

EAST COAST MIGRANT HEAD START HELPS SECURE CHILDREN'S FUTURES WITH CHECK POINT



Customer Profile

East Coast Migrant Head Start Project

Industry

Non-Profit

Challenge

- Protect patient Personally Identifiable Information (PII)
- Prevent phishing, virus and malware attacks on both fixed and mobile endpoints
- Improve productivity of IT resources

Solution

- Check Point Harmony Mobile
- Check Point R80
- Check Point Quantum NGFW

Results

- Gained comprehensive security for their entire network against Gen V cyber threats
- Prevented phishing and malware across all endpoints
- Improved IT efficiency through improved visibility and security management

“Before Check Point, the team spent much of their time reacting to phishing attacks. With this constant stream of attacks now blocked by Check Point firewalls, the team can now work proactively to roll out more security features.”

—Lincoln Nguyen, Technology Solutions Specialist, East Coast Migrant Head Start Project

Overview

East Coast Migrant Head Start Project

East Coast Migrant Head Start Project (ECMHSP) is committed to preparing the children of migrant and seasonal farmworkers for success. They provide high-quality early childhood education services for children and families in a nurturing, culturally-sensitive environment and by providing services and advocating for children and families in their other areas of need. ECMHSP has 37 centers throughout the Southeastern United States from Pennsylvania to Florida, supporting almost 2500 students from first grade through high school.

Business Challenges

Protecting Private Personal Information

As a Federal Head Start Program, ECMHSP must comply with strict government security rules about the people it serves. The primary challenge facing the IT Security team at ECMHSP was to prevent their employees and the network from being undermined by phishing attacks, which accounted for up to 90% of their security breaches. The new security architecture had to support remote access from 100's of employees, using a wide variety of mobile devices across a wide geographical area. Also, given limited IT resources, ECMHSP wanted to improve the efficiency of its IT team as well as make its employees more productive by preventing them from being overwhelmed with spam, phishing, and other malicious attacks.



“Check Point gave us the coverage we needed to protect our client’s private information and ensure our compliance with government regulations in the face of an ever-changing array of threats.”

—Lincoln Nguyen, Technology Solutions Specialist, East Coast Migrant Head Start Project

Solution

Check Point Provided the Features, Flexibility and Efficiency Required

After evaluating multiple vendors, the ECMHSP IT team selected Check Point Next Generation Firewalls with SandBlast Network to provide the foundation of the company’s security architecture. In addition to the Check Point Firewalls, the team installed IPS, VPN support, URL Filtering, as well as Anti-Bot, Anti-Virus, and Anti-spam protection. These features stopped virtually all incoming attacks.

According to Lincoln Nguyen, Technology Solutions Specialist for ECMHSP, “Check Point gave us the coverage we needed to protect our client’s private information and ensure our compliance with government regulations in the face of an ever-changing array of threats.”

With many ECMHSP employees working remotely with clients in the field, the security team also had to ensure they could block any mobile attacks without diminishing their employees’ productivity. They needed a solution that worked with virtually any smartphone and was simple to install, use, and support. They chose Check Point SandBlast Mobile to handle this task. It proved a huge success: all employees use it without any burdensome oversight, and IT can install the app remotely in less than two minutes per device.

In addition, with more than 50 Firewalls required to support their sites and a large staff spread across the Southeastern United States, IT team members were a scarce and precious resource at ECMHSP. To manage their new system, the security team chose to install Check Point R80 Unified Security Management on a virtual machine. R80 not only proved vital in meeting the organization’s security challenges but vastly increased the efficiency of their IT team members. With the R80 features, the team finally had the tools it needed to monitor the entire network from a single location. This unified approach to security management allowed the team to work proactively on potential issues, rather than reacting to each new phishing threat that hit the wires.

“Managing our firewalls became a much easier task with the R80 System installed,” Nguyen said. “Policy creation and implementation are very straightforward. We can move a lot faster in pushing out new policies than we could before Check Point.”

“We’ve received only positive responses from our users.”

—Lincoln Nguyen, Technology Solutions Specialist, East Coast Migrant Head Start Project

Results

Check Point Firewall Yielded Immediate Results

ECMHSP saw meaningful results immediately upon cutting over to the new Check Point system. The hundreds of potentially dangerous phishing, malware, or viral emails the organization received on average each week dropped to zero overnight. Given that 85-90% of security issues were related to phishing attacks, the IT team’s productivity increased in direct proportion.

“Before Check Point, the team spent much of their time responding to phishing attacks,” Nguyen explained. “With this constant stream of attacks now blocked by Check Point firewalls, the team can now work proactively to roll out more security features.”

SandBlast Mobile Secured Access for All

With the majority of ECMHSP employees using their personal mobile devices for work, the IT team needed SandBlast Mobile to prevent malicious attackers from accessing the network remotely. The results exceeded the team’s as well as the users’ expectations.

Explained Nguyen: “SandBlast Mobile not only blocks access to malicious sites but also prevents attacks if an employee logs on to an insecure Wi-Fi network. The solution also monitors applications running on the phones to make sure they are always clean. With the application running quietly in the background, employees felt relieved to know that they could use their mobile devices safely without jeopardizing client information.”

The application also consumed far less compute resources than other solutions the team had tested.

“SandBlast Mobile had even less impact on users than we hoped,” added Nguyen. “We’ve received only positive responses from our users.”

Saving Critical Resources with R80 Unified Security

After stopping the attacks, Nguyen said the next most significant impact on the ECMHSP came from the implementation of R80.

“R80 gives us a single pane of glass to look through instead of needing to look in multiple locations,” said Nguyen. “And because it acts as a single, unified system, we can now implement policies that follow updates to our network, making our work much easier and our team more productive.” With R80 Unified Security in place to manage the Check Point infrastructure, the ECMHSP IT team felt it had implemented a complete security architecture that met today’s needs and would continue to do so far into the future

For more information, visit: <https://www.checkpoint.com/products/>