HUNTRESS

Securing Smiles: A Timely Response to a Ransomware Crisis

How Cytek saved a dental surgery practice threatened by data extraction, thanks to the 24/7 vigilance of Huntress

It was 3:30am, Sunday, December 11, 2023, and the Cytek team received an alert that could have spelled disaster. Huntress' Security Operations Center (SOC) had detected ransomware on a client server. Jessica Payne, Cytek's cybersecurity operations manager, recalls the moment when the potential crisis unfolded.

"I woke up an hour later and just so happened to look at my phone. I saw Huntress' email and I couldn't believe it - this was significant. The worry set in."

However, that worry was short-lived. Huntress had already isolated the server, preventing the ransomware from spreading further. "It was stopped as quickly as it started," notes Payne. "Between the timespan of receiving the alert and isolating the server, we were only looking at two to three major machines affected. Those machines did not all have Huntress deployed."

With Huntress in their corner, Cytek swiftly took action.

"All in all, we were completely resolved by December 19," remembers Payne. "Thankfully, we had good backups, and that helped us get the client back up and running the following day—allowing our focus to shift to forensics on the impacted servers."

By deploying Huntress agents on all workstations, the Cytek team gained valuable insights into what processes were running.

"We started isolating every single computer in the office via the Huntress agent," Payne explains. "We went through each machine, one by one, and ultimately found out that there was a script running in the registry, which the Huntress SOC worked with us to remediate."

Cytek

Company Name
Cytek

Location
Tulsa, Oklahoma

Threats Encountered
Ransomware attack, data extraction

Cytek Prevents the Domino Effect

Cytek's focus is on dentistry clients, who are particularly vulnerable when it comes to cyberattacks due to the industry's stringent security regulations and vast amounts of patient data. This client was no different.

"My first concern is always the same when dealing with healthcare clients: How are we going to protect patient information? To what extent has it been impacted?" explains Payne. "These attacks are typically motivated by money. So, not only are you dealing with a potential ransom that you might be forced to pay to retrieve your files, but can you trust that the attacker will give them back to you, and delete them off the web?"

And the potential fallout from a ransomware attack in the healthcare industry is not just confined to money. The ripple effect extends to credibility, patient trust, and regulatory compliance.

"HIPAA's fines are based on the security efforts of the practice," mentions Theresa Wacker, Cytek's chief operating officer. "If it's clear that the practice has nothing in place to protect itself, then any fines will be calculated based on that negligence. And it's not unheard of for these to run up to seven figures."

"The ramifications of a breach are extremely serious, especially when it comes to HIPAA compliance," Payne adds. "In addition to all the fines and fees, there's also the hit to credibility. And if the data is sold on the dark web, you're looking at a breach."

Had it not been for Huntress' lightning-quick threat detection and the Cytek team's timely intervention, the consequences could have been much more severe.

While that reality thankfully remains a 'what if,' the client, who is part of a larger group owning about 90 oral surgery practices, faced a moment of truth in this case.

"After this attack threatened this one practice, with the group's agreement, we decided to roll out Huntress across every single workstation under its umbrella, which is thousands," states Wacker. "This was all a direct result of this incident. After all, Huntress saved us and saved the practice."

Under the Watchful Eye of Huntress

The swift detection of the threat, coupled with Huntress' ability to isolate the affected server and collaborate with Cytek's team, showcased the power of proactive cybersecurity. And for Payne, she shudders at the thought of what would have happened without that initial tip-off from Huntress.

> **"After this attack threatened this one practice, with the group's agreement, we decided to roll out Huntress across every single workstation under its umbrella, which is thousands. This was all a direct result of this incident. After all, Huntress saved us and saved the practice."**

"There's no telling how this incident would have panned out," she says. "I mean, the attack would have gone unnoticed. It was 3am! We could have easily gone from three to four workstations and a couple servers to the entire office encrypted before we discovered the ransomware. By then, it would have been too late."

Instead, the Cytek team was empowered to act swiftly and decisively to resolve the issue and do what they do best: protect their clients.

"I was so impressed by the responsiveness," remembers Payne. "The minute it happened, Huntress was on it, which allowed us to do our job that much faster. Knowing that you have that kind of expertise behind you 24/7, even when you're asleep, is invaluable."

While Cytek operates with a diverse security stack, Huntress comes out on top for Payne.

"We work with multiple partners and the innovation and quality are definitely top-notch in comparison, as well as the support," she says. "If you have a problem, Huntress is on it right away. That willingness to help and the sheer amount of knowledge makes our job so much easier."

In fact, as Wacker stresses, Huntress has become the gold standard at Cytek.

"At this point, having Huntress is absolutely non-negotiable," she says. "It's a requirement for any new clients coming on board; they must agree to deploying Huntress on all workstations. We used to only require the protection in place on servers, but that's not an option anymore."

Learning and Evolving

The ransomware attack served as a crucial learning experience for Cytek, shedding light on the evolving nature of ransomware and the need for constant vigilance.

"Every strain is a little bit different," says Payne. "And now with ransomware-as-a-service, it's starting to become more and more challenging to spot. That's why we, like Huntress, must continue to evolve and adapt to attackers' changing tactics."

And for Payne and her team, this incident underscores the importance of proactive measures when it comes to security.

"Really, it's about being proactive instead of reactive," she summarizes. "All it takes is one vulnerable moment for an attacker to strike. Sometimes, they can be lurking in the system for as much as a month before the attack. Huntress can spot the signs of this, meaning we can take care of it, potentially a month before an attack can take effect.

"Not only is it saving our clients, but it's saving our business too. Huntress is a lifeline."

> **"I was so impressed by the responsiveness. The minute it happened, Huntress was on it, which allowed us to do our job that much faster. Knowing that you have that kind of expertise behind you 24/7, even when you're asleep, is invaluable."**

About Cytek

Cytek is a leading provider of cybersecurity and HIPAA compliance for dental practices and other industries. The company offers best practices for prevention, network architecture, vulnerability, patch management, and assessment of both internal hosts and external services that criminals are using to gain a foothold. Its cybersecurity and HIPAA compliance solutions are perfect for small and medium size companies.

Cytek is revolutionizing cybersecurity with products and services that proactively prevent, rather than reactively detect the execution of advanced persistent threats, and malware. Its technology is deployed on over four million endpoints, and protects hundreds of enterprise clients worldwide including Fortune 100 organizations and government institutions.

About Huntress

Huntress is the leading cybersecurity partner for small- and mid-sized businesses (SMBs) and the managed service providers that support them. Combining the power of the Huntress Managed Security Platform with a fully staffed, 24/7 Security Operations Center (SOC), Huntress provides the technology, services, education, and expertise needed to help SMBs overcome their cybersecurity challenges and protect critical business assets. By delivering a suite of purpose-built solutions that meet budget, security, and peace-of-mind requirements, Huntress is how SMBs defend against cybersecurity attacks.

Founded in 2015 by a group of former National Security Administration (NSA) operators, Huntress has more than doubled over the past couple of years to support 4,300 partners and more than 105,000 organizations, now protecting more than two million endpoints. The company recently closed a $60M series C led by Sapphire Ventures. For more information about Huntress, visit huntress.com or follow Huntress on social media.

To learn more, visit huntress.com or follow Huntress (@HuntressLabs) on social media.

HUNTRESS.COM