หน้า	27
	0	My	Account	หน้า	28
	0	Key	rcode	หน้า	29
	0	Abo	but SecureAnywhere	หน้า	29
	0	Sup	port / Community	หน้า	29

คู่มือการใช้งานโปรแกรมป้องกันไวรัส (Webroot) บนเครื่องคอมพิวเตอร์ เวอร์ชั่น 2.0

Webroot SecureAnywhere[®]

- ก่อตั้ง ปี 1997 สำนักงานใหญ่อยู่ที่สหรัฐอเมริกา
- สำนักงาน อยู่ที่อเมริกา ยุโรปและเอเชีย
- ผลงานที่ดำเนินการผ่านระบบ Cloud Service ประกอบด้วย Endpoint, Web และ Mobile security
- ได้รับรางวัล Winning SaaS 2007 Award
- ใด้รับรางวัล Winning Webroot SecureAnywhere Endpoint Protection Award
- ได้รับรางวัล Won IT Security Innovation & Product Excellence Awards
- มีผู้ใช้งานและพันธมิตรทั้งหมดมากกว่า 30 ล้าน
- เทคโนโลยีของ Webroot ที่มี Partner ต่างๆ นำไปใช้งาน



<u>ความต้องการของระบบ</u>

Management Portal Access:

- Internet Explorer[®] version 8 and newer
- Mozilla[®] Firefox[®] version 3.6 and newer
- Chrome 11 and newer
- Safari 5 and newer
- Opera 11 and newer

Supported PC Platforms:

- Windows 8, 8.1, 32 and 64-bit
- Windows 7, 32 and 64-bit
- Windows Vista[®], 32 and 64-bit
- Windows[®] XP Service Pack 2 and 3, 32 and 64-bit

- Windows XP Embedded
- Mac OS X v.10.10 "Yosemite"
- Mac OS X v.10.9 "Mavericks"
- Mac OS X v.10.8 "Mountain Lion"
- Mac OS[®] X v.10.7 "Lion"

Supported Server Platforms:

- Windows Server 2012 Standard, R2
- Windows Server 2008 R2 Foundation, Standard, Enterprise
- Windows Server 2003 Standard, Enterprise, Service Pack2, 32 and 64-bit
- Windows Small Business Server 2008, 2011, 2012
- Windows Server Core 2003, 2008, 2012
- Windows Server 2003 R2 for Embedded Systems
- Windows Embedded Standard 2009 SP2
- Windows XP Embedded SP1, Embedded Standard 2009 SP3
- Windows Embedded for POS Version 1.0

Supported Virtual Server Platforms:

- VMware vSphere 5.5 and older (ESX/ESXi 5.5 and older), Workstation 9.0 and older, Server 2.0 and older
- Citrix XenDesktop 5; XenServer 5.6 and older; XenApp 6.5 and older
- Microsoft Hyper-V Server 2008, 2008 R2, 2012 and 2012 R2
- Virtual Box

SecureAnywher	e.		3. 🛶 🗱 Adv	? _ X
Protected + 1.			🥺 PC Security 🔶	4. #
SecureAnywhere is protecting your computer. No active threats have been detected.	Last scan Last scan duration Next scan Total scans Threats removed	9 minutes ago 2m 8s Starts in 23 hours 86 11	Realtime Shield Web Shield Firewall	On On On
Stay informed. Join the discussion. For security news, produces the security news of the secu	2. uct questions, and exp community.	5. 7. bert advice,	 Identity Protection Utilities H My Account Support / Community 	8.

หน้าหลักโปรแกรมป้องกันไวรัส (Webroot) บนเครื่องคอมพิวเตอร์

ภาพแสดงหน้า<mark>จ</mark>อหลักโปรแกรมป้องกันไวรัส (Webroot)

หน้าจอหลักมีเมนูที่ใช้กวบคุมการทำงานดังรายการต่อไปนี้

- 1. สถานะการทำงาน
- 2. Stay informed Join the discussion
- 3. Advanced settings
- 4. PC Security
- 5. Identity Protection
- 6. Utilities
- 7. My Account
- 8. Support / Community

1. สถานะการทำงาน โปรแกรม แสดงสถานะการทำงานของ โปรแกรมป้องกันไวรัส (Webroot

6

secure anywhere) ซึ่งมีการแสดงรายละเอียดดังนี้

Protected 1.1			
SecureAnywhere is protecting your	Last scan	18 hours ago	
computer. No active threats have	Last scan duration	1m 45s	
	Next scan	Starts in 10 hours	
Scan My Computer	Total scans	20	
Scall Ply computer	Threats removed	4	
 1.1. ส่วนที่แสดงสถานการณ์ทำงานมี 2 ส่ 	้ เ่วน ได้แก่	Pro-	
 1.1. ส่วนที่แสดงสถานการณ์ทำงานมี 2 ส่ O Protected โปรแกรมกำลังทำงาน O Scanning โปรแกรมอยู่ระหว่างส 1.2. เมนู Scan My Computer ใช้กรณีที่ด้อง 	ร่วน ได้แก่ แกนคอมพิวเตอร์ องการให้โปรแกรมทำศ	าารสแกนเครื่องคอมพิวเต	ອຸຊຸ
 1.1. ส่วนที่แสดงสถานการณ์ทำงานมี 2 ส่ O Protected โปรแกรมกำลังทำงาน O Scanning โปรแกรมอยู่ระหว่างส 1.2. เมนู Scan My Computer ใช้กรณีที่ต้อง 	ร่วน ได้แก่ แกนคอมพิวเตอร์ องการให้โปรแกรมทำก	าารสแกนเครื่องคอมพิวเศ	อร์
 1.1. ส่วนที่แสดงสถานการณ์ทำงานมี 2 ส่ O Protected โปรแกรมกำลังทำงาน O Scanning โปรแกรมอยู่ระหว่างส 1.2. เมนู Scan My Computer ใช้กรณีที่ด้อง 	ร่วน ได้แก่ แถนคอมพิวเตอร์ องการให้โปรแกรมทำศ ? - × 1.2.1 เมื่อ	การสแกนเครื่องกอมพิวเห ทำการคลิกปุ่ม Scan My	อร์
 1.1. ส่วนที่แสดงสถานการณ์ทำงานมี 2 ส่ O Protected โปรแกรมกำลังทำงาน O Scanning โปรแกรมอยู่ระหว่างส 1.2. เมนู Scan My Computer ใช้กรณีที่ต้อง 	ห่วน ได้แก่ แกนคอมพิวเตอร์ องการให้โปรแกรมทำก 1.2.1 เมื่อ Computer โ	การสแกนเครื่องคอมพิวเต ทำการคลิกปุ่ม Scan My ปรแกรมจะทำการสแกน	อร์ ครื่อ
 1.1. ส่วนที่แสดงสถานการณ์ทำงานมี 2 ส่ O Protected โปรแกรมกำลังทำงาน O Scanning โปรแกรมอยู่ระหว่างส 1.2. เมนู Scan My Computer ใช้กรณีที่ต้อง 	ห่วน ได้แก่ แถนคอมพิวเตอร์ องการให้โปรแกรมทำศ 1.2.1 เมื่อ Computer โ ดอมพิวเตอร์	การสแกนเครื่องคอมพิวเต ทำการคลิกปุ่ม Scan My ปรแกรมจะทำการสแกน โดยจะแสดงสถานะระ1	อร์ ครื่อ ว่าง

