テスト
レポート

Tolly.

#212117
2012 年 5 月
シマンテックからの委託

Symantec Endpoint Protection 12 対 Trend Micro Deep Security 8

VMware vSphere 5 仮想環境におけるマルウェア対策のパフォーマンス

概要

IT エンジニアは、仮想デスクトップインフラ（VDI）ソリューションの配備を拡張する際、「常時接続」のリソース要件やエンドポイントセキュリティシステムなどの使用頻度の高いコンポーネントを意識する必要があります。仮想環境では、ベンダーはすべてのセキュリティ処理がクライアントで行われるクライアントベースのエージェント、ウイルス対策（A/V）の作業負荷を処理する仮想アプライアンス、またはこの 2 つのアプローチの何らかのハイブリッドとして、ソリューションを実装できます。

シマンテックは、VMware vSphere 5 仮想環境内の新しい Symantec Endpoint Protection（SEP）12 と Trend Micro Deep Security（DS）8 のパフォーマンスのベンチマークテストを Tolly 社に委託しました。具体的には、オンデマンドおよびオンアクセススキャンの実行時と、分散されたウイルス定義の更新時の各ソリューションのシステムリソース要件を中心としてテストを実施しました。（次ページに続く）

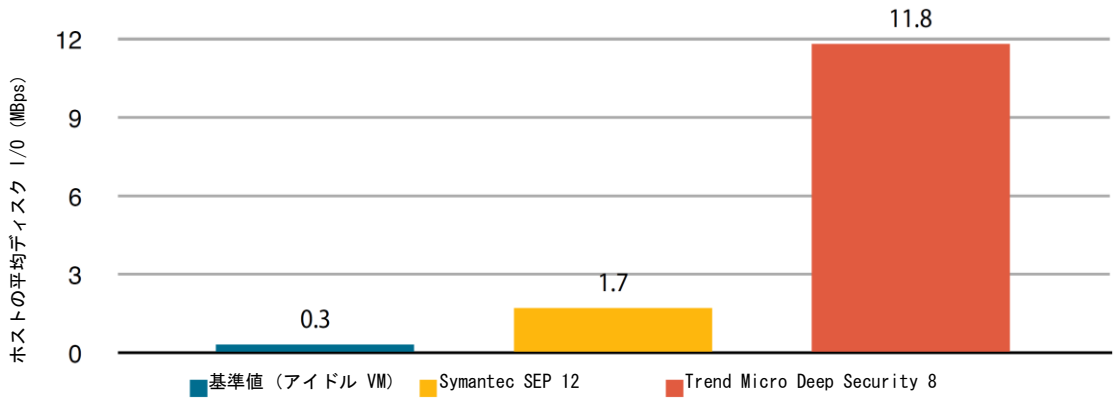
テストのハイライト

Symantec Endpoint Protection 12:

1. オンデマンドスキャン時に、Trend Micro Deep Security 8 と比較してディスク帯域幅の使用量を 86%、CPU の使用量を 37% 軽減

2. オンアクセススキャン時に、Trend Micro Deep Security 8 と比較してディスク帯域幅の使用量を 21%、CPU の使用量を 36% 軽減

オンデマンドのマルウェア対策スキャンのリソース使用量
VMware ESXi 5.0u1 ホストのディスク I/O
VMware vCenter によるレポート（数値が小さいほど、システムにかかる負荷が小さい）



注：1. ESXi 5u1 ホストのレポート結果には、すべての仮想デスクトップおよび DSVA が含まれます。2. Windows 7 Professional 64 ビット VM。ソリューションには 50 台の VM のスキャンを指定。163.2MB の一意のデータを各テストの各 VM に導入。詳細については、テスト手法のセクションを参照してください。3. スキャンを最適化するように SEP Shared Insight Cache を設定。配備後初の SEP スキャンでは、VM 当たりの I/O は平均 2.9 MBps、それ以降のオンデマンドスキャンでは、上記に示すように平均 1.7MBps。4. DS8 では、各 VM のスキャンを完了するのに 17 分から 18 分を要しました。SEP では、各テストイテレーションの最初の 2 つの VM では 16 分から 21 分を要し、それ以降の VM では 6 分 から 8 分を要しました。ソリューションでスキャンされるデータの量は、動的なデータおよびキャッシュによって異なりました。詳細については、レポートテキストを参照してください。どのテストでも A/V ストームは検出されませんでした。5. テスト期間（14 時間 16 分）は、DS8 が 50 台の VM を連続してスキャンするのに必要な最大時間によって決定しました。SEP は 14 時間以上にわたってスキャンをランダム化するように設定されました。

