SOLUTION BRIEF

Reinventing Endpoint Cybersecurity for Government

August 2019

APPGUARD

703.786.8884
sales@appguard.us
www.appguard.us

Reinventing Endpoint Cybersecurity for Government

Up to 1 million new malware strains are released every day. AppGuard prevents all breaches from both known and unknown cyber threats.

AppGuard Benefits

- **Defeat Emerging Malware** – defeats new emerging malware that other approaches cannot stop, such as when malware utilizes existing Windows capabilities and tools for malicious reasons.
- **Defeat Weaponized Documents** – protects endpoints against weaponized document attacks by preventing the execution of malware and ransomware in the first place.
- **Versatile Defense through Runtime Processes** – runtime process protections provide a versatile defense that extends the protection to endpoint processes, server processes, and insider threats.
- **No Update Ever Needed** – does not require constant updates; AppGuard builds lists of known security threats already identified by other sources. Its integrated software-only approach is seamless with all Microsoft Windows platforms, stands alone with no OS hooks, and includes all documented APIs.
- **No CPU Degradation** – carries a light footprint with no processor dependency and minimal system resource requirements. Transparent to the end user, AppGuard creates an efficiency management function that is less resource-intensive than even legacy antivirus platforms.
- **No User Interaction Required** – does not require user interaction once installed. AppGuard does it all for you, completely autonomously.

Overview

As the volume of sensitive and mission-critical data grows, government networks continue to be prime targets for sophisticated cyberattacks. Protecting this information is key, but agencies must also keep a close eye on the weakest link in their network – the endpoint. As breaches become more sophisticated and unknown threats bypass traditional detection-based methods, attack mechanisms are lying dormant on agency endpoints for months before being detected.

The challenge is acute. Fifty-nine percent of federal government security personnel say their agency struggles to understand how cyber attackers could breach their systems. Furthermore, 65 percent don't think the government can detect ongoing cyber attackers.[1]

As breaches continue to spiral out of control, agencies must seek to gain an understanding of these attacks and develop a proactive prevention-based security posture, one that challenges the traditional approach of detect and respond, i.e., play catch-up.

Effective Prevention for Government

A key challenge for government agencies is that conventional endpoint cybersecurity solutions either can't or don't stop an attack. Rather, they attempt to detect or contain a compromise that has already occurred, then attempt to respond in sufficient time to limit its effects.

Rather than focus on the detection of malware, industry experts stress an emphasis on prevention. With its a unique, patented, multi-layer endpoint defense, AppGuard prevents breaches from occurring by disrupting the earliest and subsequent stages of cyberattacks that other endpoint cybersecurity approaches cannot detect. Examples of these cyberattacks include zero-day malware, phishing, weaponized documents, "malvertising," watering holes, fileless malware, drive-by downloads, ransomware, memory scrapers, and other forms of escalating attacks that conventional approaches don't always detect.

[1] 2016 Survey by (ISC)2 and KPMG of Federal Cybersecurity

The AppGuard Difference

AppGuard prevents malware from detonating without requiring signature-based detection (such capabilities can be easily defeated by newly emerging undetectable malware attacks), scanning, or updates, thus preventing compromises from occurring. It delivers valuable Indicators of Attack (IOA) well in advance of conventional detection, response, and containment products which typically rely on detecting and identifying Indicators of Compromise (IOC) after a compromise has already occurred.

> "Functionally, an endpoint security suite should create an environment where malware can't load into memory or an exploit is unable to take advantage of a running process."
>
> *The Forrester Wave™: Endpoint Security Suites, Q4 2016*

AppGuard differs from traditional antivirus approaches in several ways. Antivirus technologies enable behavior-scanning and identification of malicious behaviors that disrupt productivity and expend system resources. Traditional AV protection is also only as good as the signature database or the last update, AppGuard protection does not depend on signatures, detection, scanning, or updates. AppGuard is designed to be compatible with most popular antivirus tools, which can still be useful for performing system maintenance infrequently to remove unwanted code rendered dormant by AppGuard.

Other traditional breach detection systems that use sandboxing techniques have their usefulness, but they can interfere with user productivity and introduce the possibility that a user may be operating in a compromised sandbox. In contrast, AppGuard employs dynamic containers in conjunction with its micro-isolation technology. Any application can be added to AppGuard's containment group, which AppGuard will automatically protect. Attacks are halted at the first stage, so there's no need to worry about compromised user workspaces or system resources. Plus, sandboxing is largely ineffective for addressing emerging, advanced threats such as spear-phishing, watering hole, or advertising attacks, where AppGuard excels.

Versatile, Scalable, Manageable

Built with versatility in mind, AppGuard meets a broad range of customer needs. AppGuard Enterprise places AppGuard software endpoint agents under the central administrative control of an enterprise management system. Protection policies can be customized to specific enterprise requirements for individual trust groups. Highly granular per process Indicator of Attack (IOA) event data is collected without a compromise occurring, digitally signed, encrypted, and reported through the separate system management plane to enhance situational awareness of the host environment, "on" or "off" enterprise.

AppGuard at Work

A prominent think tank in Washington, D.C., with over 300 employees had been breached on numerous occasions and was battling ongoing adversary attacks even with well-known network and endpoint security tools in place. The customer was concerned that their current endpoint breach detection was not sufficient to protect their sensitive data from undetectable threats. They turned to AppGuard in 2016 to help augment their existing antivirus protection and add an extra layer of defense to prevent advanced attacks from happening.

Following the deployment of AppGuard, an employee fell victim to an advanced targeted attack (ATA). The malware writer had targeted this employee with an email containing a malicious PDF file that appeared to have been sent from the employee's boss. When the employee clicked on the attachment, the malware instantly attempted to write a signature to both the registry and Just-in-Time memory, but AppGuard prevented both actions from happening, thus stopping the otherwise undetectable malware in its tracks before any compromise could occur. The organization was then able to safely remove the malicious file from the employee's computer, without ever needing to detect or respond to an incident. To date, the organization has not been breached after the deployment of AppGuard.

"Futureproof" Breach Prevention for Government

AppGuard delivers a breakthrough ability to prevent breaches on endpoints from emerging advanced threats that conventional cybersecurity approaches cannot address. It is engineered to deliver an effective new, compatible, scalable, and affordable layer of cybersecurity defense to address even unknown and undetectable threats now and in the future.

AppGuard Enterprise can be deployed as a fully-managed or co-managed service in the cloud, or as an enterprise site license with essentially no limit to the scalability of the management system and the number of endpoints it can manage. AppGuard Business delivers an affordable solution for small and mid-sized businesses to comprehensively protect their systems and operations without complexity or overhead.

APPGUARD

A Blue Planet-works Company

About AppGuard

AppGuard provides award-winning server, endpoint and mobile cybersecurity protection for enterprises as well as small and medium-sized businesses. AppGuard's patented inheritance technology maintains the same level of guarding and isolation on any process spawned from a risky application. The technology does not rely on detection and response, instead preventing all attacks.

Contact us to learn more about AppGuard managed security services:
www.appguard.us or **sales@appguard.us**

VA Office

14170 Newbrook Drive Suite LL-01
Chantilly, VA 20151
USA

NY Office

333 Seventh Avenue
10th Floor
New York, NY 10001
USA

LA Office

530 Wilshire Boulevard
Suite 206
Santa Monica, CA 90401
USA

Tokyo Office

(Blue Planet-works, Inc.)
Daiwa Jingumae Bldg., 3Fl2-4-11
Jingumae
Shibuya-Ku Tokyo,
150 - 0002
Japan

703.786.8884
sales@appguard.us
www.appguard.us