Small but mighty security team reduces security incidents by 80% and secures online environment for 1.5M students with Cisco Secure

> “We know we can rely on Cisco Secure to protect not only our network but also our customers and our reputation.”

Renat Vitkalov, CEO, AzEduNet

Organization
AzEduNet

Headquarters
Baku, Republic of Azerbaijan

Users
1.5 million students and 150,000 teachers at 4,300 educational institutions throughout the country

Industry
Information technology

Objective

The small, nimble team at AzEduNet must secure the Republic of Azerbaijan's entire national education network, which provides internet connectivity to more than 1.5 million students and 150,000 teachers at 4,300 schools and universities. AzEduNet's network is a constant target of cyberattacks, and the company needed a platform approach that would simplify security and speed up threat response and investigations.

Solutions

- Cisco SecureX
- Cisco Secure Firewall
- Cisco Umbrella
- Cisco Secure Email
- Cisco Secure Endpoint

Results

- Moved from ad hoc security to a platform approach that provides a unified view across the environment from a central dashboard
- Accelerated threat response and saved time on investigations and incident management, often from several hours to minutes
- Decreased the number of security incidents by 80% by stopping threats before compromise
- Simplified security solutions management

Providing a secure online environment for 1.5 million students

As the largest educational network in the Republic of Azerbaijan, AzEduNet provides connectivity and online services to the national academic, research, and educational sector. This includes serving 1.5 million students and 150,000 teachers at 4,300 educational institutions.

The government is working to diversify the information technology sector and develop IT resources for a population of 9 million people. One of the goals of the country, which had been recently torn by war, is to increase digital resources and e-services that are available to public schools and universities. "Everything was on paper in our country until the last few years, when the government started to automate all the education processes with online services. Now everything is online and students have to share private information on the internet. And we have to provide a safe environment for students and secure these services and the information of the Ministry of Education with state-of-the-art security," explains Renat Vitkalov, CEO at AzEduNet.

To keep up with the evolving threat landscape, AzEduNet needs to be nimble and innovative. "We are a small company and we have a small security team, but we are running a huge private network that's always a target. And we're trying to react quickly to any issues that come up," Vitkalov says. "Security has become extremely critical in the last couple of years, and we're using all possible resources to fight against threats."

Most of AzEduNet's educational services are internet-facing. Bahruz Ibrahimov, senior information security engineer at AzEduNet, estimates that about 70% of incoming connection requests originate from malicious sources. The large amount of data collected by disparate security solutions from multiple vendors, along with an extensive footprint that includes 200 Ministry of Education data center servers, created a complex environment. "We don't have enough staff to monitor every entry point into our network and correlate all the information from our security solutions," Ibrahimov says. "Our main problem was how to monitor all these systems from one central location, and managing all the solutions separately was a big headache for us."

A recent spike in security incidents emphasized how crucial it was to simplify security. AzEduNet needed to move from a piecemeal security architecture to a platform approach that accelerated threat response and saved time on investigations.

> "We are a small company and we have a small security team, but we are running a huge private network that's always a target."
>
> Renat Vitkalov, CEO, AzEduNet

Accelerating investigation and response time with a built-in security platform

One of the challenges in a complex, disparate security environment is that the telemetry data that each security tool logs is often analyzed in isolation and lacks the fidelity to detect more subtle and hidden attacks. Security analysts have to make decisions about the generated alerts in isolation—and teams with limited resources risk exposure because they lack the context to identify malicious intent. And when teams do act, the response happens one control point at a time without efficient coordination, wasting time and often failing to completely defend against the breach.

Recognizing these gaps, AzEduNet deployed Cisco SecureX, a cloud-native, built-in platform that connects the Cisco Secure portfolio and has extended detection and response (XDR) capabilities integrated with each product's console. SecureX provides unified visibility from a central console, enabling organizations to quickly visualize threats in their environment.

In addition to connecting its Cisco Secure products—Cisco Secure Firewall, Cisco Umbrella, Cisco Secure Email, and Cisco Secure Endpoint—AzEduNet integrated several third-party solutions with SecureX. "The integration with all our Cisco Secure solutions and with other vendors saves us response and investigation time, as well as saving time for our engineers. It helps us to simplify the monitoring of all these security devices from one point instead of separately from different monitors," Ibrahimov says.

By collecting and correlating data from different security sources, including threat intelligence and third-party solutions, the SecureX threat response application helps AzEduNet accelerate investigations and incident management, maximize operational efficiency with automated workflows, and reduce response time. "The orchestration capability of SecureX helps my team automate workflows based on different triggers aligned to common use cases, and therefore accelerate time to remediate," Ibrahimov explains. "We can now reduce or eliminate repetitive tasks and broaden the scope of cloud orchestration without having dedicated staff looking at every alert or notification. And in just a few minutes, we can understand 70% of what's happening and find the main source of an incident, instead of taking several hours."

> "The orchestration capability of SecureX helps my team automate workflows based on different triggers aligned to common use cases, and therefore accelerate time to remediate"
>
> Renat Vitkalov, CEO, AzEduNet

> “Now that we’ve simplified our process and saved time during investigations, we can follow the new security trends and integrate new security solutions to provide a more secure infrastructure for our educational network.”
>
> Renat Vitkalov, CEO, AzEduNet

Reduced complexity, maximized efficiencies, and increased customer trust

Cisco SecureX enabled the small AzEduNet team to meet their top objectives: simplify and automate daily tasks, accelerate investigations, and integrate security solutions for maximum efficiency. “We can create a security incident from SecureX and share this incident with our team. It helps us to automate our daily, routine work and improve workflows with SecureX orchestration services. And all of this simplifies our job,” Ibrahimov says. “Not having enough staff for everything that needs to be done is a big challenge for every company, not just for us. When we hire new engineers, we don’t need to teach them how to correlate all the events—we can give them access to the SecureX dashboard and even the more junior engineers can conduct investigations.”

With SecureX enabling the security team to stop threats before they compromise systems, AzEduNet saw an estimated 80% reduction in incidents. As a result of improved productivity, visibility, efficiency, and simplicity, AzEduNet can now dedicate time to more strategic and innovative initiatives. “Security is changing all the time and we need to follow these security trends. Without SecureX, we lost a lot of time in solving security issues and incidents. Now that we’ve simplified our process and saved time during investigations, we can follow the new security trends and integrate new security solutions to provide a more secure infrastructure for our educational network,” Ibrahimov says.

Vitkalov notes that the ability to rely on Cisco security engineers and other support resources is especially valuable for a small company with limited resources such as AzEduNet. And having a trusted partner like Cisco helps AzEduNet gain customer confidence, which results in opportunities such as joint projects with the Ministry of Education. “Cisco is doing a very good job in helping us deploy or design solutions,” Vitkalov says. “And we know we can rely on Cisco to protect not only our network but also our customers and our reputation.”