CASE STUDY

MAJOR TRANSPORTATION CORPORATION.

APPGUARD PROVIDES SEAMLESS, ZERO TRUST ENDPOINT PROTECTION TO MAJOR TRANSPORTATION CORPORATION WITHOUT COMPROMISE, EVEN FROM ZERO-DAY ATTACKS.

INDUSTRY:
Mass Transportation

CHALLENGES:
- Malware increasing cyber defense costs
- Cyber specialist staffing
- Defending remote sites

OUTCOME:
"We no longer need battalions of specialists to react to malware attacks because AppGuard blocks them at the endpoint as they strike."

ABOUT THE CUSTOMER

With approximately 40,000 employees that transport about 7,000,000 passengers around the world per year, mission critical infrastructure must always be operational to avoid major financial losses. Passengers' trust in the preservation of their safety is sacred. Any loss of reputation hurts revenues. More importantly, any cyber breach might jeopardize passenger lives.

SITUATION: COMPLEX CYBER OPERATIONS FROM YEARS OF POROUS ENDPOINT PROTECTION

Nearly 40,000 endpoints around the world access mission critical IT infrastructure 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 to endpoint attacks. Multiple teams of specialists have been required to support these layers and coordinate workflows among them, including 24 x 7 staffing to triage alerts and respond to incidents. Worklfows have grown so complex within and among the different layers that human error has grown, and cyber readiness has declined. The change management needed to offset human error slows everything, including hopes for radical improvements. Each tool added has created more data to be analyzed by specialists that could not analyze what they had before. Big data analytics promises have slowed the rate of personnel growth in general but has increased the need for harder to find and retain specialists. Cyber costs have increased year over year for over a decade, as has cyber incident volume.

The organization has dispersed offices around the globe. Some have low network bandwidth whose productivity is impacted from signature and detection engine updates. These also require personnel to spend time testing updates for disruptions and fixing affected systems when they do.

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 PROTECTION WAS COMPREHENSIVE BUT INEFFECTIVE

Multiple agents such as anti-virus, behavioral analytics, and others had been deployed that degraded system performance and end-user productivity. Yet, these did not diminish incident volume and risk.

CHALLENGE: BE MORE SECURE WITH LESS

The customer was seeking more effective endpoint protection. The greater goal was to reduce operations labor requirements for and beyond the endpoints. AppGuard was selected after intensive penetration testing vendor tools featuring AI machine learning, behavioral analytics, next generation AV, and others. Furthermore, the airline selected AppGuard because of its lighter, less skilled labor requirements observed through that testing.

SIMPLER TO MAINTAIN

Once the policy settings have been in place, 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 are sometimes hijacked via software vulnerabilities, the customer stopped rushing patches out, pulling personnel from projects, and paying personnel overtime to implement them. They let AppGuard mitigate the risks while they implemented patches at their convenience.

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. AppGuard did block some actions by legitimate applications. These were easily diagnosed and policy exceptions were defined and remotely pushed out to the agents.

PROGRESSIVELY LESS INCIDENT RESPONSE (IR) STAFFING

Moving forward, the customer expects a significant reduction in IR staffing. Early indications are that they can potentially reduce the staffing by 30 perecent compared to the 24 x 7 approach being done today. Overtime, attrition, opportunity costs (value of tasks that could not previously be worked), and other factors will boost cost savings beyond reduced labor hours.

FROM 'REACTIVE' TO 'PROACTIVE' TO FREED UP

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

BLUERIDGE® NETWORKS

sales@blueridgenetworks.com
1-800-722-1168
BlueRidgeNetworks.com
linkedin.com/company/blue-ridge-networks
@BlueRidge