BlackBerry | CYLANCE

CASE STUDY

County Government Takes on Cybersecurity

The Organization

The government of one of the 44 most populous counties in the United States, which provides a comprehensive range of services to more than a million citizens.

The Situation

Local governments are a treasure trove of data for a determined attacker, replete with personal information, including mortgage documents, deeds, medical records, Social Security numbers, as well as birth, marriage, and death notices. CISOs are often hamstrung in their attempts to protect this data due to political and budgetary constraints that make it near-impossible to implement an effective security architecture across a gaggle of semi-independent government agencies. As a result, local governments are often woefully unprepared to deal with today's increasingly treacherous threat environment. It's not surprising, then, that state and local agencies experience a material data breach an average of every 12 weeks and that local governments rank at the very bottom with respect to their overall cybersecurity posture. Against this backdrop, the government of this southeastern U.S. county was a standout among its peers, having experienced no major public breaches and maintaining an excellent record for business continuity.

Despite these successes, however, the county's CISO was far from satisfied with the status quo. "Our security and network staff couldn't keep up with the flood of malware infecting our endpoints, which forced us to devote significant time and resources every month to remediate and re-image systems," he says now. "We'd been lucky so far, but it was only a matter of time before our existing AV product failed us entirely. The stakes were too high for us to gamble on a product that repeatedly showed it did not work."

The Process

The CISO and his team evaluated several AV vendors and conducted a rigorous proof of concept and business case process before selecting BlackBerry Cylance as the county's sole endpoint solution provider. "Our analysis confirmed that

Industry

- County Government

Environment

- Over 40 county departments encompassing 17,500 user endpoints

Challenges

- Prevent zero-day and advanced persistent threats (APTs) from infecting user endpoints with malware
- Reduce costs for incident response and system remediation/re-imaging
- Improve the productivity and morale of IT and security employees

CylancePROTECT and its artificial intelligence technology is extremely effective in proactively detecting and blocking zero-day threats and malware, and preventing the execution of malicious scripts and potentially unwanted programs in real time."

It took a little over a month for a team of ThreatZERO consultants, assisted by a single internal IT resource, to decommission the legacy AV product and deploy CylancePROTECT on 17,500 user endpoints.

The Results

According to the CISO, "Our ThreatZERO consultants not only ensured that our transition to CylancePROTECT was seamless, they also helped us implement best practices with respect to our network architecture, patch management protocols, and methods for hardening potentially vulnerable internal- and external-facing services."

Since deploying CylancePROTECT, the county has documented a 99% block rate for zero-day malware and potentially unwanted programs. This has virtually eliminated the need to re-image endpoints, producing an estimated $110,000 in annual cost savings. The county has also reported a 40% increase in productivity by its team of 12 full-time IT and security employees. This translates into another $734,000 in yearly risk-adjusted savings. Overall, according to a Total Economic Impact (TEI) study conducted by Forrester Research, the county achieved a 251% ROI with CylancePROTECT and a net present value of $5,503,996 over the three-year period covered in the study.

"There's been a dramatic uptick in employee morale now that we're no longer on the brink of a calamitous data breach or some other serious security incident," says the CISO. "With BlackBerry Cylance as a partner, we're confident in our ability to maintain the public trust."

About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.

BlackBerry
CYLANCE

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

MKTG 19-0202 20200309