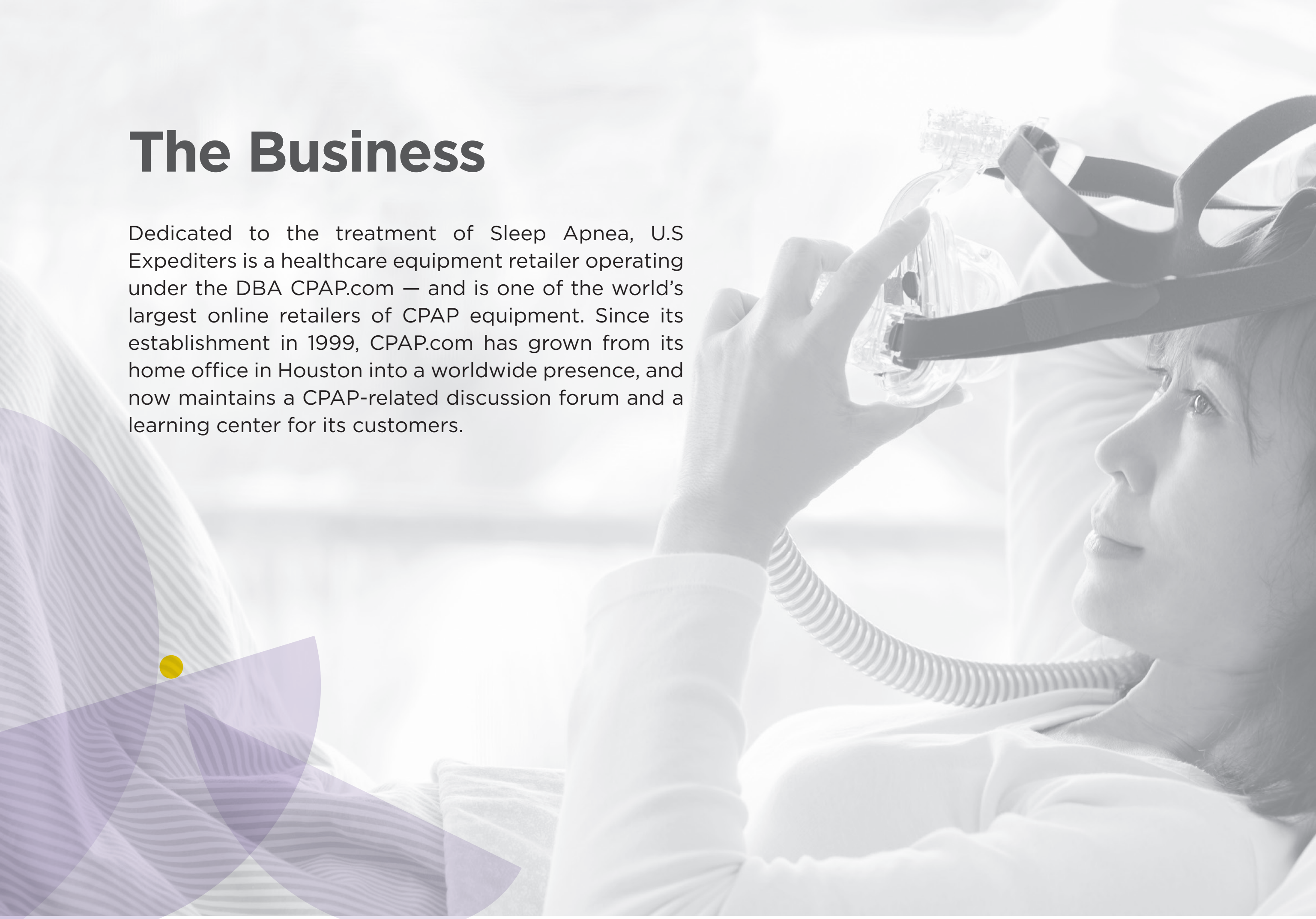
PERCH

CASE STUDY

CPAP.com Develops Threat Intelligence Progam To Detect and Respond to Threats NH-ISAC Warns About

The Business

Dedicated to the treatment of Sleep Apnea, U.S Expediters is a healthcare equipment retailer operating under the DBA CPAP.com — and is one of the world's largest online retailers of CPAP equipment. Since its establishment in 1999, CPAP.com has grown from its home office in Houston into a worldwide presence, and now maintains a CPAP-related discussion forum and a learning center for its customers.



The Challenge

While CPAP.com is a smaller heath care organization under 200 employees, it maintains and protects a large volume of patient information. They share the same requirements and expectations that larger organizations face to stay ahead of the threats emerging in the healthcare vertical – which is a daunting task.

