"Inspired" EDR Protects Coffee County SD to Preserve Learning Time

Based in Douglas, Georgia, Coffee County School District consists of 13 schools that serve 7,600 students from kindergarten through 12th grade. The district provides students and staff with the technology needed to learn and work in today's connected world, which includes a network that's among the fastest in the state. This high-speed WAN supports all of the district's network-connected devices, including desktop computers, laptops, Chromebooks, printers, telephones, and more.

When he stepped into his Director of Information Systems role, Logan Evans assessed that the district's security investments were at a base level and didn't meet the state compliance for some particularly important security-related requirements. Given the 44 percent increase in cybersecurity attacks in the education sector, Evans recommended building out a best-practice security framework, including an endpoint protection and a response plan that would stop zero-day threats and remove complex malware and ransomware before a breach could occur.[1]

With these essential requirements in mind, the district selected ThreatDown Endpoint Detection and Response (EDR) to safeguard its 1,160 workstations and servers.

Coffee COUNTY SCHOOLS

Partner-At-A-Glance

Customer
Coffee County School District
1,160 endpoints

Industry
Education

ThreatDown Solutions
ThreatDown Nebula Platform, including:

- Endpoint Detection and Response
- Endpoint Detection and Response for Servers

Results

- Full-featured EDR product at great price value
- Impressive ease of use with Nebula cloud consoles
- Essential remediation and rollback capabilities for fast IT response
- Integrated web security that protects 'click-happy' students
- High confidence in support and vendor relationship

*Infosecurity-Magazine Education Sector Experienced 44% Increase in Cyber-Attacks, October 2022.

ThreatDown
Powered by Malwarebytes

> **"ThreatDown EDR's 72-hour ransomware rollback and automated malware remediation capabilities are a great sales point. If we have a detection, we can go into that machine and hit the rollback, and we basically go back in time to before there was an infection."**

Logan Evans, Director of Information Systems
Coffee County School District

Gaining superior response capabilities

The district's ten IT professionals have a big job managing the school's infrastructure and daily learning operations. A top priority for the team: ensuring students can access their technology and work throughout the school day. Evans shared, "We're a learning organization, so it all revolves around the students and making sure they're ready to learn all the time."

For student machines to remain operational, ThreatDown EDR prevents threats with built-in Endpoint Protection, remediation of threats and ransomware recovery to return machines to pre-threat status. ThreatDown EDR safeguards the district's machines with advanced capabilities for threat detection, and if an issue is found, the IT team can rapidly address it, levering EDR's effective isolation, thorough eradication, and rollback features.

"ThreatDown EDR's 72-hour ransomware rollback and automated malware remediation capabilities are a great sales point. If we have a detection, we can go into that machine and hit the rollback, and we basically go back in time to before there was an infection," said Evans.

Top marks addressing unique K-12 security concerns

A unique challenge of K-12 is protecting the tech-savvy student population from themselves. As Evans points out, "The students are geniuses. We basically have 7,000 computer hackers that show up and work every day, so controlling that environment is tough."

One area that's easy for the district to control, thanks to ThreatDown EDR, is web usage. With Malwarebytes' integrated web protection capabilities, the district can prevent student and staff access to malware-laden websites, ad networks, and phishing schemes. "When I look at our ThreatDown reports, malicious websites are our number one attack vector. We block a ton of malicious websites and domains," said Evans.

Security awareness training is also a big part of the district's security approach, and ThreatDown, powered by Malwarebytes, helps there, too. "Fortunately, with ThreatDown reports we have vision into the web security risks that the solution is stopping," said Evans, explaining that "we can translate that information over to our users and let them know just one in every 1,000 clicks they make on the internet is a potential disaster, and that increased awareness makes a big difference in helping to adjust their behavior.

Equipped with machine learning

and layers that protect against unkown threats

Insightful reports

that support security awareness training program

Packing a punch with innovation and ease of use

"Besides the great value for the price, we've been very impressed with the ThreatDown Nebula interface and how easy it is to navigate," said Evans. With the ThreatDown, powered by Malwarebytes', cloud console, the IT team can remotely manage all aspects of endpoint prevention, detection, and response, as well as see the state of all machines in a single view, whether a user's machine is on or off campus.

Cybercriminals are always changing their tactics and, with ThreatDown in place, Evans has confidence in the district's protection against zero-day threats. ThreatDown EDR uses award-winning, security innovations such as anti-exploit protections, anomaly detection, ransomware mitigation, and more to immediately stop threats at every stage of the attack cycle from pre-delivery, through pre-execution and post-execution.

As Evans explains, "ThreatDown, powered by Malwarebytes, uses machine learning to assess behavior that's out of place, like a Word file that's running an executable, and then can trigger an alert that way. That's a neat trick right there. And that lets us know ThreatDown is inspired to find the threats they don't know about — those new emerging threats."