SOLUTION BRIEF

Reinventing Endpoint Cybersecurity for Financial Services

August 2019

APPGUARD

703.786.8884
sales@appguard.us
www.appguard.us

Reinventing Endpoint Cybersecurity for Financial Services

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

Financial services organizations are increasingly high-value targets of malware-based cyberattacks. Bank ATMs and other endpoints are particularly vulnerable to malware, which can threaten and expose sensitive customer data, and cause untold financial and reputational damage. With new and advanced threats such as fileless code, memory-based attacks, and stolen signing certificates, financial organizations are at risk more than ever from increasingly sophisticated, targeted, and undetectable attacks.

How have things escalated to this point? Much of the problem stems from the fact that traditional antivirus, machine learning, and artificial intelligence learning solutions can't stop an attack. Instead, they attempt to detect or contain a compromise that has already occurred, then attempt to respond quickly enough to limit its effects. But as recent headlines have shown, these attacks are going unnoticed for weeks and, in some cases, even months.

Effective Breach Prevention for Financial Services

Rather than focus on the detection of malware (an approach that is clearly failing), industry experts place a strong emphasis on *prevention*. With its unique, patented, dynamic 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 traditional approaches can't and don't stop.

ATM Breach Prevention Stops Even Undetectable Malware Attacks

ATM malware is on the rise, but the threat is changing. A shift away from physical methods of attack, such as card skimmers, is making it easier and safer for adversaries to steal money and credit card information. ATMs are typically connected to a bank's network where a virus with escalation privileges can quickly find devices and compromise them.

Traditional security approaches to such threats, such as whitelisting, are ineffective. Whitelisting is costly with high costs of maintenance and management overhead. Plus, it provides zero protection once the application is running and is easily defeated by signed malware. Antivirus requires signature-based detection; such features can be easily defeated by newly emerging undetectable malware attacks. Furthermore, most conventional ATM protection methods are not compatible with legacy ATMs that often run on older operating systems that are difficult to upgrade and lack the capability to support the large overhead inherent in most detection and response protections.

AppGuard is versatile, scalable, manageable. AppGuard works to prevent unauthorized ATM intrusions from any malware-based attack:

- Unauthorized scripts or malware are prevented from executing a first-stage attack on the ATM or running malware from a USB device or CD-ROM used for maintenance.
- AppGuard does not rely on scanning, detection, or signature identification to provide protection, thus reducing system overhead.
- AppGuard always protects without requiring updates or patches, reducing risks from ATM system maintenance delays. When ATM maintenance is implemented, AppGuard enforces an orderly process with a security audit to maintain system integrity.

AppGuard is fully compatible with Windows XP SP3 through Windows 10, mitigating risks for new generation as well as legacy ATM systems. Existing enterprise System Management tools can be used to distribute the software and collect AppGuard Event Logs from the ATM Windows Event Viewer. Default policies are simple to manage and incorporate the ever-changing vendor images.

> “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*

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.

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 workspace 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 – "Futureproof" Breach Prevention for Financial Systems

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 at Work

This use case is of a large Mortgage lender in Northern Virginia with more than 500 employees on staff. Being a high value target in the financial industry, the organization was repeatedly battling ongoing attacks. The year prior to AppGuard's deployment, the organization had been the victim of three separate ransomware attacks in which adversaries were able to exfiltrate sensitive data, customer information, and files. While the repercussions of these events were contained to a minimum, the organization knew that it was only a matter of time before an advanced attack would devastate the company. The company approached AppGuard in 2016 to prevent cyberattacks from further compromising sensitive data. AppGuard was rapidly and seamlessly deployed for all of the customer's endpoints and worked with the customer to establish custom security policies. To date, this customer has not been successfully breached with AppGuard deployed.

APPGUARD *A Blue Planet-works Company*

To learn more about AppGuard managed security services, visit **www.appguard.us** or contact **sales@appguard.us**

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