SecureAge

SecureAPlus

Intuitive application control

Layers of Essential Security

SecureAPlus is the unique amalgamation of essential security features that protect enterprise endpoints against multiple attack vectors - known or unknown, file or file-less, internal or external.
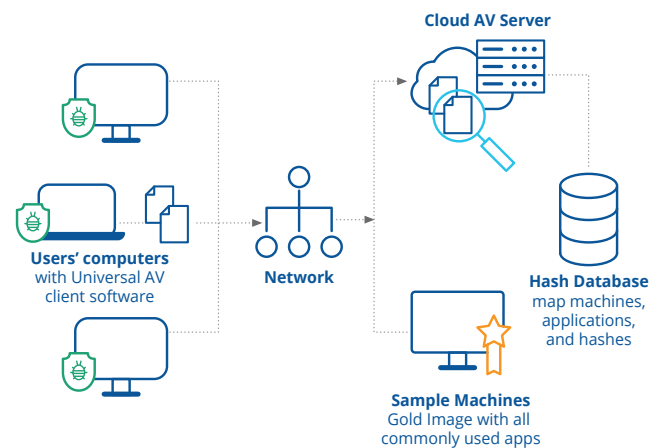
Universal Anti-Virus
Advanced Detection Technology in the Cloud

No single anti-virus engine is capable of detecting anywhere close to 100% of every threat and certainly, none of them are created equally with some better at detecting certain types of threats.

Universal AV combines multiple anti-virus engines to scan files to enjoy a higher detection rate normally not possible with traditional anti-virus at any given time. It does all this in the cloud so that it doesn't consume local resources for scanning and leaving your endpoint with options to use an existing local anti-virus engine.

The combined diagnosis serves as critical intelligence for real-time protection and making decisive choices for Application Control.

Cloud AV Server

Users' computers
with Universal AV
client software

Network

Hash Database
map machines,
applications,
and hashes

Sample Machines
Gold Image with all
commonly used apps

Combine diagnosis from multiple AV engines

Detected threats are diagnosed by more than a single AV to provide for at least a second opinion for every scan.

Scanning technology in the cloud

Maintain peak endpoint hardware performance by delegating scanning processes in the cloud.

Fast full system scans

Automatically done on a regular basis as well as easily accessible within a few clicks and completes its scanning cycle quickly.

A scan for every situation

Fast full system scans upon booting and on regular intervals, On-Demand scans allow users to check any file at any time, while real-time scans defend against potential threats that enter your system.

Configurable scan settings

Enable or disable certain scan options, exclude sensitive folders from scanning in the cloud, set file upload size limits, and more.

Compatibility with offline solutions

With scanning processes in the cloud, endpoints have the option of making use of existing or future third-party offline scanning solutions without compatibility issues.

SecureAge APEX Engine
Threat Detection Powered by Artificial Intelligence

As more and more threats are mutating into advanced forms at an alarmingly rate, solely relying on traditional detection technologies that are designed to identify existing threats leaves endpoints very vulnerable to zero-day and mutated malware attacks.

The SecureAge APEX Engine harnesses the power of artificial intelligence (AI) with deep learning to take on the threats of today and tomorrow.

