TREND MICRO™

Securing Your Journey to the Cloud

Sichern Sie Ihre **virtuelle Desktop-Infrastruktur (VDI)**

Mit der VDI-Technologie vereinfachen Sie nicht nur die Bereitstellung und Verwaltung, sondern schöpfen auch Ihre Investitionen in Endpunkt-Hardware besser aus. Darüber hinaus lassen sich private Geräte Ihrer Mitarbeiter leichter integrieren. Ihre Desktops laufen auf geschützten Servern in Ihrem Rechenzentrum, und Sie behalten mit VDI die Kontrolle und Sicherheit, die Sie brauchen. Um virtuelle Desktops sicher zu gestalten, brauchen Sie jedoch eine Sicherheitslösung, die die besonderen Herausforderungen dieser IT-Umgebung berücksichtigt. Eine Sicherheitslösung für physische Desktops zum Schutz virtueller Desktops zu verwenden, kann die Leistung beeinträchtigen, die VM-Dichte senken und Ihre Rendite verringern. Stattdessen können Sie Schutz und Leistung erhöhen, indem Sie eine virtualisierungssensitive Sicherheitslösung verwenden, die speziell zur Optimierung der gemeinsam genutzten Ressourcenumgebungen virtueller Desktops entwickelt wurde.

HERAUSFORDERUNGEN BEI DER SICHERHEIT FÜR VIRTUELLE DESKTOPS

Ressourcenkonflikte

Bei der VDI-Technologie teilen sich mehrere Desktops die Hardware-Ressourcen des Hosts, meist in einem Verhältnis von 60:1 oder höher. Es kann bei einer so hohen VM-Dichte vorkommen, dass gleichzeitig durchgeführte, ressourcenintensive Vorgänge, wie z. B. größere Sicherheitsupdates und vollständige Systemüberprüfungen, zu einem dramatischen Verlust der Desktopleistung führen. Die Beeinträchtigung kann so schwerwiegend sein, dass der Host vollständig lahmgelegt wird. Die Sitzungsverbindungen von Anwendern werden beendet und können oft über einen längeren Zeitraum nicht wiederhergestellt werden.

Verteilung veralteter Sicherheit

Virtuelle Desktops können schnell bereitgestellt, geklont, auf eine Vorgängerinstanz zurückgesetzt, angehalten oder neu gestartet werden. Schwachstellen und Konfigurationsfehler können auf diese Weise unwissentlich verbreitet und inaktive Desktop-Images mit veralteter Sicherheit reaktiviert werden.

LÖSEN DIESER HERAUSFORDERUNGEN

VDI-fähige Sicherheit

Ressourcenkonflikte können mit Hilfe von VDI-Intelligenz überwunden werden, die virtualisierte Desktops in VMware View und Citrix XenDesktop erkennt. VDI-fähige Sicherheit führt Suchläufe und Updates zeitversetzt durch, um die Systemleistung und -verfügbarkeit nicht zu beeinträchtigen.

Weiße Listen

Sie können herkömmliche VDI-Bereitstellungsmethoden nutzen, um Standard-Images, Klone oder verknüpfte Klone zu erstellen. Dann können Sie mit der richtigen, innerhalb eines Standard-Images installierten Sicherheit starten, um einen aktuellen Schutz zu gewährleisten. Wenn Sie die Inhalte dieses Standard-Images im Vorfeld durchsuchen und zu einer weißen Liste hinzufügen, werden sie von nachfolgenden Suchläufen ausgeschlossen. Danach müssen nur noch vom Anwender hinzugefügte Dateien, also ein kleiner Bruchteil des VDI-Images, durchsucht werden. Indem das mehrfache Durchsuchen identischer Dateien auf verschiedenen VDI-Images verhindert wird, kann die Systemleistung und -verfügbarkeit gesteigert werden.

Dedizierte Sicherheitsappliances

Ein weiterer Ansatz, der aktuelle Sicherheit gewährleistet und gleichzeitig die Leistung virtueller Desktops maximiert, ist die Verwendung einer dedizierten, sicherheitsoptimierten virtuellen Maschine. Über die Hypervisor-APIs kann die VM auf jeder Gast-VM auf einen Treiber mit sehr geringer Speicherbelastung zugreifen, um zeitversetzte Updates und Suchläufe zu koordinieren. Ressourcenintensive Vorgänge, wie vollständige Systemprüfungen, werden von der separaten Sicherheits-VM aus durchgeführt. Dies gewährleistet die Sicherheit inaktiver virtueller Desktops sowie die Installation aktueller Sicherheitsupdates, sobald die Desktops aktiviert werden. Diese „ständig aktive“ agentenlose Sicherheit führt auch virtuelles Patching durch, um vor Zero-Day-Angriffen zu schützen und damit Notfall-Patching auf virtuellen Desktops überflüssig zu machen.

Funktionsweise virtueller Desktops

Die Desktops werden als verwalteter Service von Ihrem Rechenzentrum bereitgestellt. Virtuelle Desktops werden über eine private Cloud überall dorthin verteilt, wo sie gebraucht werden – in lokalen und externen Büros sowie in Zweigstellen. Anwendungen und Desktops können so schneller und zuverlässiger an ein breiteres Spektrum von Clients verteilt werden.

Geschützte Punkte: Virtuelle Desktops

- Citrix XenDesktop
- VMware View

VDI-Verteilung

- 52 % der Unternehmen weltweit setzen bereits eine VDI ein oder testen sie gerade
- In Unternehmen, die bereits eine VDI nutzen:
  - sind durchschnittlich 42 % der Endpunkte virtualisiert
  - sollen in den nächsten 12 Monaten bis zu 60 % der Endpunkte virtualisiert sein

Quelle: Trend Micro Umfrage, Mai 2011

VIRTUALISIERTE DESKTOPSICHERHEIT – WELCHEN WEG WÄHLEN SIE?

