SecureAge

SecureAPlus

Get Total Control over PC Security with
Application Whitelisting & 10+ Anti-Viruses Combined

Layers of Essential Security Features

Redefining Zero-Day Protection

Application Control & Whitelisting

When close to a million pieces of malware are created each day, chances are that an anti-virus is not going to keep up. The latest and most advanced forms of malware are nigh undetectable with zero-day threats always a step ahead of any anti-virus available in the market.

Application Whitelisting puts you ahead of the curve. The block-first approach ensures that zero-day malware can do no harm till they're identified and cleared to launch. It stops advanced malware on its tracks, even the likes of ransomware, and puts you in control.

With SecureAPlus, Application Whitelisting is straightforward to setup, easy to manage, and a click away to update – Giving you total control, all the time.

Easily Setup & Manage Whitelist

Total Protection with Block-First Security

Works Well Online & Offline

Advanced Protection from the Cloud

Universal Anti-Virus

The 2 key flaws of anti-viruses are that not a single one can detect close to every threat, and that they are not created equals.

Universal AV is the next best thing to a 100% detection rate all the time. It combines more than 10 comprehensive anti-virus engines in the cloud to enjoy the highest detection rates possible without slowing PC performance.

Combined with SecureAPlus Whitelisting, not only do you get a fast and efficient real-time and on-demand malware scanner, you also get one of the most comprehensive second opinion scanner.
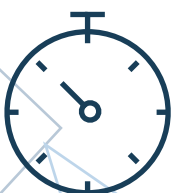
Fast Full System Scans

Automatic Scans & Updates

Powerful On-Demand Scanner

Sophisticated Protection Underneath
A Simple User Interface

A Mode for Every Security Need

Select Interactive Mode for maximum information and flexibility.
Use Lockdown Mode for maximum security while Trust All Mode let's you trust plenty of programs with ease.
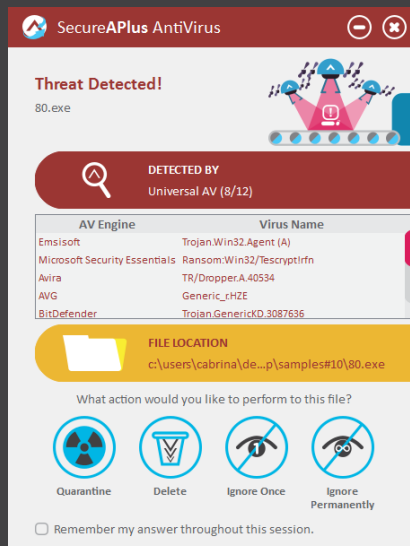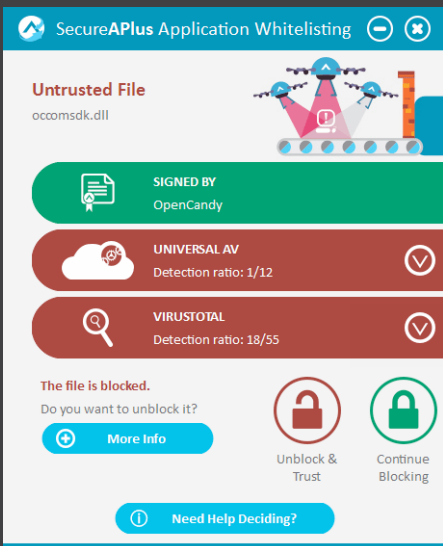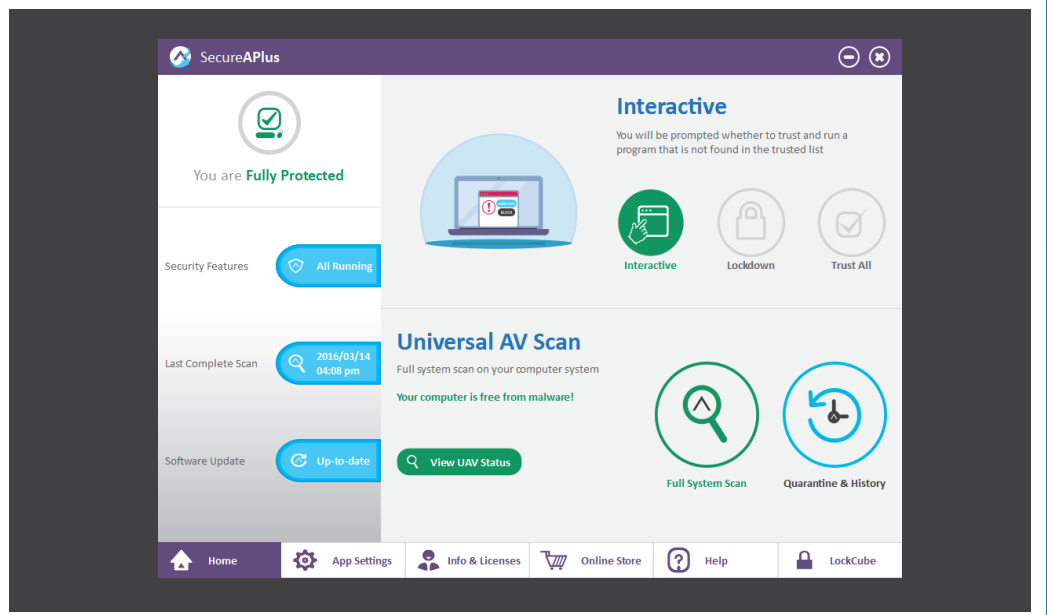
Easily Scan Your Entire System

Doing a full system scan is just a click away from the main interface and it usually takes less than a minute to finish.