Leveraging on the power of big data, the APEX engine goes beyond traditional scanners by effectively and reliably spotting malicious patterns to efficiently allow for quick decisions based on prior experience. It can adaptively update its knowledge against newer and unseen malware variants that may attempt to infect endpoints during an outbreak.
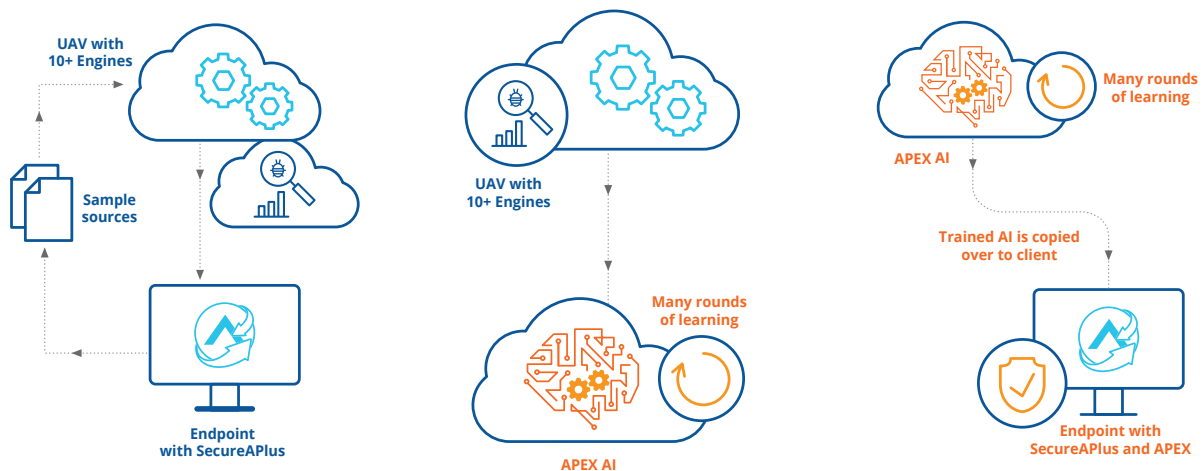
Two-pronged approach to detection	APEX complements contemporary and traditional scanning technologies like the Universal AV and the included or third-party offline AV engines to effectively cover known and unknown malware variants.
Deep Learning technology	Able to identify threats without using signature-based techniques, instead, relying on previously learned data to identify threats.
Improvements via training	Leveraging cloud technology to train with massive amounts of data ensures that the engine is updated with trained versions resulting in a smaller file footprint when compared to traditional virus signatures.
Offline operation	Trained and stored locally to allow it to operate without relying on an internet connection to be able to detect the latest threats.
Compatible with other scanning technology	Works alongside the Universal AV and/or other offline third-party AV engines.

Application Control & Whitelisting
At the Core of Your Endpoint Security Strategy

With close to a million new variants of malware created each day, traditional anti-virus solutions struggle to detect these threats upon their initial release in the wild. Making matters worse, advanced forms of malware adapt against established security measures, giving them a step ahead of and are nigh undetectable by any available anti-virus in the market.

Application Control & Whitelisting puts you ahead of the curve by implementing security-by-design. The block-first approach ensures any file that is still not trusted can do no harm until they are identified and cleared for launch. It stops advanced and zero-day malware on its tracks and puts you, not the malware, in control every time.

|	
Ease of whitelist creation	Install on an endpoint to create the initial whitelist using a strong cryptographic hash function.
Import & export whitelist	Export the whitelist from a baseline machine for deployment of the secured whitelist on other endpoints in the organization.
A mode for Privileged & Non-Privileged users	Interactive mode lets you update whitelists on-the-fly while Lockdown mode limits non-privileged users from launching non-trusted files.
Advanced modes for situational uses	Trust All, Observation, and Silent Mode to cater usage on controlled environments.
Defend against wider attack vectors	Coverage against portable executable, malicious scripts, and fileless attacks with command line rules.
Reliable intelligence	Highlight blocked threats with supporting intelligence from multiple detection sources to allow informed decisions when adding non-trusted files to the whitelist.
Notifications at a glance	Easily discern relevant information with the use of aptly color-coded elements from any blocked file or application while getting notifications in Interactive Mode.
Contextual Actions	Block or trust a non-trusted file while options for deleting or quarantining are available when a threat is detected.
Online & offline operation	Application Control & Whitelisting works locally on every endpoint regardless of internet or network connectivity.

Large-Scale Centralized Security Management

For enterprise or larger deployments, endpoints normally number in the hundreds and even thousands. Scaling the benefits of application control and whitelisting while making it manageable at all times is a crucial requirement that needs to be addressed to successfully deploy SecureAPlus.

