



Lake Dallas ISD Chooses BlackFog to Prevent Data Exfiltration

Company Bio

Lake Dallas Independent School District

Vertical: Education

Location: Denton County, Texas

Employees: 650

Students: 4000

Locations: 5 campuses, 4 faculty buildings

 [ldisd.net](https://www.ldisd.net)

Lake Dallas ISD serves about 4,000 students in Denton County with a focus on providing big-school opportunities while maintaining a small-town atmosphere. Located adjacent to Lewisville Lake in North Texas, approximately 30 miles from downtown Dallas, the school district covers 9.8 square miles and includes all or part of Lake Dallas, Shady Shores, Corinth, and Hickory Creek. With a focus on family and community, Lake Dallas ISD is excited about the growth and achievement of students at its three elementary schools, one middle school, and one high school.

The Challenge

Like most school districts the main challenge is a lack of time; too much to do with not enough resources. At Lake Dallas ISD an IT

Department of six has responsibility for 650 staff members, 4000 students, 5000 Chromebooks, and 1500 windows devices. Mike Dabney, the Director of Technology at Dallas ISD shared his thoughts

on the day to day stress of the job, “with so much to manage 24/7, we are constantly in fire-fighting mode. The risk of cyberthreats has never been higher, and we must contend with the threats from both inside and outside of the district network. Being a previous victim of a ransomware attack, we know all too well that the external threat from bad actors is very real, but as vigilant as we are, lack of time is our biggest concern.”

The Solution

Following a ransomware attack last spring, Lake Dallas ISD began using an EDR solution recommended by the vendor tasked with helping with the remediation. In the months following, Mike decided to look into other solutions to help mitigate the risk of further attacks. Lake Dallas ISD was introduced to BlackFog while evaluating a few other EDR solutions. Lake Dallas ISD made the decision to deploy BlackFog to select devices to evaluate the

solution. “We were so busy it was hard to find the time to evaluate multiple solutions, but the concept of anti data exfiltration technology was interesting, so we decided to give BlackFog a try.”

The Approach

“BlackFog’s Enterprise console was straightforward and intuitive. We didn’t need to read any manuals to be comfortable with the product. It worked well alongside the EDR solutions which was also a big plus. During the trial we deployed BlackFog across some of the student lab computers and all of our servers and we found that BlackFog was reporting on different things. Whereas EDR was looking at what was coming into the network, BlackFog was watching the back door, which was an interesting approach,” commented Mike.

The Results

During the trial Mike and his team became comfortable with the solution and deployed it on additional systems. Until school started Mike and his team didn’t see a lot of interesting activity in the console, so they felt they needed more time to use the product. Mike commented, “we decided to purchase some additional licences and we are really glad to have it.



BlackFog reports in a different way, and from a different angle to other solutions, so we are seeing things we don’t usually get to see. I’m in the console every day and it’s not a chore to manage, but the biggest plus is that it’s doing something specific and unique. I particularly like the Threat Hunting feature where I can drill into specific events for more details; it can help you discern if it’s a false positive or not or dig deeper. ”

Mike Dabney, Director of Technology, Lake Dallas ISD

BlackFog reports in a different way, and from a different angle to other solutions, so we are seeing things we don’t usually get to see. I’m in the console every day and it’s not a chore to manage, but the biggest plus is that it’s doing something specific and unique. I particularly like the Threat Hunting feature where I can drill into specific events for more details; it can help you discern if it’s a false positive or not or dig deeper. The hourly impact report is also interesting. If I see activity in the middle of the night, I want to know what that is”. When

asked if he would recommend the solution to other school districts, Mike commented, “Absolutely. The BlackFog solution has proven to be a great resource in helping protect our data, and I am grateful to have this resource at our disposal. BlackFog will manage it for you, 24/7, providing another resource to help ensure your data doesn’t end up in the hands of cybercriminals. I’d recommend any organization do what they can to mitigate cybersecurity risks, as the fallout is always worse than you expect. Prevention really is key.”

About BlackFog

BlackFog is the leader in on-device data privacy, data security and ransomware prevention. Our behavioral analysis and anti data exfiltration (ADX) technology stops hackers before they even get started. Our cyberthreat prevention software prevents ransomware, spyware, malware, phishing, unauthorized data collection and profiling and mitigates the risks associated with data breaches and insider threats. BlackFog blocks threats across mobile and desktop endpoints, protecting organizations data and privacy, and strengthening regulatory compliance.