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®

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

Stay Connected®
Mobile Device Security for Healthcare Organizations

Powered by Absolute

Secure your sensitive healthcare data and prove compliance

Secure your sensitive healthcare devices, data, and applications

- Protect patient data with in-depth data awareness
- Improve security and IT operations with faster discovery and remediation across all endpoints
- Automate incident response: geolocation, device freeze, and remote data delete

Support HIPAA & HITECH Compliance

Ongoing compliance checks and automated reports so you are always audit-ready

- Probe for violations across all endpoints
- Validate patient data integrity with self-healing endpoint security
- Reduce the time to prepare audits with ongoing compliance checks across your endpoint population

Data security for distributed healthcare delivery

Fortify personal health information (PHI) for your telehealth, home health, and mobile clinical staff

- Pinpoint device locations and put a fence around where your data can go
- Protect your providers and avoid data exchange errors that lead to non-compliance
- Take action with custom commands to restore security on distributed devices

Protect data across your evolving federated healthcare network after a merger or acquisition

Easily merge your health systems, with seamless endpoint orchestration

- Sync your expanded attack surface with uniform security controls for instant compliance
- Integrate systems, controls, users, and machines with precision commands

Tamper-proof device visibility and protection

The Stay Connected® Platform for Healthcare Organizations is the only endpoint visibility and control platform that provides a persistent, self-healing connection between your IT and Security teams and all of your devices — on or off your network

- Boost IT and security staff productivity and secure all devices across different platforms
- Automate endpoint hygiene, speed incident detection and remediation, and reduce IT asset loss
- Uniquely able to survive malicious attacks, even after hard drive or OS wipes

CASE STUDY

BACKGROUND

Apria Healthcare provides at-home clinical services to their patients across the United States. Employing more than 8,000 healthcare providers, Apria is at the forefront of a growing movement to take healthcare out of hospitals and into the homes of patients.

CHALLENGE

Most of Apria's team members are geographically dispersed, using laptops and other mobile devices. While this provides efficiencies and allows Apria to provide the highest level of in-home healthcare services, it also creates potential vulnerabilities. Precautionary security measures were required. The IT team needed a solution that would help them:

- Mitigate the potential risk of exposed data
- Extend their visibility to include remote devices
- Protect the personal health information of patients to avoid a healthcare data breach

SOLUTION

Apria selected Mobile Device Security to solve their endpoint security challenges. The reliable two-way connection to each device provided value to the organization right away. Once the agent was activated, the IT team had visibility across all of their devices. "Each of our devices is tied to an individual," said Janet Hunt, Senior Director, IT Quality & Support Services, at Apria. "We can establish groups that we categorize by employee, location, and function."

To consistently deliver a high level of security, new devices are activated at the factory before they are shipped. "When we purchase new hardware through our vendor, the first thing we do is load the software onto the devices," said Ms. Hunt. "If any details change, like a username or location, we receive an alert so we can investigate further and take prompt action by either freezing or wiping the device as required."

RESULTS

Apria is now confident in their ability to see and control all of their devices and secure sensitive information, keeping them in compliance with HIPAA and other health regulations. They can track and report on inventory, device location and activity — no matter where the device is located.