APPGUARD
The Malware Disruptor

TECH SHEET

Defend Government Assets from Sophisticated Attacks with AppGuard's Pre-Detection Endpoint Protection

Recent high-profile and widespread cyberattacks on local, federal, and national government entities have disrupted people, economies, and critical national infrastructure across the globe. These attacks are often reminders that reactive technologies that detect the presence of malware and then attempt to remedy the harm are no match for today's sophisticated attacks. Antivirus and other detection-based methods fail because they attempt to monitor and parse almost infinite volumes of detection and indicator of attack data, requiring more tools, more personnel, and more skills. AppGuard is different.

Outsmart Malicious Attacks with Pre-Detection Endpoint Protection

AppGuard's patented pre-detection endpoint protection prevents breaches that bypass conventional detection-based endpoint cybersecurity tools, disrupting malware at its earliest and subsequent stages of cyberattacks. Whether it's a zero-day, phishing, weaponized document, "malvertising," fileless malware, ransomware, supply chain, memory scraping, or another form of escalating attack, AppGuard stops these attacks - before harm is done.

AppGuard: A Proven Government Security Ally

AppGuard has long been a strong presence and resilient leader in protecting governments from harm, ensuring emerging threats, no matter how sophisticated or new, cannot exploit security gaps to compromise endpoints. Government organizations of all sizes across the globe, including the U.S. Department of Defense; Shiroishi City, Japan; Mahnomen County Sheriff's Office; and numerous City Councils across Europe, rely upon AppGuard's pre-detection endpoint protection to secure their institution and assets.

Reduced Attack Surface: Greater Protection and Optimization of Cyber Tools

Even the best threat identification technologies (e.g. NGAV and EDR) cannot find and stop fast-striking, well obfuscated, or truly new malware - leaving a dangerous time gap. AppGuard reduces the attack surface in ways that detection-based tools cannot. It minimizes the overall risk of compromise by reducing the number of action pathways that malware can use to achieve its goals. It protects before a threat is identifiable.

With less risky activity to monitor and investigate, AppGuard alleviates the workload of other cyber defense tools and programs - making them more efficient and cost-effective.

Complements Detection-based Protection Deployed

AppGuard is designed to be compatible with most popular antivirus tools. They can still be useful against recognizable attacks, which make up over half. AppGuard takes care of attacks launched by sophisticated actors that make their malware unrecognizable. AppGuard blocks malware attacks where no pattern matching detection data yet exists in the cyber community.

A Valuable Addition for Both Large and Small Organizations

For small government organizations that lack a trove of cyber security tools and security resources, AppGuard's added protection alleviates the resource demands that detection-based defenses put on organizations. AppGuard does not require whitelists to maintain or machine learning to tune.

> *"Once AppGuard was installed, we could tell the computers were insulated and protected because we could see the malware trying to get back into the machine without success."*
>
> — Josh Guenther, Sheriff with Mahnomen County

For large government entities that are prime targets for nation-state attacks, AppGuard closes the time gap. By blocking malware from executing, without having to recognize the malware, AppGuard affords AV and EDR tools - and personnel - time to identify the damage. Detect and respond tools downstream in the cyber stack will detect fewer incidents and will fire off fewer alerts. Reducing the number of alerts needing investigating and remediation, security analysts gain back time to focus on more strategic issues and overall security hygiene.

AppGuard's Simple, Effective Pre-Compromise Security

- No alerts to investigate, just notifications
- No performance impact on hosts
- No need to rush application patches out
- No whitelists to maintain
- No artificial intelligence or machine learning
- No dependence on Indicators of Compromise/Attack

In the course of a few months hackers managed to breach the U.S. Department of Homeland Security, Ireland's National Health Services, the Metropolitan Water District of Southern California, New Zealand's central bank, and New York City's Metropolitan Transportation Authority, disrupting critical services. These attacks are often reminders that reactive technologies that detect the presence of malware and then attempt to remedy the harm are no match for today's sophisticated attacks. Like many national, state, local and tribal attacks, these attacks could have been avoided – with the right tools.

Prevention Without Detection

Outsmart malicious actors before malware causes harm. AppGuard prevents malicious code from executing without having to detect malware or its effects. Alternatives only succeed if they recognize malice. AppGuard succeeds regardless.

Zero Trust within the Endpoint

Adaptive containment and isolation block malware's intended actions. AppGuard limits application launches to the demonstrably trustworthy and limits what the high-risk trustworthy may do.

Universal, Virtual Patching

Unpatched applications are attractive attack surfaces for adversaries. Keeping up with patches is not easy. AppGuard's auto-adaptive containment blocks adversaries trying to take advantage of missing patches.

Greater Security with Less Effort, Less Resources

Adaptive, preventative controls mean no alerts, no investigations, no threat hunting, and no whitelists to maintain – increasing protection while reducing operational and labor costs

Low CPU and Memory

No CPU or user productivity degradation. Carries a light footprint with no processor dependency and minimal system resource requirements.

About AppGuard

AppGuard, Inc., a Blue Planet-Works company, provides endpoint protection software that blocks malware in real-time, before endpoints are compromised, without having to detect or recognize it. AppGuard was founded on the belief that prevention is a critical component of an effective defense-in-depth strategy and complements detection-based tools that often are unable to detect new malware variants. Today, over 6,000 organizations leverage AppGuard's patented technology to outsmart malicious actors by disrupting known and unknown, fileless, and Zero-day exploits before they cause harm.

©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