CYLANCE

CASE STUDY MANUFACTURING

American Cement Takes on Cybersecurity

INDUSTRY

Manufacturing

ENVIRONMENT

- 155 employees, 28 virtual servers, 8 physical servers, and 85 PC endpoints

CHALLENGES

- Keep endpoints secure from phishing attacks, ransomware, and other malware threats

SOLUTION

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

ACC

The Customer

Founded in 2006, American Cement Company provides the cement its customers in Florida need to construct their piers, building foundations, roads, bridges, reinforced concrete buildings, reservoirs, and more. If you live in or visit Florida, chances are you have walked on, driven over, or entered a building built using cement from American Cement.

When you think of cement manufacturing, you probably don't think about phishing attacks, ransomware, or other types of malware risks, but Jeremy Mayfield, IT director at American Cement, certainly does.

The Situation

One of the primary security challenges that concerns Mayfield is making sure that the 155 employees of American Cement don't make the simple mistake of clicking on the wrong link or opening the wrong attachment and falling victim to a phishing or ransomware attack. But if they do, Mayfield wants to make sure those employees' endpoints are protected.

Mayfield manages a tight IT department consisting of himself and a colleague. Unfortunately, just like most organizations, American Cement has been experiencing more attack attempts and malware seeking to compromise its business technology systems. Considering they are two-person IT team, when it comes to securing their environment, they have to make every minute count. "We have to be very automated and very efficient," says Mayfield.

155
EMPLOYEES

28
VIRTUAL SERVERS

American Cement's environment consists of 28 virtual servers, 8 physical servers, and about 85 PC endpoints. "We're just as vulnerable as everybody, but phishing is the most common attack we see. They are always trying to get people to click on links. Trying to get our users to go down that rabbit hole so the attackers can take over their computer," he says.

To keep its systems secure, American Cement invests considerably in employee cybersecurity awareness training, as well as security at the network, perimeter, and endpoint levels. One of American Cement's primary endpoint security providers, however, moved many of their processes to the cloud, which broke some functionality on endpoints. Another provider began to constantly require upgrades. "I could spend hours just trying to get computers to reconnect and sync with the cloud to make sure definitions were downloading. It was endless downloading and updating, and making sure virus definitions were synchronizing," he says.

Despite having used one of the endpoint security products for decades, and not having looked at the market for years, the newfound management hassles raised Mayfield's curiosity to seek a better way. "I asked myself: What is one area where we can improve and how can I get us there? I knew that our current endpoint security tool had a large footprint on the desktop. It used a lot of processor capacity and a lot of RAM. Not really a lot, it just seemed to when you installed it. The PC seemed to slow down just a little bit," he says, "so I started researching."

The Process

As Mayfield looked at a handful of endpoint security products, a few showed some promise, but he remained largely unsold until he found CylancePROTECT.

"CylancePROTECT looked impressive. It was much faster than the other options we were evaluating. It just shattered everyone else. Cylance claimed that they did things differently, such as not having to download virus definition files, and combining artificial intelligence to block malware, and additional security controls that safeguarded against other types of attacks," says Mayfield.

"I decided to deploy CylancePROTECT, and it was very straightforward," Mayfield continues. "You go to the cloud portal, download the software, and roll it out. I didn't have to touch a computer. CylancePROTECT is actually a solution that protects the enterprise end-to-end and does so very efficiently. I found that once I installed CylancePROTECT, I quickly became a believer. It works as promised and we haven't had an incident since it was installed."

The Results

Today, Mayfield says CylancePROTECT provides American Cement greater flexibility in the IT department's day-to-day operations. "I don't have to spend as much time now updating antivirus applications and malware definitions, or worrying about computers getting out of sync," he says.

Following the installation of CylancePROTECT, Mayfield found that not only were they able to displace two other endpoint protection tools, but that CylancePROTECT immediately identified threats that previously went unnoticed. "We actually had a few alerts for malware we didn't know we had, which was exciting and alarming at the same time. All of the sudden something that you thought was safe turned out not to be. We're grateful CylancePROTECT caught the threat," he says.

In addition to the improved security, Mayfield found staff computers ran with more snap, as well. "CylancePROTECT runs very streamlined. Our users report that their computers are running more smoothly and faster now that the previous antivirus software is gone," he says. Mayfield also reports budget savings because there are fewer security applications they must renew. "For the endpoint, we went from having to pay for three products to one, and that's had a positive impact on my budget," he says.

Finally, Mayfield is happy that he no longer has to get on the phone looking for endpoint security support. "CylancePROTECT just works."

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
400 Spectrum Center Drive, Irvine, CA 92618

CYLANCE