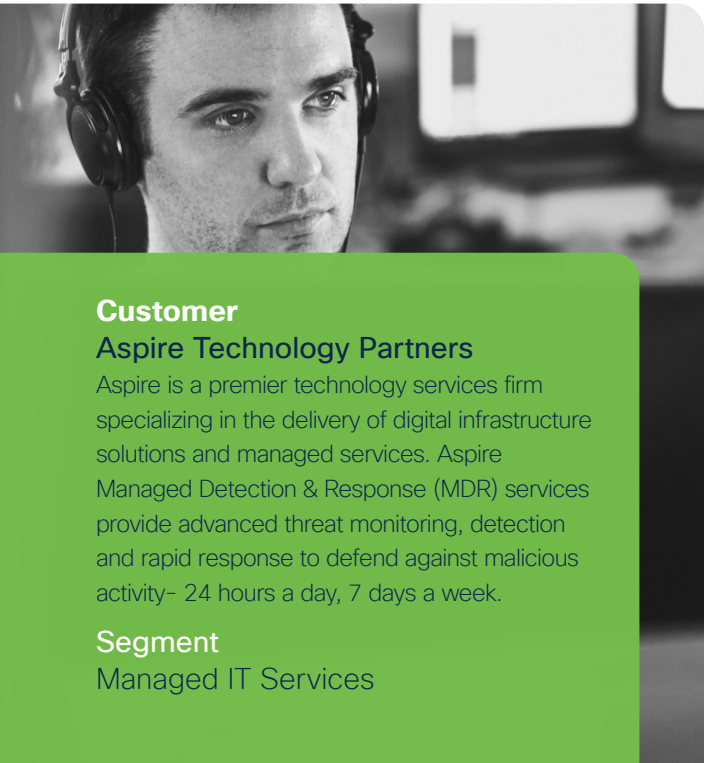
CISCO
SECURE

Case Study
Public

Stealthwatch Cloud, an invaluable tool for Managed Security Service Providers, tracks malware through east-west traffic



Customer

Aspire Technology Partners

Aspire is a premier technology services firm specializing in the delivery of digital infrastructure solutions and managed services. Aspire Managed Detection & Response (MDR) services provide advanced threat monitoring, detection and rapid response to defend against malicious activity- 24 hours a day, 7 days a week.

Segment

Managed IT Services

About Network Detection and Response

Network Detection and Response (NDR), formerly known as Network Traffic Analysis (NTA), is a new market category as defined by Gartner in the 2020 NDR Market Guide. NDR tools must be able to analyze raw packet traffic, such as NetFlow, in near real time. They must also analyze and model behavior over time in both north-south and east-west traffic and must provide automatic or manual response capabilities to users, enabling quick action based on detections.

Cisco Stealthwatch Cloud meets all of these requirements and more.

The solution offers both SaaS-delivered private network monitoring and public cloud monitoring. It will protect your hybrid and multi-cloud environments and can even detect suspicious activity in encrypted traffic without decryption, which no other NDR tool can do.

Stealthwatch Cloud comes pre-built with Cisco SecureX, the broadest and most integrated security platform that unifies visibility, simplifies threat response and enables automation for Cisco security solutions.

Why Stealthwatch Cloud?

Aspire provides managed security services to a wide variety of customers. For one of its customers, Aspire recommended installing Stealthwatch Cloud but the customer wasn't ready to purchase it at the time.

Sometime later, Aspire discovered unusual PowerShell activity on various endpoints within the same customer's network and advised them to intervene and respond. Malicious PowerShell scripts are often a critical component of many forms of fileless malware and are a strong indicator of a ransomware attack. However, it was too late: the malware was popping up on endpoint after endpoint, and although endpoint security solutions can remediate threats on specific devices on which they are installed, they are unable to track malware through east-west traffic once the network is compromised. Think of this as a game of whack-a-mole. Aspire was stomping on each endpoint as it became infected but did not have the right tool to track the malware and stop it for good. It soon became clear that the customer's entire network was in danger.