図 1

出典 :Tolly 社（2012 年 4 月）

シマンテック

Symantec Endpoint Protection 12

仮想化のパフォーマンスを向上させるエンドポイントセキュリティ

テスト時期 2012 年 4 月

概要（続き）

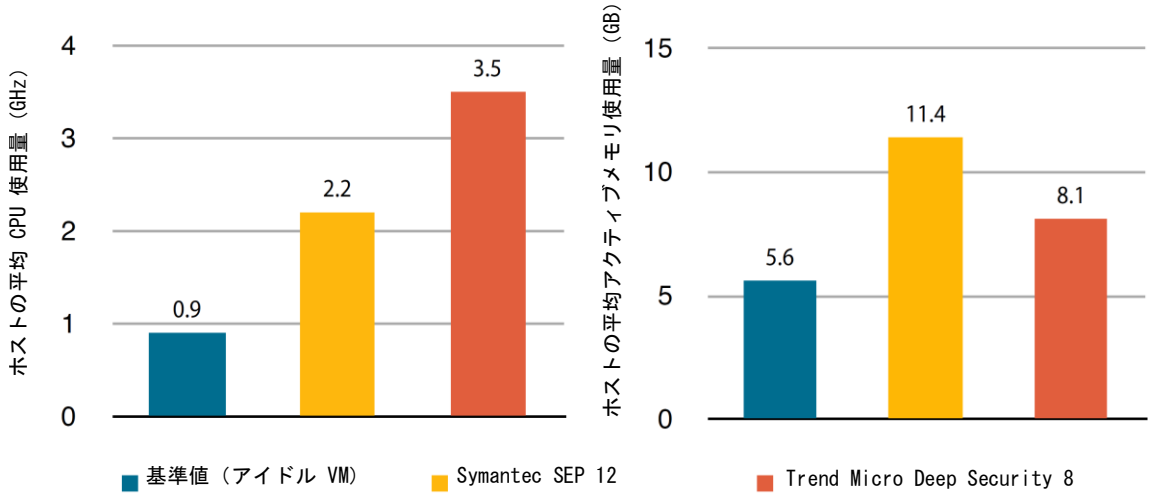
SEP 12.1 は、各仮想デスクトップシステム上で動作するエージェントとして配備されます。Trend Micro Deep Security 8 は、セキュリティ活動を処理するための中心点としての役割を果たし、VMware の vShield Endpoint Agent を使用してクライアントと接続する VMware 仮想アプライアンス（DSVA）として実装されます。

テストにはさまざまなスキャン機能およびシステム更新機能を取り込み、50 台の Microsoft Windows 7 Professional （64 ビット）仮想マシンを使用して実施しました。Tolly 社のエンジニアは、仮想マシンと VMware ホストの両レベルで重要なシステムリソース、ディスク入出力（I/O）、CPU の消費量、メモリ使用量を測定しました。

Symantec Endpoint Protection 12 では、システムタスクの開始にランダム化アルゴリズムを使用することで、オンデマンドスキャンやシグネチャ更新などのリソースを大量に使用するタスクを数時間の期間に自動的に分散できるため、リソースの過剰な消費や、いわゆるアンチウイルス（A/V）「ストーム」が回避されることが判明しました。

アナリストは「ストーム」という言葉を用いて、リソースを大量に使用するタスクが多くの仮想マシンで同時に開始され、同じホスト上の他の仮想マシンが使用できるリソースが非常に少なくなる状況を表しています。

