APPGUARD
The Malware Disruptor

DATASHEET

# AppGuard: Endpoint Protection for Small to Medium Business

If you're a small or medium size business and think you are not big enough to be a target for cyber criminals, think again. According to Ponemon Institute, 63% of SMBs experienced a data breach in 2019. That's because hackers are opportunistic – they realize that SMBs typically have fewer, less trained resources dedicated to fighting cyber adversaries and are more likely to pay off ransomware demands without the resources to remediate. Staying ahead of malicious actors is difficult, especially for small and mid-sized companies. Unfortunately, that challenge is even greater now that the COVID pandemic has altered the way we conduct business.

The shift to remote and hybrid work environments, prompted by COVID, has only compounded the risks facing SMBs. Managing a mobile workforce that is using new digital services and products fundamentally increases the attack surface as employees move away from corporate networks and security safeguards. A once hardened perimeter is now blurred, porous, and open to cyberattacks. Now, more than ever, SMBs need to up their security game to protect endpoints from being compromised.

## AppGuard: Simple, Effective Endpoint Protection

AppGuard empowers SMBs to overcome the challenges of limited staff and security budgets. Whether managing endpoint security in-house, or with support from an MSSP, AppGuard gives you the protection you need to disrupt malware before it causes harm.

## Better Protection, Less Resource Consumption

Without taxing your already overworked staff, AppGuard allows your business to do what it needs to do, while disrupting malware from doing what it wants to do. Initially developed to protect U.S. intelligence high-risk personnel and data, AppGuard requires minimal human resources and compute power to run. Unlike other tools that need an army of security professionals to manage, AppGuard is simple to deploy and can be managed by a single Windows administrator. Adaptive prevention controls mean no alerts, no investigations, no threat hunting, and no whitelists to maintain – just increased protection with reduced operational and labor costs.

## Prevention without Detection

Most endpoint protection tools take a reactive approach – they detect when a system has been compromised and then attempt to control the damage. AppGuard takes a different approach. Instead of detecting malware, AppGuard proactively disrupts malware to prevent security breaches – providing better protection with less effort and less stress.

AppGuard outsmarts malicious actors by applying autonomously adaptive policy controls over application behavior. AppGuard policy controls restrict the type of actions that malware must execute on endpoints in order to cause harm (e.g. command and control or data exfiltration). Blocking actions based on context, AppGuard protects systems in real-time against malware, regardless of the attack vector or type of attack – without the limitations and post-compromise costs of detection-based tools. Prevention at the endpoint reduces work at outer layers and increases the ROI for existing security tools. If malware does not breach the endpoint, non-endpoint tools (e.g. network intrusion detection, deception grid, SIEM, etc.) will have fewer indicators of compromise to detect and will produce less false positives. Preventive controls at the endpoint reduce lateral movement and the workload of other tools, thereby increasing the efficiency of resources and the effectiveness of security programs.

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

## Zero Trust within the Endpoint

Zero Trust security is no longer just a lofty concept. The key principle of the Zero Trust security model is ensuring only trusted actions are executed. Given the endpoint is the target for most hackers, ensuring Zero Trust within the endpoint is key to thwarting attacks and preventing malicious lateral movement within the network. By applying Zero Trust within the endpoint, AppGuard ensures applications and utilities cannot be exploited by hackers to penetrate endpoints to cause harm.

AppGuard achieves Zero Trust within the endpoint using adaptive containment and isolation to block malware's intended actions by containing unacceptable actions or processes from high-risk applications and utilities. By limiting what actions are allowed within the endpoint, instead of having to explicitly recognize good vs bad or normal vs. abnormal behavior, AppGuard increases attack resilience and improves your organization's security posture without exhausting internal resources. AppGuard's Zero Trust approach to securing endpoints enables you to stop attacks before they begin.

## Policy Driven Protection

AppGuard operates from the OS kernel, allowing it to use real-time process data to referee application activity and block untrustworthy executables and scripts from launching. From the kernel, it can see the parent-child execution path for every process (e.g. what triggered the process and the interim steps taken to get to the high-risk action). AppGuard adapts its controls and blocks high-risk actions only when they start from an untrusted source.

Out of the box, agents are fully operational and protective using the default or initial policy settings, Agents run smoothly for months or years without policy updates. Application updates, patches, or other changes on the system (including malware evolution) do not alter AppGuard's efficiency or operations because policies are not application or utility specific. Exceptions to default policies can be made if an administrator chooses to allow a high-risk action in a certain context for some operational reasons. For enterprise deployments this is controlled in the AppGuard Management System (AGMS).

## Don't Settle for Limited Anti-Virus Protections, Make Them Better

Traditional anti-virus tools provide some value but have significant limitations because they rely on identifying previously seen malware. In fact, reports estimate that


many popular anti-virus solutions are only able to detect 40 percent of attacks since many successful breaches are due to unknown, zero-day, or fileless malware – categories which are undetectable by the anti-virus signature-based detections.

Plus, because they scan only periodically and not in real-time, even when they do find malware it is often too late. AppGuard acts as the perfect complement because it disrupts malware activity in real-time by ensuring only acceptable processes that adhere to established policies can execute. You stay safe while your anti-virus gets the time it needs to clean up later on.

## AppGuard: Protecting Endpoints, Securing Business

Good security should make life easier for overworked IT and security departments, not harder. Organizations must adopt a strategy of prevention and not merely rely on detection or remediation solutions. With AppGuard in place, organizations can have peace of mind knowing their endpoints won't be compromised.

## Simple, Effective Pre-Compromise Security

- No alerts to investigate
- No whitelists to maintain
- No artificial intelligence or machine learning
- No application isolation or sandboxing
- No Indicators of Compromise or Indicators of Attack
- No disk scanning

## Platforms Supported:

- Windows XP – Windows 10
- Windows Server OS, 2008 R2 SP1, 2012 R2, 2016, and 2019
- Red Hat Enterprise Linux Server OS, 7.4, 7.5, and 7.6

## 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.



APPGUARD
The Malware Disruptor

www.appguard.us | sales@appguard.us