Sie entscheiden sich vielleicht für VDI, um eine Vielzahl von Szenarien mit virtuellen Desktops zu unterstützen: von kioskartigen Einzelanwendungen in öffentlichen Umgebungen bis hin zum vollständigen Ersatz Ihrer physischen Desktops. Doch egal welchen individuellen Ansatz Sie für Ihre virtuelle Desktop-Infrastruktur wählen, Trend Micro hat eine Sicherheitslösung, die speziell dafür entwickelt wurde, Ihren Weg zur VDI zu schützen.

1. Möglichkeit: Erweitern der physischen Endpunktsicherheit zum Schutz virtueller Endpunkte

- Sie möchten Ihre physischen und virtuellen Endpunkte mit einer einzigen Sicherheitslösung schützen?
- Nutzen Sie schon OfficeScan?
- Möchten Sie Ihre virtuelle Desktopsicherheit in Citrix integrieren, um die Leistung zu steigern?

Trend Micro OfficeScan
OfficeScan ermöglicht es Ihnen, Ihre Endpunktsicherheit in einer einzigen Lösung zu konsolidieren – sowohl für physische als auch für virtuelle Desktops. Im Gegensatz zu Sicherheitslösungen für physische Endpunkte, die nicht für den Einsatz in virtuellen Umgebungen vorgesehen sind, erkennt OfficeScan, ob ein Agent sich auf einem physischen oder einem virtuellen Endpunkt befindet, und optimiert Schutz und Leistung der jeweiligen Umgebung entsprechend. Auf virtuellen Desktops führt OfficeScan Suchläufe und Updates zeitversetzt durch und fügt Standard-Images und bereits durchsuchte Inhalte zu weißen Listen hinzu, um die Ressourcen des Hosts zu schonen.

2. Möglichkeit: Erweitern der Bemühungen bei der Servervirtualisierung auch auf virtuelle Desktops

- Sie sind auf der Suche nach einer Sicherheitslösung, die virtuelle Server und virtuelle Desktop-Infrastrukturen schützt?
- Sie möchten Ihre VMware Umgebung nutzen, um durch die Verteilung agentenloser Sicherheit eine Leistungssteigerung zu erreichen?
- Sie möchten die physischen, virtuellen und cloudbasierten Server Ihres Rechenzentrums sowie virtuelle Desktops mit einer einzigen Sicherheitslösung schützen?

Trend Micro Deep Security
Trend Micro ist das erste Unternehmen, das durch die Nutzung von VMware vShield Endpoint und anderen VMware APIs eine agentenlose Sicherheit für virtuelle Server und Desktops bereitgestellt hat. Eine dedizierte, sicherheitsoptimierte virtuelle Maschine greift über die VMware Hypervisor-APIs auf einen Treiber mit sehr geringer Speicherbelastung auf jeder Gast-VM zu, um zeitversetzte Updates und Suchläufe zu koordinieren, ohne dass dafür ein Sicherheitsagent installiert werden muss. Dadurch, dass Agenten auf Gast-VMs nicht mehr notwendig sind, wird die Ressourcenbelastung des zugrunde liegenden Hosts verringert und damit die Leistung gesteigert und die VM-Dichte erhöht. Eine agentenbasierte Version ist für virtuelle Desktops mit Hyper-V- oder Xen-basierten Hypervisor-Umgebungen sowie für virtuelle Desktops im lokalen Modus ebenfalls verfügbar.

Wählen Sie die optimale Endpunktsicherheit für Ihr Unternehmen

Je nach individueller Umgebung können Sie am Endpunkt beginnen und den Einsatz Ihrer OfficeScan Lösung dann ausweiten, um konsistenten Schutz sowohl für physische als auch für virtuelle Desktops zu gewährleisten. Oder Sie machen sich Ihre Virtualisierungsbemühungen mit VMware auch in Ihrem Rechenzentrum zunutze und setzen DeepSecurity als agentenlose Sicherheitslösung ein. Egal welchen Weg Sie wählen – Ihre Ressourcen werden geschont und Ihre Konsolidierungsraten gesteigert. Lassen Sie sich vom anerkannten Marktführer im Bereich virtueller Sicherheit dabei helfen, die VM-Dichte, Sicherheit und Rendite zu erzielen, die Sie von Ihrer virtuellen Desktop-Infrastruktur erwarten.

VDI-Komponenten

OfficeScan VDI-Schutz

- Virenschutz
- Anti-Spyware
- Anti-Rootkit
- Firewall
- Schutz vor Internetbedrohungen
- Skalierbare, zentrale Verwaltung

Weitere OfficeScan Plug-ins:

- Data Loss Prevention
- Intrusion Defense Firewall
- Mobile Security
- Security for Mac

Deep Security VDI-Schutz

- Anti-Malware
- Firewall
- Erkennung und Abwehr von Eindringlingen
- Schutz von Webanwendungen
- Anwendungssteuerung
- Virtuelle Patches
- Integritätsüberwachung
- Protokollprüfung
- Skalierbare, zentrale Verwaltung

Trend Micro Smart Protection Network

Trend Micro Sicherheit für virtuelle Desktops enthält auch Schutz aus dem Smart Protection Network, einer cloudbasierten Client-Architektur, die im Internet auf Bedrohungsinformationen zugreift, um so den Schutz schneller zur Verfügung zu stellen, während gleichzeitig die Ressourcenbelastung der Endpunkte verringert wird.

TREND MICRO™