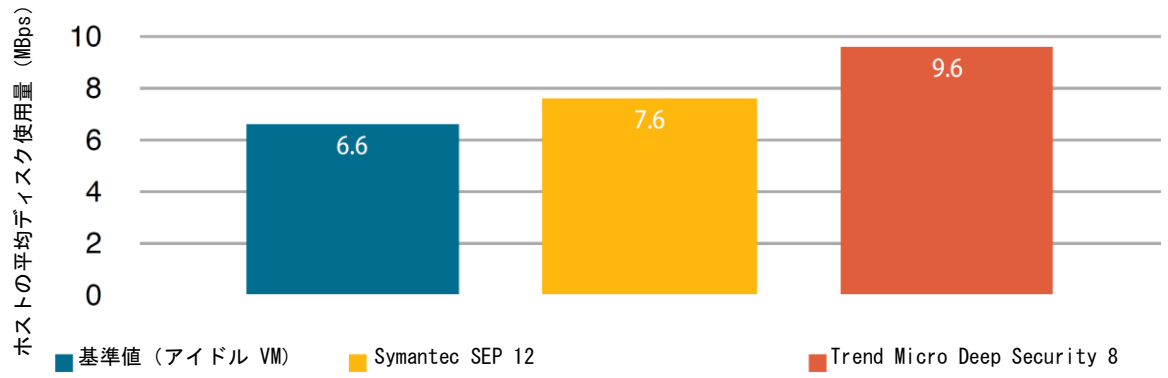
オンデマンドのマルウェア対策スキャンのリソース使用量
VMware ESXi 5.0u1 ホストの CPU およびメモリの動作
VMware vCenter によるレポート（数値が小さいほど、システムにかかる負荷が小さい）



注:1. ESXi 5u1 ホストのレポート結果には、すべての仮想デスクトップおよび DSVA が含まれます。2.Windows 7 Professional 64 ビット VM。ソリューションには 50 台の VM のスキャンを指定。163.2MB の一意のデータを各テストの各 VM に採用。詳細については、テスト手法のセクションを参照してください。3. スキャンを最適化するように SEP Shared Insight Cache を設定。4. DS8 では、各 VM のスキャンを完了するのに 17～18 分を要しました。SEP では、各テストイテレーションの最初の 2 つの VM では 16 分から 21 分を要し、それ以降の VM では 6 分から 8 分を要しました。ソリューションでスキャンされるデータの量は、動的なデータおよびキャッシュによって異なりました。詳細については、レポートテキストを参照してください。どのテストでも A/V ストームは検出されませんでした。5.テスト期間（14 時間 16 分）は、DS8 が 50 台の VM を連続してスキャンするのに必要な最大時間によって決まりました。SEP は 14 時間以上にわたってスキャンをランダム化するように設定されました。

出典 :Tolly 社（2012 年 4 月）

オンアクセスのマルウェア対策スキャンのリソース使用量
VMware ESXi 5.0u1 ホストのディスク動作
VMware vCenter によるレポート（数値が小さいほど、システムにかかる負荷が小さい）



注: これは、すべての仮想デスクトップと Deep Security 仮想アプライアンスをホストする ESXi ホストについての結果を表しています。Windows 7、64 ビットのインストール環境。50 台の VM では、Microsoft Word、Excel、PowerPoint、Internet Explorer、Adobe Reader、およびネットワークファイル転送を実行し、作業負荷はすべて同じです。

出典 :Tolly 社（2012 年 4 月） 図 3

テスト結果

オンデマンドのマルウェア対策スキャン

いくつかの理由から、IT セキュリティ管理者は数十ものクライアント上で「オンデマンド」でフルスキャンを実行する場合があります。このようなタスクはリソースを大量に使用し、同時に実行した場合、ホストシステムに多大な負担がかかり、仮想システム全体のパフォーマンスが低下する恐れがあります。

このテストでは、各システムで 50 台すべての VM のオンデマンドスキャンを実行するように指定しました。Trend Micro Deep Security ソリューションは、スキャンを自動的に連続化して、リソースが過剰に消費されないようにします。Deep Security は、3 回のテストにおいて、それぞれ 13 時間 49 分、14 時間 16 分、14 時間 5 分で 50 台の VM のフルスキャンを完了しました。Tolly 社のエンジニアがテスト時間として使用した最長実行時間は、14 時間 16 分でした。