Quick Access to Quarantine & History

Access your quarantined files and view security right from the main interface.

Accessible Navigation

Easily get around SecureAPlus with an omnipresent menu bar at the bottom of the main interface.

SecureAPlus

You are **Fully Protected**

Security Features — All Running

Last Complete Scan — 2016/03/14 04:08 pm

Software Update — Up-to-date

Interactive
You will be prompted whether to trust and run a program that is not found in the trusted list

Interactive   Lockdown   Trust All

Universal AV Scan
Full system scan on your computer system
Your computer is free from malware!

View UAV Status

Full System Scan   Quarantine & History

Home   App Settings   Info & Licenses   Online Store   Help   LockCube

---

SecureAPlus Application Whitelisting

Untrusted File
occomsdk.dll

SIGNED BY
OpenCandy

UNIVERSAL AV
Detection ratio: 1/12

VIRUSTOTAL
Detection ratio: 18/55

The file is blocked.
Do you want to unblock it?

More Info

Unblock & Trust   Continue Blocking

Need Help Deciding?

SecureAPlus AntiVirus

Threat Detected!
80.exe

DETECTED BY
Universal AV (8/12)

AV Engine	Virus Name
Emsisoft	Trojan.Win32.Agent (A)
Microsoft Security Essentials	Ransom:Win32/Tescrypt!rfn
Avira	TR/Dropper.A.40534
AVG	Generic_rHZE
BitDefender	Trojan.GenericKD.3087636

FILE LOCATION
c:\users\cabrina\de...p\samples#10\80.exe

What action would you like to perform to this file?

Quarantine   Delete   Ignore Once   Ignore Permanently

Remember my answer throughout this session.

Notifications at a Glance

Easily discern relevant information from any file or application blocked by SecureAPlus using color coded elements.

Universal AV & VirusTotal Integration

Readily available diagnosis from both Universal AV's 10+ engines and a second opinion from VirusTotal's 50+ engines.

Choose from Contextual Actions

Trust or Block applications outside your whitelist and get expanded options to Delete or Quarantine when a threat is identified.
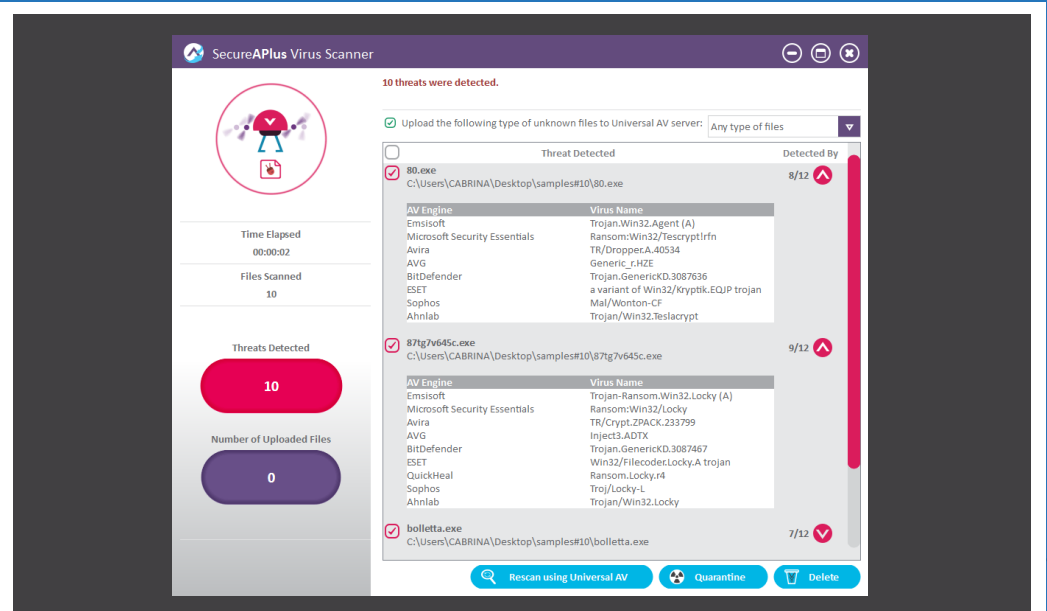

Current Scan Statistics

Allow or disallow file-type uploads as well as get real-time summary of your current scan.

