BlackBerry | CYLANCE

CASE STUDY

Orange Unified Takes on Takes on Cybersecurity

The Customer

The Orange Unified School District operates 27 elementary, five middle, four high schools, a continuation high school, a K-8 math and science magnet school, and two special schools. Nineteen of its 40 schools have been recognized as California Distinguished Schools. Three of its high schools are consistently listed among Newsweek's "1,000 Best Public High Schools in America". The district has 3,000 employees and serves 29,000 students.

The Situation

Tam Nguyen, the Director of Information Technology for the school district, is responsible for building and maintaining the district-wide network. This includes securing highly sensitive information, such as children's personally identifiable information, which is very valuable on the black market. The district must also comply with the Family Educational Rights and Privacy Act or FERPA. Non-compliance could result in a major public relations issue for the district.

The district was experiencing an escalating volume of targeted cyber attacks, including malicious file downloads, ransomware, and spam. The district had stopped investing in signature-based AV because it proved ineffective more than 50% of the time. According to Tam, "The end-user would notify us before the AV solution did." He added, "With these new threats, we were scrambling. We were essentially seeing zero-day attacks on the network." The district's IT team was in reaction mode, and could not prevent unknown attacks. Tam noted they were hit with a threat just 19 hours after it had been reported in the security community, which proved too soon for the AV definitions to be updated. "We had a combination of increasing attacks and no solution."

The final straw was a high-profile ransomware attack on the human resources department that encrypted critical sensitive files. Fortunately, the district's data is backed up nightly, so the information was restored. Only a day's worth of work was lost. Tam said, "We knew then that we had to get something better than what we had."

Industry

- Education

Environment

- CylancePROTECT® is safeguarding 3,000 laptops, desktops, and Windows servers, including SQL, Microsoft Exchange, and application servers.

Challenges

- Ineffective antivirus (AV) unable to protect endpoints from growing number of zero-day threats
- Sustained a ransomware attack where critical, sensitive human resources files were encrypted

Solution

- Deploy CylancePROTECT to safeguard staff machines from zero-day threats, including ransomware

ORANGE UNIFIED SCHOOL DISTRICT
ORANGE, CALIFORNIA

The Process

Tam heard from a CISO at a conference that government entities were considering BlackBerry® Cylance® endpoint protection. He learned BlackBerry Cylance offers a fundamentally different approach to endpoint security by blocking attacks pre-execution using artificial intelligence. Tam said, "If we are going to invest in endpoint security, I want the one with the most probability of being successful."

The district's team conducted a head-to-head test with CylancePROTECT, their current solution, and a competing advanced endpoint security product. They downloaded 25 of their own viruses, malware, and spyware, and then put them into a scrambler to rehash the threats to produce an additional 25 zero-day threats. The traditional AV caught several known viruses, but failed to detect any zero-day threats. The competing advanced endpoint security product was more successful than the traditional AV, but failed to detect quite a few threats. With CylancePROTECT, the team had a difficult time loading the files because they were detected in memory.

The team then deployed CylancePROTECT and a competing next-generation AV solution on 200 machines as part of a multi-vendor proof of concept (POC). Tam said "The competing product found very close to nothing, while CylancePROTECT delivered a gigantic report of detected threats." The technical team was so impressed with CylancePROTECT that they bought the commercial version of the software for their home computers that day.

The Results

To deploy CylancePROTECT, the team began with a POC at the department level for employees with access to critical data. They found threats never reported by the previous AV, including potentially unwanted programs that had been lurking on client systems for upwards of five years. CylancePROTECT identified wireless key dumps, password sniffers, and files made to pass encrypted data.

The district's security team ultimately conducted a complete AV rip and replace on staff machines. Tam said, "We quarantined nearly 500 items and have not had any issues with ransomware, viruses, or infections since deploying CylancePROTECT. It is a set-and-forget application because you don't have to worry about whether it is updated. You know that it is loaded and protecting your systems." CylancePROTECT has also proven very easy for the staff to administer.

Tam also sees value in the BlackBerry Cylance score, which makes use of the collective experience of all BlackBerry Cylance customers to help users make decisions, for example, how many BlackBerry Cylance customers quarantined a file. He said, "When you see a file was blocked by 100% of all BlackBerry Cylance customers, you can easily determine if it is good or bad."

The district's IT team also appreciates the lightweight quality of CylancePROTECT. According to Tam, "With the previous AV, when it caught a threat, it bogged down the system and performance ground to a halt. BlackBerry Cylance silently quarantines and catches threats with no perceivable impact to our users."

In closing, Tam said, "BlackBerry Cylance offers a new approach to AV that works. This is a new, effective technology."

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 20-0110-20200310