APPGUARD
Stops malware EDR/XDR miss

TECH SHEET

HOW APPGUARD WORKS

Unlike most endpoint protection tools that defeat malware if and when there is some form of pattern recognition, whether it be file or behavioral. AppGuard's approach is controls based. AppGuard defeats malware without having to recognize the malware itself by not allowing malware to do what it needs to do.

Malware Attacks use your Applications and OS Utilities Against You

There are many examples familiar to you: exploit an application vulnerability, weaponize a document, trick a user into downloading and running a file, etc. If there were restrictions on what applications and OS utilities could run and what they could do, then malware attacks would fail. AppGuard does this.

Malware's Success Depends on Performing Actions within Endpoints

Once in, malware attacks execute a variety of actions. Some examples include: altering a file or registry key, planting one or more files someplace, launching an executable or script, injecting code into the memory of an application process, sending instructions to an OS utility to perform actions, loading a DLL file into the memory of another application, copying data from files or memory, encrypting or deleting files, or many other actions.

Any malware attack consists of a combination of these and other actions. Combinations of those actions are known in the industry as malware techniques. For each of these, there practically an infinite variety of files and behavior patterns, which overwhelm detection technologies.

A Completely Different Approach to Stop Attacks

AppGuard is focused on blocking the actions that make up the malware techniques. Put simply, it defeats malware attacks by not allowing malware to do what it must do. This approach does not involve any form of pattern recognition, making AppGuard the ideal complement to antivirus (AV), endpoint detection & response (EDR), extended detection & response (XDR), and other tools in one's cyber stack. They only succeed if and when they recognize something as malicious. With an entirely different approach, AppGuard can stop what they miss or detect too late.

AppGuard Protection Combines: Launch, Containment, and Isolation Controls

The policies that an AppGuard agent running on a laptop or server enforce consists of a combination of policies for these three type of controls.

Launch

Prohibit launches from risky folders or of dangerous OS utilities

Many malware actions involve getting files to execute or load from the endpoint. AppGuard applies launch controls to high-risk folders. Many different malware attacks fail because AppGuard does not allow their files to execute or load. AppGuard allows launches of applications that are digitally signed by trusted publishers.

AppGuard's launch controls also restrict what OS utilities can be used. Many malware techniques utilize legitimate OS utilities to do their harmful actions. Such attacks fail when OS utilities cannot be used. These prohibitions are not always absolute, some are conditional, allowing legitimate use while simultaneously thwarting other uses.

Containment

Prevent harm by restricting what risky applications may do

The name AppGuard is a recognition that many malware attacks use an enterprise's own applications and utilities on the endpoint against the enterprise. In effect, they hijack applications or utilities to do harm. AppGuard containment allows high-risk applications and utilities to do what they must but does not allow them to do what they must not. Put simply, AppGuard containment defeats many attacks by not allowing them to do what they must to succeed.

AppGuard containment works across up to six dimensions: file (restrict read/writes), registry (restrict read/writes), memory (restrict read/writes), child process (e.g., restrict what app can launch what app), privilege (i.e., restrict its privilege so it cannot use harmful system APIs), and communication operations.

Should for example, Microsoft Word, Google Chrome, or Adobe Acrobat become hijacked due to an exploit of a software vulnerability, AppGuard does not all them to write files into or alter existing files in folders where AppGuard does not restrict launches. AppGuard's containment actually simplifies its launch control.

Isolation

Only specific Apps may access or change critical data or settings

Where containment protects the host from its applications, isolation protects parts of the host from the rest of the host. Remember, AppGuard defeats malware attacks that other tools do not detect by not allowing the malware to perform actions it must. Some attacks require altering or adding one or more registry keys or files to corrupt the normal operations of the endpoint. If for example one attack needs to instantiate a malicious service, an AppGuard isolation control prevents changes to that "part" by anything else.

AppGuard is also a last line of defense for protecting credentials, which are cached in various "parts" of the host so users need not constantly re-enter them. Google Chrome, like other web browsers, caches a user's website credentials in a file. AppGuard isolation controls can prevent everything else on the host from accessing that file at all. On servers, one might use isolation to grant exclusive access of select folders with sensitive data to just one application. So, even if malware somehow, someway is able to run, AppGuard can prevent it from stealing or destroying valuable data.

Defeating Malware without having to Recognize it

AV, EDR, XDR, and other malware detection tools must recognize malware to defeat it. The number of signatures and behavior patterns to identify malware is enormous. Millions of yet more malware samples are created daily.

However, malicious files and behavior patterns might vary, malware attacks must perform specific actions to be successful. AppGuard's focus is to block those actions rather than to recognize the malware itself.

Easily Adjusted for Specific Needs and even Tighter Protection

AppGuard's default policies are designed to defeat malware techniques yet stay out of the way of legitimate workflows. Most users can do what they need to do. Sometimes, however, policy adjustments need to be made. After initial adjustments, AppGuard agents typically run months, sometimes years, without need of policy changes.

Some security-conscious organizations take advantage of AppGuard's capacity to enforce additional, optional policies that make AppGuard protection even better.

Patented Technology makes AppGuard Easier and Better

Endpoints are constantly changing because of application updates, security patches, application plug-ins, and other reasons. Why don't AppGuard customers bear the terrible administrative burden of application control tools? AppGuard avoids that problem with technology that enables it to automatically adapt to these changes. Some application control tools try to provide customers with constantly updated "allow" lists. But not all of your high-risk applications are covered. AppGuard containment and isolation controls can be applied to almost any application. Once this is done, the rules seldom need to be revised. This is evidenced by the fact that AppGuard software agents typically run months, sometimes years, without need of any policy updates. Consequently, customers get great protection without having to bear the burden of something administratively onerous.

About AppGuard

AppGuard is a cybersecurity company on a mission to fill an urgent need for better protection from malware attacks due to the inability of detection technologies to tell bad from good among nearly infinite possibilities. AppGuard's approach is completely different; it is controls based. AppGuard defeats malware without having to recognize the malware itself by not allowing malware to do what it needs to do.

APPGUARD
Stops malware EDR/XDR miss

www.appguard.us | sales@appguard.us