Infrassist
Managing I.T.

Case Study

Implementing Synchronized Security to secure IT Network during Work-from-Home

The Customer:
Aktiv Software

Industry:
Information Technology

Location:
Ahmedabad, India

India based Aktiv Software is a Software Consulting company that provides Business process automation by making the use of custom ERP tailored to organizations need.

Aktiv Software makes use of Odoo as an open-source ERP and create a custom module/package looking at customer's specific need.

Overview

Aktiv Software was facing challenges in having transparent visibility on activities occurring in their IT network. With the new work-from-home model, complaints of malware increased, unproductive browsing started happening, and several malwares were found on endpoints

Challenges

Technical Challenges

Because of adapting the work-from-home model, there was a lack of transparency on activities occurring in their IT network.

With the new model, unproductive browsing started taking place, and several malwares were found on the endpoints.

With no central control ready, the current endpoint protection was stand-alone and unmanaged. There was a heavy bandwidth utilization and users complained of less speed.

The primary resolution the challenges required:

- Failover links - so the connection between branches is stable in case of ISP issues
- An up-to-date endpoint agent on all devices
- The scanners, printers, phones, etc., and external users such as contractors or guests to be whitelisted or bypassed from the Heartbeat rule

Solution

Solution

Our team provided a complete solution that involved the security of a UTM/Firewall along with AV protection. These communicate and work with each other to protect against any unforeseen attacks. E.g. If a user's machine is infected, it could spread to all the network drives that the machine is connected to. Before that happens, it is necessary to curtail it to minimize data loss in the event of an attack.

Infrassist helped enable Sophos Endpoint Agent to communicate with the XG firewall. If it detects that the device has been compromised, it will immediately signal the firewall and block all internal and external communications to minimize the spread.

- We used Sophos central to manage Client and Server Endpoints. and XG Firewalls from a single place for all the customers. Malware and Virus threats, Firewall configuration and firmware upgrades, as well as license management for customers can be done centrally.

Solution

Below are the key steps followed:

- Setup Sophos XG Firewall on all branches with the Firewall rules and Web and application policies as per requirement

- Setup VPN Tunnels between the head office and branches for inter-branch connectivity

- Setup SSL VPN or Sophos Connect for remote or for work-from-home users

- Install Endpoint Agents on all devices

- Enable Sophos Synchronization on XG and ensure that the Control Center displays the device status and Security Heartbeat

- Configure minimum Heartbeat and block devices with no Heartbeat on the firewall rules

- Heartbeat can also be enabled for connections coming in via VPN

- Use RED devices to connect the branches

- Endpoint policy blocks USB and applications

- QoS on Firewall that separates noise from business traffic with priority

- Reports bookmarked and sent on schedule to user email

- Use synchronized authentication for transparent login

- This will isolate the infected device and disconnect it from internet and internal network if the Endpoint detects an attack until its resolved

- The firewalls can also be managed from Sophos Central to push policies and updates from a single location instead of accessing each individual firewall to make the same changes

- Affected machines and threats can be viewed for all customers from the Central Dashboard, and we can also access one of the customers' dashboards to investigate in detail

- Sophos Central also sends alerts if any VPN tunnel or gateway on a managed firewall is down

Result Technologies

Technologies used

Sophos Synchronized Security

Accomplishment

- Enabled an endpoint management solution based on Client – Server architecture
- We also were able to enable Malware reporting and isolate infected endpoints
- Seamless VPN operations were enabled
- Enabled transparent User authentication without installation of any clients on endpoints/AD
- Interconnect branch traffic – backhaul through head office with complete visibility
- Blocked USBs and applications that can download malware on endpoints
- We blocked unproductive browsing for users on network as well

About Infrassist

Empowering MSPs by leveraging technology and human talent to help them transform and scale their business. We act as a catalyst and provide next-generation services and processes with reliable, cost-effective, agile and scalable IT solutions. Assisting MSPs with solutions that are designed to meet the demands of today's always-connected, digital world.

India
B1 - 9th Floor, Westgate
Business Bay, SG Highway,
Makarba, Ahmedabad, Gujarat,
India- 380051

Australia
St. Kilda Road towers, Level 1,
1 Queens Road,
Melbourne,
VIC 3000, Australia

UK
Norton Park Ascot,
Berkshire
SL5 9BW London,
UK

✉ **partners@infrassist.com**

50+ Technology Experts

75+ MSPs Served

2015 Year of Establishment

30000+ nodes

24x7x365 operations

27001:2013 Certified

3 Offices India | Australia | UK