

ENA Customer Success Story



Metro Nashville Public Schools Repels Rising Tide of DDoS Attacks

Unfortunately, today's cyber-savvy students don't have to look far to bring a school district's network to its knees. That's precisely what happened to one Idaho school district. For \$2 an hour, a student who didn't want to take a standardized test paid a so-called DDoS-for-hire criminal operation to flood the district's Internet access with illegitimate traffic, thereby shutting down its curriculum-delivery tools and information systems for an entire week.

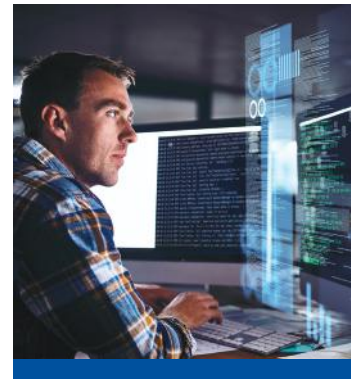
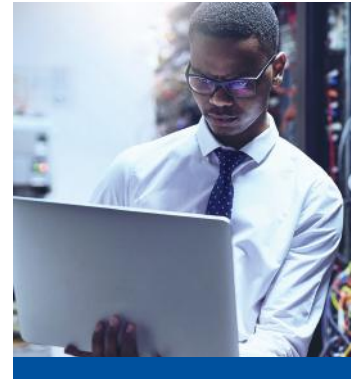
Devastating attacks such as this are why Metropolitan Nashville Public Schools (MNPS) elected to deploy ENA NetDefender, an advanced, on-demand DDoS mitigation and scrubbing service.

As the second-largest school district in Tennessee, MNPS had watched the rising tide of cyberattacks to its classrooms and operations with increasing alarm for some time. Determined to uphold its mission "to deliver a great public education to every student, every day," MNPS's IT department reviewed multiple offerings in the marketplace but ultimately decided that ENA's 24x7x365 DDoS mitigation service ticked all the essential boxes for the district.

THOUSANDS OF POTENTIAL VICTIMS

MNPS launched ENA NetDefender in October of 2017, but cybersecurity had been squarely on their radar, and therefore in their budgeting considerations, for at least two years prior.

Says MNPS Director of Enterprise Network Operations John Teeter, "We knew the threat of DDoS attacks was real to us and had been growing over time. We knew that there were players out there that might come after us, with DDoS, ransomware, and other forms of malware. We have exactly the kind of data cybercriminals are looking for. Eighty thousand students who aren't even registered to vote yet, not to mention 10,000 employees-that's a goldmine of data. K-12 is a real target, just like corporations, whether educators want to admit it or not."



SET IT AND FORGET IT

The threat was clear, but MNPS-like most school districts-had a very fundamental challenge to addressing the impending calamity: limited staffing.



“My staff doesn’t have the luxury of someone sitting around waiting for these DDoS attacks to commence so that he or she can react to them. We had to have a tool that was already in place, ready to respond and capable of taking care of the attack by itself. It had to be that proactive. It was that cut and dry for us.” – John Teeter, MNPS Director of Enterprise Network Operations

The district carefully explored the marketplace for solutions but found that many of them came up short. Several required the district to monitor their own network for attacks, notify the provider of each attack, and then wait while the provider did some complicated routing to scrub their Internet traffic, potentially incurring serious latency problems in classrooms across the district. Other solutions were expensive, required hands-on expertise from staff members along with ongoing maintenance, and offered unacceptable efficacy since mitigation would begin only after the attack had filled up the district’s Internet access connection.

These solutions were simply unacceptable for Teeter and his department. “It had to be a solution that did all the work, activating in real time without it being incumbent upon us to analyze the threat and then make the mitigation request of the provider. What we needed was to just be notified after mitigation with a ‘here’s what happened, we took care of it, you’re in good shape, keep moving.’”

A PURPOSE-BUILT, PARTNERSHIP-BASED SOLUTION

Unsatisfied with the capabilities of other solutions on the market, MNPS collaborated with ENA, their longtime Internet access, content filtering, firewall,



and VoIP provider, to fine-tune ENA’s DDoS-mitigation solution. ENA listened to the district’s challenges and goals and engineered that input directly into their solution.

THWARTING 205 ANOMALIES AND COUNTING!

In the first seven months of the MNPS deployment, ENA NetDefender has mitigated 205 anomalies-without the district, as Teeter describes it, “feeling a single thing. We’ve had absolutely no events impact our classroom whatsoever.” Nor has his IT staff expended any time or other resources on mitigation either.

“It is exactly the outcome we were hoping for,” sums up Teeter.

REPORTING PROVES ROI, EARNS LEADERSHIP’S TRUST

Besides ENA NetDefender’s “set-it-and-forget-it” nature and thus-far perfect track record, its reporting capabilities are Teeter’s other favorite feature.

“For me as an administrator, ENA NetDefender’s reporting is such a great tool,” he explains. “I can see what’s going on in my district in real time. And the ability to show each attack instance and each mitigation result back to the district’s

leadership, what an easy win. It's a clear demonstration that what we as an IT department tell our leadership is important and what we do for our leadership is important. The outcomes are what we in IT expected and what we told our leadership they'd be. That kind of credibility goes a very long way."



"We entered into this DDoS-mitigation venture as we enter all ENA ventures: as a partnership." – John Teeter, MNPS

5 DDoS-MITIGATION DEPLOYMENT TIPS FROM AN EXPERIENCED NETWORK DIRECTOR

1. Ask yourself, what's your loss? What impact does a DDoS attack have on your operation? Make sure you communicate the severity of the impact to your administration.
2. Sell the ROI. You need to show your administrators and school board the gains going forward. Cybersecurity prevention and mitigation is a cost of doing business, from both an operations and a curriculum-delivery perspective.
3. Don't get the tool that works, get the tool that works for you. Get the tool that aligns to what you need and don't need.
4. Is the vendor a seller or a partner? What are your conversations like? Are they talking or are they listening? Is it all about their features or is it about your needs and objectives?
5. Stay informed and think like a corporation. K-12 cybersecurity concerns continue to grow. It's no longer a business-world problem. It's important for educational leaders to understand that school districts and student data are prime targets.



Need help with
your cybersecurity
strategy? Visit
www.ena.com/security.



Education Networks of America

CONTACT US TODAY!

For more information about ENA, contact your ENA account service manager or visit our website at www.ena.com.

GENERAL INQUIRIES: 866-615-1101 | info@ena.com **SUPPORT:** 888-612-2880 | support@ena.com

ABOUT ENA

Education Networks of America® is the leading provider of Infrastructure as a Service (IaaS) solutions to K-12 schools, higher education institutions, and libraries. Since 1996, we have worked with our customers to ensure they have the robust and reliable connectivity, communication, cloud, security, and software solutions they require to meet the present and emerging technology needs of the communities they serve. For more information, please visit www.ena.com, call 866-615-1101, or email info@ena.com.