Key Benefits

As part of the Business Process Desktop solution, Deep Security protects business-critical applications and data from breaches and business disruptions without expensive emergency patching, delivering:

- **Higher Density** by offloading security scans from individual virtual machines to a single security virtual appliance on each vSphere host
- **Optimized Resources** by eliminating antivirus storms and resource contention from multiple security agents
- **Simplified Management** by eliminating agents and the need to configure and update each one
- **Safety and Compliance** for business-critical applications by virtual patching, integrity monitoring, and application protection
- **Stronger Security** by providing instant-on protection for new virtual machines and tamperproof security coordinated by the dedicated security appliance, clear mapping to PCI DSS 2.0

Securing the Remote or Outsourced Workforce

Many companies are taking advantage of business process outsourcing (BPO) as a way to improve customer satisfaction and reducing operating costs. Providers of these services are seeking solutions that can scale easily, increase revenues, provide cost savings and ensure data and application security and compliance.

VMware® has worked with Trend Micro to develop a solution to address the challenges of the remote or outsourced workforce—the VMware View® Business Process Desktop™. With the Business Process Desktop, VMware and Trend Micro are enabling customers looking to outsource or offshore business processes to scale their business by deploying and managing agent desktops centrally and securely, and provide end users with a standardized and secure desktop experience across the LAN and WAN.

As the security component of the VMware View Business Process Desktop solution, VMware View™ and VMware vSphere™ products, together with Trend Micro Deep Security, allow IT to offload AV to secure virtual machines. This provides high levels of isolation between resource pools and networks, allowing IT to apply policies across virtual machines and pools of users.

Challenges of a BPO Environment

Let us examine the challenges of a classic BPO environment such as an offshore call center. Call center IT organizations are being asked to reduce cost per agent, deploy a quickly scalable infrastructure, secure client data, and meet increasing compliance requirements.

**Key Business Issues**

**Scalability** - Call centers need to be able to scale quickly and efficiently to meet the demands of their clients. Scaling up to hundreds or thousands of virtual machines is inefficient when deploying agents to each. Administrators need to provision security agents in new virtual machines, continually reconfigure these agents as the virtual machines move around or change state, and roll out pattern updates on a regular basis. This can be extremely time consuming and still result in security gaps.

**Compliance** - Financial transactions or sensitive data that is virtualized and taken across borders will trigger complex issues such as PCI. With the ease of provisioning and mobility of virtual desktops, it can be difficult to maintain an auditable record of the security state. Yet, many regulations require proof of current antimalware protection.

**Software Patching** - Regular software patches allow a system to meet new needs, respond to new developments, or address emergent weaknesses. A system left unsupported by regular patching, will quickly find itself impacted by emergent threats, particularly in the form of zero-day viruses and malware. The use of Manual Patching of virtualized business-critical applications or instant on-gap issues caused by dormant virtual machines creates greater management burden and increased security risk.
Securing the Business Process Desktop

As part of the Business Process Desktop solution, Deep Security addresses these issues with a comprehensive, optimized, and efficient security solution that protects business-critical applications and data from breaches and business disruptions without expensive emergency patching.

Within a Business Process Desktop Environment, Deep Security components are located on Virtual Desktop ESX hosts as the Deep Security Virtual Appliance and on the Management Cluster as the Deep Security Manager. The Deep Security Virtual Appliances provide the agentless security services to the hypervisor while the Deep Security Manager manages these Deep Security Virtual Appliances and stores all configuration settings and events.

**Deep Security Virtual Appliance** - Transparently enforces security policies on VMware vSphere virtual machines for agentless anti-malware, IDS/IPS, integrity monitoring, web application protection, application control, and firewall protection, coordinating with Deep Security Agent, if desired, for log inspection and defense in depth.

**Deep Security Manager** - Powerful, centralized management enables administrators to create security profiles and apply them to servers, monitor alerts and preventive actions taken in response to threats, distribute security updates to servers, and generate reports. Event tagging functionality streamlines the management of high-volume events.
Solution Elements

Trend Micro Deep Security with VMware View and VMware vSphere maximize virtual desktop protection and performance. Key solution elements include:

VMware View
The cornerstone of the View Business Process Desktop solution, VMware View modernizes desktops and applications by moving them to the cloud and delivering them as a managed service. With View, IT has the ability to grant or deny access to desktops, data and applications according to endpoint device configuration, network location and user identity.

VMware vSphere
VMware enables optimized antivirus and anti-malware security for virtual environments via integration with VMware partners. vSphere Endpoint™ provides the intermediary for anti-malware and deep packet inspection. This allows security technology partners to offer more efficient antivirus and anti-malware protection for virtual hosts, including VMware View desktops. It does so by offloading antivirus and anti-malware functions from individual virtual machines to a centralized secure virtual appliance that protects the host and all virtual machines on it. This approach streamlines security management and provides added protection against antivirus “storms,” performance bottlenecks, and botnet attacks.

Trend Micro Deep Security
Trend Micro Deep Security provides a comprehensive server security platform integrated with the Business Process Desktop solution. Trend Micro was the first security vendor to integrate with VMware vSphere APIs to provide you with better protection, less administrative complexity, and increased performance through cutting-edge agentless technology.

Deep Security provides a wide range of security options for VMware virtual machines:

• **Anti-Malware** - Integrates new VMware vSphere Endpoint APIs to provide agentless anti-malware protection for VMware virtual machines with zero in-guest footprint.

• **Intrusion Detection and Prevention** - Shields known vulnerabilities from unlimited exploits until they can be patched. Helps achieve timely protection against known and zero-day attacks. Uses vulnerability rules to shield a known vulnerability.

• **Integrity Monitoring** - Detects malicious and unexpected changes. Event tagging and cloud-based whitelisting reduce the complexity of administrative operations.

• **Application Control** - Increases visibility into, or control over, applications accessing the network. Identifies malicious software accessing the network and reduces the vulnerability exposure of your servers.

• **Firewall** - Centralizes management of server firewall policy using a bi-directional stateful firewall. Supports virtual machine zoning and prevents Denial of Service attacks.

• **Log Inspection** - Collects and analyzes operating and application logs for suspicious behavior, security events, and administrative events across the datacenter.

• **Web Application Protection** - Enables compliance with PCI Requirements for the protection of web applications and the data that they process. Defends against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities.

Summary

The Business Process Desktop is a managed solution that integrates technology from VMware and Trend Micro to ensure a secure and seamless experience for virtual desktops, allowing IT to provide the new remote or outsourced workforce access to their desktops, applications, and data in a secure, compliant, and efficient manner.

Learn More about the Business Process Desktop