Cancel Scan 🔀



No threats found			
Files scanned	8,910	Threats detected	
Processes		Time elapsed	14 seconds
Total scans		Last infected scan	Tue 07-04-2015 20:49:31
Total threats removed		Active threats	

เมื่อโปรแกรมทำงานเสร็จเรียบร้อย 1.2.2 ์โปรแกรมจะแสดงผลการทำงานทั้งนี้ ผู้ใช้งานสามารถทำการบันทึก Log โดยคลิก ปุ่ม Save Scan log หรือถ้ำต้องการสแกนอีก ครั้งให้คลิกปุ่ม Scan Again

1.3. แสดงผลการทำงานของโปรแกรมโดยมีรายละเอียดดังนี้

- จำนวนชั่วโมงที่โปรแกรมทำการสแกนล่าสุด O Last scan
- <u>จำนวนระยะเวลาที่โปรแกรมทำการสแกนล่าสุด</u> O Last scan duration
- O Next scan
- Total scans \cap
- 0 Threats removed

<mark>เวลาที่โปรแกรมจะทำกา</mark>รสแกนครั้งต่อไป รวมจำนวนที่โปรแกรมทำการสแกนทั้งหมด <mark>้จำ</mark>นวนที่โปรแกรมได้ทำการลบไฟล์ที่เป็นอั<mark>น</mark>ตราย ต่อเครื่องคอมพิวเตอร์

2. Stay informed Join the discussion เว็บไซต์เพื่อแจ้งปัญหาและแลกเปลี่ยนความรู้รวมไปถึง ปัญหาที่เกิดขึ้น

3. Advanced setting เมนูสำหรับกำหนดการตั้งค่าโปรแกรมป้องกันไวรัส (Webroot Secure Anywhere) โดยมีแถบเมนูดังนี้

Settings - Currently being managed by the Web Console						
Install Settings	Automatically download and apply updates					
Scheduler	Show a shortcut on the desktop		1			
Scan Settings	 Show a system tray icon Show a status notification screen on bootup 					
Shields						
Firewall	Show a Start Menu shortcut					
Access Control	Allow SecureAnywhere to be shut down manually					
Proxy						
Heuristics						
Import / Export						
System Optimizer						
Secure Erase						
Reset to defaults	Save Cancel					

Install settings การตั้งค่าการติดตั้งโปรแกรมโดยมีรายละเอียดดังนี้

คู่มือการใช้งานโปรแกรมป้องกันไวรัส (Webroot) บนเครื่องคอมพิวเตอร์ เวอร์ชั่น 2.0

O A	utomatically	download	and	apply	updates
-----	--------------	----------	-----	-------	---------

- O Show a shortcut on the desktop
- O Show a system tray icon
- O Show a status notification screen on bootup
- O Show a Start Menu shortcut
- O Allow SecureAnywhere to be shut down manually

อัพเดทและดาวน์โหลดอัตโนมัติ แสดงไอคอนโปรแกรมที่หน้าจอหลัก แสดงไอคอนโปรแกรมที่แถบเมนู แสดงสถานการณ์แจ้งเตือนเมื่อ คอมพิวเตอร์เริ่มต้นเครื่องใหม่ แสดงโปรแกรมที่ Start menu อนุญาตให้ปัดการทำงานของ โปรแกรมด้วยตัวเอง

• Scheduler การกำหนดตารางเวลาในการสแกนและการเพิ่มประสิทธิภาพในการทำงานโดยมี รายละเอียดดังนี้

Settings - Currently being	managed by the Web	Console	x	
Install Settings	Scan Schedule Sy	stem Optimizer		
Scheduler				
Scan Settings				
Shields	Scan Frequency:	Gcan every day 💌		
Firewall	Time:	Gcan at 10:00 am when resources are available ▼		
Access Control	Scan on bootup if	f the computer is off at the scheduled time		
Proxy	Hide the scan pro	gress window		
Heuristics	Do not perform s	cheduled scans when on battery power		
Import / Export	Do not perform s Randomize the tir	cheduled scans when a full screen application or game is open		
System Optimizer	Perform a schedu	led Quick Scan instead of a Deep Scan		
Secure Erase				
Reset to defaults	٩	Save Cancel		
แถบเมนู Scan schedul	e			
O Enable Scheduled S	Scans	เปิดการใช้งานการสแกนอัตโนมัติ		
O Scan Frequency		กำหนดความถี่ในการสแกน		
O Time		กำหนดเวลาของการสแกน		
O Scan on bootup if the	O Scan on bootup if the computer is off ทำการสแกนเมื่อคอมพิวเตอร์ถูกปิด			
at the scheduled time ในเวลาที่กำหนดให้โปรแกรมทำงาน				

0	Hide the scan progress window	ซ่อนหน้าต่างการทำงาน
0	Do not perform scheduled scans	กำหนดห้ามทำการสแกนเมื่อ
	when on battery power	คอมพิวเตอร์ใช้พลังงานจากแบตเตอรี่
0	Do not perform scheduled scans when a full screen	กำหนดห้ามทำการสแกนเมื่อ
	application or game is open	โปรแกรมอื่นๆ หรือ เกมส์ทำงาน
0	Randomize the time of scheduled scans up to one hour	กำหนดให้โปรแกรมสุ่มการสแกน
	for faster scanning	ภายใน 1 ชม

