

**CASE STUDY**

## Securing every single entry point, keeping patient data protected in healthcare services

In a time where healthcare organizations are heavily targeted by hackers, United Networks of America uses Red Sentry to protect their network of healthcare organizations.

### INTRODUCTION

United Networks of America is one of the largest providers of value added managed care products and services in the United States. UNA has more than 240,000 participating Providers serving more than 120.1 million members.

With this great reach comes great responsibility, which is why UNA focus so heavily on cybersecurity and making sure their entire network is secure.

### CHALLENGE

Networks of organizations face unique cybersecurity challenges, because one weak point in the network can give an attacker access to all other organizations within it. Even if 95% of companies in the network are secure, one open door is all a hacker needs. Because of this, group-wide security solutions are more crucial now than ever.

In addition, being a healthcare network creates even greater responsibility, because healthcare companies are being targeted more and more frequently.

### SOLUTION

UNA utilizes Red Sentry for all of the organizations under their umbrella. With multi-tier visibility, they're able to look quickly at a dashboard, prioritize, and send resources efficiently. They can then dive deeper into specific groups wherever needed.

One of the groups under UNA that benefit from benefiting from this UNA solution is the American Cosmetic Surgery Network. As a network under UNA, they not only have protection within their own organization, but they are protected against vulnerabilities found in other UNA groups that they may have less control over.

### BENEFIT

With a network-wide cybersecurity focus, all companies affiliated with UNA can stay secure.

### RESULT

UNA and its affiliates can continue to be leaders in the healthcare space, while keeping sensitive data within their entire network secure.



"Great enterprise tools for risk assessments. We were up and running on the software in just one day. Very easy team to work with and extremely affordable for the amount of visibility and features you get."

**David Lewandowski**  
CTO, United Networks of America



"The Healthcare sector has been heavily affected by cyber attacks this past year. As we have so much sensitive data in our business, security is one of my main concerns. Since we've been using Red Sentry, I feel more confident because my team knows which patches need to be applied first and how to test them afterwards."

**Dana White**  
CTO, American Cosmetic Surgery Network