For CPAP.com, meeting this challenge meant going beyond the typical security controls like antivirus and firewalls. “For years, passive defenses like that were usually enough,” says John Nelson, Security Officer for CPAP.com. **“The modern threat landscape demands a more proactive approach. We must continually assess that landscape and our security posture within it. We should be actively identifying and mitigating vulnerabilities within our environments that others in our industry have warned us about.”**

In the healthcare vertical, joining NH-ISAC as a member is the key first step. NH-ISAC is an information security community primarily focused on sharing timely, curated and relevant threat information with one another. However, while CPAP.com was a member of NH-ISAC, they were still unable to use its threat intelligence cost-effectively.

“We have very high quality, actionable threat data available to us that is published by NH-ISAC for its members,” Nelson says. “In fact, that’s why we joined the community. We’ve found that **NH-ISAC intelligence is several orders of magnitude better than anything else we use.**” But CPAP.com was manually processing and reviewing every threat published by NH-ISAC and correlating for matches. It was a time consuming and tedious process that was not effective for a smaller organization.

The Solution

Perch Security provided CPAP.com with a network sensor that evaluates all network traffic and downloads threat intelligence automatically from NH-ISAC. Within a few hours, Nelson had the sensor properly configured and running in the network environment. The sensor was able to review all network traffic and automatically correlate with threats reported by other members of the NH-ISAC community.

“The difference was immediate,” Nelson said. “Our old manual process generated a lot of noise. When Perch generates an alert, we know it’s actionable.” He was glad to see that manual processing and review of alerts was automated by Perch Security.

Every threat alert that Perch Security generates for CPAP.com goes into an easy-to-review web application. Nelson can see and review his entire threat landscape within a single dashboard. While he logs in often to review the alerts, Perch threat analysts always take the lead in the first round of alert review and triage.

One key deliverable to an effective threat intelligence program is having threat analysts on staff to triage alerts and look for important intelligence that effects the organization. However, smaller organizations simply do not have these resources. CPAP.com is no different. “I like that Perch has my back,” says Nelson. “They provide the triage and only get me involved when I need to be.”

> “
>
> OUR OLD MANUAL PROCESS GENERATED A LOT OF NOISE. WHEN PERCH GENERATES AN ALERT, WE KNOW IT’S ACTIONABLE.
>
> **John Nelson**
> Security Officer
> CPAP.com

Results

1. CPAP.com now receives **only a few alerts per day** from the intelligence that NH-ISAC provides. They get high quality, actionable alerts that don't require time for Nelson unless the alert warrants that attention.

2. With Perch, CPAP.com has **much deeper network visibility into threats** that other security controls don't provide. "We have visibility now into all sorts of anomalies," Nelson said. "We're able to see file downloads with macros, policy violations such as unencrypted web traffic, and threat data from malicious sources that other healthcare organizations warn us about."

3. CPAP.com can consume and use the threat intelligence feed provided by NH-ISAC. They have a **fully-functioning threat intelligence program** staffed with experienced threat analysts from Perch Security. Alerts are judiciously triaged, reviewed and assessed; keeping CPAP.com ahead of the threats they face alongside others in the industry. "Perch Security has delivered a solution for us that typically only the largest of hospitals would have the budget to build out. Perch Security allows organizations of all sizes to develop an affordable and effective threat intelligence program."

Visit NHISAC.org/Perch to sign up for the Perch Security / NH-ISAC Parntership program

> PERCH SECURITY HAS DELIVERED A SOLUTION FOR US THAT TYPICALLY ONLY THE LARGEST OF HOSPITALS WOULD HAVE THE BUDGET TO BUILD OUT
>
> **John Nelson**
> Security Officer
> CPAP.com

NH-ISAC
NATIONAL HEALTH - ISAC

National Health Information Sharing and Analysis Center, is a non-profit, member-driven organization offering healthcare stakeholders a trusted community and forum for sharing vital Cyber Threat Intelligence with each other to create situational awareness, inform risk-based decision-making and mitigate against threats. Membership becomes an extension of your security operations team.

nhisac.org

PERCH

Founded in 2016 in Tampa, FL, Perch Security was created to meet cybersecurity needs by enabling institutions of any size to detect the threats their sharing community warns them about — without costly equipment or analyst hours. Perch's goals are to help our customers detect 100% of the threats shared with them, connect them with their best sources of intelligence, and to strengthen sharing communities through increased participation.

PerchSecurity.com