シマンテックソリューションは、リソースが過剰に消費されないようにするために、14 時間以内で 50 すべてのスキャンをランダム化するように設定しました。

図 1 および 2 に、シマンテックと Trend Micro 社の結果をまとめました。

配備後最初の SEP のオンデマンドスキャンテストでは、ホストの平均ディスク I/O は 2.9 MBps でした。シマンテックが提供するキャッシュ機能により、以降のテストでは、ディスク I/O に対する負担がおよそ 1.7 MBps に軽減されました。Trend Micro 社のソリューションでは、ディスク I/O の負担はシマンテックの 6 倍でした（図 1 を参照）。

Trend Micro Deep Security ソリューションは、クライアント仮想マシンと Trend Micro Deep Security Virtual Appliance（DSVA）の 2 つのコンポーネントから構成されます。どちらのコンポーネントもシステムリソースに負担がかかります。

Tolly 社のエンジニアはオンデマンドスキャンに、Trend Micro Deep Security が Symantec SEP 12 よりも 59% 多く CPU を使用することを発見しました。

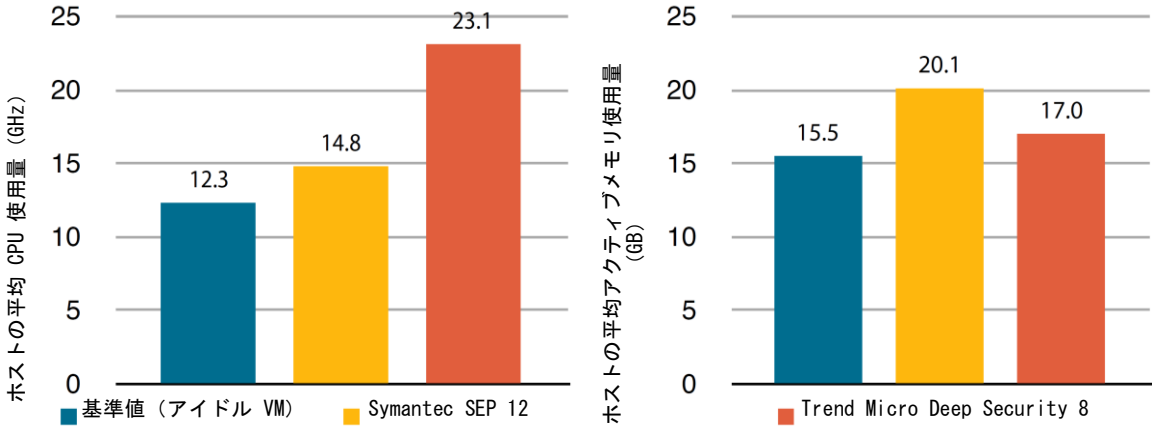
両者のソリューションの処理性能およびメモリ使用量を図 2 に示します。

注目すべき点は、テストした 2 つの製品は、どのファイルをスキャンするのかを判断するために異なる方式を使用しているため、スキャンを完了する時間および合計ディスク I/O 量が異なるという点です。

Symantec Endpoint Protection 12 は、Shared Insight Cache を使用して、スキャンされるデータの量を減らします。また、ベースイメージ上のすべてのファイルのスキャンをバイパスする機能もありますが、この機能はデフォルトでは有効ではなく、Tolly 社のエンジニアはどのテストでもこの機能を有効にしていません。この機能を使用すると、SEP のスキャン活動をさらに軽減できます。

VM が完全にキャッシュされないようにするため、Tolly 社のエンジニアは、各オンデマンドのテストイテレーション前に各 VM 上の 163.2 MB の動的ファイルを変更しました。詳細については、テスト手法のセクションを参照してください。

オンアクセスのマルウェア対策スキャンのリソース使用量
VMware ESXi 5.0u1 ホストの CPU およびメモリの動作
vCenter によるレポート（数値が小さいほど、システムにかかる負荷が小さい）



注：このレポート結果は、すべての仮想デスクトップと Deep Security 仮想アプライアンスをホストする ESXi ホストに関するものです。Windows 7、64 ビットのインストール環境。50 台の VM では、Microsoft Word、Excel、PowerPoint、Internet Explorer、Adobe Reader、およびネットワークファイル転送を実行し、作業負荷はすべて同じです。

