Secure Your Remote Employees with APPGUARD

A novel virus named COVID-19 is rapidly spreading across the globe. Cybercriminals have already started leveraging the fear connected with COVID-19 pandemic as a tool to spread misinformation, steal passwords, data, and harm critical infrastructure.

Employees are now increasingly working from locations outside of the traditional corporate network environment. These remote workers bypass legacy perimeter-based security controls,leaving enterprises exposed and vulnerable to data loss, and advanced cybersecurity threats. A preventative ZERO-TRUST security solution is needed to provide robust protection to remote employees without compromising productivity.

Employees are struggling with providing security for remote employees:

- Traditional security solutions are typically located in data centers, are costly, and need constant monitoring and triage activities which are limited in a remote work environment
- These solutions are not capable of protecting employees working outside the traditional perimeter-based security controls, leaving organization exposed
- The remote access VPNs used to connect devices with centralized resources is unstable and bypasses most security control. Moreover, all traditional solutions need constant internet access to offer any level of protection

SECURING REMOTE WORKERS WITH APPGUARD

AppGuard's unique patented dynamic defense prevents breaches from occurring by disrupting the earliest and subsequent stages of a cyber-attack. AppGuard does not require any user interaction or cause CPU degradation. It simply protects the endpoint irrespective of network connection and does not need a team of analysts to monitor and remediate alerts.

AppGuard's policy-based, zero-trust framework mitigates application misuse and hijacking risks by Enforcing policies, so applications do only what they are supposed to do. Blocking actions that do not conform to policies. Adapting in real-time to application updates, patches, and other changes to avoid administrative burdens and mitigate unanticipated attack vectors.

During this time of uncertainty, how can enterprises secure critical infrastructure? WITH APPGUARD SOLO. We are offering free AppGuard Solo licenses for the next 90 days to protect your enterprise. After the 90 day trial, we will work with you to convert licenses to AppGuard Enterprise or continue with Solo at a 60% discount

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.

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.

Defeat Weaponized Documents

protects endpoints against weaponized document attacks by preventing the execution of malware and ransomware in the first place.

No Update 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 User Interaction Required

does not require user interaction once installed. AppGuard does it all for you, completely autonomously.

Versatile Defense through Runtime Processes

runtime process protections provide a versatile defense that extends the protection to endpoint processes, server processes, and insider threats.

APPGUARD

The AppGuard Difference

AppGuard prevents malware from detonating without requiring signature-based detection (newly emerging undetectable malware attacks can easily defeat such capabilities), scanning, or updates, preventing compromises from occurring. It delivers valuable Indicators of Attack (IOA) well in advance, unlike conventional "detect and response" 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.

Other legacy detection systems that use sandboxing techniques can interfere with user productivity and introduce the possibility that a user may be operating in a compromised sandbox; this is a big challenge, especially with remote workers. 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. Moreover, 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 Solo operates with similar principles on individual workstations, without the centralized administrative control.

AppGuard – Breach Prevention for Remote Workers during COVID-19

Protect Your Enterprise Now: Implement AppGuard Solo NOW for free for the next 90 days to immediately combat cyber threats in the emergency remote work environment.

Harden Your Enterprise for the Future: Work with us after the initial implementation to develop the right future plan for your enterprise, which can include:

- Continued use of AppGuard Solo at a 60% discount
- Strategic transfer to centrally managed Enterprise solution after the present crisis has abated.

Home Run for AppGuard

"Distributing AppGuard to my members secured our remote devices and increased membership and usage by quelling their fears."

~ CIO of the Financial Institute