Cisco Umbrella

CASE STUDY

How a global medical manufacturer routs out ransomware.

octapharma

Organization snapshot

Company:
Octapharma

Headquarters:
Lachen, Switzerland.

Number of users and locations protected:
Octapharma's deployment secures 5,000 employees across 31 countries and guest Wi-Fi offered to 15,000 daily donors across 60 U.S. donation centers.

Challenge:
Bolster security against ransomware and other threats with no impact to global network performance.

Solution:
Cisco Umbrella

Impact:

- Drastic decrease in exposure to ransomware
- Streamlined security management
- Improved internet performance

"We have covered a great risk in the web attack vector of ransomware, and greatly improved our user experience in regards to internet connectivity."

Jason Hancock
Global Senior Network Engineer
Octapharma

The challenge

Fighting infinite security challenges with finite resources

In the decades since its 1983 founding, Octapharma has steadily become one of the world's largest human protein manufacturers. With a corporate initiative designed to double production capacity and increase overall efficiencies by 2019 now underway, however, the company is experiencing unprecedented expansion.

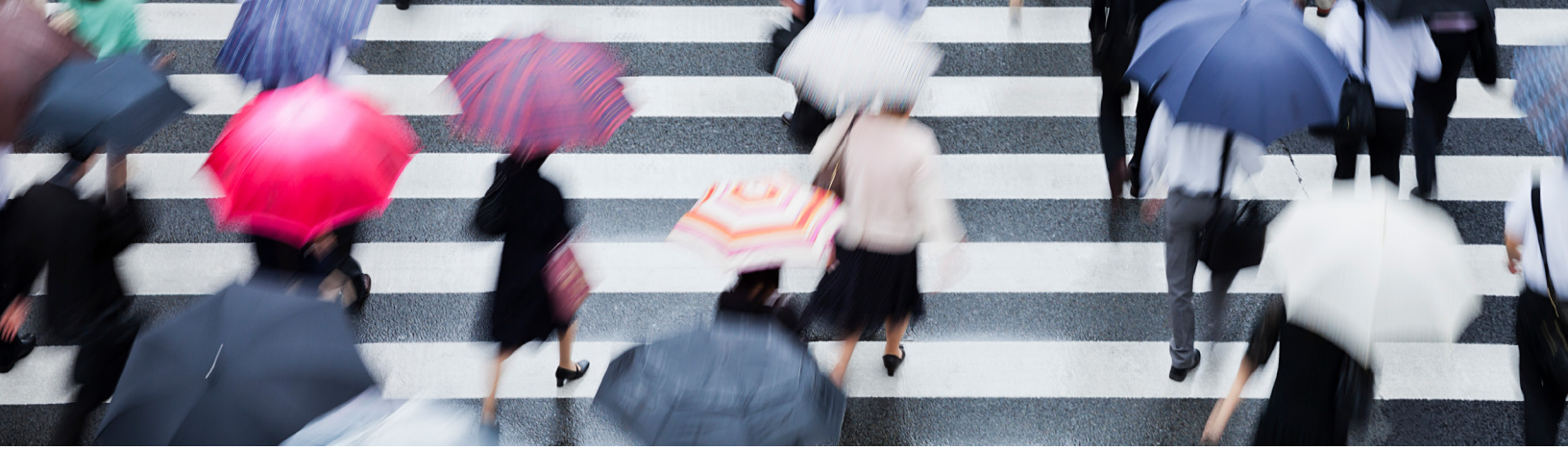
The impact of this growth spurt is evident throughout the organization – even at the network level. "As we add more employees in more locations using more mobile devices and cloud services, we also add new network security vulnerabilities," says Octapharma global senior network engineer, Jason Hancock. "We've seen a spike in a variety of malicious activities, including ransomware."

"Rather than trying to cover any exposures by hiring the kind of trained security practitioners already in short supply, identifying new solutions to address those vulnerabilities and aligning with organizational efficiency objectives has been a priority," he adds.

