School district protects 26,000 endpoints from cyberattacks

Time spent on security administration drops 90 percent

The Socorro Independent School District (SISD) in El Paso County, Texas operates 47 schools spanning pre-kindergarten through high school. It serves more than 46,000 students with innovative programs that focus on college and career readiness.

Industry
Education

Headquarters
El Paso, Texas, USA

Employees
6,900 (IT staff, 15)

Results
- Security breaches eliminated entirely, versus two incidents per week previously

- System administration time cut 90 percent

- Weekly trouble calls about performance and security issues reduced to zero from 10

THE CHALLENGE

Providing IT capabilities for a school district as large as SISD requires a massive infrastructure — and security software that prevents breaches. But SISD's Kaspersky Labs solution was missing viruses, malware and ransomware, reporting too many false positives, frustrating users and causing security administration headaches.

When ransomware encrypted campus servers, for example, it could take administrators hours to restore each infected machine. The entire environment could be down for up to a day.

"Our solution wasn't proactive enough, so we ended up fighting too many fires," said David Akers, SISD's Coordinator, Technical Services. "Whenever we ran virus scans, users immediately complained about their systems slowing down."

"The breaking point came when we deployed a new desktop management package. Our security software saw the desktop client as an attack and deleted it on 4,000 machines. Kaspersky's support team never solved the problem. I knew we needed something better.

THE SOLUTION

SISD evaluated solutions from Bitdefender, Carbon Black, Cylance, ESET, Kaspersky Labs, Sophos and Symantec. Ultimately, the school district chose Bitdefender GravityZone Enterprise Security, including GravityZone Security for Endpoints and GravityZone Security for Virtualized Environments. SISD also plans to use Bitdefender Hypervisor Introspection (HVI) for Citrix virtual desktops and servers.

Bitdefender secures 26,000 endpoints, 100 physical servers, 211 virtual servers and 6,000 virtual desktops in operating environments including Microsoft Windows, Linux, Citrix and Apple Mac OS X.

"Bitdefender is cost effective for a school district's budget and their sales engineer worked with me throughout product testing," Akers says. "GravityZone ran well and even identified infected PST and OST files the prior solution missed. Deployment only took a couple of hours. And Bitdefender regularly checks in to make sure we're OK. Their service is outstanding."

THE RESULTS

SISD saw immediate improvements with Bitdefender. The school district has not suffered a single security breach since implementation five months ago, compared to a couple per week before. Akers says Bitdefender has eliminated the need for weekly security-related trouble calls.

He also notes that performance has improved dramatically. "Whenever we ran virus scans before, user systems slowed to a crawl," he says. "It could take up to a minute for an application to open. With Bitdefender, systems respond immediately. We run virus scans any time without worrying about performance issues."

TIME AND COST SAVINGS

Time spent on security management has dropped more than 90 percent with Bitdefender. "We used to work on security about two hours a day," Akers explains. "Now it's more like 10 minutes. We can devote the saved time to other projects, confident that our environment is secure. Bitdefender is a perfect fit for us."

He says IT also expects to save time and money due to quicker server maintenance and other enhancements. Bitdefender also consumes less processing resources, which reduces power consumption and may result in fewer servers.

SIMPLIFIED SECURITY ADMINISTRATION

System administration used to be frustrating and time consuming. The old solution required splitting the environment into three zones and running the security software on three servers to support the entire district.

Oscar Dominguez, SISD's Manager, Systems and Data Center Administration, says: "Changing multiple servers every time we did upgrades or new security policies was a big headache. But Bitdefender runs on a single centralized server, making it easy to support all 26,000 endpoints."

SECURING THE VIRTUAL INFRASTRUCTURE

One reason SISD chose Bitdefender is its strong relationship with Citrix Systems. The two companies have developed Bitdefender Hypervisor Introspection (HVI), a memory-level security layer for Citrix environments that malware and viruses can't compromise or evade.

"We use Citrix to virtualize 6,000 desktops and more than 40 servers," Akers says, "but we've never been able to protect them fully. We're looking forward to adding HVI to our Citrix environment soon. It will certainly give us more peace of mind."

"We used to work on security about two hours a day. Now it's more like 10 minutes. We can devote the saved time to other projects, confident that our environment is secure. Bitdefender is a perfect fit for us."

— David Akers, Coordinator for Technical Services, Socorro Independent School District

Bitdefender Footprint
- Bitdefender Hypervisor Introspection
- GravityZone Enterprise Security
- GravityZone On-Premises Management Console

IT Environment
- Citrix XenDesktop
- Citrix XenServer

Operating Systems
- Apple (Mac)
- Linux
- Microsoft Windows