Technology Innovator Improves Cyber Defenses with 24/7 Security Cover

Aligned Automation offers solutions and services that fuel digital transformation, which helps clients tap into the benefits of technological innovation for better business outcomes. The company acts as a key enabler of business strategy driving seamless connectivity between processes, people and technologies. The company's focus is on driving exponential growth and it was aware that achieving scalability without a robust cybersecurity framework could create security issues that impede growth. It wanted to move from a legacy approach to endpoint security to a more proactive security framework, which led them to adopting Sophos Managed Threat Response.

CUSTOMER-AT-A-GLANCE

ALIGNED AUTOMATION

Aligned Automation

Industry
Technology

Website
www.alignedautomation.com

Sophos Solutions
Central Intercept X Advanced with XDR and MTR Advanced
Central Intercept X Advanced with XDR and MTR Advanced for Server
Central Device Encryption
Phish Threat
Professional Services for Endpoint

> *"Our existing security solution was offering us limited protection against the latest threats and ransomware. It was an on-prem endpoint solution, that was proving difficult to update and not scalable to keep in step with our growth. We therefore wanted to move to an advanced endpoint solution and managed security services to build a dynamic SOC delivering comprehensive cybersecurity."*
>
> Shrirang Salway, Director - Data Shared Services, Aligned Automation

Challenges

- Inability to adopt 'hot pursuit' to identify and mitigate threats.
- Failure to detect threats that are hidden on the network and waiting for the right time to wreak havoc.
- Building a security operations center from the ground up to manage the security environment better.
- Ramping up security operations without aggressively hiring a security team

Why move to a security approach that combines human-led investigation, threat hunting, real-time monitoring, and incident response?

With exponential growth comes a greatly increased attack surface. Mr. Salway, Director - Data Shared Services, Aligned Automation was acutely aware of the sophisticated threat environment the company had to address in line with its growth. Aligned Automation's existing endpoint security solution was not delivering value on multiple counts creating a need to upgrade to more advanced security that offered layered protection, was easy to manage and offered comprehensive protection against known and unknown threats.

While the IT team wanted to monitor the security environment 24/7, it was unable to find the time to do so. A core challenge being creating a security operations team without aggressive hiring.

"I wanted to enhance our security operations with support from extremely well-qualified security professionals, well-versed in maximizing the value of EDR tools," says Mr Salway.

Another key requirement was to move away from a defensive approach to cybersecurity to a more proactive approach, which Mr. Salway felt was counterproductive. He wanted the ability to hunt for threats and neutralize them before they became a problem, rather than sit back and wait for an attack to occur and then react.

> *"With Sophos MTR, we now have improved confidence in the reliability, robustness and comprehensive nature of our security setup. We recommend this managed services solution to all organizations who want to transition to a proactive security approach to combat advanced threats, both known and unknown."*

Shrirang Salway, Director - Data Shared Services, Aligned Automation

What are the threat hunting requirements that address the advanced threats faced by the organization?

"There is always a danger of threats lurking undetected on the network. The time between threats entering the network and being identified is critical to ensuring these don't cause havoc across the network, and it is this time we wanted to curtail with threat hunting," explains Mr. Salway.

Why did you choose Sophos MTR?

"While conducting a thorough research of available MDR options, we realized that many vendors offer automated threat hunting to identify potentially malicious activity that merits further investigation, by human analysts, and it ends there, but Sophos MTR goes a step further to offer lead-driven and lead-less threat hunting," says Mr. Salway highlighting one of the key differentiators of Sophos MTR.

With lead-driven threat hunting, Sophos MTR uses a manual process of identifying and investigating events and activities that are not flagged by alerts but can indicate new attack behavior. Sophos leverages lead-less threat hunting that combines threat intelligence, data science, and deep-seated knowledge of attacker behavior, underpinned by a sound understanding of the Aligned Automation environment. This helps anticipate attacker behavior and authenticate detection and response capabilities.

Sophos MTR also offers a security health check to ensure all Sophos installations at Aligned Automation operate at peak performance. Summaries of case activities improve prioritization and communication to ensure Mr Salway and his team are up to speed with all threat detections subsequent actions. Other Sophos Central products help extend telemetry to offer visibility into the full spectrum of malicious activities and the IT team can directly call Sophos SOC, thus benefiting from around-the-clock support.

What are the key business outcomes delivered by Sophos MTR?

From a security perspective, Sophos MTR has delivered immense value. The team has identified more suspicious activities, potentially unwanted application and malware, which has helped kept threats at bay. The improved visibility into security incidents and adversarial activities stops threats at the gates. This enhances peace of mind and allows the IT team to focus on other business-centric activities knowing the Sophos MTR team is taking the necessary actions on their behalf.

For more information
visit sophos.com/mtr

2022-04-19 CS-EN (PC)

SOPHOS