APPGUARD
The Malware Disruptor

SOLUTION BRIEF

Optimizing the Power of Microsoft's AV and EDR with AppGuard

Microsoft provides a broad range of security protection and detection capabilities that protect endpoints from a wide spectrum of threats. The company's anti-virus, Microsoft Defender, included free in every version of Windows, and Microsoft Defender for Endpoints, a full-blown Endpoint Detection and Response (EDR), are widely deployed. But, even the best threat identification technologies (e.g. NGAV and EDR) cannot find and stop fast-striking, well obfuscated, or new malware, leaving a dangerous time gap.

AppGuard is a critical element in the cyber stack because its malware disruption techniques stop malware from causing harm, buying NGAV and EDR technologies the time they need to identify the danger. AppGuard's policy controls reduce the attack surface and minimize the number of actions and pathways that malware can use to achieve its goals, reducing the overall risk of compromise. Providing protection even before a threat is identifiable, AppGuard allows detection technology tools to operate more accurately and efficiently since there is less risky activity to monitor. Adding AppGuard to your cyber defense strategy allows you to optimize the power of Microsoft's AV and EDR, while ensuring greater protection with less effort.

AppGuard and Microsoft: Better Together

For companies looking to optimize their Microsoft environment to provide greater protections against today's most sophisticated threats that bypass traditional anti-virus tools, and wish to reduce alert fatigue impacting security staff, AppGuard is the answer.

AppGuard's patented malware prevention technology works seamlessly alongside most Microsoft products. This includes software that is used for overall management, like InTune, as well as Microsoft Defender and Microsoft Defender for Endpoints.

While Microsoft's endpoint security tools provide protections, there is a gap between the time sophisticated attacks occur and the time Microsoft Defender or Windows Defender for Endpoints detect them. AppGuard closes that gap by preventing malware attacks in real-time, without the need for assistance from a cloud.

Reduce the Attack Surface

AppGuard is a pre-compromise solution that prevents, rather than detects malware. By applying auto-adaptive policy rules over system behavior, AppGuard is able to dramatically reduce the attack surface and the number of actions malware can use to compromise your environment. AppGuard complements and augments Microsoft's AV solutions by providing a more powerful approach than signature-based or AI/ML based detection methods. While advanced versions of Microsoft Defender Antivirus do have some attack surface reduction options to enable, AppGuard's ability to apply more advanced, granular, controls and automatically adapt them to a changing environment allows it to overcome the challenges that Microsoft's control face, like constant rule maintenance and day-to-day business operations interference.

Prevent Advanced Attacks

AppGuard needs no malware-specific tuning or unique indicators of compromise (IoCs) to protect endpoints. As a result, AppGuard was prepared for the SolarWinds and Exchange Server attacks on day zero. History shows that Microsoft tools often don't recognize such attacks until one, or many months after the attack. Generally, these tools are far less effective at protecting against unfamiliar malware, not just zero-day exploits. Such attacks tend to involve living off the land (LoL) binaries, as well as fileless methods. While Microsoft tools strive to tell good from bad and normal from abnormal; AppGuard simply restricts behavior

> *"AppGuard should be on every Windows system in the world."*
>
> — Bob Bigman, CISO, CIA (ret.)

to what is allowed, applying zero trust principles within its host.

AppGuard blocks malware in real-time before endpoint compromise, and before remediation is required. AppGuard's success does not depend on recognizing malware or its effects. At some point, applications such as Microsoft Exchange Server or SolarWinds Orion may be hijacked by adversaries. AppGuard expects this. It applies containment controls so malware cannot do harm to the rest of the host; launch controls to high-risk folders so only trustworthy things can launch; and isolation controls that protect high-value or high-security 'settings' (e.g., hardening policies in Windows registry or GPO) from all else on the host. While these controls might seem familiar, they are uniquely enhanced via simplifying abstractions that enable them to adapt to lifecycle changes. This means administrators seldomly have to revise policies for deployed agents, and administrators do not have to anticipate all permutations in adversary techniques. Less experienced administrators and analysts have the power to operate AppGuard, unlike EDR tools that require experts.

Most importantly, AppGuard dynamically contains high-risk applications and isolates high-value applications to prevent harmful actions regardless of whether Microsoft tools recognize malicious files or behaviors. By blocking actions that are not allowed, AppGuard logs reveal indicators of attack that EDR can miss, fail to recognize, or fail to capture before artifacts are destroyed by the malware itself, such as in the SolarWinds attacks. Many AppGuard customers have found these logs reveal insights their EDR missed entirely.

Optimize EDR Tools and Staff

With Microsoft's current endpoint security tools, judgments are based on a confidence model. While Microsoft's confidence model is proprietary, most threat detection tools rely upon known threat patterns to identify potential

> *"We no longer need battallions of specialists to react to malware attacks because AppGuard blocks them at the endpoint as they strike."*
>
> — Director, Security Operations, Global Airline

threats. Clever adversaries craft their malware to mimic legitimate behaviors. This results in low statistical confidence detections or none at all. When judgments are wrong, they are called false positives or false negatives. An organization's most talented people try to tune these out. Such tuning never ends because changes in the enterprise, applications, and adversary techniques are constantly evolving, requiring constant updates to detection lists.

Combining AppGuard with Microsoft EDR yields two major benefits. First, it blocks what Microsoft detection tools fail to recognize as a threat. Second, AppGuard reduces the workload of alerts, investigations and endpoint remediations, as well as reduces post compromise activities that must take place at other layers in the security stack. Additionally, AppGuard can further complement and augment Microsoft's EDR solution by providing enriched endpoint meta data, with less false positives, all while lowering the overall cost and staff impact associated with remediation efforts.

AppGuard: A Critical Component of Your Defense in Depth Strategy

No single cyber tool is perfect. Optimal protection is best achieved with a defense in depth strategy. Prevention is key when combating malware attacks. AppGuard prevents malware from causing harm, detects threats not recognized by Microsoft Defender, and reduces the workload of your security team. By adding AppGuard to your Microsoft ecosystem you achieve greater security with less effort.

About AppGuard

AppGuard is a cyber security company on a mission to set a new standard: true cyber protection for all. AppGuard's patented technology prevents compromises before they happen by disrupting malware activity from causing harm without having to recognize it. Unlike detection-based solutions, AppGuard outsmarts malicious actors to ensure businesses can do what they need to do, and malware can't do what it wants to.

©2021 AppGuard, Inc. AppGuard® and all associated logos and designs are trademarks of AppGuard, Inc. All other registered trademarks or trademarks are property of their respective owners.

APPGUARD
The Malware Disruptor

www.appguard.us | sales@appguard.us