ARE·ON

Case Study

New MDR Thinking Delivers Full-Spectrum Visibility for State Educational Network

The Arkansas Research and Education Optical Network (ARE-ON) is a not-for-profit consortium of all public degree-granting institutions in the state and other selected higher education organizations. ARE-ON is a "collaboratory" of learning and innovation through advanced networking, technology, and research, based upon leveraging shareable resources. But shared information also brings with it a shared threat—one that impacts educational institutions across the country.

At a Glance

Provides a high-speed fiber optic backbone network throughout the state with 1Gb, 10Gb, and 100Gb Ethernet connections

Network consists of approximately 2,200 miles of long-haul fiber optic cable and about 85 miles of metro fiber in twenty-four cities and four neighboring states

High-profile institutions include University of Arkansas, University of Arkansas for Medical Sciences (including telemedicine) and Little Rock Central High School

Core Agendas

- Education
- Telemedicine
- Research
- Emergency Preparedness

CRITICALSTART

ARE·ON

Case Study

The rise of eLearning and mobility has enabled education to happen across an ever-expanding environment.

> **Everything from servers at institutions to laptops in professors' homes must be protected. While these potential vulnerabilities are growing, the assets needed to secure them are often neglected.**

"Much like every other public institution, education has struggled for funding for the past 20 years, so the amount of personnel available to protect the digital backbone of this network is very small," said Robert Nordmark, Executive Director of ARE-ON. "The team cannot meet the workload necessary to identify threats from malicious groups and mount the necessary response. In the past, much of this infrastructure was only protected by simple anti-virus solutions. Honestly, up to this point, the best security was simply found in the anonymity of being in a primarily rural state."

This soon changed. In 2019, ARE-ON's network of institutions suffered 9 breaches. These breaches threatened to impact the ability for universities to process tuition payments and can directly impact the remote learning ability of students. ARE-ON responded by putting together a security working group comprised of Chief Information Security Officers from member institutions to tackle what the organization saw as one of its greatest vulnerabilities: the lack of real-time visibility into breaches when they occur, and the need for a team, process and technology to isolate – and ultimately mitigate – the impact of those breaches.

ARE-ON evaluated the idea of a student-led Security Operations Center (SOC) or possibly building up the full-time staff to gain the visibility needed, but neither of these options were feasible or cost effective. However, after meeting CRITICAL**START**, a specialist in Managed Detection and Response (MDR), during a Lunch and Learn security networking event, ARE-ON started to rethink the problem.

Education at Risk

One of the most high-profile security breaches in ARE-ON's institutions, occurred when network penetration allowed members of a foreign government to contact professors, attempting to coerce them into turning over experimental seeds that were being developed.

CRITICALSTART

ARE·ON

Case Study

CRITICAL**START**'s Approach to Surveillance and Mitigation

> CRITICAL**START is deploying its MDR methodology, teams and technology to 36 campuses across the State of Arkansas.**

This approach is unique in how CRITICAL**START** treats security alerts indicative of a potential attack. When traditional SOCs are overwhelmed by the sheer volume of alerts received, they tend to prioritize their response to only critical or high alerts. But today's ransomware attacks may only register as a low or medium alert. This is why CRITICAL**START** is working with ARE-ON to develop a trusted registry of "normal" activity, which will bring the alert volume down to a point where every alert, low, medium, high, or critical, can be treated equally.

Reinforcing the value of this approach is Cortex XDR from Palo Alto Networks. Cortex XDR is a detection and response application that natively integrates network, endpoint and cloud data to help the CRITICAL**START** team identify sophisticated attacks. A key feature of this technology is that it helps the team trace penetrations back to the root cause to speed up investigations. Since ARE-ON already worked with Palo Alto Networks with some of its firewall components, it had an existing relationship that made this technology a natural fit for the new deployment.

"We like integrating with Cortex XDR in that it gives us rich data points to work with," stated Randy Watkins, Chief Technology Officer at CRITICAL**START**. "It allows us to triangulate on an event in a customer's environment and take action to identify potential breaches or other issues. With the data points provided, we can respond swiftly and definitively to security events, keeping customers safe."

ARE-ON Secured

Here's an example of how a breach to ARE-ON's network can be handled in the future:

1. An endpoint is compromised during an attack.
2. Palo Alto's Cortex XDR generates an alert, in this case a medium priority alert.
3. CRITICAL**START**'S SOC evaluates the alert, comparing it to the Trusted Behavior Registry.
4. Within 10 minutes, the alert is identified as a hostile attack, and the SOC takes direct action on behalf of the institution under attack.
5. The endpoint is isolated from the network, with a notification sent to the end user's mobile device. Affected passwords are changed, and the attacker is unable to move deeper into the system.
6. CRITICAL**START** traces the source of the attack using Cortex XDR and provides a full report of the incident to ARE-ON, including recommendations on any updates to security procedures.

CRITICALSTART

ARE·ON

Case Study

Ensuring a Successful Deployment

Elizabeth Mann, Finance Director for ARE-ON, shared what she felt is a key step for educational institutions if they are to be successful when rolling out their own MDR solution: "You've got to engage with the teams from the institutions you'll be protecting," she shared. "It's critical to get their buy-in from the beginning and give them a sense of ownership and a voice in the project. You may often be dealing with professionals that are not used to sharing the level of information required for this type of security, but what we found was that by engaging and listening to them, it was these teams that were able to define the need and come up with some great ideas that enabled this project to be successful."

"It's also extremely helpful when organizations like CRITICAL**START** and Palo Alto Networks are willing to invest the extra effort to support these overworked and understaffed institutions," she added. "When they're helping all of these different schools understand the process, why it's so important, and then to have a definitive action plan to support them at every step of the deployment—it's really what we need to take the next step."

"This new security environment will enable us to check many boxes when we're pursuing National Science Foundation grant opportunities, specifically standards in cybersecurity that we'll now be able to meet. Hitting these new thresholds will also hopefully open new opportunities for federal funding coming into the state."

— Elizabeth Mann, Finance Director for ARE-ON

CRITICALSTART

ARE·ON

Case Study

Moving Forward

Mann shared her insight on what she feels that ARE-ON will gain from this new MDR process and the relationships developed with CRITICAL**START** and Palo Alto Networks: "And then there's the value of avoiding the serious financial impact of these breaches," she continued. "That's funding dollars that we'll be able to protect and assign to areas where they will certainly do more good. Our staff will also be liberated from chasing down alerts—which was a skillset we really didn't have in the first place—and now we can assign those resources to more mission-critical tasks. The really big thing here is that CRITICAL**START** and Palo Alto Networks provided us with an economically feasible solution that was able to align with the tight demands of an educational system budget."

"But I also want to highlight one of my personal expectations from this experience," she concluded. "And that is the fact I want to be able to sleep at night. I truly believe this new approach to security will help get me there. Knowing that we have a plan and process in place to mitigate threats relieves my anxiety on the diverse levels of vulnerability we had with our institutions. Once they are protected, we can all focus on our efforts to grow ARE-ON well into the future."

Forecasted Results

- Thirty-six institutions protected including an estimated **100,000 endpoints**
- Over **100 million projected alert**s to be processed monthly
- Projected accuracy is **99.5%**

Want more information on CRITICAL**START?**
To see how we can help, contact us at www.criticalstart.com

CRITICALSTART