APPGUARD
The Malware Disruptor

DATASHEET

Disrupt Malware **Before** it Does Damage

Endpoints are vulnerable, and defeating malware is hard. Despite increased spending on cybersecurity tools and personnel, malware continues to bypass existing security controls to gain access to endpoints. Traditional security defenses such as firewalls, secure email gateways, IPSs, signature-based solutions, and next generation endpoint protection platforms can play a role in your defense-in-depth strategy, but they continue to fall short on protecting against advanced threats and zero-day exploits.

Endpoints without Compromise

The ultimate goal for investing in endpoint protection tools is to ensure business can do what it needs to, and malware can't do what it wants to. 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 prevent malware from executing 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 (no alerts to chase, no signatures to detect, no army of security analysts drowning in data), thereby increasing the efficiency of security teams and the effectiveness of security programs.

Prevention without Detection

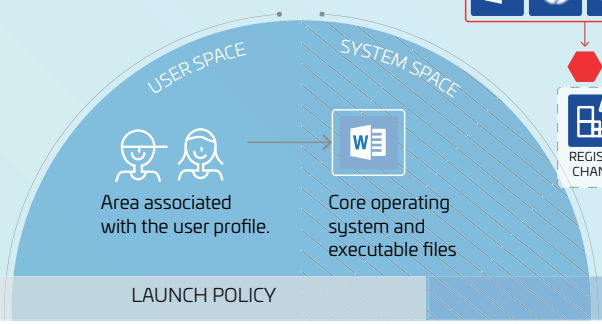
AppGuard's "prevention without detection" philosophy negates the guesswork involved with detecting good from bad activities. By controlling and constraining the

Prevent Breaches with 3-Point Policy Protection

Zero Trust Space
LOCATION-BASED POLICY

Key operating system folders are separated into System Space. **Applications and utilities can only launch from the System Space** unless a "trusted" exception is granted.

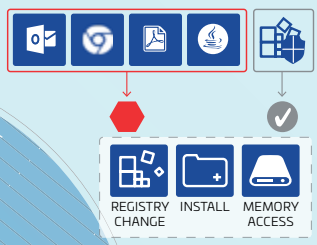
User Space is "untrusted" territory, where executables are blocked from launching.



Isolation
OS INTERACTION POLICY (PATENTED)

Applications in System Space are grouped into **high-risk** and "normal" applications.

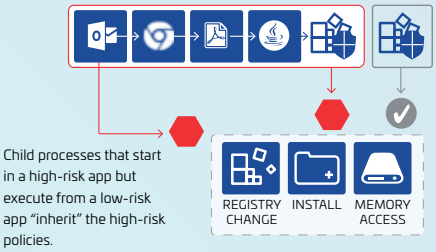
High-risk apps are blocked from executing processes malware requires to cause harm.



Inheritance
PROCESS EXECUTION FLOW POLICY (PATENTED)

Inheritance ensures that isolation rules are automatically adapted for more precise controls with less management burden.

Advanced malware cannot hide its actions using a normally unrestricted application.



Child processes that start in a high-risk app but execute from a low-risk app "inherit" the high-risk policies.

LAUNCH POLICY

POST-LAUNCH POLICIES

behavior of applications and utilities, AppGuard ensures processes executed adhere to established policies, thereby reducing the risky actions that malware can take, regardless of the form it takes – new or old. This allows AppGuard to protect assets from unknown malicious processes of unknown origins without having to recognize malware or its effects.

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

Disrupting Malware at the Source

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.

Secure Architecture

For enterprise deployments, policies are controlled centrally in the AppGuard Management System (AGMS). The AGMS console generates agent install packages, creates and distributes policies, and collects and reviews endpoint logs. Policies are distributed through a relay server that the agent checks periodically, removing the possibility of a backdoor. Out of the box, agents are fully operational and protective using the default or initial policy settings and run smoothly for months or years without policy updates or internet connectivity. Application updates, patches, or other changes on the system (including malware evolution) do not alter its 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.

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

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 adaptive containment blocks adversaries trying to take advantage of missing patches.

Greater Security, Less Effort, Less Resources Required

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

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