MSP Helps Customer Recover from a Severe Ransomware Attack with MTR

Headquartered near Cleveland, Ohio, Ashton Technology Solutions has been a business technology consultant and managed service provider (MSP) for 25 years and a Sophos Partner since 2014. As a member of Encore Strategic Consulting's national peer group which shares data and best practices, Ashton holds itself to the highest levels of accountability and industry standards. Ashton focuses primarily on small and medium-size businesses with 20 to 200 users across multiple sectors: finance, legal, not-for profit, manufacturing, industrial, architecture, construction, and engineering, amongst others. The key differentiator for the MSP are their focus on next-generation security solutions for their clients as well as threat response and resolution.

PARTNER-AT-A-GLANCE

Ashton TECHNOLOGY SOLUTIONS

Ashton Technology Solutions, Inc.
Beachwood, Ohio

Industry
Tech

Sophos Certifications
Sophos MSP Connect Partner
Sophos Synchronized Security Partner
Sophos Firewall Partner
Sophos Endpoint and Server Partner
Four Sales Certifications
Three Engineer Certifications
Three Architect Certifications

Sophos Solutions
Sophos Firewall
Sophos Central
Sophos Intercept X
Sophos Intercept X for Server

'When it comes to cybersecurity, we know it's an ever-evolving landscape. With MTR and the front-line services and solutions built into the Sophos roadmap, we are confident that collectively we are headed in the right direction.'

Travis Grundke - Executive Vice President, Operations, Ashton Technology Solutions

Executive Summary

Beginning in 2014, Ashton has cultivated a trusted and highly collaborative relationship with Sophos. As a forward-thinking technology provider, Ashton has incorporated numerous cutting-edge Sophos products into its comprehensive, end-to-end portfolio, which includes everything from next-generation firewalls and artificial intelligence (AI)-based endpoint protection to cloud security and, most recently, Sophos Managed Threat Response (MTR).

The technical staff at Ashton makes a point of staying up to date on the latest Sophos offerings so they can ensure the right fit for their customers. The organization has a deep appreciation for the Sophos integrated approach to security—with products that communicate with one another and provide visibility across the entire infrastructure—and excellent communication with customers. These key ingredients make life easier for both Ashton and its clients. Ashton team members value their relationship with Sophos and know they can rely on the vendor to be honest, consistent, and accountable with them and their customers, especially when challenges arise.

The addition of MTR has brought added visibility to client networks as well as a human aspect to the technology already in place. True 24x7 eyes on networks recently enabled quick recovery from a global client's serious ransomware attack.

A Less than Ideal Situation Remedied by MTR

One of Ashton's customers, a large, fast-growing global manufacturer, was hit with a weekend ransomware attack when few people were monitoring the network. At the time, Sophos Central Intercept X Advanced had not been fully rolled out across the entire enterprise, due to the disparate nature of the customer's subsidiaries. Those devices running Intercept X were protected, but others remained open and at risk. With experience and an understanding of the value of MTR, the Ashton team immediately sprang to action, engaging the Sophos MTR team. This just-in-time, highly effective investigation and remediation effort saved the customer from having to pay a hefty $18 million ransom to decrypt the impacted machines.

'Within the cybersecurity space, you can't control the threats, but with Sophos we can control how we react, which influences the impact on our clients. At the end of the day, that's one of the most important things.'

Jim Abbott - Vice President, Client Solutions, Ashton Technology Solutions

The highly knowledgeable top-tier MTR engineers at Sophos supported Ashton's engineering team at every level. The Ashton technical team was especially impressed with how quickly the Sophos MTR team responded when the ransomware issue came to light.

Jim Abbott, Vice President, Client Solutions at Ashton, sums up how a strong vendor relationship and the right solution saved the day: "The communication between Sophos, Ashton, and our customers is always open and transparent. With this customer being hit with ransomware, our engineers acted quickly, and we knew that it was this immediate action that saved the customer's business. Within the cybersecurity space, you can't control the threats, but with Sophos we can control how we react, which influences the impact on our clients. At the end of the day, that's one of the most important things."

The Trajectory and Consequences of a Ransomware Attack

Anthony Colecchi, Senior Systems Engineer at Ashton, worked quickly to engage the Sophos MTR team. He and his colleagues had the highest confidence in the effectiveness of MTR, and that confidence was rewarded; Response time was swift, which is critical in these types of attacks that often occur at night or over the weekend.

The customer's VPN server was attacked, and, as a result, the threat was able to jump from the server to the administrator's machine, where bad actors gained access to a password list. Because the list did not contain a large set of data, this threat could easily have been missed, were it not for Sophos MTR.

Adam Burley, Ashton Systems Engineer, underscores how valuable MTR is in a mission-critical scenario like this one. "An attack like this is like something out of a zombie movie," he says. "There is so much potential damage that can happen to us and to a client. By engaging the Sophos MTR team, we ensured the threat actors didn't do any further damage to the client, and we were able to prevent the customer having to pay a ransom."

The Value of MTR for MSPs

As Abbott states, the Sophos-certified Ashton sales team doesn't just sell Sophos products, they sell the complete Ashton managed services solution. That just happens to include Sophos as the end-to-end security component.

Ashton Technician David Stiles points out that working with the Sophos MTR team felt like working with a company primarily focused on support. "The MTR team was not just forthright in their communication but clear in the information they communicated," says Stiles. "The MTR team could speak at the technical level but also used every-day language to make the situation clear to our client." Armed with these insights and backed by the MTR team, Ashton was empowered to show the customer the path to resolution and recovery, which increased the customer's level of trust and confidence in Ashton.

Travis Grundke, Executive Vice President, Operations understands the true value of the premium service offered by Sophos. He observes that MTR helps identify and remediate the malicious activity that occurs on the network that enables data exfiltration—and these tactics are so stealthily deployed that most end users are completely unaware such activity is going on behind the scenes. He acknowledges that the Sophos MTR team immediately stepped in to help and analyze the data that was accessed by the ransomware actors. Fortunately for the manufacturing customer, the level of data exfiltration was minimal. Nonetheless, for an MSP, Grundke remarks that it's important to look at the downstream ramifications and liability of potential data exfiltration at a larger scale: "Sophos helps us protect our reputation and our customers."

A Look to the Future of Cybersecurity

After success in this particular scenario, Ashton knows they can continue to rely on Sophos without question. Ashton saw how the MTR team was always laser-focused on resolving the customer's issues. In addition, they were impressed with the regularity, frequency, and clarity of the communication. As Stiles notes, it felt as if they were working with an extension of the Ashton team and not a large, amorphous company.

"When it comes to cybersecurity, we know it's an ever-evolving landscape," asserts Grundke. "With MTR and the front-line services and solutions built into the Sophos roadmap, we are confident that we are headed in the right direction."

In Jim Abbott's words, "Sophos just works." This could never be truer - since standardizing to Sophos solutions, Ashton has not seen a single successful ransomware attack among their clients.

SOPHOS

'There is so much potential damage that can happen to us and to a client. By engaging the Sophos MTR team, we ensured the threat actors didn't do any further damage to the client, and we were able to prevent having the customer pay a ransom.'

Adam Burley - Systems Engineer, Ashton Technology Solutions

For more information on the Sophos MSP Connect Program, please visit sophos.com/msp

22-02-22 PCS (PS)