Detailed Detection Information

Easily locate threats detected as well as access complete information on the type of threat detected from multiple sources.

Take Action with Latest Threat Assessment

Get the most up to date diagnosis on previously detected files by calling a rescan with Universal AV and decide whether to Quarantine or Delete them.

SecureAPlus Virus Scanner

10 threats were detected.

Upload the following type of unknown files to Universal AV server: Any type of files

Threat Detected	Detected By
80.exe C:\Users\CABRINA\Desktop\samples#10\80.exe	8/12

AV Engine	Virus Name
Emsisoft	Trojan.Win32.Agent (A)
Microsoft Security Essentials	Ransom:Win32/Tescrypt!rfn
Avira	TR/Dropper.A.40534
AVG	Generic_rHZE
BitDefender	Trojan.GenericKD.3087636
ESET	a variant of Win32/kryptik.EQJP trojan
Sophos	Mal/Wonton-CF
Ahnlab	Trojan/Win32.Teslacrypt

Threat Detected	Detected By
87tg7v645c.exe C:\Users\CABRINA\Desktop\samples#10\87tg7v645c.exe	9/12

AV Engine	Virus Name
Emsisoft	Trojan-Ransom.Win32.Locky (A)
Microsoft Security Essentials	Ransom:Win32/Locky
Avira	TR/Crypt.ZPACK.233799
AVG	Inject3.ADTX
BitDefender	Trojan.GenericKD.3087467
ESET	Win32/Filecoder.Locky.A trojan
QuickHeal	Ransom.Locky.r4
Sophos	Troj/Locky-L
Ahnlab	Trojan/Win32.Locky

bolletta.exe C:\Users\CABRINA\Desktop\samples#10\bolletta.exe	7/12

Time Elapsed
00:00:02

Files Scanned
10

Threats Detected
10

Number of Uploaded Files
0

Rescan using Universal AV   Quarantine   Delete

Enterprise Secuity with SecureAPlus

Easily Deploy and Activate for Enterprise
SecureAPlus can be easily installed en masse to enterprise workstations with the ability to push an approved whitelist for newly deployed devices.

Allow Users to Request for Approvals
Users who are in Lockdown mode can easily send requests for approvals to install and run applications that are not included on the company whitelist.
In turn, IT Administrators can remotely respond to requests via the SecureAPlus Portal.

Activate/Deactivate Scanners from the Portal
IT Administrators can enable or disable scanning features of SecureAPlus protected workstations. This is useful for catering workstations that are in network sensitive environments while still preserving the robust protection of application whitelisting.

Remotely Change Modes of Enterprise Workstations
IT Administrators can easily switch the Application Whitelisting mode of enterprise workstations. This is especially useful for enabling users to trust, install, and run applications based on their judgement securely with Interactive Mode while also allowing for a swift way to revoke these privileges by switching them back to Lockdown mode.
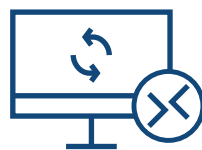
Remotely Update Advanced Settings
Company approved certificates, applications, script rules, and even administrator users and groups can be customized remotely in order to adapt the security settings for the use case at hand.

Closed Network Enterprise Protection
SecureAPlus is compatible with the SecureAge Management server for closed network enterprise protection. This allows for all the advanced protection and remote capabilities off Application Whitelisting without the use of the online SecureAPlus Portal.

SecureAPlus Benefits at a Glance
- ✔ Higher Detection Rates
- ✔ Uninterrupted PC Usage
- ✔ 24/7 Scanning
- ✔ Total PC Control
- ✔ Easy Whitelisting
- ✔ Block with Uncertainty
- ✔ Flexible Offline Security
- ✔ Maximum Compatibility
- ✔ Added Layers of Defense
- ✔ Light on PC Resources
- ✔ User Friendly
- ✔ Fully Automated

Technical Specifications
2 GHz Pentium 4 or higher processor
1GB of RAM or as recommended by the Windows OS whichever is higher
300 MB hard disk free space or more
Local hard disk that is formatted with NTFS file system.
Minimum screen resolution: 1024×768 (At 100% Scale)
Supported Operating Systems:
    Windows 10 (32-bit and 64-bit)
    Windows 8.1 (32-bit and 64-bit)
    Windows 8 (32-bit and 64-bit)
    Windows 7 Home Basic and above (32-bit and 64-bit) and above
    Windows XP SP3 (32-bit and 64-bit)
    Windows Vista SP2 and above (32-bit and 64-bit)
    Windows Server 2003 R2 SP1 & above (32-bit & 64-bit)
    Windows Server 2008 SP1 & above (32-bit & 64-bit)
    Windows Server 2008 R2 & above (64-bit)
    Windows Server 2012 (64-bit)
    Windows Server R2 2012 (64-bit)

Need More Information?

www.secureaplus.com   secureaplus@secureage.com