Wysetek modernizes server security for a leading co-operative bank

WYSETEK

The bank's old and outdated servers and software applications were secured by Trend Micro Deep Security solution implemented by Wysetek.

Established in 1906, it is one of the oldest Urban Co-operative Bank in India set up with the primary objective of assisting the less fortunate members of the community in its economic enterprises. The co-operative bank was formed to encourage savings and to create funds for providing financial aid to deserving members.

The banking industry at large has been the prime target for hackers globally and in India. The advent of digital banking and mobile Apps makes it more imperative for banking CIOs and IT teams to secure

Pain Points

Securing the server is the major pain point for the banking industry as the hackers search Internet of things (IoT) connections for vulnerabilities time and again. As the number of attacks increases and the types of attacks become more sophisticated, the banking authorities are pressurized to implement more advanced server and cyber security protection to mitigate the risks of losing sensitive and confidential information.

The bank (Wysetek's customer)currently had critical applications installed on Physical, virtual servers, running Windows, Rhel and AIX operating systems etc. for supporting its core business functions. Most of the servers and software applications were old and outdated in their IT infrastructure. The bank was also facing many difficulties and frequent challenges for applying security patches for management, accessibility etc.

Expect Analysis

The main goal to upgrade server security was to achieve protection to the Physical, Virtual Servers by applying advance security features to the legacy software application, which would ease the manageability and also increase the server productivity.

After complete study survey conducted by high profile technical team of Wysetek Systems Technologists, the outcome was to deploy the security which could protect physical , virtual and cloud Servers with advanced features such as (vulnerabilities, Malwares, firewall etc.). There was a need for a comprehensive, centrally managed platform that can help simplify security operations (DC, DR) while enabling regulatory compliance and accelerating the ROI of virtualization and cloud projects.

To achieve the needed server security, TrendMicro Deep Security with Business continuity was proposed by Wysetek to the bank. Deep Security provides advanced server security for physical, virtual, and cloud servers. It protects enterprise applications and data from breaches and business disruptions without requiring emergency patching.

Resolution by Wysetek

The comprehensive, centrally managed platform helps simplify security operations while enabling regulatory compliance and accelerating the ROIof virtualization and cloud projects. The tightly integrated modules of Deep Security (Anti-Malware with Web Reputation and Intrusion Prevention) easily expand the platform to ensure server, application, and data security across physical, virtual, and cloud servers, as well as virtual desktops.

Anti-Malware with Web Reputation module of Deep Security delivers an anti-malware agent to extend protection to physical, virtual, and cloud servers, including AWS, Microsoft, and VMware environments. It also integrates with the Trend Micro Smart Protection Network global threat intelligence forweb reputation capabilities that strengthen protection for servers and virtual desktops.

Deep Security's module of Intrusion Prevention examines all incoming and outgoing traffic for protocol deviations, policy violations, orcontent that signals an attack. It automatically protects against known but unpatched vulnerabilities by virtually patching(shielding) them from an unlimited number of exploits, pushing protection to thousands ofservers in minutes without a system reboot. It includes out-of-the-box vulnerability protection for all major operating systems and over 100 applications, including database, web, email, and FTP servers. And it provides increased visibility and control over applications accessing the network.

Key Benefits of Veritas NetBackup and Appliance5240 (53TB) to Customer

- The bank received numerous benefits from the solutionTrendMicro Deep Security with Business continuity which was much needed for better security posture.
- The solution helped in easy manageability as the Agent based setup provides better security with enhanced anti- malware, features like memory scanning, registry scanning.
- All modules of the solution can be deployed on just one agent via the centralized management console.The modules can be turned on or off on the agents via the management console remotely.
- Importantly, the agent deployment on servers is a onetime activity and later all other activities like agent upgrade, agent activation/deactivation can all be managed from Deep Security Manager without the need to access the remote servers.
- The India's oldest urban co-op bank has a better server security due to the implementation of Trend Micro Deep Security by Wysetek team.

Prime Challenges with Server Securityat the bank

- As number of attacks increases and the types of attacks become sophisticated, there is need to implement advanced server and cyber security protection to mitigate the risks of losing sensitive and confidential information.
- The bank had critical applications installed on Physical, virtual servers, running Windows, RHEL and AIX operating systems etc. for supporting its core business functions.
- Most of the servers and software applications were old and outdated in their IT infrastructure.
- Facing many difficulties and frequent challenges for applying security patches for management, accessibility etc.

Key benefits of trend micro deep security for co-op bank

- Agent based setup provides better security as it has enhanced anti- malware, features like memory scanning, registry scanning.
- All modules can be deployed on one agent via centralized management console and the modules can be turned on/off on the agents via the management console remotely.
- The Agent deployment on servers is a onetime activity.
- All other activities like agent upgrade, agent activation and deactivation can be managed from Deep Security Manager without the need to access the remote servers.