出典 :Tolly 社（2012 年 4 月） 図 4

オンアクセスのマルウェア対策スキャン

エンドポイントセキュリティソリューションは、1 日中、ファイルやその他のレジストリ/RAM にアクセスしたときに、その内容をスキャンするために呼び出されます。

このテストでは、各種 Microsoft Office 機能およびネットワークファイル転送を使用するスクリプトを 50 台すべての VM で実行し、VMware ホストレベルでリソースを測定しました。

ホストの平均ディスク使用量が 7.6MBps の場合、Tolly 社のエンジニアは、SEP 12.1 では基準値の測定値からわずか 1MBps 増えるのに対し、Trend Micro では 3MBps 増えたことを発見しました（図 3 を参照）。

Deep Security Virtual Appliance では、スキャンするファイルをキューに入れる必要があるため、ファイル転送時間は SEP 12.1 よりも長くなりました。

また、Symantec SEP 12 は、Trend Micro Deep Security 8 よりも CPU の使用量（GHz）が軽減されています。14.8GHz では、シマンテックの CPU 使用量は、Trend Micro 社の使用量と比べると、平均して最大 35% 低くなりました。Deep Security Virtual Appliance では、CPU の使用量を平均して 75% 未満にしておくため、6 台の vCPU が割り当てられました（図 4 を参照）。

シグネチャの更新

エンドポイントセキュリティシステムは、新しい脅威を検出して、除去する上で有効な「シグネチャ」と呼ばれる更新情報を定期的に取得します。

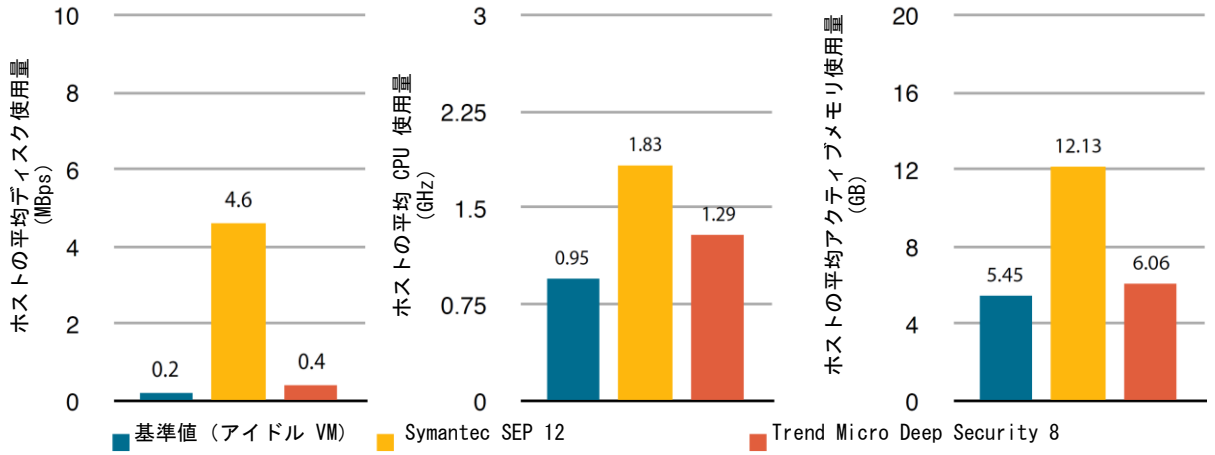
オンデマンドスキャンよりも使用するリソースは少ないものの、複数のシグネチャ更新が同時に実行された場合、IT 管理者は VMware ホストサーバー上のパフォーマンスに与える影響を当然意識します。

Trend Micro Deep Security は、ファイルの単一コピーが仮想アプライアンスにダウンロードされるアーキテクチャを実装します。シマンテックのエンドポイントエージェントでは、シグネチャの更新を個々にダウンロードして実行したのに対し、Symantec Endpoint Protection では、デフォルトで定義の更新プロセスの一環として各 VM でアクティブスキャンを実行し、最近発見された脅威がシステム上にないことを確認しました。

Trend Micro Deep Security は、ホストに多少の影響があったものの、5 分でシグネチャの更新を完了しました（図 5 を参照）。

Tolly 社のエンジニアは、シマンテックのランダム化アルゴリズムが、開始時に所定の 4 時間 15 分のウィンドウに 50 台のクライアントに対するダウンロードタスクを効果的に分散することを確認しました。Tolly 社のエンジニアは、その期間のリソースの消費量を測定しました。そのレポートによれば、シマンテックの平均ディスク I/O が 4.6 MBps、CPU 消費量が 1.83 GHz、メモリ消費量が 12.23 GB でした。「ストーム」または VMware システムの低下は認められませんでした。詳細については、図 5 を参照してください。