9

O Perform a scheduled Quick Scan instead of a Deep Scan กำหนดให้ทำการสแกนเชิงลึก

แถบเมนู System Optimizer

Settings - Currently being	managed by the Web Console	x	
Install Settings	Scan Schedule System Ontimi	izer	
Scheduler			
Scan Settings	Enable scheduled optimization		
Shields	 Optimize only on the following day 	'S:	
Firewall	Monday	Thursday Sunday	
Access Control	Uesday Wednesday	Friday Saturday	
Proxy			
Heuristics	Optimize at specific time of day:	2:00 pm	
Import / Export		hours	
System Optimizer	• opumze every.	nou s	
Secure Erase	Run on bootup if the system was off	at the scheduled time	
Reset to defaults	Save	Cancel	
O Enable scheduled o	ptimization	<mark>เปิดการเพิ่มประสิทธิภาพข</mark> องโปรแกรม	
		โดยอัต โนมัติ	
O Optimize only on the	ne following days	<mark>กำหนดวันที่ต้องการ</mark> ให้โปรแกรมทำงาน	
O Optimize at specifie	c time of day	กำหนดเวลาที่ต้องการให้โปรแกรมทำงาน	
O Optimize every		กำหนดช่วงระยะเวลาที่ต้องการให้	
		โปรแกรมทำงานต่อชั่วโมง	
• Run on bootup if th	e system was off	กำหนดให้โปรแกรมทำงานเมื่อคอมพิวเตอร์	
at the scheduled tim	2	เริ่มทำงานถ้าคอนพิวเตอร์ ไม่เปิดใช้งาน	
at the scheduled thi		4 °	
		ตามเวลาทกาหนด	

Scan Settings การตั้งค่าการสแกนโดยมีรายละเอียดดังนี้

Settings - Currently being managed by the Web Console						
Install Settings Scheduler Scan Settings Shields Firewall Access Control Proxy Heuristics Import / Export System Optimizer	 Enable rootkit detection Scan the Master Boot Record Scan archived files Detect Potentially Unwanted Applications Enable right-click scanning in Windows Explorer 					
Secure Erase Reset to defaults	Save Cancel					

0	Enable rootkit detection	กำหนดการเปิดใช้งานการตรวจสอบ Rookit
0	Scan the Master Boot Record	กำหนดให้ทำการสแกน Master boot Record
0	Scan archived files	กำหนดให้ทำการสแกนไฟล์ที่จัดเก็บ
0	Detect Potentially Unwanted Applications	กำหนดให้ทำการตรวจส <mark>อ</mark> บโปรแกรมที่อาจเป็น
		ภัยคุกคามเครื่องคอมพิวเตอร์
0	Enable right-click scanning in Windows Explorer	กำหนดให้โปรแกรมทำงาน เมื่อมีการคลิกขวา
		ที่เมนูของ Windows Explorer

 Firewall กำหนดการตั้งค่า Firewall มีรายละเอียดการตั้งค่าดังนี้ 					
Settings - Currently being managed by the Web Console					
Install Settings	Detect and block malicious websites				
Scheduler	Show safety ratings when using search engines				
Scan Settings	 Automatically protect newly installed browsers 				
Shields	Enable realtime anti-phishing				
Firewall					
Access Control					
Proxy					
Heuristics					
Import / Export					
System Optimizer					
Secure Erase					
Reset to defaults	Save Cancel				

 Access Control การควบคุมการเข้าถึงคอมพิวเตอร์สามารถกำหนดสิทธิ์ให้ใช้หรือปฏิเสธ การเข้าถึงฟังก์ชั่นบางอย่าง การควบคุมการเข้าถึงเหล่านี้ยังปกป้องคอมพิวเตอร์ของคุณจากโปรแกรม ภัยคุกคามที่พยายามจะเปลี่ยนการตั้งค่าในโปรแกรมโดยมีรายละเอียดดังนี้

Settings - Currently bein	g managed by the Web Console	x
Install Settings	Enable Password Protection	
Scheduler	Password:	
Scan Settings	Repeat Password:	
Shields		
Firewall	 Protect against process termination 	
Access Control	Protect against process tampering	
Proxy	 Require the completion of a CAPTCHA when changing critical features Require the completion of a CAPTCHA when changing any configuration option 	
Heuristics	 Allow users to remove threats without entering a password 	
Import / Export	Allow non-administrative users to modify configuration options	
System Optimizer	Allow uninstallation by non-administrative users	
Secure Erase	Allow access to advanced reatures by non-administrative users Hide the keycode on screen	
Reset to defaults	Save Cancel	

- O Enable Password Protection
- O Password:
- O Repeat Password
- O Protect against process termination
- O Protect against process tampering
- Require the completion of a CAPTCHA when changing critical features
- Require the completion of a CAPTCHA when changing any configuration option
- Allow users to remove threats without entering a password
- Allow non-administrative users to modify configuration options

เปิดใช้งานการป้องกันด้วยรหัสผ่าน กำหนดรหัสผ่าน ทำการกรอกรหัสผ่านที่กำหนดอีกครั้ง กำหนดห้ามผู้ใช้งานทำการยกเลิก กระบวนการทำงานใดๆ ของโปรแกรม กำหนดห้ามผู้ใช้งานทำการปลอมแปลง กระบวนการทำงานใดๆ ของโปรแกรม กำหนดให้กรอก CAPTCHA (การยืนยันตัวตน) เมื่อทำการเปลี่ยนแปลงคุณลักษณะที่สำคัญ กำหนดให้มีกรอก CAPTCHA (การยืนยันตัวตน) เมื่อมีการเปลี่ยนการตั้งก่าต่างๆ อนุญาตให้ผู้ใช้งานทำการย้ายไฟล์ โดยไม่ต้องใส่รหัสผ่าน อนุญาตให้ผู้ใช้งานที่ไม่ใช่ผู้ดูแลระบบ เปลี่ยนแปลงการตั้งก่าต่างๆ ได้

- O Allow uninstallation by non administrative users อนุญาตให้ผู้ใช้งานที่ไม่ใช่ผู้ดูแลระบบ
- Allow access to advanced features by non-administrative users
- O Hide the kekycode on screen