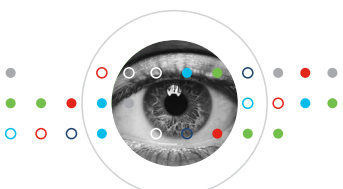
Aspire contacted its customer and advised on the need for comprehensive Incident Response (IR) and suggested Stealthwatch Cloud once more. While the 3rd party IR team continued its reactive approach to getting rid of this malware, the Aspire SOC was able to quickly deploy Stealthwatch Cloud and respond appropriately.

> "The speed at which our team was able to launch a trial and deploy Stealthwatch Cloud was a huge factor in quickly identifying and containing this threat. Because the threat was able to be isolated so quickly after the deployment, the team was able to prevent an actual data breach."
>
> John Rossiter,
> Security Principal Consultant and CISO

There are a few different reasons why this solution was absolutely critical to not only figuring out where this malware had spread, but also stopping it dead in its tracks.

1. Stealthwatch Cloud showcases immediate value

The Aspire SOC team deployed Stealthwatch Cloud on the customer's network and within just 2 hours the solution was live. Instead of waiting for endpoints to show signs of infection, the MSSP was instantly able to start looking through east-west traffic flows and hunt down the threat. The solution provides immediate visibility into network traffic without the need for any agents or sensors, and only gets better over time. This solution offers intuitive views of session traffic, amount of encrypted traffic in transit, top hosts and devices and much more immediately upon deployment. The Aspire SOC was able to immediately dive in to network traffic and realize that the malware's foothold was through a 3rd party Network Attached Storage (NAS) appliance.



2. Stealthwatch Cloud detects threats behaviorally

Even with top notch endpoint and firewall solutions, your network may still be at risk. Some threats get in disguised as benign network traffic. Some threats are allowed in through phishing attacks and user-initiated activity. Stealthwatch Cloud uses the network itself as a sensor to identify anomalies that may be indicative of threats. In this case, the security team was able to trace the malware's movement back to its origin and identify the foothold of the attacker. NAS appliances come pre-packaged and cannot be protected by endpoint agents. This specific appliance happened to have a critical vulnerability that opened the door for malware to slip in unnoticed. Stealthwatch Cloud analyzes network behavior and through an integration with Cisco Talos, the largest nongovernmental threat intelligence organization in the world, can alert on interactions with known malware, malicious IPs, domains and more.

The SOC team was able to look through all of the network behavior to track the malware through internal traffic. Without Stealthwatch Cloud in place, the SOC team would not have been able to identify the vulnerable 3rd party device, the real patient zero.

"The deployment of Stealthwatch Cloud in this instance showcases the need for a multilayered security approach and the value of security context. Stealthwatch Cloud is a core element of our Managed Detection & Response (MDR) service, enabling our SOC analysts to reduce the mean time to identify and remediate security threats on behalf of our managed services clients."

Doug Stevens
VP, Managed Services

Be sure to check out Cisco SecureX, the broadest and most integrated security platform, to learn how to simplify your Cisco Security experience, unify visibility between Cisco products and maximize efficiency within your security portfolio.

3. **Built-in remediation methods and integration with SecureX enable quick response to threats**

Not only did Stealthwatch Cloud allow the SOC team to see what was happening and trace it back to the source, but it also gave the team various ways to alert users and deal with the malware and NAS device appropriately. After discovering where the attack originated, Aspire created a simple firewall rule for its customer that blocked communication with that device, permanently blocking the malware. It was as simple as that. Stealthwatch Cloud is connected to numerous collaboration tools, email services and 3rd party applications that allow users to deal with threats appropriately. And now, through the SecureX platform, customers can easily pivot into other Cisco solutions like Talos, Umbrella and more. Alerts and the associated IPs from Stealthwatch Cloud can easily be sent into your other Cisco solutions, allowing for simple remediation when incidents do occur.

Conclusion

Security tools that protect the perimeter, endpoints and other on-prem devices are a critical part of your security portfolio, but without an NDR solution like Stealthwatch Cloud in place, your network is still at risk. Aspire was able to deploy this solution almost instantly and gain an incredible amount of visibility and a quick fix for this dangerous malware. Stealthwatch Cloud was critical in understanding how and where the attack was happening. This tool is an ideal complement for your existing security tools because with this in place, anything that gets by your traditional perimeter or endpoint agent-based solutions can be spotted before any real damage occurs.

To learn more about Stealthwatch Cloud please visit our webpage and get started with a 60-day free trial today.