ウイルス定義の更新: VMware ESXi 5.0u1 ホストのリソース使用量
vCenter によるレポート（数値が小さいほど、システムにかかる負荷が小さい）



注:1. このレポート結果は、すべての仮想デスクトップと Deep Security 仮想アプライアンスをホストする ESXi ホスト関するものです。2. Symantec Endpoint Protection はデフォルトで定義の更新プロセスの一部として各 VM でアクティブスキャンを実行しました。3. 異なるベンダーが異なるメカニズムで異なる時間で定義の更新を行いました。示されている結果は、4 時間 15 分間の平均的な ESXi ホストのリソース消費量です。詳細については、レポートテキストを参照してください。

出典 :Tolly 社（2012 年 4 月）

図 5

テスト手法

50 台すべての Windows 7 Professional（64 ビット）の仮想マシンを、VMware View 5.0 を使用して、リンクされたクローンとして配備しました。永続型のプールは、1 つの vCPU、2GB の RAM、および 30GB のシックプロビジョニングされたディスクのゴールデンイメージから構成されます。

被テストシステムの全リストについては表 1 を、VMware 仮想環境の詳細については表 2 を参照してください。

Deep Security のテストでは、Trend Micro 社の提案に従い、マルウェア対策プロファイルを 50 台すべての VM に使用し、手動によるスキャンおよびスケジュールされたスキャンの CPU 使用率を Deep Security ポリシーで「HIGH」に設定しました。Deep Security Virtual Appliance のデフォルトの設定では、2 台の vCPU を使用します。しかし、ほぼすべてのオンアクセステスト期間の CPU 使用率は 100%でした。Tolly 社のエンジニアは、Trend Micro 社の推奨に従い、DSVA の平均的な CPU の使用率が 75% 未満になるように、vCPU を 6 台に増加しました。

Symantec Endpoint Protection のテストでは、まず管理対象 SEP クライアントをゴールデンイメージ上にインストールしました。その後、レピュテーションが有効になるように、このイメージを 3 時間以上インターネットに接続したままにしました。次に、Symantec Virtual Image Exception ツールをコマンド “vietool.exe c:--hash” と一緒に使用して、最初のスキャンを行うことができるように、ディスク上のファイルをハッシュしました。続いて、“SMC -stop” を実行ラインから実行し、Hadware Key の config XML ファイル sephwid.xml のすべてのコピーを削除し、HKLM¥Software¥Symantec¥Symantec EndpointProtection¥SMC¥Sylink¥Sylink¥” にある HardwareID、ComputerID、HostGUID を消去して、Symantec Endpoint Protection Manager が再接続されたときに各複製イメージを固有のクライアントとして認識できるようにします。ベースイメージファイルのスキャンバイパス機能は、SEP ではデフォルトで有効になっていません。

