PRODUCT DATA SHEET

DIGITALGUARDIAN®

Savant Protection Application Whitelisting

QUICKLY DEPLOY THE MOST SECURE APPLICATION WHITELISTING

Application whitelisting adds a critical layer of defense against evolving threats such as zero-day attacks that endpoint anti-malware frequently fail to detect. But most of today's whitelisting products are too difficult to deploy, time-consuming to manage, and reliant on a centralized database. Savant Protection is easy to deploy, transparent to existing operations and the most secure application whitelisting for Retail POS systems and industrial control systems.

> There is no silver bullet in information security, but if managed correctly application whitelisting solutions at the endpoint provide exceptional protection from zero day and targeted attacks.

-The Power of Whitelisting, Neil MacDonald, Gartner

Gartner®

DEPLOY APPLICATION WHITELISTING IN MINUTES

Savant agents install in minutes and begin protecting endpoint systems immediately. Our software doesn't require you to determine in advance which applications and libraries are required by each user. Once installed the Savant agent automatically creates a unique whitelist that determines what executables are permitted to run on that device.

BLOCK UNKNOWN AND UNAUTHORIZED EXECUTABLES ON WORKSTATIONS, SERVERS, POS DEVICES AND INDUSTRIAL CONTROLS

As soon as our agent is operational, it prevents new unauthorized applications from being installed. Upon confirmation of the approved whitelist, execution of any unauthorized application will be blocked, whether malicious applications (such as viruses, Trojans, or Bots) or unwanted/ unknown applications. Savant Protection is proven in the most critical environments such as Retail POS and industrial control systems.

STOP MALWARE BEFORE IT LANDS

Savant agents keep hard drives clear of dangerous executables that may attempt to relaunch in the future.

PREVENT UNAUTHORIZED CHANGES TO APPLICATIONS & EXECUTABLES

Savant agents block any attempts at unauthorized additions, deletions or modifications and log both authorized changes and unauthorized attempts.

AUTOMATE CONTAINMENT

If pre-existing malware or malicious code goes undetected by scans and antivirus prior to the installation and creation of the initial whitelist, our agent will automatically contain any potential negative effects from the presence of that malware only to that device.

AUTOMATE APPLICATION WHITELISTING MANAGEMENT

Through the designation of trusted agents, Savant enables you to use your normal methods for patching, updating and installing software without having to explicitly look at or manage a whitelist. Our trusted agent feature allows organizations to efficiently keep all authorized applications on endpoints updated and patched without requiring any additional intervention by the end user or IT.

DIGITALGUARDIAN® by VERDASYS

For more information, visit
www.digitalguardian.com

WHY SAVANT PROTECTION FOR APPLICATION WHITELISTING

1 MORE SECURE BECAUSE THE WHITELIST IS STORED LOCALLY AND PROTECTED FROM ALL ACCESS

Only Savant Protection uses a patented, encrypted whitelist on each endpoint. The whitelist is always stored locally, encrypted and protected from all access by the driver.

2 STOPS PROLIFERATION OF ANY POTENTIAL COMPROMISE TO OTHER ENDPOINTS

Our unique whitelist on each endpoint prevents propagation of any malware that might somehow slip through.

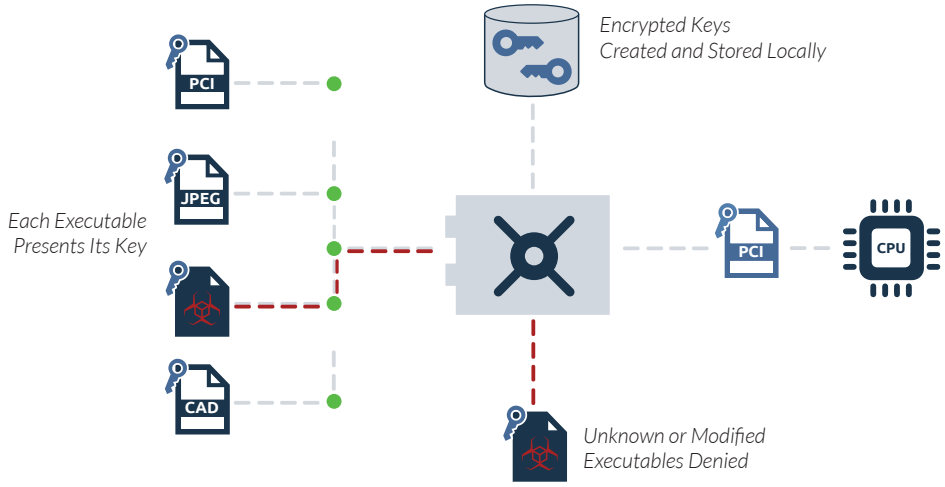
3 STRONGER SECURITY BECAUSE THERE IS NO SINGLE POINT OF FAILURE

Many application whitelisting products use a centrally managed whitelist. With this approach a compromise of the central whitelist or global software registry is a compromise for all systems.

4 GREATER FLEXIBILITY THROUGH A COMPLETE CLIENT USER INTERFACE (UI)

Our local UI enables our agent to work both on and off the network and supports total lockdown of industrial systems that are completely network disconnected. It also enables authorized users to install software seamlessly.

HOW IT WORKS



Savant Protection software associates a unique, invisible key with each authorized application (including associated components and identified scripts) on each end system. When an executable file is read or accessed, our agent compares the previously known key with the key that is presented. If there is a match, the application is allowed to execute on the system. If there is not a match or the application is unknown, access to the CPU is denied. In lockdown mode, new executable files are prevented from even being written to disc. In a more open environment where users may be granted more flexibility in adding software to their devices, options are presented for handling the unknown application.

ABOUT DIGITAL GUARDIAN

Digital Guardian is the only data aware security platform designed to stop data theft. The Digital Guardian platform performs across traditional endpoints, mobile devices and cloud applications to make it easier to see and stop all threats to sensitive data. For more than 10 years we've enabled data-rich organizations to protect their most valuable assets with an on premise deployment or an outsourced managed security program (MSP). Our unique data awareness and transformative endpoint visibility, combined with behavioral threat detection and response, let you protect data without slowing the pace of your business.

SHARE