DATA SHEET

APPGUARD

Overview

AppGuard effectively protects computers from the kinds of malicious code threats that otherwise keeps CISOs awake at night because their traditional antivirus products do not, and advanced alternatives have blind spots and/or unacceptable operational costs. Security experts and analysts recommend that enterprises supplement their endpoint protection platform with advanced protection agents such as AppGuard.

Does AppGuard replace your AV?

Yes, but AppGuard is not a scanning product. It operates in an entirely different manner. Many of our clients have replaced their traditional AV with Microsoft's free Windows Defender to satisfy regulatory mandates that explicitly require periodic scanning of endpoints. This combination protects endpoints from advanced threats and satisfies regulatory mandates. Other customers have kept their traditional AV. AppGuard generally co-exists with all endpoint security tools.

What is AppGuard and how is it different?

AppGuard defeats all forms of consumer malware, advanced malware, exploitless (e.g., PowerShell or other scripts that use legitimate utilities to do harm), and file-less (reside in memory only) attacks on endpoints. It does so by avoiding the quagmire of telling good from bad files or normal from abnormal behaviors amongst infinite, ephemeral possibilities. That's why alternatives fail and incur high operational costs. Instead, AppGuard's patented approach uniquely blends low-level controls that dynamically block unacceptable yet deterministic actions. Adversaries can easily change how malicious code looks and behaves, but changing what it ultimately does without sacrificing their goals is extremely rare. Endpoint attackers cannot achieve their goals without successfully executing these finite actions.

In short, these controls do not allow applications and whatever they spawn to implant persistent malware by altering system-space (e.g., Windows, Program Files directories, important registry nodes, etc), inject code into other processes, or steal data from the memory of other applications (memory-scrapers). They also block untrustworthy executable launches from user-space. They do allow user-space launches for digitally signed executables from trusted publishers, but these are subject to the aforementioned protective controls.

AppGuard also mitigates the risks from exploit-less malware or malware-less attacks that use scripting engines and other legitimate utilities on endpoints. It does so by either via default-deny access to these resources, selectively disabling unneeded ones, and/or limiting what they may do. However, AppGuard accommodates legitimate use of these resources by IT-Ops. These and other AppGuard controls combine to defeat all forms of endpoint malware attacks, even zero-day.

sales@blueridgenetworks.com | 1-800-722-1168 | BlueridgeNetworks.com

Nips Cyber Costs in the Endpoint

AppGuard's effective, low-Ops endpoint compromise prevention slashes alert/ incident volume for the enterprise. Consider the last five years, chronically failing AV has been increasing the volume of data breaches. This has been driving up IT-Ops and Sec-Ops costs required to prevent, detect, and respond to them. These costs manifest in the forms of tools, services, personnel, business processes, and readiness exercises for areas such as: cyber hygiene, security incident and event management (SIEM), next generation firewall, breach detection system (BDS), incident response, forensics, remediation, threat intelligence, and operations optimization. Endpoint incident/alert volume directly relates to all of these downstream costs. AppGuard nips these costs in the endpoint.

Reduces Enterprise Skills Gap

AppGuard was designed for competent Windows administrators. Editing policies is as simple as adding a song to a playlist. Because AppGuard simply blocks unacceptable actions, administrators are not put in the position of having to analyze and react to alerts as is required of EDR and some post-execution products. AppGuard alleviates the pervasive cyber skills gap in two ways. First, it lowers the skills required to protect endpoints. Second, its highly effective protection reduces all forms of incident/alert volume downstream from potentially compromised endpoints. Most organizations, which lack AppGuard-like endpoint protection, have deployed many different cyber functions downstream that exacerbate the skills gap.

Blocks Adversary Enterprise Lateral Movement

However, the first one or more enterprise endpoints are compromised via a targeted attack, they typically serve as a beachhead to spread into the rest of the enterprise until the adversaries accomplish their goals. They do so by conducting pass the hash/ticket attacks. Simply put, the hash and ticket are not perceived by end-users despite the great convenience they provide them. Otherwise, end-users would have to answer a logon challenge anytime they accessed something in the enterprise. The operating system replays these hashes/tickets to spare endusers. Unfortunately, adversaries can copy these from an endpoint's memory to impersonate end-users. Worse, the memory also frequently includes high privilege credentials. Why waste time infecting other machines when impersonating existing identities is so much easier? Microsoft released features to mitigate these risks, but pen testers and hackers alike soon after overcame them. Alternative products assert that they mitigate these risks, but there are two major caveats. First, they do so, provided they stop the early stages of an attack. Second, they detect and react. AppGuard blocks these credential thefts with no caveats and does so in a true set and forget manner.

Indicator of Attack / Threat Intelligence Data

While AppGuard does not need IoA or IoC data to protect endpoints, it does collect fine-grained IoA data on attacks that most EPPs and other tools cannot detect until weeks or months later, and even longer for weaponized documents. And when the others catch up, they are capturing IoC data, which lacks insights found in IoA data. Further, AppGuard IoA data differs from alternatives in that no endpoints have to be compromised to capture threat intelligence data. All of this is available on the backend for SIEM and other tools to utilize.

Alleviates Patch Management Pressure

With IT practitioners conceding that they cannot keep up with software patches, AppGuard is an excellent compensating control. Its design assumes that endpoint applications have unknown exploitable vulnerabilities. Hence, the product is named AppGuard because many of its controls effectively place these applications under 'guard' so they can do no harm. Unpatched applications are just known vulnerabilities to AppGuard. We still advocate patching judiciously however, because a future vulnerability exploit could theoretically elude even AppGuard. The patching pressure that AppGuard alleviates can free limited resources to do other important tasks.

True Set & Forget Endpoint Protection

By preventing endpoint compromises without signatures, exploit patterns, or other ephemeral or near-infinite data streams, AppGuard requires no updates or help from the cloud to protect endpoints from the latest threats. AV detection rates rapidly decline with time when offline. Machine learning (ML) products do as well, despite vendor claims. End-users view email attachments offline on airplanes. Industrial control systems and other special function endpoints must be isolated from the Internet and normal IT space. Had AppGuard been deployed on all retailer PoS machines five years ago with no updates since, none of the retailer breaches that hit the headlines would have occurred.