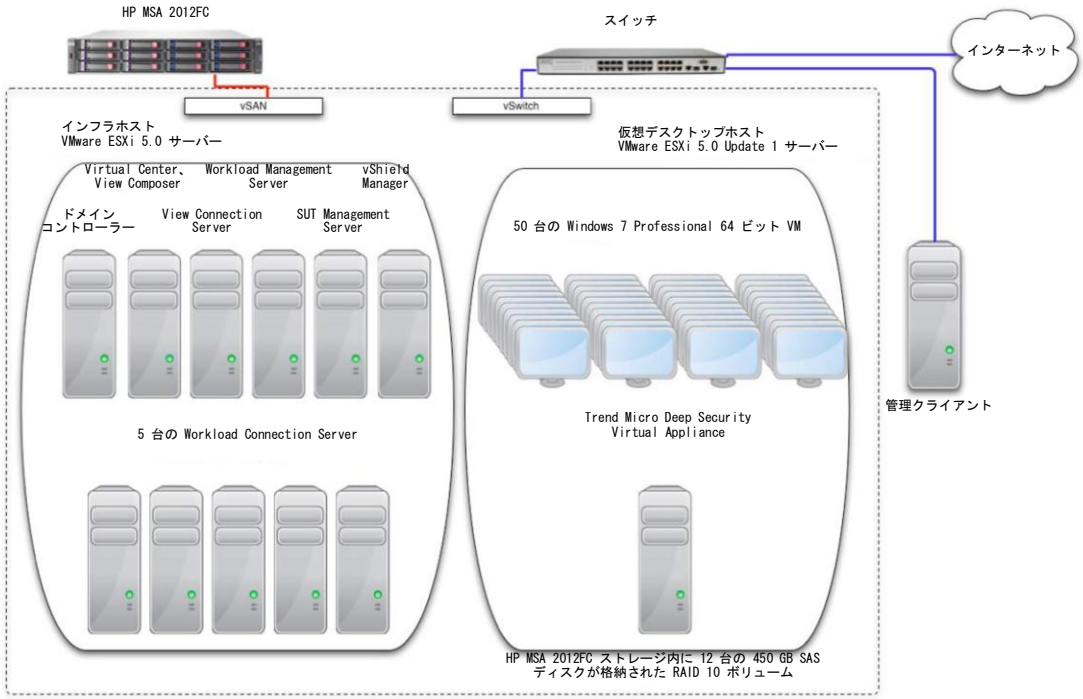
オンデマンドのマルウェア対策スキャン

すべての VM をアイドル状態にしました。テスト期間（14 時間 16 分）は、Deep Security が 50 台すべての VM のスキャンを完了する最長時間によって決定されました。

最初のオンデマンドテストの前に、489.6 MB のファイルを各クライアントに保存しました。そのうちの 244.8 MB のファイルは各クライアントで同じファイルで、残りの 244.8 MB のファイルは各クライアントで固有です。各実行/イテレーション間で、Tolly 社のエンジニアは各クライアントについて 163.2 MB のファイルを変更しました。そのうちの 81.6 MB のファイルは、すべてのクライアントで同じであり、残りの 81.6 MB のファイルは各クライアントで固有です。各オンデマンドスキャンテストの前に、更新テストを実行しました。

Symantec Endpoint Protection は、Deep Security によって決定されたテスト期間に基づいて、14 時間のウィンドウ内のランダムな開始時間で 50 台すべての VM をスキャンするようにスケジュールリングされました。

テスト環境:仮想デスクトップおよび Deep Security Virtual Appliance



出典 :Tolly 社 (2012 年 4 月) 図 6

1 分間隔でパフォーマンス結果を VMware Virtual Center からエクスポートしました。

オンアクセスのマルウェア対策スキャン

各 VM では Microsoft Word、Excel、PowerPoint、Internet Explorer、Adobe Reader アプリケーションを実行、バックグラウンドでネットワークファイル転送を実行し、作業負荷はすべて同じです。

バッチファイルを使用して、各 VM 内のファイルを転送しました。スクリプトで実行するタスクは次のとおりです。20 秒間 127.0.0.1 を ping する -> ファイルサーバーから VM に 10MB のファイルを転送する -> 20 秒間 127.0.0.1 を ping する -> VM からファイルサーバーに 10MB のファイルを転送する -> 繰り返す。

このスクリプトを 25 回のイテレーションで実行しました。転送したファイルは、1MB の docx ファイル、1MB の pdf ファイル、1MB の pptx ファイル、1MB の xls ファイル、1MB の zip ファイル、別の 3 つの pdf ファイル、別の 1 つの ppt ファイル、別の 1 つの doc ファイル、1 つの VMware-vShield-Endpoint-Driver-1.0.msi ファイルなどです。

テスト期間は 40 分間です。20 秒間隔でパフォーマンス結果をリアルタイムで VMware Virtual Center からエクスポートしました。

シグネチャの更新

すべての VM をアイドル状態にしました。Symantec Endpoint Protection を、4 時間内のランダムな開始時間で 50 台すべてのクライアントを更新するようにスケジュールしました。Trend Micro Deep Security は Deep Security Virtual Appliance を更新するのみであったため、所要時間は 5 分足らずでした。

Symantec Endpoint Protection は、デフォルトでは、定義更新プロセスの一環として各 VM でアクティブスキャンを一度ずつ実行しました。アクティブスキャンオプションはチェックマークを外すことができます。