อนุญาต เหผู เชงานท เม เชผูดูแลระบบ ถอนการติดตั้งโปรแกรมได้ อนุญาตให้ผู้ใช้งานที่ไม่ใช่ผู้ดูแลระบบ เข้าใช้งานคุณลักษณะขั้นสูงได้ กำหนดให้ซ่อน Keycode จากหน้าจอ

 Proxy มีรายละเอียุคการตั้งค่าดังต่ 	iอไปนี้	
Settings - Currently being managed by the	e Web Console	×
Install Settings Proxy Type Scheduler Authentication Meth Scan Settings Host Shields Port	Do not use a proxy server od Any authentication	
Firewall Username Access Control Password Prove		
Heuristics Import / Export System Optimizer Secure Erase		
Reset to defaults	Save Cancel]
O Proxy TypeO Authentication Method	เลือ กำ ห	กชนิดของ Proxy เนดวิธีการตรวจสอบ
O Host	วะบ	ุโฮส
O Port	ระบุ	ุ่พอร์ต
O Username	วะบ	J Username
O Password	រះរ	l Password

Heuristics การตั้งก่าการวิเกราะห์พฤติกรรมการใช้งานของผู้ใช้งาน ซึ่งมีรายละเอียดดังต่อไปนี้



- O Disable heuristics
- O Enable standard heuristics
- O Enable enhanced heuristics based on,

the behavior origin, age, and popularity of files

- O Enable maximum heuristics
- Warn when any new program executes that is not specifically whitelisted
- O Enable Webroot Infrared

กำหนดให้หยุดการวิเกราะห์พฤติกรรมการใช้งาน เปิดใช้งานมาตรฐานการวิเกราะห์พฤติกรรมการใช้งาน เปิดใช้งานการตรวจสอบฐานข้อมูลเพื่อทำการวิเกราะห์ พฤติกรรมการใช้งานที่เพิ่มขึ้นจากเดิม เปิดใช้งานการวิเกราะห์พฤติกรรมขั้นสูงสุด กำหนดให้มีการแจ้งเตือนเมื่อพบการทำงาน ของโปรแกรมที่ไม่ได้รับอนุญาต เปิดการใช้งานฟังก์ชั่น Infrared

14

Import / Export เป็นการถ่ายโอนการตั้งค่าไปยังคอมพิวเตอร์เครื่องอื่นและเป็นการนำเอา

การตั้งค่าจากคอมพิวเตอร์เครื่องอื่นมาคัคลอกใหม่

Settings - Currently bein	g managed by the Web Console	x
Install Settings	SecureAnywhere offers the option to back up your configuration settings in case you	
Scheduler	need to reinstall, or want to transfer the same settings to another computer.	
Scan Settings	You can also import your settings from another computer using this screen.	
Shields		
Firewall		
Access Control		
Proxy		
Heuristics		
Import / Export		
System Optimizer		
Secure Erase		
	Import Export	

 System optimizer สำหรับเลือกข้อมูลที่ต้องการทำความสะอาคเพื่อเพิ่มประสิทธิภาพอย่างใด อย่างหนึ่งในการทำงานของระบบ ทั้งนี้ โปรแกรม (Webroot) จะทำคึงข้อมูลของโปรแกรมต่างๆ ที่ผู้ใช้งานทำการติดตั้งบนเครื่องคอมพิวเตอร์โดยอัตโนมัติ 15

Settings - Currently beir	ng managed by the Web Console	
Install Settings	Select the data you would like desced whereaver Outers Optimizer was either	
Scheduler	on-demand or on a schedule:	
Scan Settings	Clipboard contents	^
Shields	✓ Windows Temporary folder	
Firewall	System Temporary folder	
Access Control	Windows Update Temporary folder	
Proxy	Windows Registry Streams	
Heuristics	Default logon user history	
Tieurisues	Memory dump files	
Import / Export	CD burning storage folder	
System Optimizer	Flash Cookies	
Secure Erase	Recycle Bin	~
Reset to defaults	Save Cancel	

• Secure Erase การเพิ่มประสิทธิภาพในการลบไฟล์ เมื่อผู้ใช้งานได้ทำการลบไฟล์ ซึ่งระบบ จะทำการย้ายไปยังถังรีไซเคิล (Recycle Bin) และผู้ใช้งานสามารถ Restore กลับมาได้ หรือหากทำการ ล้างถังขยะ (Recycle Bin) แต่ข้อมูลจะยังคงอยู่บนฮาร์คดิสจนกว่าจะมีการเขียนทับด้วยข้อมูลอื่นๆ

ทั้งนี้ การตั้งค่า Secure Erase ในการถบไฟล์ จะสามารถกำหนดไว้ที่เมนู Windows Explorer โดย ทาการคลิกขวาเพื่อลบไฟล์อย่าง คุณลักษณะ shredding นี้เป็นวิธีที่สะดวกเพื่อให้แน่ใจว่าไม่มีใคร สามารถ เข้าถึงไฟล์ด้วยเครื่องมือการกู้กืน โดยมีรายละเอียดดังนี้

Settings - Currently bein	g managed by the Web Console	x
Install Settings	Enable Windows Explorer right click secure file erasing	
Scheduler	Control the level of security to apply when removing files. Higher security levels reduce	
Scan Settings	the possibility of recovering data but will require longer to dean.	
Shields	Normal	
Firewall	Clean files using standard file deletion techniques, bypassing the Windows Recycle Bin.	
Access Control		
Proxy		
Heuristics		
Import / Export		
System Optimizer		
Secure Erase		
Reset to defaults	Save Cancel	G

 Enable Windows Explorer right click secure file erasing

เปิดใช้งานการลบไฟล์ด้วยโปรแกรม Webroot เมื่อทำการคลิกขวา

- O ระดับการลบไฟล์แบ่งออกเป็น 3 ระดับดังนี้
 - Normal ระดับปกติ เป็นการลบไฟล์ที่ไม่ได้เขียนไฟล์ทับ
 - Medium ระดับปานกลาง เป็นการลบไฟล์และทำการเขียนไฟล์ทับจำนวน 3 ครั้ง
 - Maximumระดับสูงสุด เป็นการลบไฟล์และทำการเขียนไฟล์ทับจำนวน 7 ครั้ง
- 4. PC security การกำหนดการป้องกันเครื่องคอมพิวเตอร์ของผู้ใช้งาน

