CROWDSTRIKE

DRISCOLL HEALTH SYSTEM

CASE STUDY

A LARGE HEALTHCARE ORGANIZATION USES THE FALCON PLATFORM TO GAIN INSIGHT INTO ITS ENDPOINTS AND 24/7 COVERAGE

As healthcare becomes more entwined with technology, the attack surface has ballooned. The adoption of IOT and connected medical devices, along with the need to share data with many other healthcare and government entities, has not just expanded the perimeters of these organizations — it has eliminated perimeters altogether. At the same time, sophisticated threats like fileless malware are emerging and evolving more rapidly than in the past, straining security teams that may not have the skills to respond with the speed necessary to protect their organizations.

One large healthcare organization, Driscoll Health System, sought to reduce its organizational risk to an acceptable level at an acceptable cost. "The impact of an event shouldn't bring the business to a standstill or interfere with patient treatment," says George Irungu, CISO of Driscoll Health System. "We needed to get actionable insights from our data that enabled faster and accurate decision-making from our security team."

Driscoll Health System operates a hospital, health plan, and remote clinics. "There are so many threats coming our way being in such an attractive industry for bad actors. Our approach has been to be deliberate and thorough, and not to throw technological solutions for a quick fix. Technology solutions that we bring in have to complement the processes in place, and more importantly; an aid to our strongest line of defense – our workforce members," says Irungu. "Every solution we purchase has to reduce risk in a way that adds business value."

QUICK FACTS

COMPANY OVERVIEW

Driscoll Health System comprises Driscoll Children's Hospital, Driscoll Health Plan and more than 30 pediatric medical and surgical specialties throughout South Texas, including Corpus Christi, the Rio Grande Valley, Victoria and Laredo.

Employees: 2562
Health Plan members: 175,000
Endpoints: 4000+

A CLEAR SET OF DECISION POINTS GUIDED THE SEARCH FOR EFFECTIVE EDR

Priorities focused on extending resources for faster responses

When Irungu began the search for an endpoint detection and response (EDR) solution, he had two priorities: first, as much as possible, provide a holistic end-to-end view and protection of the organization. Second, the vendor needed to complement the existing Driscoll's security team, by freeing them from the mundane, day-to-day, low-level tasks, thus enabling them to concentrate on where they add more value — enabling the business "We were looking for a solution that would give us the biggest bang for our buck," says Irungu.

Irungu also wanted a real-time view of the files, drives, programs and executables that were on his network and on which devices. "Our leverage depends on knowing our environment better than any adversary. If we know our environment, we can act quickly to kick out bad actors," says Irungu, "To be honest, that was a challenge before we had CrowdStrike."

While the vendor selection process was in progress, fileless malware was on the rise. Fileless malware is difficult to identify and mitigate because it can look like any benign process in a system. That leaves security teams faced with difficult choices when deciding whether to whitelist or blacklist questionable processes. In the past, Driscoll Health System's security team responded to fileless malware attacks by physically collecting a computer, wiping it and reimaging the machine. "That took a lot of our time and spooked a lot of users," Irungu says. "We needed a solution that would be seamless and transparent to end users."

"CROWDSTRIKE'S SPEED AND THE ACCURACY BLEW US AWAY"

The bake off was over as soon as it began

Driscoll Health System began its selection process with a bake off between CrowdStrike® Falcon® and a competing EDR vendor. To ensure unbiased results, Driscoll created its own test environment, used its own malware samples, and procured fileless malware unknown to both solutions from a third-party provider.

The results rapidly became clear. "The difference between CrowdStrike and the other solution was night and day," says Irungu. "It was incredible how quickly we were able to identify the third-party fileless malware. I was alerted immediately when something was going on, and CrowdStrike actually isolated the machine. The speed and the accuracy blew us away."

"CISOs have to speak the language of business and articulate threats in context so executive management and the board can make good decisions. We are their risk advisors, but they are the bearers of risk."

"From the beginning, we've been able to understand which processes are legitimate and which are malicious."

"The icing on the cake is the 24/7 monitoring with professional threat hunters."