全テスト期間は 4 時間 15 分でした。パフォーマンス結果を 1 分間隔で、VMware Virtual Center からエクスポートしました。

テスト環境

Intel® Xeon® X5680 プロセッサ (6 コア、3.33GHz) 2 基および 128GB RAM を搭載した 1 台の HP DL380G7 サーバーを使用して、VDI 環境をホストしました。1 台の HP MSA2012FC ストレージ (HP MSA2 450GB 3G 15K の 3.5 インチ SAS HDD を 12 基収容) を使用して、すべての VM を格納しました。ホストとストレージは、16 ポート 4Gb SAN スイッチで 4G FC によって接続しました。

すべての仮想デスクトップは、12 基のドライブを装備した RAID 10 ボリューム内に格納しました。Trend Micro Deep Security Virtual Appliance もすべての仮想デスクトップと同じボリューム内に格納しました。テストベッド図については、図 6 を参照してください。

被テストシステム

ベンダー	製品	コンポーネント	実装
シマンテック	Endpoint Protection 12	Symantec Endpoint Protection Manager 12.1.601.4699; Symantec Shared Insight Cache 1.0.0.409	オンデマンドスキャン最適化用に Shared Insight Cache を搭載したエンドポイントクライアント
Trend Micro 社	Deep Security 8	Trend Micro Deep Security Manager バージョン 8.0.1448; Deep Security Virtual Appliance 8.0.0.1199; ESX Filter Driver 8.0.0.1189; 事前に設定された Windows Anti-Malware セキュリティポリシーを適用済み	単一の仮想アプライアンス。エージェントレスクライアントが VMware vShield API を介して通信。

出典 :Tolly 社 (2012 年 4 月) 表 1

このレポートで用いたテスト手法は、Tolly 社の Common Test Plan #1105: Anti-Virus Endpoint Performance in Virtual Environments で定義されているテスト手順、評価指標、文書化の方法に準拠しています。

VMware パフォーマンスのホストテストベッドコンポーネント

コンポーネント	バージョン/ビルド
VMWare ESXi	5.0.0, 623869
VMware vCenter サーバー	5.0.0, 455964
VMware View Composer サーバー	2.7.0, 481620
VMware View Connection サーバー	5.0., 481677
VMware vShield Manager	5.0, 473791
サーバーのハードウェア	128 GB の DDR3 RAM を搭載し、3.33GHz で動作する Xeon x5680 (Hex-core) × 2
ストレージエリアネットワーク	HP StorageWorks MSA が 4GB FibreChannel を介して接続
ゲスト VM リソース	2GB RAM および 1 台の vCPU、30 GB ディスク (シックプロビジョニング)
ゲストオペレーティングシステム	Microsoft Windows 7 Professional 64 ビット

出典 :Tolly 社 (2012 年 4 月) 表 2

Tolly 社について…

Tolly グループは 20 年間にわたり世界中で IT サービスを提供しています。Tolly 社は IT 製品、コンポーネント、サービスのベンダーに対する第三者評価サービスを提供する代表的なグローバルプロバイダです。

連絡先は sales@tolly.com、または電話 +1 (561) 391-5610 です。

Tolly 社の Web サイトは http://www.tolly.com です。

競合企業との関係

当社の比較テストの実施プロセスに従い、Tolly グループは競合ベンダーに連絡し、公表に先立ち、テスト手法およびテスト結果を確認するよう求めました。この要求に応え、Trend Micro 社は、仮想デスクトップで Windows Anti-Malware プロファイルを使用すること、手動によるスキャンおよびスケジュールされたスキャンのポリシーの CPU の設定を「HIGH」に変更すること、および CPU の使用率を 75% 未満にするために DSVA の vCPU の数を増加することについて提案をしました。Tolly 社はこのすべての提案に従い、テストを実施しました。

Tolly 社はテスト結果を Trend Micro 社および VMware 社に提供しましたが、公表に先立ち、その後コメントや反応は一切ありませんでした。

Tolly Fair Testing Charter の詳細については、次の Web サイトを参照してください。http://www.tolly.com/FTC.aspx

利用条件

212117-tb-11-mts-yy - 2012-05-07-Verl