APPGUARD
The Malware Disruptor

International Airline Reduces Cyber Costs, Increases Security Posture with AppGuard

CASE STUDY: GLOBAL AIRLINE

CHALLENGES:

- Managing cyber defense costs while improving security posture
- Complex endpoint protection tools require cyber specialists

OUTCOMES:

- Reduced cyber incident response costs by 76%
- Greater security with less resources and efforts
- Reduced patch management burden

About the Airline

Major global airline with approximately 50,000 employees that transports about 7,000,000 passengers around the world per year. Critical infrastructure must be operational 24x7 to avoid major financial losses. A cyber breach could jeopardize passenger lives, harm reputation, and significantly impact revenue.

Situation: Complex Cyber Operations and Years of Porous Endpoint Protection

Nearly 100,000 endpoints access mission critical IT infrastructure from around the world at all times. The company's increased attack surfaces have driven growth in cyber operations for more than 10 years.

Multiple layers of tools had been deployed to detect and react to endpoint attacks. Multiple teams of specialists were required to support tech layers and to coordinate workflows among them, including 24x7 staffing to triage alerts and incident response. Resulting workflows were complex, increasing the possibility of human error and negatively impacting cyber readiness. Additional tools added to the security stack created more data to be analyzed. Finding and retaining qualified cyber security analysts and staff required to maintain the various tools resulted in increased year-over-year cyber costs. Yet, despite the heavy investment in technology and personnel, cyber incident volume continued to increase.

Inadequate Endpoint Protection Despite Significant Cyber Security Investments

An endpoint protection suite from one of the most widely recognized brands had been deployed years ago. It included numerous protection features: anti-virus, machine learning binary analysis, behavioral

analytics, EDR, application control, HIPS, anti-exploit, URL/domain blacklisting, and more. While a single agent managed the suite from a single pane of glass, each tool required considerable labor to configure, maintain, and support. The complexity and unintended consequences of different capabilities limited what cyber controls could be used. Additionally, a large staff was required to manage the suite and additional staff was required to manage threats that bypassed the suite.

AppGuard: Greater Security, Less Effort

Realizing the status quo was inefficient and risky, the airline selected AppGuard due to its unique ability to block malware in real-time, and its ease of deployment and maintenance. Unlike other tools that require trained security personnel to manage them, AppGuard can be managed by a Windows administrator. This was important given the cost and scarcity of trained security analysts.

During the evaluation, a third party pen test proved AppGuard's effectiveness at blocking malware. By providing pre-compromise protection, AppGuard eliminates the need for monitoring, investigating, and remediation efforts – reducing overall cyber security staff and budget requirements while increasing the airline's security posture.

Reduced Patch Management Burden

AppGuard's unique, patented isolation technology protects endpoints from the applications and utilities that are commonly hi-jacked via software vulnerabilities. This enabled the airline to reduce patch management efforts, and allowed security

staff to focus on more strategic issues. This also eliminated the need for paying personnel overtime to implement patches. With AppGuard mitigating risks, application exploits were reduced to zero.

Fewer Alerts and False Positives

AppGuard is not a detection tool. It doesn't judge a file as good or bad, or endpoint activities as normal or abnormal. It blocks non-conforming actions and reports on them. No specialists are required to analyze alerts. AppGuard can easily be configured to establish policy exceptions that are remotely pushed to agents to ensure legitimate applications are never blocked.

Reduced Incident Response (IR) Costs

AppGuard's pre-compromise protection provides multiple benefits – including the ability to reduce incident response costs. Using AppGuard, the airline was able to reduce incident response staffing from 24x7 operations to 24x5 operations. After continued success with AppGuard they further reduced IR operations to 8x5. With AppGuard inhouse, the airline continues to scale back IR operational costs.

As a result of moving to a 8x5 operation, the airline was able to reduce IR labor costs by 76%. This not only reflects a significant cost-savings, it also frees security staff to focus on initiatives that increase the organization's cyber security effectiveness and improve the company's overall cyber security posture.

Endpoints without Compromise

By deploying AppGuard, the airline has achieved greater security while reducing cyber security costs. AppGuard enables the airline to do what it needs to do, while preventing malware from doing what it wants to do. AppGuard allows the airline to be more secure with less effort and gives them peace of mind knowing their endpoints won't be compromised.