"In keeping with that focus," says Hancock, " first we needed to keep the network from going down every 15 minutes and improve efficiencies both for our team and users. When I joined the company in 2014, my initial objective was to get things stabilized so I could focus on preventing incrementally more aggressive malware, such as a CryptoLocker breach that we encountered."

"My initial objective was to get things stabilized so I could focus on preventing incrementally more aggressive malware, such as a CryptoLocker breach that we encountered."

Jason Hancock
Global Senior Network Engineer
Octapharma



The solution

Functionality that fits

"Before I came to Octapharma, the team had been working for some time to migrate from on-premises web security appliances to the same vendor's cloud service, selected by a predecessor. I was initially tasked with completing that deployment," recalls Hancock. "As soon as I saw what I was being asked to work with, I knew it wasn't going to meet our needs."

"We encountered significant issues that caused concern as to the product's viability in our environment, starting with internet functionality." Notes Hancock, "Our team received a lot of feedback from users who were dissatisfied with internet service, which was attributed to both the cloud service and the endpoint client on users' machines."

"Outside of that," he continues, "the feature set was inconsistent with our needs and there was widespread difficulty throughout the team around administration. This meant we had to provide a lot of training to support very detailed, non-intuitive management of policies and various components."

"After an issue-laden North American deployment, our network was down on a regular basis. The unreliability of having no internet for hours at a time reflected unfavorably on our team, and was not resolvable through the product's support channels," Hancock explains. "Finally, they suggested we abandon our migration to the cloud in favor of virtual appliances, which required redirection of traffic from more than 50 global locations, which was undesirable and in some cases not possible."

"That's when I raised my hand and said, 'the only way to solve this problem is Cisco Umbrella, and I can have it deployed and protecting our global network within six weeks.' After investing so much in a solution that didn't work for us, we were ready for a solution I knew from previous experience would succeed: Umbrella."

"After investing so much in a solution that didn't work for us, we were ready for a solution I knew from previous experience would succeed: Umbrella."

Jason Hancock
Global Senior Network Engineer
Octapharma

The results

Drastic reduction in ransomware

After an easy deployment, Octapharma saw immediate results. “Since we put Umbrella in place, we’ve had no web security compromises,” Hancock says.

“We have drastically reduced our exposure to ransomware, and since deploying Umbrella, we have not been a victim of ransomware as a result of clicking a malicious link. We actually see tens of thousands of blocks per week due to security policy; that doesn’t count blocks based on category policies,” he adds. “We have covered a great risk in the web attack vector of ransomware, and greatly improved our user experience in regards to internet connectivity.”

“We’ve even identified a few phishing emails and tested them by trying to click on their links; thanks to Umbrella, the sites were not accessible.”

Another unexpected benefit? Says Hancock, “By correlating the great data that comes out of the Umbrella dashboard with our internal systems, we’ve found infected machines that were previously undetected.”

With Octapharma’s security stack now able to block threats at the DNS layer, Hancock looks to keep reinforcing the network with proactive security management. “While Umbrella is very capable of blocking sites based on category policies, it’s most effective as a security tool and with that as a focus in our deployment, it’s a critical component of our defense-in-depth strategy. I’m currently investigating additional tools that are part of Cisco’s security portfolio to continue bolstering that strategy,” Hancock notes. “I am considering firewall enhancements, malware protection for endpoints, and greater coordination among the products in our security toolset.”

For Jason Hancock, seeing has always been believing. “I’ve been using Umbrella at home for years,” he says. “And now that I’ve seen it succeed in two different organizations as well, my colleagues tell me that they too just can’t say enough about Umbrella’s unique and highly effective approach to security.“

“We have drastically reduced our exposure to ransomware, and since deploying Umbrella, we have not been a victim of ransomware as a result of clicking a malicious link.”

Jason Hancock
Global Senior Network Engineer
Octapharma