Infrassist
Managing I.T.

Case Study

SB Partners Kaseya

The Customer:
Zen Tech

Industry:
cloud solutions

Location:
Brussels, Belgium

Zen Tech pride themselves with having expertise on cloud solutions and 24/7 support, flexibility to adapt to the customers need and Proximity to customers being based in Brussels, Belgium.

Zen Tech provides complete IT Infrastructure solutions to the clients so that they can have efficient computer system to perform their job. Zen Tech core areas of focus are: Managed services, ServiceDesk, SaaS solutions and Project Management.

Overview

Zen Tech wanted to get an RMM Audit done of the Kaseya RMM Tool they were using to serve their clients.

(*As we are white-labelled service providers, we cannot disclose the actual names or locations of our customers. Hence all customer names that we use in our case studies are hypothetical- unless they give us the permission to use their names)

Challenges

Solution

Technical Challenges

Zen Tech team was looking for Kaseya RMM Configuration and Audit to scan various monitor settings, Patch profiles (OS, AV & Third-Party Software's), rules etc. configured for workstations, servers & network devices of their customers and recommend best practices around same to make best out of Kaseya platform by leveraging all key capabilities of Kaseya VSA RMM Tool & supported integrations.

Observations from the report:

Post audit, we divided the report into 4 modules and these were our observations:

The observation from Antivirus Module:

- 60-70% of devices (including workstations & servers both) had Kaspersky Antivirus Product installed. While majority had Windows Defender along with a mix of antivirus solutions from different vendors (McAfee, ESET & Trend Micro)
- There were separate Kaspersky AV profiles created for many customers.

The observation from Software Management Module:

Currently neither OS nor any 3rd party software updates are managed by Kaseya VSA

The observation made for Monitoring Module were as follows:

- There are many discovered devices prompted as assets but not having any Kaseya Agent installed; they mainly comprise of Linux Servers & Mac systems. Also, there are few managed assets (with Agent Installed) that are running an older version of agent.
- Out of the total discovered devices within Zen Tech's Kaseya VSA Portal only few of the customers have probe software installed in their respective Active Directory Servers
- From Monitoring perspective, mainly following Agent based Monitoring is configured at present for couple of managed assets-
  - Agent alerts
  - Event Log Alerts
  - Monitor Sets
- SNMP based Monitoring is not configured for any of the Network devices whether it be Printers, Scanners, Switches, Routers or Firewalls
- There is resource utilization monitoring configured under Network Monitor Module (CPU, Memory, Bandwidth, Process etc.) for few of workstations, servers along with External Probing for Public DNS Server to monitor Internet Connectivity from hosts.

Solution

Module-wise Suggestions:

Post the module-wise categorizations, the team gave the following module-wise suggestions to Zen Tech

For Antivirus Module:

- After the effective use of all supported integrations (ESET, Trend Micro, Bit Defender etc.) we will be able to monitor & manage the anti-virus across all devices. Currently Zen Tech had it limited to Kaspersky AV.
- Common AV Profile creation & assignment to most of the customers rather than how it's configured currently.

For Software Management Module:

- Optimal use of all available features within software management module to get all your customer's devices updated on a regular basis. This will help make them compliant & avoid any sort of security issues.
- Assign settings to machines using different profiles for scanning, deployment, alerts, 3rd party software & patch overrides.
- Scanning & Analyzing profiles to support two different strategies for managing software updates, out of which we recommend Kaseya Update one where in we can specify whether to approve, reject or review patches based on pre-assigned impact classification & it applies to Windows, Apple & 3rd Party Software patches.

Deployment profiles specify how deployments occur, on a recurring schedule. This includes:

- Reboot preferences
- The optional running of agent procedures both before and after deployment
- Optional blackout windows, to prevent scheduling deployments during business hours. Includes patch approvals, which lets you approve or reject specific patches.

For Monitoring Module:

- Installing agents on all assets & setup automated agent upgrade for all assets as Kaseya VSA provides agents for all operating systems including Linux & Mac.
- Setup SNMP based monitoring for all discovered assets (including printers, switches, rout ers, firewalls etc.) by either utilizing standard device-based SNMP Monitoring sets available within the Kaseya VSA platform or through a custom vendor-supplied MIB database file. It also includes setting up SNMP traps alerts configuration for all discovered assets.
- Optimum use of agent-based monitoring for all managed assets by leveraging all available built-in alert types, event log & monitor sets for workstations, servers to monitor overall Health (CPU, Health status, RAM, Network bandwidth), various server roles & services including Microsoft Exchange, SQL Database, IIS server along with ticket creation for Critical & Error Event logs under workstations and servers.

Technologies

Result

Technologies used

Accomplishment

- Creation of Single Dashboard page within RMM to get clear insights into overall health of their customer's ICT Infrastructure at a glance.
- Providing user friendly report on a scheduled basis to customer as a validation.
- To do a detailed audit of the various modules of the Kaseya VSA and to suggest the best solution based on industry standards and our experience while working with MSPs.

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