	- 246		1111 0011176106611101
Realtime Shield	On	• Web Shield	การป้องกันเว็บไซ <mark>ค์</mark>
Web Shield	On	• Firewall	การทำงานของ Firewall
 Learn More ອ້າລ່າ DC Sequeity (1 	พิ่นเตินใช้ทำการคลิก	*	
 แถบเมนู Scan 	& shields การตั้งค่าก	าารส <mark>แกนแ</mark> ละการป้องกัน	ซึ่งมีรายละเอียคคังต่อไปนี้ ? – ×
SecureA	nvwhere.		Advanced Settings
	- <u>y</u>		A Pavance scange
Scan & Shields Scan 4 1	Quarantine Block/Allov	w Files Shields and Firewall 👍	PC Security
Scan & Shields Scan 4 1 Scan My Comput	Quarantine Block/Allov	w Files Shields and Firewall 👍 Realtime Shield Rootkit Shield	PC Security 2 On On
Scan & Shields Scan 4 1 Scan My Comput Last scan	Quarantine Block/Allov ter 4 hours ago	w Files Shields and Firewall Realtime Shield Rootkit Shield Web Shield	PC Security 2 On On On
Scan & Shields Scan 4 1 Scan My Comput Last scan Last scan duration	Quarantine Block/Allov ter 4 hours ago 2m 58s	w Files Shields and Firewall 4 Realtime Shield Rootkit Shield Web Shield USB Shield	PC Security 2 0n 0n 0n 0n
Scan & Shields Scan 4 1 Scan My Comput Last scan Last scan duration Next scan	Quarantine Block/Allov ter 4 hours ago 2m 58s When idle	w Files Shields and Firewall Realtime Shield Rootkit Shield Web Shield USB Shield Offline Shield	PC Security 2 On On On On On On On On On
Scan & Shields Scan 4 1 Scan My Comput Last scan Last scan Next scan Total scans	Quarantine Block/Allov ter 4 hours ago 2m 58s When idle 83	w Files Shields and Firewall Realtime Shield Rootkit Shield Web Shield USB Shield Offline Shield	PC Security 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Scan & Shields Scan 4 1 Scan My Comput Last scan Last scan duration Next scan Total scans Threats removed Active threats	Quarantine Block/Allov ter 4 hours ago 2m 58s When idle 83 11 0	w Files Shields and Firewall Realtime Shield Rootkit Shield Web Shield USB Shield Offline Shield Firewall	PC Security 2 0n 0n 0n 0n 0n
Scan & Shields Scan 4 1 Scan My Comput Last scan Last scan duration Next scan Total scans Threats removed Active threats	Quarantine Block/Allov ter 4 hours ago 2m 58s When idle 83 11 0	W Files Shields and Firewall Realtime Shield Rootkit Shield Web Shield USB Shield Offline Shield Firewall Wiew Active Connect	PC Security 2 0n 0n 0n 0n 0n 0n
Scan & Shields Scan (1) Scan My Comput Last scan Last scan duration Next scan Total scans Threats removed Active threats Custom Scan	Quarantine Block/Allov ter 4 hours ago 2m 58s When idle 83 11 0	w Files Shields and Firewall Realtime Shield Rootkit Shield Web Shield USB Shield Offline Shield Firewall Wiew Active Connect	PC Security 2 0n 0n 0n 0n 0n 0n 0n 0n 0n
Scan & Shields Scan 4 1 Scan My Comput Last scan Last scan duration Next scan Total scans Threats removed Active threats	Quarantine Block/Allov ter 4 hours ago 2m 58s When idle 83 11 0	W Files Shields and Firewall Realtime Shield Rootkit Shield Web Shield USB Shield Offline Shield Firewall Wiew Active Connect	PC Security
Scan & Shields Scan 4 1 Scan My Compute Last scan Last scan duration Next scan Total scans Threats removed Active threats	Quarantine Block/Allov ter 4 hours ago 2m 58s When idle 83 11 0	w Files Shields and Firewall Realtime Shield Rootkit Shield Web Shield USB Shield Offline Shield Firewall Wew Active Connect	PC Security 2 0 0 0 0 0 0 0 0 0 0 0
Scan & Shields Scan (1) Scan My Compute Last scan Last scan duration Next scan Total scans Threats removed Active threats Custom Scan	Quarantine Block/Allov ter 4 hours ago 2m 58s When idle 83 11 0	W Files Shields and Firewall Realtime Shield Rootkit Shield Web Shield USB Shield Offline Shield Firewall Wew Active Connect	PC Security 2 0 0 0 0 0 0 0 0 0 0 0 0 0
Scan & Shields Scan 4 1 Scan My Comput Last scan Last scan duration Next scan Total scans Threats removed Active threats	Quarantine Block/Allov ter 4 hours ago 2m 58s When idle 83 11 0	W Files Shields and Firewall Realtime Shield Rootkit Shield Web Shield USB Shield Offline Shield Firewall Wew Active Connect	PC Security

1. Scan แสดงรายละเอียดผลการทำงานของโปรแกรม (Webroot)

Scan My Computer การสแกนคอมพิวเตอร์ โดยทันทีตามที่ โปรแกรม ได้กำหนด ไว้

17

 Custom Scan การเลือกไครฟ์และ โฟลเดอร์ที่ผู้ใช้งานต้องการสแกน โดยมีรายละเอียด ดังนี้

	Custom	ized Scan
	\bigcirc Q	ick Surface scan of files in active memory
	⊖ Fu	I Scan all local hard drives
	D	Scan for rootkits, trojans, and other threats (Recommended)
	ο α	stom Scan only the files and folders selected below:
	Files	and folders to scan Add File / Folder Remove
		Start Scan Cancel
0	Quick	การสแกนไฟล์ที่ใช้งานอยู่ในหน่วยความจำอย่างรวคเร็ว
0	Full	การสแกนฮาร์ดดิสก์อย่างเต็มรูปแบบ
0	Deep	การสแกนหา Rootkit, โทรจันและภัยอุกคามอื่น ๆ อย่าง
0	Custom	จำกัดการสแกบไปยังโฟลเดอร์และไฟล์อลิกกำหนดเองป่มอลิกเพิ่มไฟล์ /
Ū	Custom	रा रुग २ ते त रा र भारते
		เพลเคอรบุมและคลก Add เพอเลอก เพลเคอรและ เพลทจะสแกน
0	ปุ่ม Add	File / Folder ท <mark>ำการเพิ่มไฟล์ หรื</mark> อโฟลเคอร์ที่ต้องการสแกน
0	า่ไป Remo	we ทำการลบไฟล์ที่เลือกไว้
J	นึ่ง เวิริแต	
. Shie	lds and Fi	rewall การป้องกันและการตั้งค่าไฟวอลล์
	D 1.1	

