



# Trellix MOVE AntiVirus Performance Advantages

# Trellix MOVE AntiVirus Performance Advantages

Trellix Management for Optimized Virtual Environments AntiVirus (Trellix MOVE AntiVirus) for virtual desktops and servers is uniquely designed to relieve the overhead of traditional antivirus and provide even better protection. Our performance tests show that by optimizing and offloading virus scanning, Trellix MOVE AntiVirus enables you to minimize the performance impact on virtual servers and reduce security resources. Here are some of the advantages that Trellix MOVE AntiVirus offers over traditional endpoint security.



Benefits	Traditional Antivirus	Trellix MOVE Antivirus
Smaller foot print in each virtual machine (VM)	✗	✓
Higher VM consolidation ratios	✗	✓
No virus definition (DAT) updates in every VM	✗	✓
Antivirus scan storms eliminated	✗	✓
Scan avoidance leveraging a clean file cache	✗	✓
Reduced power consumption	✗	✓
Optimized scheduling for on-demand scans	✗	✓

## Test Setup

All performance tests use this setup

Host	Dell R620 Server, Intel Xeon CPU E5- 26900 @ 2.899 GHz (total 16 core) and 192 GB RAM
Virtual Machine	Microsoft Windows 7 x64, 1vCPU, 2 GB
vSphere ESXi	ESXi 6.0
Virtualization Software	XenDesktop 7.6
Network	Broadcom gigabit switches
Storage	Dell EqualLogic 70-0400 iSCSI SAN
Scan Configuration	Default Product settings
Microsoft Office	Office 2010

## Performance Test Results

### DAT storm test

All test clients for traditional antivirus receive DAT updates in parallel, creating a heavy load on the underlying hypervisor. Trellix MOVE AntiVirus performs updates on the offload scan server so that they do not negatively impact virtual machines (VMs), resulting in significant advantages over traditional antivirus.

- 87% less CPU usage
- 93% less network usage
- 92% less disk usage

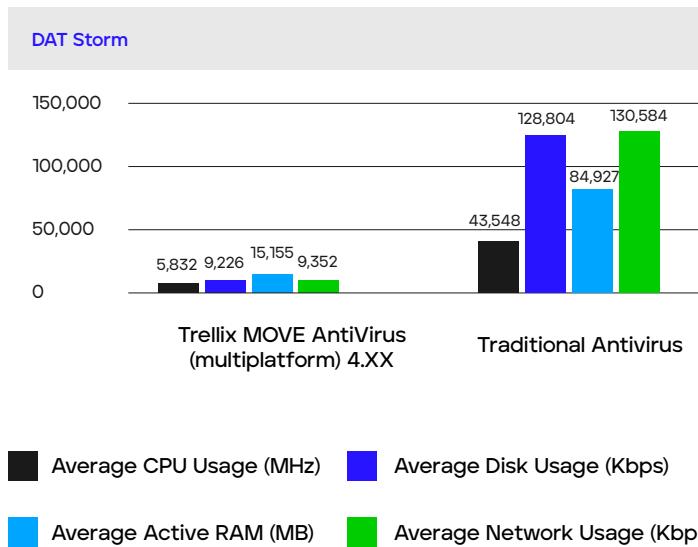


Figure 1.

Trellix MOVE AntiVirus performance during a DAT storm. All parameters were recorded at the host level. Trellix MOVE AntiVirus used one offload scanner with 150 clients.

### On-demand scan (ODS) storm with cache test

Due to numerous concurrent scans, host resources with clients running traditional antivirus are severely impacted during an ODS storm. Clients with Trellix MOVE AntiVirus perform much better because caching avoids repeatedly scanning the same files across clients. This produced these improvements over traditional antivirus during an ODS storm.

- 70% less CPU usage
- 75% less network usage
- 75% less disk usage

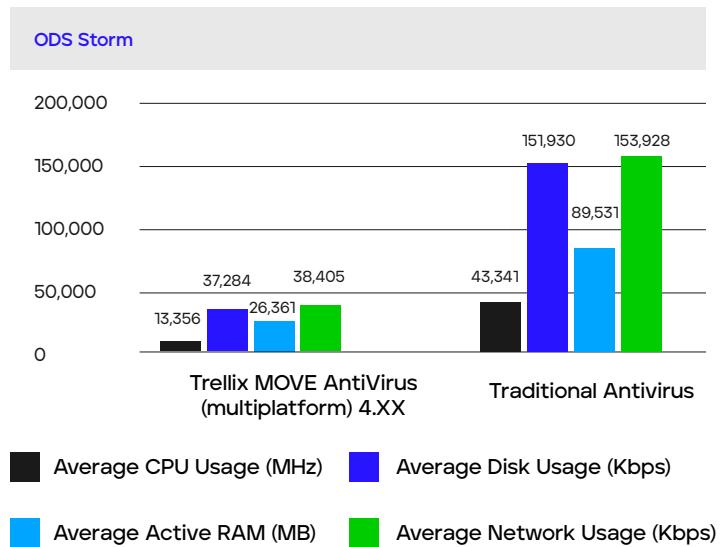


Figure 2.

The graphic depicts resource utilization at the host level when simultaneously running ODS on 150 VMs. All clients have a repopulated cache.





## Enablement of Trellix Threat Intelligence Exchange Test

Trellix Threat Intelligence Exchange is available for multiplatform deployment of Trellix MOVE AntiVirus. When a Trellix Threat Intelligence Exchange server is configured with Trellix MOVE AntiVirus, fewer files are transferred to the offload scanner, resulting in significant scan avoidance.

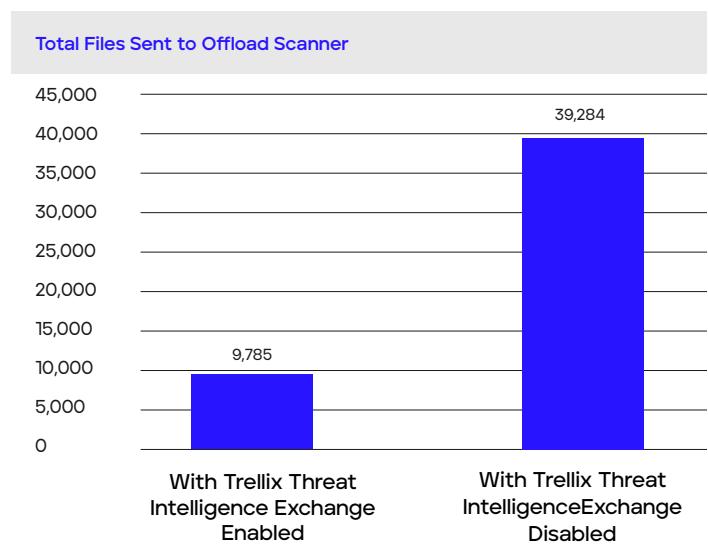


Figure 3.

This test, which runs an ODS on 70 VMs with Trellix Threat Intelligence Exchange enabled and a pre-populated cache on the offload scan server, shows a 75% reduction in file transfer between client and offload scan server.

## Summary

Trellix MOVE AntiVirus improves the security of workloads deployed on virtual infrastructure without impacting performance and resource utilization.

Visit [Trellix.com](https://Trellix.com) to learn more.

**Trellix**

### About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.