Case Study

Leading MSSP Wactel Communications (WTS) Relies on Cynet for Proactive Protection

The Company Background

WTS is a leading MSSP in the southeastern US. When one of their large clients was hit by malware in mid-2020, the company spent weeks trying to remediate the threat, but the malware somehow persisted. They could not identify the source of malware on the network with the security tools they had in place. Ken Webber, Director of Data Services, quickly realized they needed a platform that could proactively and reliably detect all malware threats on their clients' endpoints before damage could be done.

The Challenge. Looking for a Proactive EDR/ Breach Protection Solution

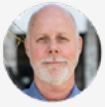
The WTS Data Services team had been using a mix of antivirus and endpoint detection and response (EDR) tools for years, but these tools were unable to alert them in real time to issues and failed to identify some malware attacks. They understood that better solutions were likely available but were unsure where to look.

"Then one of our big customers got hit with a ransomware attack. We spent several exhausting days going out to every one of their sites and putting on every piece of software we could to remove the threats. We isolated the infected machines and kept them off the networks until we thought they were clean," explained Webber. "Then a week later, we got indications that malware had hit their servers again."

The Data Services team knew they had to find a platform that would enable them to detect and respond to threats on their clients' networks in real time. They needed something that would be responsive, adaptive and proactive.

Security Goals:
Preventing threats such as ransomware from infiltrating their clients' networks

Key Benefits of Cynet:
- 7/24 responsive
- Adaptive
- Proactive security



Ken Webber,
Director, Data Services Team

"No other company we've worked with has quarterly meetings where they do a quick conference call to check if everything is going well and see if there is anything else they can do. We get a call from our account manager every quarter — What other company does that?"

Discovering Cynet

Webber had heard about Cynet from a colleague in his previous company. That's when he reached out to Cynet and explained what was going on. "Cynet didn't even blink-within an hour, we got a call saying, 'Hey it's all set up; here's the agent, push it out," he said.

With Cynet in place, WTS pinpointed exactly where the attack was coming from and what PC it was coming in on. They immediately set up the logic at the server level to block the traffic from the hosts that were permeating the threats. They then isolated the two infected PCs and cleared them completely, all without losing any data.

"With Cynet, it took us a few hours to totally clean up an issue that had taken us over a week to unsuccessfully remediate."

At that point, WTS signed a contract.

The Data Services team deployed Cynet 360 to all WTS clients. Now, when suspicious activity occurs, Cynet's 24x7 managed detection and response (MDR) team instantly notifies them. The Cynet platform already has the logic in place for what to do when things happen, such as isolate the PC. For WTS, this is one of the strengths of the platform: it's highly customizable and they can dictate what it should do.

"Cynet was great. They went above and beyond. They didn't have to do it--they could have said, 'Okay, you have to sign a contract before we help.' But they didn't. When they said 'Here, deploy it without any strings attached', that sealed the deal for us."

Benefit & Results

- The WTS Data Team can provide their customers with unparalleled protection from even the most advanced threats, thanks to Cynet's proactive and automated breach protection.
- Cynet enables The Data Team to respond to and mitigate threats with unmatched speed and accuracy for optimal results.
- The unique multi-tenancy allows WTS to manage all their customers from one Cynet instance
- The partnership is helping WTS establish itself as a regional leader in the MSSP space.

Cynet's Remediation Capabilities and Multitenant Architecture

The Data Services Team uses Cynet's automated remediation capabilities and can tailor it differently for each client. Webber says that Cynet isn't just a one-template-fits-all solution. Cynet's multitenant architecture gives them the ability to adjust and adapt for each situation and for each client.

"For a certain situation, we can shut down a server for one particular client and take a different course of action for another. The multitenancy, which is different from most others, allows us to manage all clients on a single Cynet instance, which is a huge advantage, without a doubt."

Expanding MSSP Expertise with Cynet

The team also sees Cynet as a strategic growth partner.

"We use Cynet as a marketing tool for every client we go out and pitch to; I tell them that one of the reasons they should go with us is that we use the most state of the art extended detection and response (XDR) software available. It will help us gain more clients in the long run and it definitely helps us keep clients, because our clients aren't seeing the devastating effects of ransomware that so many others in our area have."

Deploying Cynet to Clients

Webber reports that deploying the agent to clients is simple and straightforward. WTS hasn't had to create firewall rules at any clients and though they were worried about clients running PCI scans every 6 months, they haven't had any issues. The Cynet agent resource utilization is minimal and WTS clients haven't experienced any slowdowns.

Monitoring the SOC

The Data Services team monitors for alerts via a dashboard and the Cynet SOC sends them alerts via email as well. Webber explained, "When a serious threat comes in at 2:00am, the SOC notifies us that there's something happening. Before, we would have slept through something like that. So it's a mix of the two factors — our monitoring and the 24/7 SOC, which is very helpful. We'll get a threat notice and we'll send the signature to the SOC. They'll tell us if it's insignificant or if there's a potential issue. If it is significant, the SOC advises us to create a rule, so when something similar occurs in the future, we already have the steps in place to remediate the threat."

Cynet — going above and beyond

One more thing stands out:

"When COVID-19 hit, clients started thinking about enabling employees to work from home. Before we had a chance to address the need, Cynet reached out to us and said, 'We know this is going to be a problem, go deploy the tool out to these home sites, no extra costs.' Thanks to Cynet, we have been able to make sure that people accessing corporate networks via VPN from home are as protected as they'd be in-office, at no extra cost. Who else would have done that? No one else we know of."

Ken Webber,
Director, Data Services Team