Critical Insight

Case Study

United Derm Partners

United Derm Partners' mission is to deliver patient-centered, physician-focused services to its 26 dermatology locations nationwide.

Introduction

> We needed one partner who could do it all — soup to nut — with a pricing model that made sense for practices like ours.
>
> **Nathan Wright**
> **Director of IT**

Organizations spend an average of $408 per patient record due to a healthcare breach.

United Derm Partners (UDP) formed in 2016 with the acquisition of its first dermatology practice and quickly expanded to 4 practices nationwide with 24 locations by the end of 2018. The practices that UDP acquired needed guidance and resources to mature their security programs. UDP's HIPAA risk assessment energized the team to add value quickly in prioritizing the information security program across all newly acquired practices.

Nathan Wright, Director of IT, leads a small department with many competing priorities. He prepared UDP's response to the risk assessment giving clarity to three significant priorities: monitoring, endpoint management, and network security. He immediately recognized the need for a partner who could deliver a complete solution that tackled all three priorities and began by focusing his evaluation on Managed Detection and Response (MDR) providers.

Critical Insight solved the problem

Among the solutions Wright evaluated, Critical Insight stood out. Instead of leading with technical jargon, Critical Insight demonstrated a focus on putting people first, paired with technical ability in kind.

Wright recalls that Critical Insight said, "We have great people with the pedigree and background you need. We understand healthcare security, and we will guide you, as needed, every step of the way."

By adding Critical Insight, UDP did not need to build an internal security department across their various practices and locations. Implementation was easy with an entirely agentless solution, and the pricing model was all-inclusive and structured in a manner that made the solution scalable for an organization looking to grow. It was equally attainable for both small and large practices with a highly distributed footprint.

Knowing they needed what Critical Insight had to offer, UDP selected MDR, continuous vulnerability identification (CVI), Office 365 monitoring, and began working towards Azure monitoring as well.

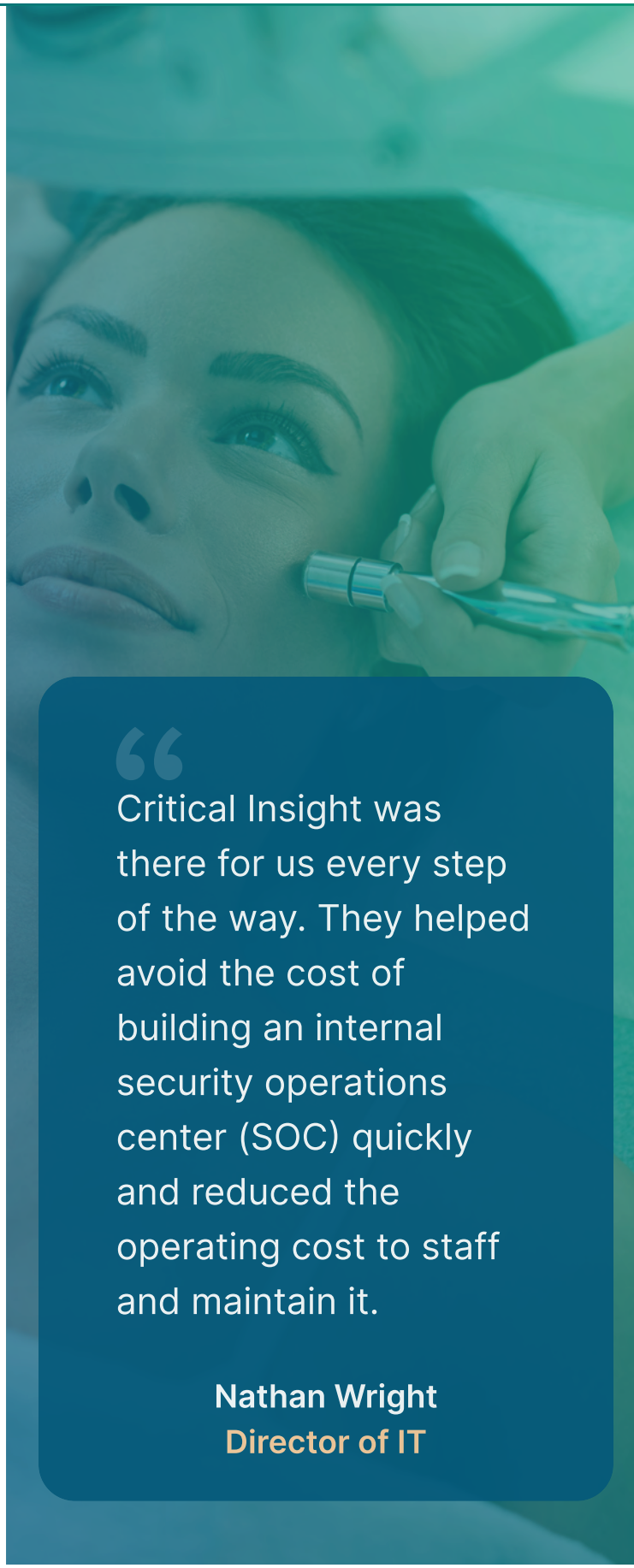
> "Our challenge was to help operate multiple clinics with a small IT department delivering on many competing priorities. We needed a partner who could provide the right kind of coverage for our organization that had healthcare knowledge. Critical Insight did that for us.
>
> **Nathan Wright**
> **Director of IT**

Critical Insight now monitors all of UDP's practices, reducing risk in many critical areas.

Continuous vulnerability scanning is performed, and analysts in the Critical Insight Security Operations Center defend UDP 24/7. UDP receives high-value reports about incident investigations rather than having to sift through logs themselves.

At a time when cyberattacks are becoming more frequent, Wright says, "CI gives us notice of what's going on faster than we would detect without them. They communicate clearly and quickly. It's a real value-add for UDP's practices and patients."

Beyond compliance, the decision to partner with Critical Insight made good business sense because it reduced the costs associated with building and staffing an internal security operations center (SOC). Critical Insight's MDR solution touched on more risk-reducing factors than any other solution available for the dollar spent.



> "Critical Insight was there for us every step of the way. They helped avoid the cost of building an internal security operations center (SOC) quickly and reduced the operating cost to staff and maintain it.
>
> **Nathan Wright**
> **Director of IT**