Securing SLED Clients with Exceptional Managed Services, Security Expertise, and Fortinet Solutions from Exclusive Networks

Introduction

Ty Harris is the CEO of Edge Smart Solutions, a certified Minority Business Enterprise. Ty is based in Orlando, Florida, and helps clients solve IT and cybersecurity challenges by offering an extensive portfolio of managed services and industry-leading Fortinet Security Fabric products including Next Generation Firewalls (NGFW), Software-Defined Wide Area Networks (SD-WAN), Distributed Denial of Service (DDoS), and other security solutions for mobility, cloud, and the Internet of Things (IoT).

> *"K-12 schools have unique cybersecurity and IT challenges. They have limited budgets and staff but have been especially hit hard by ransomware and other security attacks."*
>
> **TY HARRIS**
> CEO OF EDGE SMART SOLUTIONS

Ty earned a stellar reputation across more than two decades in the security industry for providing clients with unparalleled expertise, exceptional quality, and unwavering integrity. Ty has serviced customers in a variety of fields but specializes in education and State and local government (SLED) organizations. This afforded him an introduction into various Kindergarten through twelfth grade (K-12) schools where he formed close relationships with educators and technology professionals.

"K-12 schools have unique cybersecurity and IT challenges," says Ty. "They have limited budgets and staff but have been especially hit hard by ransomware and other security attacks."

In December 2020, the FBI warned of dramatic increases in cyber threats against SLED organizations—and especially against K-12[1]. Reports show a near-doubling of attacks as compared to other sectors1 from numerous malware strains including ZeuS trojan against Windows platforms and Shlayer loader on Mac desktops. Also, five primary strains used in ransomware and DDoS attacks that disrupt operations and eLearning classes. With the average ransom now exceeding $300,000[2], and the cost of downtime nearly as high, schools can’t afford to risk exposure to a security attack.

“One large school district had concerns about potential security vulnerabilities that could result in ransomware, bots, or DDoS attacks,” says Ty. “I had developed a close relationship with the technical team, so they asked me to complete a vulnerability assessment and recommend the best security solutions and services to address these concerns.”

To complete the assessment, Ty leveraged his relationship with Fortinet—the world’s largest security firm, and Exclusive Networks—Fortinet’s largest distribution partner. Although the school district had a Written Information Security Program (WISP) in place based on National Institute of Standards and Technology (NIST) guidelines, a thorough assessment uncovered several vulnerabilities that could lead to potential threats.

“Due to the pandemic, the school district had created new eLearning classes for remote students,” says Ty. “This increased Virtual Private Network and Remote Desktop Protocol usage, which in turn exposed the district to botnets, ransomware, and DDoS attacks.”

Brute force attacks against RDP has become the primary vector used by attackers to perpetrate ransomware. Also, bots—short for malicious robots—can cause network performance degradation. DDoS attacks can cause network and website interruptions and lead to expensive organizational downtime. The school district wanted to reduce these risks while improving visibility, scalability, and ease-of-use through “single pane of glass” management.

“The professionals from Exclusive Networks were fantastic,” Ty says. “Along with Fortinet, they helped my team complete a thorough assessment for the school district and then recommended a variety of solutions to address the client’s needs. Exclusive Networks provided us with a dedicated account manager, white-labeled managed security services to enhance our offerings, implementation and solution expertise, and ultra-fast response times.”

> *The team at Exclusive Networks seamlessly became an integral part of my team. They allowed us to expand our business and compete on a larger scale while providing Fortinet Security Fabric expertise, implementation, training, and services.”*

With network security breaches and ransomware escalating, a disintegrated point solution approach for educational institutions can create the equivalent of a classroom full of undisciplined children. Security postures should adhere to best practices, such as those prescribed by the SANS Institute[3] and the Consortium for School Networking (CoSN)[4]. This can help ensure agility to keep abreast of constant changes in education, regulation, and cybercrime. Also, this approach can help reduce costs, personnel needs, and security risks. The Fortinet Security Fabric includes Next-Generation Firewalls (NGFWs), FortiSwitch network switches, FortiDDoS protection, and FortiAP secure wireless access points to address these needs.

“The team at Exclusive Networks seamlessly became an integral part of my team,” says Ty. “They allowed us to expand our business and compete on a larger scale while providing Fortinet Security Fabric expertise, implementation, training, and services.”

Today, the school district has dramatically increased their security posture while reducing cyber threats for ransomware, bots, and DDoS attacks. Through his continued relationship with Exclusive Networks, Ty Harris has been able to expand his business and offer clients in SLED and other markets exceptional managed security services and award-winning Fortinet Security Fabric solutions.

[1] CISA and FBI warn of rise in ransomware attacks targeting K-12 schools | ZDNet
[2] Average ransomware payouts shoot up 171% to over $300,000 (tripwire.com)
[3] “The CIS Critical Security Controls for Effective Cyber Defense,” SANS Institute, accessed May 8, 2018. 4: CoSN Cybersecurity Leadership Initiative, CoSN, accessed May 8, 2018
[4] CoSN Cybersecurity Leadership Initiative, CoSN, accessed May 8, 2018