CARBONITE | **WEBROOT**
an **opentext** company | an **opentext** company

> **Webroot and Blackpoint Cyber offer a new layer of visibility that other vendors can't offer.**
>
> **Pedro Nunez**

At a Glance

Vertical
MSP

Year Founded
2008

Title
CEO: Pedro Nunez

Endpoints Managed
2000

Website
https://www.itsupportboston.us/

Key Findings

Time Savings
40 help desk hours per week eliminated

Efficiency
Client retention increased by 5% to 96%

Managed detection and response bolsters comprehensive, proactive security plans

About IT Management Solutions

IT Management Solutions is a managed services provider that supports 85+ clients across New England. About half of its clients are in healthcare and the others are spread across the finance, insurance, construction, manufacturing and professional services industries.

Pedro Nunez, CEO of IT Management Solutions, is closely involved in maintaining client security. He's automated over 100 processes and keeps group policies current and synced. Nunez also makes sure his clients are using the latest technology, runs updates and patches frequently, and keeps subscriptions up to date. Nunez, who joined the army 24 years ago, says that's where he learned his proactive strategy. He brings his experience in the military to training his team and building proactive and reactive response plans for his clients.

But Nunez also says he's worked with many security teams who haven't had enough people with the right skillsets monitoring client networks. He cautions that, "You cannot rely on any one vendor too much." To increase effectiveness, Nunez recommends teams, "Establish a relationship with vendors that can help you augment your current staff with contractors dedicated to your organization." The security tools he's deployed to his clients' endpoints are only a piece of his strategy, "A wide array of tools and people make up a successful team. Success is achieved when the company works together."

As a believer in finding the right combination of security tools for his clients, Nunez began shopping around after being disappointed with a previous vendor.

Before Blackpoint Cyber + Webroot

Nunez had used Sentinel One in the past. The company had a managed SOC, but Nunez noticed a level of visibility was missing. He decided to integrate Blackpoint Cyber with his Webroot® Business Endpoint Security to marry the benefits of a managed SOC with a high-performance antivirus.

Webroot Business Endpoint Protection plus Blackpoint Cyber's managed detection and response (MDR) services turned out to be an ideal solution; Webroot is able to alert the Blackpoint SOC of anomalies across the whole network, including IOT devices, and Blackpoint Cyber's threat hunters are able to quickly address the issue.

Additionally, Nunez saw his costs drop when he removed Sentinel One, savings which he quickly invested into Blackpoint Cyber's integration with Webroot. "Webroot and Blackpoint Cyber offer a new layer of visibility that other vendors can't offer," he says.

After Blackpoint Cyber

Nunez now has increased context surrounding threats spotted by Webroot on customer environments from within the Blackpoint Cyber console. Adding this integration with Webroot increased Nunez' trust that his clients' endpoints were protected.

"MDR has provided a whole different layer of security that didn't exist before. It gives me peace of mind."

That peace of mind would prove useful.

Beginning in July 2020, the Blackpoint Cyber console displayed alerts about suspicious activity. A Romania-based group began targeting one of Nunez's customers with APTs attempting to breach their network. Nunez recalled the beginning of the attack, "A client received an email and within 30 minutes of clicking it, the battle began."

As usual, Nunez was proactive, and Webroot plus Blackpoint Cyber amplified his team's efforts. "I received an alert from Blackpoint. MDR was working away killing PowerShell commands." Every area of security avenue had been tested prior and continued to hold up.

The attack reminded Nunez of his days in the military. "[We were] up at 3 a.m., working as a team. The attacker wanted to take down the critical systems of an entire city. Everyone on my team, working together, yet working on their own part, is what saved the city." Nunez explained his strategy, "When you're under attack, you don't scream, you move in."

Nunez communicated with his client daily, set expectations and kept them calm during the attack. After nearly a month, he repelled the attack and his clients were not compromised.

Conclusion

So, what advice would Nunez give other MSPs facing similar threats?

He recommends creating simulations of worst-case scenarios and running drills to defend against them.

"Test all plans and continue to run drills at least every six months. Huddle with team members on the rapid response team. When everyone works together, that's how you get results."

Next on Nunez' agenda: boosting his offerings for client security awareness training.