

AppGuard Enterprise

The Most Important Cyber Stack Layer to Add

AppGuard Enterprise delivers patented, kernel-enforced controls that stops advanced malware, zero-days, ransomware, and living-off-the-land attacks by blocking the malicious actions and techniques used by all malware. The result is that AppGuard stops what detection-based defenses miss as well as stopping attacks *prior* to the “damage window” that detection-based tools expose to enterprises.



Complements EDR/XDR

AppGuard works seamlessly alongside EDR/XDR on the same endpoint. While EDR/XDR excels at detecting known threats and generating alerts, AppGuard stops unknown, zero-day, and evasive malware that slips through the “detection gap”, preventing real damage without adding operational friction.

Closes EDR/XDR “Detection Gap”

EDR/XDR rely on pattern-matching to recognize malware. They successfully detect and alert on most threats but sophisticated or new malware evades detection, creating a dangerous “detection gap” where attacks can progress.



Close EDR/XDR “Damage Window”

The “damage window” is the critical period between initial execution and response. With EDR/XDR alone, this window can last seconds to weeks, allowing data exfiltration, credential theft, ransomware staging, lateral movement, and cybersecurity tool impairment. Appguard closes it instantly by blocking malicious actions before harm occurs.

Launch

Protected by Contain & Isolate,
allows all launches (Windows, Program Files)

Only Allowed Exes, Scripts, DLLs
can Launch from high-risk folders
(downloads, documents, desktop,
Windows\Temp, and other high-risk folders)

Launch—AppGuard restricts what can run from high-risk folders, greatly reducing attack surface. By relying on “Contain” and “Isolate” controls to protect other folders, AppGuard requires far fewer policy rules than alternatives. The result is simpler administration and less risk of disrupting end-user workflows.

Contain—AppGuard restricts what the running can do. This applies to high-risk applications, preventing them from making changes they shouldn’t as well as preventing them from interfering with other applications.

Contain

Windows
Registry

App
Memory

Program
Files

Windows
Memory

Child
Processes

Windows
Files

HIJACKED LEGITIMATE
APPLICATION

Isolate

High Value App

Windows
Registry

Folders
& Files

Malware

Isolate—AppGuard isolates parts of the host from the rest of the host to prevent illegitimate access or changes that could result in corrupting legitimate applications’ memory, stealing credentials, and/or altering security settings.

The AppGuard Difference makes it the Perfect Complement

- Stops what other defenses miss entirely or detect too late
- Essential layer of protection for your cyber stack
- Reduces malware attack risks, reduces cyber operations costs
- Avoids the end-user disruptions other application control & containment tools inflict
- Mitigates risks from applications with missing patches or unknown vulnerabilities from zero-day attacks

Proven Outcomes for Enterprises

- Fewer malware incidents — stops what detection tools miss entirely or detect too late
- Less cyber noise & chaos — dramatically reduced alerts, investigations, and remediations
- Lighter cyber operations
- No performance impact — one-fifth the footprint of Microsoft Defender; auto-adapts to app updates
- Stops real-world threats: Qilin/Warlock ransomware (BYOVD EDR-killers), ClickFix clipboard hijacks, Chrome zero-days, Claude AI agent exploits

All Nippon Airlines (ANA)

- “No successful malware attacks since AppGuard was fully deployed in 2019”, Akihiro Wada, Digital Transformation Office, General Manager, Information Security and Infrastructure Strategy
- No help desk tickets due to AppGuard obstructing applications or end-user productivity
- SOC teams had 66%+ hour reduction at major airline with 40k endpoints
- Significant cost savings — >\$750,000/year minimum at enterprise scale (\$18+/PC/year)

Availability

- Fully managed (Expert MSSP 24/7 x365)
- Do-it-Yourself

Supported Endpoints

- Windows XP SP3 – Windows 11
- Windows Server 2008 R2 SP1 – 2025

READY TO STOP WHAT YOUR EDR/XDR MISSES?

AppGuard Enterprise is the essential, additional layer that makes your entire cyber stack more effective and dramatically less expensive.



About AppGuard

AppGuard is a cybersecurity company on a mission to fill an urgent need for better protection from malware attacks due to the inability of detection technologies to tell bad from good among nearly infinite possibilities. AppGuard's approach is completely different; it is controls based. AppGuard defeats malware without having to recognize the malware itself by not allowing malware to do what it needs to do.