

Use Case of Cyber Security

EPP & EDR for threat hunting



Jaikumar Srinivasan, the CISO of Capital Bank, was concerned about the security of their systems. He strongly believed in prevention being better than cure, especially with the increasing reports of cyber attacks and hacking. To address his concerns he reached out to CMS IT Services.

CMS IT understood his challenge and proposed EPP (Endpoint Protection Platform) and EDR (Endpoint Detection and Response) solution. They explained to Jaikumar how this solution could effectively hunt for threats that might go unnoticed by traditional security measures.

The solution gathers various types of data about endpoints such as process activity, file changes, and network traffic which are then analyzed to identify any suspicious activity that could indicate a potential threat. If necessary, the solution can quarantine the suspect file or data, and closely monitor its activities. In extreme cases, it can permanently delete and block the file.

Jaikumar was highly satisfied with the CMS IT team and their solution to his security concerns.

This is a real life use case. Names have been protected.

Reach out for Endpoint Protection

