Miraj Group Gets Proactive Against New and Emerging Threats with Sophos MTR

The Miraj Group's business footprint cuts across many sectors including printing and packaging, foods, pipes and fittings, real estate, film productions, engineering, hospitality, entertainment, retail, and the digital sphere. The company and its IT team has always put a premium on cybersecurity, using Sophos solutions for comprehensive security cover. But, its dramatic growth, an evolving attack surface and a need for a more proactive approach drove its need for another layer of security to further safeguard its business, so it turned to Sophos Managed Threat Response (MTR).

CUSTOMER-AT-A-GLANCE

MIRAJ GROUP
SINCE 1987
आपका विश्वास ही हमारी पहचान

Miraj Group

Industry
Multi-Sectors

Website
www.mirajgroup.in

Sophos Solutions
Sophos Intercept X with MTR
Sophos XG/XGS Firewall
APX Services Access Points

"We wanted to adopt a big picture approach to cybersecurity, backed by security operations that responded immediately to security incidents. While we were confident our existing security solutions were delivering a comprehensive security framework, we also wanted to adopt a human-led approach wherein skilled professionals hunt for threats and remediate them before they cause any problem."

Devendra Singh Panwar, IT Head

Challenges

- Inability to monitor security environment 24x7
- Lack of skilled cybersecurity personnel
- Inability to augment SOC capabilities
- Wanted a team of skilled security professionals without aggressively hiring
- Response times not quick enough to protect mission critical servers
- Inability to enhance uptime and overall resiliency towards services

What issues prompted you to adopt Sophos MTR?

The Miraj team led by Mr Panwar has always been up to speed with its security deployments and is fully aware of the sophisticated threats its network and endpoints are subject to. The team's security belief is driven by a need to stay one step ahead of any prospective attacker, that seeks to exploit any weakness in Miraj's cybersecurity posture.

"We had experienced a few ransomware incidents and felt we needed to transition to a more attacking security posture, wherein we did not wait for an attack to take place, but hunted for threats, neutralizing them," explains Mr Panwar.

The existing team is extremely talented but lacked certain security operations skills and also didn't have the time to constantly monitor the Miraj security environment. The team was stretched to its limits and the addition of key mission critical servers meant it needed to strengthen Miraj's security framework to anticipate threats and respond to them immediately.

What were the security requirements that led to a MTR solution?

Mr Panwar knew Miraj already had a robust security posture but felt skilled security professionals, who could leverage the full potential of capabilities of existing security deployments, would further

"We recommend Sophos MTR to all organizations, who want improve their security operations and move to a more dynamic security approach underpinned by continuous and advanced threat hunting."

Devendra Singh Panwar, IT Head

bolster this posture. He also wanted a constant eye on the company's security ecosystem for swifter implementation of security controls and policies across the network.

Cybercriminals only need to get their attack kill chain right once, but organizations need to get it right every time. Therefore, Miraj wanted its security environment monitored 24/7 by a team of professional security experts. Also, it recognized the need to focus on both lead-driven and lead-less threat hunting allowing them to cover the spectrum of threat hunting. Mr Panwar and his team also wanted threat hunting to offer better visibility into indicators of compromise and be better aligned with the MITRE ATT&CK® framework.

Why did you choose Sophos MTR?

"We conducted a thorough market research of vendors and felt Sophos MTR came with key differentiators. While some vendors delivered limited response capabilities, Sophos MTR delivered full-response capabilities taking proactive action on our behalf with a human-led response," says Mr Panwar.

Sophos MTR delivers 24/7 lead-driven threat hunting, wherein threat hunters aggregate and investigate security events to identify new and previously unseen vectors of attack. MTR also goes a step further to deliver leadless threat hunting, backed by the intuition of experienced threat hunters, comprehensive threat intelligence and application of data science to anticipate attacker behavior.

Miraj also experiences the benefit of enhanced telemetry that extends beyond the endpoint to deliver a holistic view of adversary activities. Security health checks that drive optimum performance of all Sophos products, easy to understand activity reporting and other advanced features, give Mr Panwar the confidence that Miraj's security is in safe hands.

How did Sophos MTR's security ROI drive improved business results?

Miraj immediately benefitted from the number of man hours saved from introducing Sophos MTR. It saved 15 man-hours per week and saw 2.6 times uptick in productivity and improvement in IT and services performance. Its network performance also improved by 38%, which enhanced business continuity and overall organizational productivity.

Today, the team benefits from more focussed visibility into security events and alerts as Sophos MTR cuts out the clutter. This has also resulted in peace of mind, and a justifiable confidence that it doesn't have to worry about threats falling through security gaps. These have been identified and plugged by security experts, who leave no stone unturned to identify threats and mitigate them before they become a problem.

www.sophos.com

SOPHOS

2022-04-06 CCS-NA (NP)