APPGUARD

Case Study

Center for Strategic and International Studies (CSIS)

Industry:

Defense and National Security Think Tank

Challenges:

- Nation-State Target without Nation-State Cyber Resources
- Most Software based Endpoint Protection Tools Fail to Block Advanced Attacks

Outcome:

"For over 2 years, AppGuard has been a cost-efficient and effective endpoint protection solution that made our network more secure,"

Ian Gottesman,CIO

Center for Strategic and International Studies (CSIS)

About CSIS

It is a bipartisan, nonprofit policy research organization dedicated to providing strategic insights and policy solutions to help decision makers chart a course toward a better world. CSIS is regularly called upon by Congress, the executive branch, and the media to explain the day's events and offer bipartisan recommendations to improve U.S. strategy. For the past six years consecutively, the University of Pennsylvania has named CSIS as the number one think tank for international study.

Situation: Government Customers Expect CSIS to Withstand Cyber Attacks from Their Adversaries

The topics and customers that CSIS supports make it a target of interest to nation-state cyber intelligence agencies, organized crime, hacktivists, and other sophisticated cyber adversaries. A single data breach could devastate the reputation and trust customers have had in CSIS. It cannot afford to be lax. However, the nature of its business requires its personnel to meaningfully interact with the world so CSIS can provide the insights its customersexpect. Thisincreasesitsexposuretoadvanced attacks through the laptop and desktop computers of its personnel.

Challenge: Practical Protection from Advanced Endpoint Attacks

CSIS had deployed the industry's most recognized application whitelisting product to supplement its traditional AV and to reduce incident volume on those other cyber layers that are affected by what happens at the endpoint. Looking back at this experience, "it was too hard to manage", said Mary P. Van Engelen, Network Infrastructure Manager.

But even when configured perfectly, application whitelisting is a poor defense against fileless attacks. Different reports assert that over 50% of targeted enterprise attacks are fileless.

CSIS Contrasts its AppGuard Experience with Application Whitelisting

“Our previous application whitelisting tool was impossible for our small team to maintain. AppGuard has been more efficient and much easier to manage”, said Gottesman.

“Maintaining a whitelist was a bear. With AppGuard, we don’t have to do that”, recalled Van Engelen. It “blocks things at the process level, stopping things whitelisting misses”.

AppGuard blocks attacks on endpoints without having to recognize the malicious code or having to know those ever-changing details of the endpoint’s applications. It not only adapts automatically to application updates but it also compensates for missing security patches.

A Weaponized Document Attack Soon Showed AppGuard’s Value

Not long after AppGuard was deployed, CSIS was attacked with 56 maliciously crafted PDF documents. Neither the AV nor the EDR agents detected these attacks. A representative of the well-known EDR vendor defended his agent, “looks like AppGuard has stopped the attack, so there was nothing (e.g., compromise) to report.”

On multiple endpoints, AppGuard blocked Adobe Acrobat Reader from altering a sensitive registry key to implant malware. Moments later, AppGuard observed Acrobat Reader spawning a fileless process to do the same.

AppGuard blocked this too because it had been spawned by Acrobat Reader. This dynamic inheritance technology is responsible for many of AppGuard’s abilities to block different malicious code attacks. “AppGuard has stopped the bad things from happening”, said Gottesman.

AppGuard is a Great Choice for Organizations with Alerts Fatigue and Limited Man-Hours

Their CIO pointed out that “we get thousands of alerts everyday; we definitely have alerts fatigue. The hours we get from our personnel are probably the most precious of our resources. The team doesn’t have extra bandwidth. So, it’s nice to have a tool like AppGuard that’s pretty self-sufficient and can do a lot of things for us that doesn’t require a great deal of personnel time. My team and I are trying to manage the time we have, trying to consolidate down, alerting in fewer places. When we investigate something, we don’t want to have to look in 15 different systems. AppGuard does not force us to investigate yet more alerts. We are confident that it will block what should be blocked. AppGuard is great for a small team like ours.”

So many security products require personnel to triage and investigate vast amounts of data. Van Engelen recounted, “we only need to look at AppGuard log events when we suspect AppGuard might be blocking a software installation, which is a key best practice, when in doubt: block”.

“AppGuard has been self-sufficient. It’s not quite set it and forget it, but it’s pretty close”

Ian Gottesman,CIO
Center for Strategic and International Studies (CSIS)

APPGUARD

+44 (0)1452 886982
appguard@csa.limited
www.csazerotrust.co.uk

New York, NY; Chantilly, VA; Raleigh-Durham, NC; San Diego, CA; Colorado Springs, CO; Baltimore, MD; Columbus, OH; Washington, DC USA; Tokyo, Japan; Prague, Czech Republic; London, UK; Milan, Italy; Istanbul, Turkey; San Paolo, Brazil

About AppGuard

People and organizations all over the world are ever more interconnected via the endpoint devices in their lives. AppGuard delivers simple, effective solutions to the complex security challenges that threaten the interests of organizations as well as those of their customers. These endpoints range from personal computers to smartphones/tablets to IoT devices. AppGuard solutions prevent endpoint compromise; facilitate high assurance device to device authentication on behalf of their users; attest to the security posture of both endpoints so one does not share sensitive data with a user with an untrustworthy endpoint; and protect the privacy of end-users through anonymized, high assurance device-to-device authentication so they can communicate securely without revealing personally identifiable information of the end-users.