SYSTEM OVERVIEW

APPGUARD

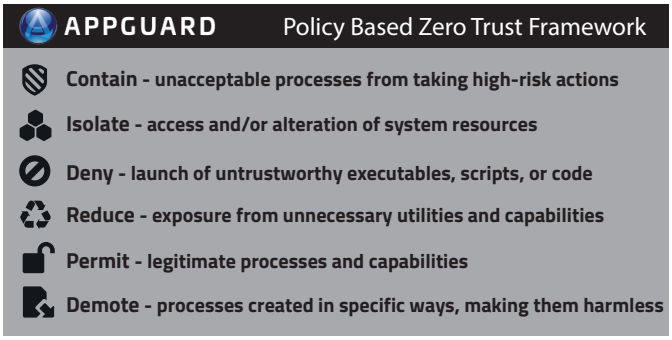
ACHIEVING ZERO TRUST ENDPOINT PROTECTION.

Traditional Endpoint Protection - Elusive and Unreliable

Typical endpoint cybersecurity methodologies continually monitor and investigate vast amounts of diverse endpoint event data to try to find evidence of attacks. These methodologies parse a constantly expanding range of possibilities to identify malicious events and compromises. Malware, ransomware, phishing, and other sources of cybersecurity attacks are constantly evolving in their ability to defeat these approaches to breach prevention. These traditional protection approaches typically require continual increases in expensive computing resources, sophisticated software tools, and skilled personnel while still leaving the endpoint vulnerable to undetectable attacks designed to evade these methodologies. Organizations should instead apply Zero Trust Endpoint protection to achieve a more resilient and dependable endpoint protection with less resources.

AppGuard© Zero Trust Endpoint Protection - Resilient and Reliable

Instead of attempting to identify every anomalous event or react to a compromise after it has already happened, AppGuard employs patented Zero Trust isolation and containment methodologies that disrupt malware's intended actions before the malware can modify or infect a system. Using Zero Trust process policy control, AppGuard blocks modification of application and utility processes that allow malicious code to do harm. It's Adaptive Policy Enforcement (APE) technology autonomously adapts in real-time to ensure that each individual process triggered by an initial process is protected from malicious actions while still allowing the application to function normally. If AppGuard cannot deterministically block a given process, then it restrains that process from launching, thereby upholding a true Zero Trust protection approach.



AppGuard's unique approach to endpoint breach prevention defeats malware in real-time without having to detect it or rely on signatures, updates, patching, or management dependencies for protection. AppGuard eliminates the uncertainties, complexity, and overhead associated with more traditional protection methodologies, alleviating resources from having to respond to constant false positive and false negative alerts. This results in dependable, resilient endpoint protection with increased efficiency of other cyber defenses. AppGuard is broadly compatible with a wide range of applications over their life-cycle.

Flexible Deployment Options

AppGuard can support an unlimited number of workstations and servers for enterprises, individual computers, and specialized endpoints such as ATMs and Point-of-Sale machines. AppGuard is offered as an enterprise software license or as a 24x7x365 service managed by Blue Ridge Networks.

sales@blueridgenetworks.com | 1-800-722-1168 | BlueRidgeNetworks.com

AppGuard Enterprise is the award-winning, breach prevention system for enterprise endpoint security management. It is compatible with all supported Windows versions, deploys with scale, does not require constant updates, and is not disruptive to users and productivity. The AppGuard management system allows administrators to establish enterprise policies that are enforced on endpoints "on" and "off" enterprise, without on-going management system dependencies for endpoint protection and reporting.

AppGuard endpoint software agents use minimal system resources and operate without disturbing legitimate user operations. More than 90% of AppGuard's enforced policies are defined by default, allowing agents to run for an extended time without policy updates. Containment control policies are enforced uniformly for all at-risk applications, beginning with its parent executable and continuing to all resulting processes. This means little information is required for policy formulation, and updates/patches do not necessitate policy updates, avoiding the application specific policy complexities of alternatives. Enterprise policies can be easily distributed by standard enterprise software management tools (e.g., SCCM) and managed in the cloud. Because AppGuard protection doesn't rely on attack detection, identification, signatures, scanning, or management system dependency, network systems aren't flooded with constant updates and user endpoint performance is not impacted.

AppGuard generates granular per process Indicators of Attack (IoA) data, providing the earliest possible threat intelligence without a compromise occurring. The log events and IoA data are created when AppGuard blocks processes that try to alter certain system components. These logs are digitally signed and encrypted, and then sent to a log retrieval point for the AppGuard Enterprise Management System. Once transmitted, these logs are removed from the endpoint to free up its system resources.

AppGuard for Servers is designed from the ground up with server defense in mind. It delivers dynamic isolation and containment of critical processes and mitigates risk while allowing critical applications to continue useful operation. Alternatives must quarantine or terminate compromised servers which impacts operations and drains IT resources.

AppGuard for Servers segregates information, delivering "walls" of defense among server processes. Using granular and manageable policies augmented by trusted publisher information and file location, AppGuard for Servers delivers application control that is both practical and effective. Additional runtime protections further establish boundaries around processes, preventing unauthorized code from making system configuration changes.

AppGuard for Servers is the only preventive technology that stops breach attempts in servers at the earliest stages of attack. It does so without scanning, relying on signatures or recognizing Indicators of Compromise (IoC) - AppGuard for Servers stops the attack and generates IoA event data.

AppGuard for Servers Supported Platforms, both cloud-based and local platforms: Windows 2008 R2, Windows 2012, Windows 2012 R2, Windows Server 2016

AppGuard is distributed by Blue Ridge Networks under agreement with joint venture partner Blue Planet-works, Inc.

sales@blueridgenetworks.com | 1-800-722-1168 | BlueRidgeNetworks.com