I.T Solutions India Pvt Ltd

D-88/5 Okhla Indl Area Phase-1 New Delhi 110020
Tel: +91-11-47695000 Fax: +91-11-26818504

A Total Solutions Company

Endpoints Security/Application and Device Blocking Solution

Customer Vertical

Government Organization

Project

Symantec Endpoint Protection

Summary of Client infrastructure

Customer is having approximately 50,000 client computers and spread over PAN India. Customer is having centralized data center at Delhi and managing all locations from this central location. Existing anti-virus solution was not providing centralized management and compliance. Users connect their MTP device with their computer and copy confidential data to Mobile or USB stick. With present anti-virus he was only able to achieve protection from virus. That was not able to provide complete end-point security (i.e. Application & Device control, Firewall, HIPS, NAC to check host integrity etc.).

Customer Challenges

- Complex Endpoint Security Environment.
- Central Console for managing all clients.
- Any kind of report for all clients should be generated from single console.
- Protect data and Endpoint from growing threats.
- Scrutinizing the malicious activity where SEP does not have built in definitions and to get the same generated from product support center.
- Reduce costs associated with managing multiple Endpoint Security Solutions.
- Chasing the antivirus/non-antivirus client machine from the malicious list generated by one of the Intrusion Detection System.
- Collecting custom registry entry/software information by applying SNAC policies
- The user should be able to install the product himself.
- No body make changes in windows registry and host file.
- Device blocking to protect their data from out of corporate network.
- Application awareness policy to open application in only application owner not open by another third party application.
- Password reset tool should always blocked.
- Advanced machine learning to understand machine language to check file is bad for good and also check the executable file behavior.

Product

Symantec Endpoint Protection

Solution

We incorporate the customer challenges to come out with a solutions and implemented the same on more than 10,000 computers all over India. We implemented the solution using Symantec Endpoint Protection (SEP) that met their security strategy. Find the below mentioned configuration and policies implemented at the customer end:

- Installation of Symantec Endpoint Protection Manager in Head office.
- Installation of one more SEPM server and configured it as replication server.
- Created an Intranet Portal so that user could come and download the required packages, check the faq's and contact the helpdesk
- The policies for Antivirus, Live update, application and device control were implemented at the server.
- For installation of SEP clients, first we needed to remove the existing Trend Micro client.
- In order to reduce the internet traffic between the users and the servers at remote locations, we needed to create GUP (Group Update Provider) servers on the remote locations. GUP server will take updates from the master SEPM server and then it will provide the updates to its clients associated.
- We were facing challenges in deploying client packages at dispersed locations. To overcome this issue we created a website and uploaded all flavor of packages to let the client download it and install.
- We created state wise packages so that we could get granularity of reporting and enables users of a particular state to fall under a specific group.
- Our team keeps on changing packages as and when new updates or upgrades happen.
- A helpdesk was created to help the users who were installing the anti-virus package by themselves
- Roaming user profiles for laptop users were created so that they could get live updates when they were at different locations.
- Weekly reports were configured to give an idea of how many users were updated and how many were facing challenges.

Benefits

- Single platform to manage Endpoint Protection and Endpoint Compliance. Also all locations endpoints can now be managed using this single console
- You can access Symantec Endpoint Protection remotely in a web-based console.
- Customer is able to get the attractive state wise reporting on threats and endpoint compliance.
- Centrally distributing AV definition, policies and packages.
- More efficient management of endpoints against known and unknown threats. Multi-tiered protection against threats.
- Customer has got NAC to fetch any kind of application information from endpoint using registry settings, running processes and services.