THE CONNECTION
"We'll Connect You to The World"

Stay Connected® Managed Breach Detection

Powered by Perch

Identify
Protect
Detect
Respond
Recover

As an added layer to our impressive multi-layer threat detection offering, we introduce Stay Connected® Managed Breach Detection.

In 2018, the Ponemon Institute found that 67% of SMBs experienced a cybersecurity attack — costing these companies an average of $400,000. But 47% of SMBs responded that they have no understanding of how to protect themselves from cyber attacks.

As an SMB, you can protect yourself affordably against this growing risk. Just like your home security system monitors for signs of intruders, we provide 24x7 monitoring on your business network for all kinds of threats. Cybersecurity monitoring is a critical need for businesses of any size – and offers the same peace of mind you gain from your home security system.

When we see a threat on your network, we immediately take action. Our experienced and credentialed security team works around the clock to assess, and when necessary, respond to any sign of threat. Cyber criminals don't limit their attacks to business hours; so we never leave your "home" unprotected.

Some of the benefits:

- 24x7 monitoring at an affordable rate
- Stop hackers and network attacks in their tracks and before damage can be done
- Prevent a damaging incident to your company's reputation
- Meet compliance and regulatory requirements

The Connection, Inc. has been providing expert support and solutions for keeping small to medium-sized businesses connected to the world since 1992.

We offer software and services that will monitor your systems and network 24x7.

Our **Stay Connected®** Suite of proactive Managed IT Services will ensure optimum network performance keeping your business connected, improve security and increase productivity by choosing the solutions that best fit your needs.

Our offerings include:

Proactive Technology Management

Network Administration

Technology Consulting

Reactive Support Services

Unified Communication Services

Security Services

NEW JERSEY'S PREMIER MANAGED SERVICE PROVIDER

Stay Connected®

CASE STUDY

Steinbrueck Health Center
Palmyra, Missouri

The Problem

For most small healthcare practices, cybersecurity concerns are a complex and insurmountable problem. Modern cyber threats are quickly changing, complex and difficult to prevent. This problem is compounded by the reality that most small healthcare practices simply don’t have the budget necessary to adequately defend their network.

Lisa Steinbrueck is no stranger to this dilemma. As the Privacy Compliance Officer for Steinbrueck Chiropractic Health Center in Palmyra, Missouri, she has experienced these challenges firsthand.

“Small practices cannot afford to hire IT personnel with specialized training that is required to maintain proper security, let alone meet HIPAA requirements,” Steinbrueck says. However, Steinbrueck knows these troubles don’t absolve a small practice from implementing the necessary security requirements to protect their patient information from cybersecurity threats.

1. Cybersecurity is a complex and insurmountable problem
2. Modern cyber threats are quickly changing, complex and difficult to prevent
3. Most small healthcare practices simply don’t have the budget necessary to adequately defend their network

The Solution

Steinbrueck was introduced to Perch Security. With a network sensor placed inside the network, the practice was able to detect and respond to the threats that others in the healthcare community warned them about.

As a Partner of Perch Security, The Connection, Inc. has the tools to continually monitor the traffic that does not make any sense to the average employee at any small to medium-sized office. The threat database that we maintain means a faster awareness in protecting everyone involved. We are able to get protections and updates in place quickly to mitigate potentially devastating consequences.

Key Advantages

For any doctor wanting to satisfy the HIPAA, OIG, Medicare and other federal requirements for protecting PHI, this service is a big win,” Steinbrueck says.

1. Protecting patient information
2. Overall cost reduction – avoiding fines and penalties
3. Preventing security breach, a potentially practice-ending event

“First, protecting patient information requires a high degree of attention to cybersecurity to truly maintain a viable practice,” Steinbrueck explains. With Perch in place, Steinbrueck’s practice now has deeper network visibility and fast response from trained threat analysts to handle any alert that may be generated. “This was something we just couldn’t do at all before Perch. Knowing that Perch’s analysts are watching for any threats and will inform me if they see one is invaluable,” Steinbrueck says.