CASE STUDY

Capstone Rural Health

Industry:

- Healthcare

Stats:

- Locations: 3 sites in Parrish, Jasper, and Nauvoo, AL
- Medical staff and employees: 36
- IT staff: 1

Challenges:

- Single IT staff member has limited time to dedicate to anomaly detection and investigation
- With healthcare being a big target for hackers, needed a robust analytics system on a budget
- Audit preparation and demonstrating policy compliance can be time-consuming and difficult

Scrutinizer enables a single IT professional to proactively secure, monitor, and optimize a multi-site network

Introduction

Capstone Rural Health is a non-profit, federally qualified health center. With core values that include “compassionate,” “community-minded,” and “patient-centered,” Capstone offers affordable primary, preventative, and wellness services to patients from all walks of life, regardless of their ability to pay for treatment.

The challenge

The healthcare industry has become a frequently targeted market for cyberattacks, including ransomware and data theft. Compliance mandates, intended to protect patient safety and ensure data privacy, mean that IT must follow best practices and demonstrate compliance with regular external audits. Proactive monitoring of every conversation traversing the network is a critical component of reducing risk, safeguarding medical records, protecting patient safety, and delivering world-class clinical care.

IT Manager Jason Workman is the sole IT professional at Capstone Rural Health; maintaining the institution’s daily operations requires him to wear many hats. Due to his diverse responsibilities he is only able to dedicate a small portion of his time to cybersecurity. Manually combing through firewall logs generated across three sites was inefficient and would not scale. Workman needed a proactive solution to constantly monitor the security of the network and alert him when anything needed his attention.

In addition, he needed a solution that provided visibility over the users and applications that consume the bandwidth resources of his clinical environment.

The solution

To gain better visibility and context into his network, Workman turned to Scrutinizer. The solution monitors the network in the background for him while he focuses on other tasks. When an alarm gets triggered, automatic email alerts let him know exactly where and when to start investigating. Then the rich context and granular data Scrutinizer provides allows him to complete root cause analysis for network and security incidents, then remediate the situation quickly. This system ensures that he uses his time much more efficiently.

Workman can also save time investigating false positives from other security platforms by cross-referencing data with Scrutinizer. When another platform sent an alarm indicating a massive infection across the network, Workman sprang into action, turning to Scrutinizer to investigate. Scrutinizer's network traffic analytics showed that traffic patterns were normal and indicated this was a false alarm. Rather than wasting precious time, he was able to return quickly to his normal duties. The next day, he received confirmation from the vendor that it had been a false positive caused by an update within their product.

"I would absolutely recommend [Scrutinizer] to all my peers," Workman says. "This is a necessity... and if you don't have it, you're missing a big piece of your security system."

Scrutinizer provides value on the networking side, as well. As Capstone implements large network projects, Workman needs to ensure that the impact on user experience and clinical workflows is as minimal as possible. Scrutinizer provides the information needed for smooth transitions during these projects.

> "I would absolutely recommend [Scrutinizer] to all my peers. ...if you don't have it, you're missing a big piece of your security system."

Results

Scrutinizer has provided Capstone with a highly efficient tool to monitor the network for incidents, whether they're security threats or user experience issues. Capstone has used Scrutinizer to:

1. **Optimize investigation time:** Scrutinizer is Workman's eyes and ears when he has to focus elsewhere. Proactive alarms and alerts tell him exactly when and where to begin his investigation; granular data and rich context make his investigation even more efficient.
2. **Minimize false positives:** By using Scrutinizer to cross-reference data from other security platforms, Workman can more easily spot false positives, saving the time he would otherwise have to invest in looking into them.
3. **Easily address compliance audits:** Historical visibility with data context and reporting for every network conversation and transaction makes it easy to answer auditor's questions and demonstrate policy compliance.

©Plixer, LLC. All rights reserved. Plixer and Scrutinizer are trademarks of Plixer. All other brand names are trademarks or registered trademarks of their respective companies.

The content in this document is for informational purposes only and is subject to change by Plixer, LLC without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, Plixer, LLC assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Plixer, Plixer, LLC has no obligation to develop or deliver any future release or upgrade or any feature, enhancement, or function.