

HEALTHCARE CASE STUDY

Morphisec Helps Houston Eye Associate Stay Agile Against Attacks



Customer Profile

Houston Eye Associates is the largest ophthalmology practice in Texas with 24 locations, 60 doctors, 600 employees, and 1,200 endpoints. In business for more than 5 years, the company does upwards of \$100 million in revenue annually through a combination of healthcare services and eye-ware sales.



Challenge

Tom Merkle serves as the CIO for Houston Eye Associates. He leads a help desk team, has some support staff, and relies on a SOC provider to analyze his logs, but Tom is otherwise the only one responsible for cybersecurity. When something goes wrong, he's the first one to hear about it and the only one to respond.

With so much responsibility on his shoulders, Tom has a strong incentive to prevent attacks as early and often as possible. No small feat. "I kept seeing new vulnerabilities appear," Tom says, "And more and more they were being exploited before the vendors could patch them." Realizing how vulnerable he was to zero-day attacks, he went searching for a solution...and then the Covid-19 pandemic started.

Like so many other businesses, Houston Eye Associates was thrown into turmoil by the pandemic. The company saw around \$8 million in business disappear, leading to belt-tightening everywhere. Tom also started noticing a huge rise in phishing attacks disguised as information about Covid. The organization faced threats both medical and digital, and each made the other one harder.

"I was losing a lot of sleep wondering when we were going to get hammered." Tom admits. But with shrinking revenues, there was no enthusiasm to hire security professionals or spend on expensive solutions. Tom saw only one option: invest in whatever tool could deliver the most protection for the least cost.

Solution

Tom and the sales team at Morphisec connected in late 2019. Tom was eager to explore how Morphisec could complement his security strategy, and he knew the cost fit comfortably into his budget. But the pandemic changed his plans. He went to the board to make the case for additional funding so he could implement Morphisec immediately.

INDUSTRY

Healthcare

ENVIRONMENT

- 1,200 endpoints running on Windows.
- 600 employees spread across 24 locations.
- CIO supplemented by help desk and basic support staff.

CHALLENGES

- Defending against increasing zero-day threats using signature-based defenses
- Managing cybersecurity as a one-person operation
- Staying secure while the Covid-19 pandemic disrupted operations and fostered new threats.

SOLUTION

- Deploy breach prevention from Morphisec on endpoints and servers
- Use proactive cyber defense to relieve pressure on other defenses and the CIO
- Rethink the cybersecurity strategy around having an effective first and last line of defense



"I told them, you've already approved a \$2 million IT budget for this year. I won't ask you for another cent if you will approve the cost of Morphisec."

— Tom Merkle, CIO, Houston Eye Associates

"I told them, you've already approved a \$2 million IT budget for this year. I won't ask you for another cent if you will approve the cost of Morphisec." The board found Tom's case compelling even if they were averse to any extra spending.

Morphisec fit organically into Tom's existing cybersecurity strategy. As essentially a one-person operation, Tom relied on layered protection supplied by multiple vendors – for antivirus, EDR, endpoint protection etc. - who could enlist his input only when it was absolutely necessary. Since Morphisec randomizes the application memory, it successfully prevents attacks and takes the pressure of response and remediation off Tom's shoulders.

The breach prevention that Morphisec deploys was also the ideal solution for the pandemic. Cyber attacks spiked throughout 2020, and hackers experimented with new attack types and exploit strategies. Signature-based protections couldn't thwart these novel attacks. Morphisec, on the other hand, makes the memory unreachable to old, new, simple, and sophisticated attacks alike.

Results

Cyber attacks added insult to injury at so many companies fighting to survive the pandemic, but not Houston Eye Associates. They experienced no significant cyber incidents in 2020 despite the elevated threat level and the complications created by remote work.

Tom estimates he receives around 5 alerts a week from Morphisec. But they're just updates: the threats have already been identified and neutralized without needing Tom's input. "I feel like you're my last line of defense," he says, which couldn't be more important in a situation with few security resources (and lots of valuable data) facing off against the most aggressive cyber attacks in history.

With Morphisec preventing so many threats, Tom has begun to reconsider his layered cybersecurity strategy. Microsoft Defender offers the same level of signature-based protection as solutions Tom pays for, except it's free and already installed on every endpoint. Plus, it works seamlessly in conjunction with Morphisec, forming a dual-layer defense that consolidates the number of solutions in play while multiplying the level protection. Houston Eye

Schedule a demo now: demo@morphisec.com