APPGUARD

Case Study

Global Airline

Industry:

Passenger Airlines

Challenges:

- Malware driving up cyber defense costs
- Cyber specialist staffing

Outcome:

"We no longer need battallions of specialists to react to malware attacks because AppGuard blocks them at the endpoint as they strike,"

About the Airline

Major global airline with approximately 50,000 employees that transport about 7,000,000 passengers around the world per year. Critical infrastructure must always be operational to avoid major financial losses. Ensuring passangers safety is important as any cyber breach might jeopardize passenger lives, harm reputation and revenue.

Situation: Complex Cyber Operations from Years of Porous Endpoint Protection

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

Multiple layers of tools have been deployed to detect and react endpointattacks. Multipleteamsofspecialistswere required to support these layers and coordinate workflows among them, including 24 x 7 staffing to triage alerts and incident response. Workfows were getting complex with increasing posibility of human error and declining cyber readiness. The change management needed to offset human error slows everything. Adding more tools to the security suite created more data to be analyzed. Big data analytics promises has made it harder to find and retain specialists. Cyber costs increased year over year for over a decade, so did cyber incident volume.

Cyber leadership strongly suspects a high correlation between what happens at the endpoints and the incident volumes of most of the layers of the cyber program.

Previous Endpoint Protectionwas Comprehensive but Ineffective

An endpoint protection suite from one of the most widely recognized brands had been deployed for years. It included numerous protection features: antivirus;machine learning binary analysis, behavorial analytics, and EDR; application control; HIPS; anti-exploit;URL/domain blacklisting; and more. It was all on one agent managed from a single pane of glass. Yet, each required considerable labor to configure, maintain, and support. The complexity and unintended consequences of different capabilities limited what cyber controls could be used. The suite required a large staff to use and an even larger one to deal with what got past the suite.

Challenge: Be More Secure with Less

The airline selected AppGuard because of its light labor requirements and its unusual approach to blocking malware attacks in real time without needing specialists to analyze data. Third party penetration tests had already revealed AppGuard's effectiveness at blocking malware attacks. The greater goal was to see how AppGuard would reduce operation labor requirements for and beyond the endpoints.

Simpler to Deploy and Maintain

AppGuard required few deployment-specific policies, fewer than one out of every ten. Policy updates have been rare. AppGuard has required a small fraction of the effort of the previous endpoint protection suite.

AppGuard Eased Patch Management

Because AppGuard uses unique, patented isolation technology to protect endpoints from the applications and utilities that were hijacked via software vulnerabilities, the airline stopped rushing patches out, pulling personnel from projects, and paying personnel overtime to implement them. They let AppGuard mitigate the risks. Successful application exploit attacks were reduced to zero.

AppGuard Produced 100% Fewer Alerts and False Positives

It's 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 them. No specialists were required to analyze alerts. AppGuard did block some actions by legitimate applications. These were easily diagnosed and policy exceptions were defined and remotely pushed out to the agents.

Practically 'Set & Forget' Protection

Aside from minor policy updates, endpoint operations personnel have moved their attentions elsewhere.

Progressively Less Incident Response (IR) Staffing

Upon reaching steady state in phased deployments across different parts of the organization, the airline employed a phased scale-back of its IR staff. Phase I began with shifting from 24 x 7 to 24 x 5 IR operations. Convinced they could scale back more, they shifted from 24 x 5 to 12 x 5 IR operations. The next phase will test 8 x 5 IR operations.

Ultimately, the airline is looking to see how much it can scale back endpoint IR. The shift to 12 x 5 alone represents a 64% reduction in labor hours. Overtime, attrition, opportunity costs (value of tasks that could not previously be worked), and other factors boost cost savings beyond reduced labor hours.

Fewer Alerts Elsewhere (non-endpoint)

Is something getting past endpoint protections? These concerns diminished as alert volumes from non-endpoint tools (e.g., network intrusion detection, deception grid, SIEM, etc.) declined below "weekend" volumes. "Weekday" volumes have always been higher than "weekend" volumes because most employee interactions with their endpoints occur during "weekdays". These other tools look for indicators of lateral movement. By stopping attacks at initial endpoints, there's no subsequent lateral movement to detect.

Trouble Tickets: from Nuisance to Rarity

The previous endpoint protection suite's frequently blocked legitimate applications because the whitelists were always changing with the changing endpoints. It caused dozens of daily help desk calls. We see only a few per month with AppGuard because it doesn't need to know about all of the different supporting executables per application. Most of those tickets, however, were either unwanted applications or unsigned executables.

From 'Reactive' to 'Proactive' to Freed Up

Until AppGuard, the experiences of most analysts and other specialists was like that of their peers elsewhere: moving from one crisis or fire-drill to the next. Teams can now spend time on tasks and training they were previously too busy to do.