 O Realtime Shield
 การป้องกัน Rootkit

 O Rootkit Shield
 การป้องกัน Rootkit

 O Web Shield
 การป้องกันเว็บไซล์

 O USB Shield
 การป้องกัน USB

 O Offline Shield
 การป้องกันแบบออฟไลน์

 O Firewall
 เปิดการใช้งาน Firewall

ปุ่ม View Active Connections ตั้งค่าการเชื่อมของโปรแกรมต่างๆ

comet.e	xe in c:\program file	es\bitcomet					^
plorer.e	ke in c:\windows						
rome.ex	e in c:\program file:	s (x86)\google\a	hrome\application				
pstorede	sktool.exe in c:\pr	ogram files (x86)\baidu security\pc app s	store\4.8.1.6	847		
nbox.ex	e in c:\program file:	s (x86)\i-funbox	devteam				
neshelpe	r.exe in c:\program	m files (x86)\įtur	nes				~
ID L	ocal Address		Remote Address	Туре	State		
88 BS	S-PISSANU: 13990	BS	SS-PISSANU:0	TCP4	Listening		
88 BS	S-PISSANU: 13990			UDP4	Open for 6 hours		
			Close	- 🗠			
• 11	<mark>.ถบเมนู</mark> Quai	rantine ราย	ยการไฟล์ที่พบว่า:	มีความเลื่	ัยง	7-	2 - 3
• II WEBI	ถบเมนู Quar ROOT	rantine 518	ขการไฟล์ที่พบว่า: ro	มีความเลื่	⁽ ยง		2 _ 2
• " veer Seo	เอบเมนู Quai Root CUreAr	rantine ราย iywhei	ขการไฟล์ที่พบว่า: re.	มีความเสื่	(ถา	Advance	?) I Settings
• II WEBR	ถบเมนู Quai Root CUreAr	rantine 578 1YWhe Quarantine	ยการไฟล์ที่พบว่าเ re. Block/Allow Files	มีกวามเลื่	261	X Advanced) I Settings Security
	เอบเมนู Quan ROOT CUTEAr ican & Shields	rantine 518 19Whe Quarantine	ยการไฟล์ที่พบว่าร FC. Block/Allow Files	มีความเสิ่	/ยง	Advanced	2 –) I Settings Security
VEB Sei Quarai	เอบเมนู Quan RODT CUTEAr Scan & Shields Itine	rantine 578 NYWHE Quarantine	ยการไฟล์ที่พบว่าว re. Block/Allow Files	มีกวามเลื่	261	🏶 Advanced PC	l Settings Security
• JI Set Quarai View a	เลบเมนู Quan ROOT CUITEAr Scan & Shields htine nd manage threat	rantine 578 TYWHE Quarantine s detected by	ยการไฟล์ที่พบว่าร /C. Block/Allow Files SecureAnywhere.	มีความเลื่	2613	Advanced	? _ ? !Settings Security
• II Set Quarai View a	เอบเมนู Quan Root CureAr Scan & Shields htine nd manage threat Removed Threat	rantine 518 1YWhe Quarantine s detected by 1	ยการ ไฟล์ที่พบว่าว่ ГС. Block/Allow Files SecureAnywhere.	มีกวามเลื่	281 Date	X Advanced PC	l Settings Security
U U U U U U U U U U U U U U U U U U U	เอบเมนู Quan Root CureAr Scan & Shields Intine Ind manage threat Removed Threat	rantine 511 TYWHE Quarantine Is detected by 1	ยการ ไฟล์ที่พบว่าร่ FC. Block/Allow Files SecureAnywhere.	มี <mark>ความเลื่</mark>	2813 Date	* Advanced PC :	1Settings Security

18

ส่วนที่ 1. รายการไฟล์ที่พบว่ามีความเสี่ยง ส่วนที่ 2. การจัดการไฟล์

2.1 Learn More	ลิงค์เว็บไซต์ข่าวสาร
2.2 Select / Deselect all	การเลือกไฟล์หรือยกเลิกการเลือกไฟล์
2.3 Delete Permanently	การลบไฟล์
2.4 Restore	การคืนค่าไฟล์

แลบ Block / Allow File การป้องกันหรืออนุญาต ไฟล์ที่โปรแกรม (Webroot) ได้ทำการตรวจพบ

			?	
SecureAnywnere.		×,	E Advanced Se	ttings
Scan & Shields Quarantine Block/Allow Files			PC Sec	urity
Block/Allow Files (Advanced)				
Add files which you would like SecureAnywhere to block, allow, or monitor.				
File	Allow	Block	Monitor	
catsrvut.dll in c:\windows\system32	٢	•	•	
		Add File	X Remove	All

0	Allow	ละเว้นไฟล์ระหว่างการสแกนและการป้องกัน
0	Block	ป้องกันไฟล์ออกจากระบบ
0	Monitor	ตรวจสอบโปรแกรมว่าถูกต้องตามกฎหรือเป็นโปรแกรมที่เกี่ยวข้อง
		กับซอฟต์แวร์ที่อาจเป็นอันตรายเพื่อป้องกันหรืออนุญาต
0	ปุ่ม Add File	ทำการเพิ่มไฟล์ที่ต้องการคำเนินการ
0	ปุ่ม Remove All	ทำการลบไฟล์ที่เลือกไว้

5. Identity Protection การป้องกันข้อมูล



การตั้งค่า Identify Protection เพิ่มเติมให้ทำการคลิกเลือก

Online Protection การป้องกันข้อมูลเมื่อคอมพิวเตอร์อยู่ในสถานะออนไลน์แบ่งออกเป็น 2 เมนูดังนี้



- 1. Shields
 - O Identity shields เปิดใช้งานการป้องกัน
 - O Phishing shields

เป็ดใช้งานการป้องกันการโจรกรรมข้อมูล

2. Website Protection แสดงรายละเอียดต่างๆ ที่มีการป้องกัน

แถบเมนู Application protection การป้องกันโปรแกรมต่างๆ โดยสามารถจัดการโปรแกรม
 ให้ทำการป้องกัน, ติดตาม หรืออนุญาตให้ใช้งานโดยไม่มีการติดตาม ซึ่งมีรายละเอียดดังนี้

