India's leading Oil and Gas Company gets an enhanced level of server posture with Trend Micro Deep Security solution.

Client Background

A leading Indian state-controlled oil & gas company produces a diverse range of products, from petrochemicals and solvents to aircraft fuel & specialty lubricants & markets them through its wide network of Petrol Stations, Kerosene Dealers, LPG Distributors, Lube Shoppes, besides supplying fuel directly to hundreds of industries, and several international and domestic airlines.

The Challenges

The customer is a renowed name and a giant in the Oil and Gas industry with headquarters in Mumbai. The company has a comprehensive server Infrastructure covering all aspects of a three-tier architecture including web services, Application services and Databases. These services run across multiple Operating Systems such as Windows, Red Hat Linux, HPUX, Suse, AIX and Sun Solaris. These Servers are placed in the De-militarized Zone (DMZ) and hence they are protected by Network firewalls.

With emerging threats and release of malwares on day-to-day basis, deployment of network based security controls such as Firewalls, Network IDS/IPS etc. alone are not sufficient to provide the adequate security for the servers. There is dire need to deploy Server Security solution that provides an intelligent shield against malwares and cyber-attacks.

The key challenges and the security risks for the server Infrastructure at the customer's datacenters were:

No Antivirus protection on non-Windows Servers: Currently, endpoint antivirus solution, deployed in Windows Servers does not offer comprehensive protection for servers. However, Non-Windows Servers at the customer datacentre contains business critical data related to SAP, Oracle, SAP-portal and many other critical services. These do not have any server security solution for that necessary protection against the modern day threats. This is likely to impose a great security hazard in case the servers are compromised with a virus or malware resulting in sensitive data leakage, unplanned downtime, business interruptions, and user's dissatisfaction leading to huge financial and reputational loss for the customer.

No Host Intrusion Prevention (HIPS) on Servers: None of the servers are protected by any Host based Intrusion detection and prevention solution (HIPS). This again makes the critical servers vulnerable to various kinds of cyber-attacks and threats such as Buffer overflows, SQL Injection and many other vulnerability Exploits. This may enable an attacker to penetrate through the critical application servers and databases. An attacker may steal business critical information, execute remote commands and can do lots of malicious activities which may severely impact the data confidentiality, Integrity and availability. This may lead to user's dissatisfaction, financial and reputational loss for the said customer.

The Right Solution

The security specialist team at Wysetek interacted with the IT team at the customer to understand the challenges they had with its very diverse data center environment. The datacentre had physical production servers as well as virtualized production servers. Wysetetk team took into consideration the fact that there were multiple OS on servers like multiple versions of Microsoft's windows, various flavors of Linux and HP UAX as well.

The detailed analysis of the business needs, technology overhaul and security posture lead to the conclusion that the customer needed a unique security solution that provides protection against malwares / viruses and their sources using in built web reputation and also they need a protection solution against intrusion prevention on the host databases.

Trend Micro Deep Security that protects enterprise applications and data from breaches and business disruptions, including newer attacks using ransom-ware, without requiring emergency patching was a solution that the customer found to be perfect for their security issues. deployed. The server-Agent (client) based solution of Trend Micro Deep Security requires no down time of servers for agent installation. Features like anti-malware, web reputation and Intrusion prevention can be turned on/off the management console is a unique feature in the market.

"Trend Micro Deep Security is a comprehensive, centrally managed platform that helps organizations simplify security operations while enabling regulatory compliance and accelerating the ROI of virtualization and cloud projects," says Rajesh Mathkar, Director, Wysetek Systems Technologists.

The Benefits

Wysetek leverages 25 years of expertise in technology solutions and best of business practices in the technology industry. Being Trend Micro certified Professional Service Partner, Wysetek deployed Trend Micro Deep Security solution at the customer's datacenters which lead to multiple benefits.

The entire data center with numerous servers and humungous databases at the customer site was secured within a span of two and half months span without any down time. The solution also helped increase patch management time line and it added a security layer against all the vulnerabilities from the day one of deployment of Trend Micro Deep Security.

Replacing desktop anti-virus solution with a more sophisticated solution from Trend Micro simplified the security management for the customer and it provided an enhanced level of security with an equal data center server security footprint.

Key security challenges of diverse datacentre environment

🔒 **No Antivirus protection on non-Windows Servers:** A security hazard in case the servers are compromised with a virus or malware resulting in **sensitive data leakage, unplanned downtime, business interruptions,** and **user's dissatisfaction** leading to huge financial and reputational loss for the customer. The entire datacentre was secured without any downtime.

🔒 **No Host Intrusion Prevention (HIPS) on Servers:** Makes critical servers vulnerable to cyber-attacks such as **Buffer overflows, SQL Injection** & other vulnerability exploits for attacker to steal business critical information, execute remote commands that may severely impact **data confidentiality, Integrity and availability.**

"Trend Micro Deep Security is a comprehensive, centrally managed platform that helps organizations simplify security operations while enabling regulatory compliance and accelerating the ROI of virtualization and cloud projects."

Rajesh Mathkar, Director, Wysetek Systems