Cisco Umbrella

CASE STUDY

How a leading academic hospital ensures the health of patient and research data.

> *"Deploying Umbrella was fast and we experienced immediate time-to-value."*

Henry Duong
Infrastructure Security Manager
The University of Kansas Hospital

The University of Kansas Hospital

Organization snapshot

Company:
The University of Kansas Hospital

Headquarters:
Kansas City, KS

Number of users protected:
10,000+

Challenge:
Strengthen security infrastructure and visibility into threats to better protect patient data and intellectual property.

Solution:
Cisco Umbrella
Cisco Umbrella Investigate

Impact:

- Decreased threats by an estimated 99 percent
- Shortened investigation time by 75 percent
- Increased visibility and automation while reducing exposure to ransomware

ZONES

The challenge

Gaining transparency to secure sensitive data

Ranked among the nation's best hospitals every year since 2007 by U.S. News & World Report, The University of Kansas Hospital is the region's premier academic medical center. Physicians teach as faculty members at the KU School of Medicine, and are at the forefront of medical discoveries taking place at the KU Medical Center, a research leader in cancer treatment and prevention, neurology and liver and kidney transplantation.

"Like every hospital, we prioritize the protection of sensitive patient data against malware and other threats. We have to safeguard all network connected medical devices, as a compromise could literally result in a life-or-death situation," says hospital Infrastructure Security Manager Henry Duong. "Unlike non-academic hospitals, however, our entwinement with medical school and research facility networks means we must also protect a lot sensitive research data and intellectual property."

"Just as ransomware was beginning to impact hospitals around the world, we set out to improve our security posture as part of our commitment to delivering the best possible healthcare experience," he notes. "As we assessed the security environment, we quickly realized that visibility was a major challenge and that most of our attacks started with DNS. We needed protection for our recursive DNS look-ups."

> *"As we assessed the security environment, we quickly realized that visibility was a major challenge and that most of our attacks started with DNS. We needed protection for our recursive DNS lookups."*
>
> **Henry Duong**
> Infrastructure
> Security Manager,
> The University of
> Kansas Hospital

The solution

Security that starts at the DNS layer

Duong partnered with enterprise cybersecurity engineer, Edwin Hart, to propose a robust security program. "To start evolving the existing security design, we initially implemented an assortment of solutions that began to provide some very rudimentary information about infected machines, but lacked full visibility into the source of the infection," recalls Hart.

"For example, we could see malicious sites being contacted, but trace infections only far enough to learn they originated from either the proxy server, IP address, or our DNS server," Hart adds. "We would spend a lot of time combing through gigabytes of logs, but couldn't discern which machines were actually calling out."

"First we just pointed our external DNS requests to Cisco Umbrella's global network, which netted enough information to prompt an instant 'Wow, we have to have this!' response," Duong says. "When our Umbrella trial began, we saw an immediate return, which I was able to document using Umbrella reporting and share with executive stakeholders. Those numbers, which ultimately led to executive buy-in, spoke volumes about the instant effect Umbrella had on our network."

> *"When our Umbrella trial began, we saw an immediate return, which I was able to document using Umbrella reporting and share with executive stakeholders."*
>
> **Henry Duong**
> Infrastructure Security Manager,
> The University of Kansas Hospital

For more information, call your Zones account executive or 800.408.ZONES today.

ZONES

The results

Bolstered security and unprecedented insight

“Deploying Umbrella was fast and we experienced immediate time-to-value. Within an hour of Umbrella going live, we could see a huge increase in visibility, protection, and blocked malicious traffic,” according to Duong. “On any given day prior to implementation, we’d see some 100,000 hits against our network, some 20-to-30 percent of which were ransomware. As soon as Umbrella came online, that number dropped to nearly zero.”

“When we enabled AD integration by connecting our Active Directory to Umbrella–a simple process that took an hour–we suddenly went from struggling to track attacks to being able to correlate users with events and trace every click of their online travels. Then, Cisco Umbrella Investigate gave us the power to understand each threat’s entire story from start to finish,” Duong says. “We’re able to dig deep into the analysis to see what users are doing, where they’re going, and pinpoint any contributing behaviors so we can mitigate most efficiently.”

“Our incident response has improved dramatically, and the results,” Hart believes, “speak for themselves. Duong agrees: “Pre-deployment, a single incident would take approximately two days using our manual process. We’ve achieved a 75 percent reduction in response time, and in some cases, need just 30 minutes.”

The University of Kansas Hospital has been able to better combat and mitigate threats like ransomware. “We actually had a ransomware incident where a device did get infected, but it was easily contained by Umbrella. When the infected device tried to connect to the remote server, it was unable to get the encryption key. So the files were never encrypted.”

“Umbrella’s console streamlines the process of updating and enforcing security policies so we can deliver network-wide protection within seconds,” says Hart.

“We’ve been able to improve our security posture and better protect patient information and research data,” affirms Duong. “Given the ever-advancing security intelligence and Cisco’s dedication to staying ahead of bad actors, Umbrella will remain a cornerstone of our security program for the long term.”

“Our incident response has improved dramatically and the results, speak for themselves. Pre-deployment, a single incident would take approximately two days using our manual process. We’ve achieved a 75 percent reduction in response time, and in some cases need just 30 minutes.”

Henry Duong
Infrastructure Security Manager, The University of Kansas Hospital

For more information, call your Zones account executive or 800.408.ZONES today.

ZONES

Cisco Umbrella