21

WEBROOT	A 1	? _ X
Secure	Anywhere.	🌣 Advanced Settings
Online Pro	tection Application Protection	Identity Protection
Application Prot	ection	
Protect applicati knowledge.	ons which may encounter your personal data to ensure th	nis information cannot be extracted without your
Application		Protect Allow Deny
mscorrc.dll in c:\	windows\microsoft.net\framework64\v4.0.30319	
		Add Application
O Protect	การติดตามพฤติกรรมการการใช้งา <mark>น</mark> เท	งื่อป้องก [ั] นซอฟต์แวร์ที่อาจเป็นอันตรายได้
O Allow	การอนุญาตให้โปรแกรมที่ถูกเลือกไว้เ	สามารถทำงานได้โดยไม่ต้องมีการตรวจสอบ
O Deny	การใช้งานที่ถูกปฏิเสธไม่สามารถดูหรื	ื่อเก็บข้อมูลที่มีการป้องกันในระบบ แต่อย่างอื
	สามารถทำงานได้ตาม <mark>ป</mark> กติ	
 ปุ่ม Add 	Application เลือกโปรแกรมที่ต้องกา	รให้ Webroot คำเนินการป้องกันไฟล์
Utilities 1170		
C CALLERY OUDING	12 1862,19891122,671111 19922211111	



 แถบ Antimalware Tools การจัดการเกี่ยวกับซอฟต์แวร์ที่อาจเป็นอันตรายต่อคอมพิวเตอร์ ซึ่งมีรายละเอียดดังนี้ 22

Antimalware Tools Reports	System Control System Optimizer	Utili
pols 4 1	Manual Threat Removal 4 2	Removal Script 4 3
Reset desktop wallpaper Reset screensaver Set system policies to defaults Reboot into Safe Mode Perform an immediate system reboot	You can remove files using SecureAnywhere and automatically remove associated registry entries.	If a Webroot researcher has instructed you to execute a Removal Script, select the provided script to begin.

ส่วนที่ 1 Tools

0	Reset desktop	<mark>ตั้</mark> งค่าหน้าจอหลักใหม่
0	Reset screensaver	ตั้งก่า Screen Saver ใหม่
0	Set system policies to defaults	<mark>ตั้งก่าข้อกำหนด (Policy) ของระบบกอ</mark> มพิวเตอร์
		เป็นก่าเดิม
0	Reboot into Safe Mode	เริ่มระบบใหม่ใน Safe mode
0	Perform an immediate system reboot	<mark>คำเนินการเริ่มระบบใหม่</mark> โดยทันที

ส่วนที่ 2 Manual threat Remove สามารถเลือกลบไฟล์ที่มีความเสี่ยงรวมไปถึงค่ารีจิสทรีที่เกี่ยวข้อง ส่วนที่ 3 Remove Script สามารถเลือกลบสคริปต์และกลับไปสคิปต์ค่าเริ่มต้น



23

ส่วนที่ 1 Report รายงานการคำเนินการ

- Scan Log การบันทึก Log ที่โปรแกรม (Webroot) ได้ทำการสแกน
 - O Save Scan Log (ทำการบันทึก Log ที่สแกน)
- Threat Log การบันทึกการลบไฟล์ที่อาจเป็นอันตรายจากระบบตั้งแต่ลงโปรแกรม
 - O Save Threat Log (ทำการบันทึก Log ที่ลบไฟล์ที่อาจเป็นอันตราย)

ส่วนที่ 2 Event Viewers แสดงเหตุการณ์ต่างๆ

- Protection Statistics แสดงรายละเอียดที่โปรแกรม (Webroot) ได้ทำการป้องกัน
 - O View Statistics แสดงสถิติการดำเนินการ

Protection Statistics			x
Protection Statistics allow you to v an individual line to view additional	iew individual events taking place a information on the granular change	cross the system. You can double click on s taking place.	
Inspected System Events	Session	Total	
File Events	1,729,113	61,489,715	
Registry Events	34, 142, 718	1,463,671,546	
Code Events	25,929	2,139,586	
Network/Internet Events	142,600	10,441,122	
Process/Thread Events	7,563,656	202,136,540	
Window/GDI Events	47,187,348,232	61,761,348,144	
Input Events	2,777	82,194	
Total Events	47,230,955,025	63,501,308,847	
SecureAnywhere has used 0.	07% of your CPU since installation and 0	.005% disk space. Average scan time is 4.9 minutes.	
	Reset	ncel	

- Execution History แสดงประวัติการเข้าดำเนินการตรวจสอบรหัส
 - O View History แสดงประวัติการคำเนินการ

Executio	n History	Displaying 2,885 process events	x
Time	Process	Status	
04:17 PM	Started: c:\windows\sysnative\dllhost.exe	Process ID: 3160	*
04:17 PM	Exited: c:\windows\sysnative\dlhost.exe	PID 5588 active 21s	
04:17 PM	Started: c:\windows\sysnative\dllhost.exe	Process ID: 5588	
04:17 PM	Exited: c:\windows\sysnative\dlhost.exe	PID 4396 active 6s	
04:17 PM	Started: c:\windows\sysnative\dllhost.exe	Process ID: 4396	
04:17 PM	Exited: c:\windows\sysnative\dlhost.exe	PID 4208 active 6s	
04:17 PM	Started: c:\windows\sysnative\dllhost.exe	Process ID: 4208	
04:16 PM	Exited: c:\windows\sysnative\dlhost.exe	PID 3428 active 5s	
04:16 PM	Started: c:\windows\sysnative\dllhost.exe	Process ID: 3428	
04:16 PM	Exited: c:\windows\sysnative\dllhost.exe	PID 5280 active 5s	
04:15 PM	Started: c:\windows\sysnative\dllhost.exe	Process ID: 5280	
04:15 PM	Exited: c:\windows\sysnative\dlhost.exe	PID 5408 active 19s	
04:15 PM	$\label{eq:exited:c:lusers} \ensuremath{\sc line label{eq:exited:c:lusers} \sc line label{eq:exited:c:luse$	PID 3952 active 2m 0s	
04:15 PM	Exited: c:\program files (x86)\google\chrome\application\chrome.exe	PID 5520 active 1m 10s (CPU 2s)	-
		()	