"The Falcon team is so skilled at threat hunting that we now know about incidents and events that would have been invisible to us before we had CrowdStrike. The difference is significant and above our expectations. CrowdStrike gives us a lot of value."

"Our goal is to follow CrowdStrike's recommendations of one minute to detect an adversary, ten minutes to perform a full investigation, and sixty minutes or less to eradicate the intruder. With CrowdStrike, we can do that."

George Irungu
CISO, Driscoll Health System

In fact, the gap between the two products was so dramatic that Irungu's team thought something had gone wrong with the tests. "We ran the tests again and saw the same thing. At that point, the bake off was over. CrowdStrike was clearly the best choice," he says.

Irungu also notes the intuitive and user-friendly portal, which he says has become "incredibly important" to Driscoll's security posture. "I can see the actual path a piece of malware has taken and identify the issue," says Irungu. "And the portal doesn't just show which devices have the Crowdstrike sensor, it also has information on discovered neighboring devices that don't have the sensor. We can identify unprotected devices and even discover devices that we may not have accounted for in the environment and take the appropriate action." This capability supports Irungu's strategy of knowing his organization's network better than any adversary in order to reduce dwell times. "We can see in real time how many servers and endpoints, Windows, Unix, and Mac machines, and other devices like printers are in the environment," says Irungu. "We weren't looking for these features when we did the bake off, but they've turned out to be extremely useful. We're really happy with the portal."

NO MORE NIGHTMARES

CrowdStrike threat hunters are always watching the environment

Driscoll Health System is a high-value target with a small security team, so the organization needs to optimize its resources. "I don't want my security professionals spending a whole day looking at logs or trying to identify whether an event is malicious or not," says Irungu. "CrowdStrike Falcon Complete™ combined with Falcon Overwatch™ frees up my people to do more strategic work."

Driscoll Health System also wanted a solution that could strengthen its security posture while easing the burden on its security team. "Before we had CrowdStrike's 24/7 coverage, I would get an alert if something happened at night and I had to respond," said Irungu. "But now I know someone is always proactively watching my environment in real time. We get a phone call or an email telling us the action CrowdStrike has already taken to mitigate the risk or making a recommendation on actions we can take ourselves."

THE STORY

CHALLENGE

Driscoll Health System needs to cover a wide perimeter and bolster its security team in order to increase response times without interrupting users.

TASK

The healthcare organization needs 24/7 visibility into devices and activity on the network.

WHY DRISCOLL HEALTH SYSTEM CHOSE CROWDSTRIKE

The healthcare organization chose CrowdStrike because Falcon Complete delivered the greatest speed and accuracy, while OverWatch threat hunters added a layer of expertise and coverage that only CrowdStrike could provide.

DEEP VISIBILITY, FAST ALERTING, AND A COMPREHENSIVE UNDERSTANDING OF THE ENVIRONMENT

Crowdstrike significantly reduces the organization's overall threat and risk profile

Deployment was so fast and seamless that the Driscoll Health System Security department is now considering using the process as the benchmark for how the organization deploys new technology. Policies were established and all 4000 endpoints across the organizations were up and running in less than two hours.

After six months of using Falcon Complete, Driscoll Health System's security team has saved at least five hours per week per person. But more important to the CISO is the greater threat identification capability and the freedom to work on high-profile activities that his team now has. "The saying 'You don't know what you don't know' has never been this relevant," says Irungu. "The Falcon team is so skilled at threat hunting that we now know about incidents and events that would have been invisible to us before we had CrowdStrike. The difference is significant and above our expectations. CrowdStrike gives us a lot of value."

According to the CISO, Driscoll Health System used to strive to reduce dwell time to less than 24 hours, which is less than the industry standard. Now, however, Irungu says, "Our goal is to follow CrowdStrike's recommendations of one minute to detect an adversary, ten minutes to perform a full investigation, and sixty minutes or less to eradicate the intruder. With CrowdStrike, we can do that."

ABOUT CROWDSTRIKE

CrowdStrike® Inc., a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

Visit
www.crowdstrike.com/seedemo
to request a demo.