APPGUARD
The Malware Disruptor

Department of Defense Healthcare Agency Adds Zero-Day Server Defenses with AppGuard

CASE STUDY: DEPARTMENT OF DEFENSE HEALTHCARE

CHALLENGES:

- Protecting against zero-day and reshaped malware attacks on servers hosting mission critical applications before detection oriented tools and personnel can react
- Eliminating high infrastructure downtime due to security incidents, despite heavy investments in resources and technology

OUTCOMES:

- Optimization of security tools and resources
- Easy deployment, fast time to value.
- Greater security, less effort.
- Hardened servers that neutralize attacks in real-time, slashing overall incident monitoring and response volume.

About Agency

The Agency manages critical healthcare data and activities related to the U.S. Department of Defense. In such a critical environment, security concerns are paramount to protect human lives.

Situation:

The Agency needed to ensure added protection and improved incident response times as they moved their critical infrastructure into the cloud. The existing approach, which included HBSS and Carbon Black, provided both insight into the server environment and a detect-and-respond approach to eliminating compromises, but did not protect the servers in real-time without significant false positives. Host-based anti-virus and behavior analytics tools only succeed when they recognize malware or its effects. Adversaries vary their tactics, techniques, and procedures to evade detection. Therefore, effective use of detect and respond solutions requires human intervention, which can increase response time from milliseconds to minutes or even hours. The longer the delay, the greater the impact and incident cost. As a healthcare organization in the DoD community, security incidents that affect operations can endanger human life.

HBSS and Carbon Black had been protecting these servers. HBSS enforces allow/deny rules within endpoints that can block malware attacks without having to recognize them or their effects. However, as hosts and adversaries change, specifying and maintaining rules is difficult, leaving potential gaps in security. Carbon Black detection, while effective at

blocking known malware and specific behaviors, still left room for improvement in overall incident response times.

Solution: Real-time Protection without Detection; Host-based Software

Over the last two years, the cybersecurity community has increasingly asserted that the enterprise, and by extension the vendors offering them tools, must do more to harden the endpoints that adversaries attack. Hardening prevents alerts that must be monitored and investigated in addition to preventing compromises that must be remediated, effectively reducing labor costs while increasing protection. Labor is the single greatest cost element in cybersecurity.

This cannot be accomplished with perimeter tools. It must be done from within the servers themselves, and while there have always been plenty of methods to do so, the traditional options are burdensome.

Traditional hardening controls require knowledge of extreme detail about both applications on a server and the host itself. Imprecise, incomplete policies disrupt operations. Acquiring this precise detail and implementing policies for their governance have always been very difficult. The second obstacle is change. Applications and their hosts often change due to feature updates, security patches, plugin additions, etc., and with them the policies must also change. Frequent alteration requirements have made hardening via policy controls intolerably onerous to deploy and maintain over time, requiring a solution for a policy engine that autonomously adapts to updates - enter AppGuard.

AppGuard: Better Protection, Less Effort

With other endpoint security agents resident on their servers, AppGuard's light footprint in CPU, memory, disk, and bandwidth were essential to avoiding server performance impacts. AppGuard's success lies in blocking attacks that would have been previously undetected by tools that rely on past behavior to determine potential attacks. AppGuard is also more effective against new variations of attack because it does not block based on previous attack patterns.

Functionally, AppGuard automatically adapts to normal lifecycle changes from feature updates, patches, and other environmental changes without the need for policy updates. Unlike other hardening tools, AppGuard is far less likely to hinder IT/Sec-Ops personnels' use of their preferred administrative tools. Its rules-based containment and isolation technology does not need nearly the same detail and precision about the hosts and their applications as does HBSS. So, AppGuard can be deployed and operated with a fraction of the effort and is far less disruptive to existing server operations.

In most breaches, applications let malware in and/or help do harm. Therefore, AppGuard contains applications along multiple dimensions so they cannot harm the OS or other applications. Wherever an application might drop a potentially malicious file, AppGuard restricts launches and loads from those locations to what is trustworthy. And, should some malicious process somehow gain run-time, AppGuard applies isolation rules to the most critical parts of the system, protecting them from being effected by the malicious process. This results in the malware being unable to cause any harm, despite gaining some foothold within the system.

For agencies facing similar challenges or initiatives, reach out to AppGuard to learn how AppGuard's patented endpoint protection technology can protect your enterprise during migrations.

About AppGuard

AppGuard is a cyber security company on a mission to set a new standard: true cyber protection for all. AppGuard's patented technology prevents compromises before they happen by disrupting malware activity from causing harm without having to recognize it. Unlike detection-based solutions, AppGuard outsmarts malicious actors to ensure businesses can do what they need to do, and malware can't do what it wants to.

©2021 AppGuard, Inc. AppGuard® and all associated logos and designs are trademarks of AppGuard, Inc. All other registered trademarks or trademarks are property of their respective owners.

APPGUARD
The Malware Disruptor

www.appguard.us | sales@appguard.us