How cloud security keeps patient and employee data safe.

Organizations:
Memorial Hermann Health System

Headquarters:
Houston, TX

Users:
24,000

Objective:
By adding Cisco Umbrella to its existing security stack, Memorial Hermann Health System achieved a significant reduction in malware and extended off-network protections for its employees.

Solution:
Cisco Umbrella
Cisco Umbrella Investigate

Impact:
• Reduced security events below .05%
• Reduced investigation time by 80%
• Extended protections to off-network devices

“Cisco Umbrella protects against threats like ransomware that target PHI and PII and jeopardize our ability to care for patients.”

Zach Phillippe
Cyber Security Manager
Memorial Hermann Health System
The challenge

Safeguarding valuable patient and employee data

Memorial Hermann Health System appreciates the power of collaboration. The largest not-for-profit health system in southeast Texas brings together care delivery, physician, and health solutions to create a truly integrated health system, underpinned by an innovative health information exchange that enables care providers to share vital patient data.

“In the course of caring for our community, our 5,500 affiliated physicians and 24,000 employees regularly come into contact with the kind of extremely sensitive data like personally identifiable information (PII) and personal health records (PHI) routinely targeted by cybercriminals,” says Zach Phillippe, cyber security manager at Memorial Hermann. “A successful malware attack may not only result in compromised patient trust and regulatory compliance, but can also impact critical systems and disrupt our ability to provide patient care.”

In keeping with its relentless focus on patient safety, Memorial Hermann sought to strengthen its security with a solution that could protect patients and providers against the ever-evolving threats of ransomware, malware, command and control (C2) callbacks, and other threats. “It had to be strong enough to protect every device connected across our system—even those working away from of our network,” says Phillippe, “and it needed to easily integrate into our existing security stack.”

“A successful malware attack may not only result in compromised patient trust and regulatory compliance, but can also impact critical systems and disrupt our ability to provide patient care.”

Zach Phillippe
Cyber Security Manager
Memorial Hermann Health System
The solution
Increased security and visibility
“We wanted better control of our network traffic, which required the kind of insight we lacked,” says Phillippe. “We were using other inline protection tools, but we couldn’t see everything that was happening on the network, and we had limited line of sight to our road warriors working from their laptops off the network.”

While several tools were initially evaluated, Memorial Hermann chose Cisco Umbrella for its threat efficacy, user visibility, and its API-based integrations. “We realized the power of stopping threats at the DNS level – before they reach the network. This also reduces the amount of traffic being inspected by our other inline tools. However when we completed our solutions evaluations, Umbrella won by a large margin. The threat correlation wasn’t available in the other products,” says Phillippe.

“After a very easy trial set-up, we were able to get a quick visualization of potential high-risk destinations,” Phillippe says. “From just a demo, we could locate issues by user and device regardless of location on or away from the network so we could better understand our traffic.”

Memorial Hermann also uses Cisco Umbrella Investigate to enrich its incident response and SIEM data. “Using the Investigate tool, we take IOCs or certain attributes that are of interest to us and gain visibility into a complete view of the relationships between domains, IPs, and malware,” Phillippe says. “Investigate gives us that next level of attribution when we’re trying to piece together what’s happening. It gives us valuable context as to what it is we’re investigating.”

“Investigate gives us that next level of attribution when we’re trying to piece together what’s happening. It gives us valuable context as to what it is we’re investigating.”

Zach Phillippe
Cyber Security Manager
Memorial Hermann Health System
The results
Driving down security events

“Deployment of Umbrella was fast and simple,” says Phillippe. Once Umbrella was deployed to protect network users, Memorial Hermann was able to rapidly and easily provision roaming protection, and extend the same security policies to off-site users. As Phillippe puts it, “Umbrella took web traffic filtering from zero to hero in mere minutes, with very little overhead and a quick return on investment. In addition, we were able to reduce investigation time by 80% with Investigate.”

“We were able to drive down malware, attempted C2 callbacks, and other threats, which Umbrella’s reporting function allowed us to easily demonstrate,” says Phillippe. “And by integrating Umbrella into our existing security stack, those reductions produced cascading results for downstream tools.” Memorial Hermann leadership is pleased with the results. “We were able to show a reduction in security events percent to below .05%,” says Phillippe.

What’s more, Umbrella yielded a much broader view of network traffic. “Post-implementation, we gained new opportunities to control egress of traffic from our network, because all of these interconnected devices on our network ultimately use Umbrella’s DNS service.” he says. “In addition, we use the Cloud Services Report to identify the cloud apps in our environment.”

“Umbrella took web traffic filtering from zero to hero in mere minutes, with very little overhead and a quick return on investment. In addition, we were able to reduce investigation time by 80% with Investigate.”

Zach Phillippe  
Cyber Security Manager  
Memorial Hermann Health System