The Security Management Server (SMS) allows IT administrators to easily monitor, update, and push approved whitelists across large numbers of endpoints to ensure minimal downtime and maximum productivity.

It takes advantage of either commercial grade hardware or a virtual machine in the cloud to implement advanced security controls that help administrators facilitate application control and whitelisting as well as other data security functions*.

*Works with SecureAge Suite solutions for integration of other data security features such as encryption

User Data **Database** **Web App**
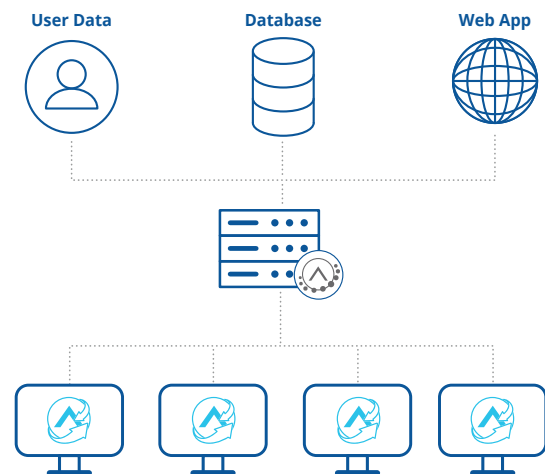
Mass deployment & activation

Easily install SecureAPlus en masse to enterprise endpoints by pushing an approved whitelist to newly deployed devices.

Web console user interface

Administrator access via a dedicated web portal to manage SecureAPlus security on any machine connected to the network.

Whitelist Management

Ensures standardized client system configurations by managing and enforcing a whitelist to allow only trusted and authorized applications to run on endpoints.

Blacklist Management

Allows for enhanced malware by building and filtering a blacklist of unwanted or unauthorized applications.

Request Whitelist Approval System

IT Administrators can remotely respond to requests by non-privileged users in Lockdown mode to add an unauthorized application to the whitelist.

Software update push controls

Push installation of SecureAPlus software updates to particular groups or endpoint devices.

Other Key SecureAPlus Features

Complementing the core protection features of Application Control & Whitelisting, Universal AV, and the APEX engine, SecureAPlus has additional features that further enhance enterprise endpoint security.

Command line rules

Extend whitelisting security coverage against fileless attacks with the inclusion of an initial set of rules that are easily customizable and expandable.

Email alerts & infection reports

Get immediate email alerts with detailed infection reports through email whenever an endpoint is detected to be infected. With Universal AV's 24/7 scanning in the cloud, IT administrators are notified even if the infected endpoint is turned off.

USB storage device access control

Control how external USB storage devices are treated by default upon insertion to endpoints. It features controls to allow or disable read and/or write access as well as whitelisting storage devices.

Password protected settings

Prevent unauthorized tampering of SecureAPlus settings through a password.

Technical Specifications

Hardware Requirements:

- 2 GHz Pentium 4 or higher
- 1GB of RAM or as recommended by installed Windows OS (whichever is higher)
- 300 MB hard disk free space or more
- Local hard disk formatted to NTFS
- Minimum screen resolution: 1024×768 (at 100% scale)

Languages Available:

Chinese (Traditional and Simplified), English, French, German, Hungarian, Indonesian, Italian, Japanese, Polish, Russian, Turkish, Vietnamese

Supported Operating Systems:

- Windows 10 (32-bit & 64-bit)
- Windows 8.1 (32-bit & 64-bit)
- Windows 8 (32-bit & 64-bit)
- Windows 7 Home Basic (32-bit & 64-bit) and above
- Windows XP SP3 (32-bit & 64-bit)^
- Windows Vista SP2 and above (32-bit & 64-bit)
- Windows Server 2016 (64-bit)
- Windows Server R2 2012 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2008 R2 & above (64-bit)
- Windows Server 2008 SP1 & above (32-bit & 64-bit)
- Windows Server 2003 R2 SP1 & above (32-bit & 64-bit)^

^Command Line Rules and APEX AI Engine are not compatible with these versions of Windows