Submit files คือ การส่ง ไฟล์ไปให้ Webroot ช่วยวิเกราะห์ความเสี่ยงที่อาจเกิดขึ้นต่อคอมพิวเตอร์
 Submit a file การส่ง ไฟล์เพื่อทำการวิเกราะห์อัตราเสี่ยง

	Second Second Second
Http://snup.webrootcloudav.com/SkyS	toreFileUpload: D 🗸 🔿 🧶 Webroot File Submission 🛛 🗴
Secure Anywne	re.
Submit a File MD5 Lookup URL Rep	
Calactia filor	Browse
Select a file:	
Reason for submission:	
	Can't read the characters?
	k X Z Try a new image
	e ^r
Enter the characters in the image:	
Terms and conditions:	I have read and agree to be bound by the terms and conditions
	Submit File

• แถบ System Control ควบคุมและดูแลการทำงานของเครื่องคอมพิวเตอร์ โคยมีรายละเอียคดังนี้

25



ส่วนที่ 1 Control Active Processes กำหนดกระบวนการทำงานของเครื่องคอมพิวเตอร์ อาทิ อนุญาตให้เปิดใช้งานโปรแกรม, ปิดกั้นหรือติดตามกระบวนการทำงานของเครื่องคอมพิวเตอร์ O Start กำหนดการทำงานของโปรแกรมในกอมพิวเตอร์ โดยมีรายละเอียดคังนี้

Process	Status	Allow	Monitor	Block	
FMAPP.exe in C:\Program Files\Realtek\Audio\HDA	Active for 1h 17m	۲	Θ		
IEXPLORE.EXE in C:\Program Files (x86)\Internet Explorer	2 Instances	۲			
iexplore.exe in C:\Program Files\Internet Explorer	Active for 1h 25m	۲	\odot	\odot	E
Photoshop.exe in C:\Program Files (x8\Adobe Photoshop	CS2 Active for 2h 12m	٠			
chrome.exe in C:\Program Files (x86)\Google\Chrome\Applic	cation 7 Instances	٠			
AUDIODG.EXE in C:\Windows\system32	Active for 3h 33m	•			
splwow64.exe in C:\Windows	Active for 6h 26m	۰	\odot	\odot	
WINWORD.EXE in C:\Program Files (x86)\Microsoft\Offic	e 15 Active for 7h 39m	٠			
snagiteditor.exe in C:\Program Files (x86)\TechSmith\Snagit	t 12 Active for 7h 40m	۰		\bigcirc	
TSCHelp.exe in C:\Program Files (x86)\TechSmith\Snagit 12	Active for 7h 40m	٠			
SnagPriv.exe in C:\Program Files (x86)\TechSmith\Snagit 12	Active for 7h 40m	۰	Θ	\bigcirc	
Snagit32.exe in C:\Program Files (x86)\TechSmith\Snagit 12	Active for 7h 40m	٠			
LINE.exe in C:\Program Files (x86)\LINE	Active for 7h 49m	۲		\bigcirc	
wmpnetwk.exe in C:\Program Files\Windows Media Player	Active for 7h 50m	۰			-



- Allow
- Monitor
- Block
- ปุ่ม Stop Untrusted Processes
- ปุ่ม More Info

 WEBROOT

 SecureAnywhere

 Verts
 Live Events

 CrProgram Files (x80)UINELINE exe

 Tim
 Pesistent Event Detais

 No new persistent system events detected in 59 seconds

อนุญาตให้โปรแกรมทำงาน ตรวจสอบการทำงานของโปแกรม ป้องกันการทำงานของโปรแกรม หยุดกระบวนการที่ไม่น่าเชื่อถือออกจากระบบ แสดงรายละเอียดข้อมูลของโปรแกรม

- Events แสดงเหตุการณ์ต่างๆ
- Custom Rules แสดงกฎข้อบังคับที่ได้กำหนดไว้
- Details แสดงรายละเอียดของโปรแกรม

ปุ่ม Close ทำการปิดหน้าต่างโปรแกรม

ส่วนที่ 2 SafeStart Sandbox การนำโปรแกรมทำการทคสอบตามข้อกำหนดที่ได้เลือกไว้

Command-line:	
Watch events originating from this process	*
Allow access to the Internet	
Allow the process to execute other processes	11
Allow access to user resources	
Allow access to administrative locations on the system	
Allow access to windows with a High integrity level	
Allow access to windows with a Medium integrity level	
Allow access to network shares	*

• แถบเมนู System Optimizer การเริ่มกระบวนการเพิ่มประสิทธิภาพการทำงานให้กับเครื่องคอมพิวเตอร์

27





- แถบเมนู Keycode แสดงรายละเอียดของโปแกรม Webroot
 - ส่วนที่ 1 My Subscription
- O Keycode แสดงรายละเอียด Keycode
 O Product แสดงชนิดโปรแกรมของ Webroot
 O Status แสดงรุ่นของ Webroot
 O ปุ่ม Copy keycode to clipboard ปุ่มทำการคัดลอก Keycode
 ส่วนที่ 2 Activate a new keycode สำหรับทำการ Activate keycode
- แถบที่ 2 About SecureAnywhere

secureAnywhere.	? — 🋱 Advanced Settings
Keycode About SecureAnywhere	My Account
Version 1	
Software Version 8,0.8.76	Copyright © 2006-2015 Webroot Inc. All rights reserved.
Check for software updates	Webroot, SecureAnywhere, and Webroot SecureAnywhere are trademarks of Webroot Inc. in the United States and other countries. View the Webroot Privacy Policy

ส่วนที่ 1 Version แสดงรุ่นของโปรแกรม Webroot ส่วนที่ 2 Legal แสดงรายละเอียดเกี่ยวกับกฎหมาย

8. Support / Community การสนับสนุนให้ความช่วยเหลือและข่าวสาร



- Get Customer Support ขอความช่วยเหลือจากเจ้าหน้าที่ Technical
- Go to the Webroot Community เยี่ยมเว็บ ไซต์ของ Webroot

•

คู่มือการใช้งานโปรแกรมป้องกันไวรัส (Webroot) บนเครื่องคอมพิวเตอร์ เวอร์ชั่น 2.0