Channel Sellsheet

Schutz von Windows 2008 Servern nach Support-Ende

Moderne Sicherheitslösung für Rechenzentren und die Hybrid Cloud

Viele Unternehmen setzen auf Microsoft® Windows® Server 2008 als Basis für kritische Geschäftsprozesse. **Am 14. Januar 2020 beendet Microsoft den Support für Windows Server 2008 und Windows Server 2008 R2.** Deshalb müssen Unternehmen und andere Organisationen jetzt analysieren, welche Risiken aus dem Weiterbetrieb von Plattformen nach dem Support-Ende entstehen und welche Optionen für einen kontinuierlichen Schutz verfügbar sind.

WIE TREND MICRO IHNEN UND IHREN KUNDEN HELFEN KANN

Trend Micro Lösungen unterstützen Sie bei dem Schutz und der Migration der Windows Legacy-Umgebungen Ihrer Kunden (inklusive Windows Server 2008, 2003 oder älter). Das Ende des Supports für Windows Server 2008 führt zu zwei Konsequenzen:

- Für neu entdeckte Schwachstellen in Windows Server 2008 werden zukünftig keine Patches mehr bereitgestellt.
- Schwachstellen werden von Microsoft nicht mehr dokumentiert oder bestätigt.

Organisationen haben zwar die Möglichkeit, eine Custom-Support-Vereinbarung mit Microsoft abzuschließen, um weiterhin Patches zu erhalten. Dies ist aber kostenintensiv und langfristig nicht wirtschaftlich. Der Betrieb von Software ganz ohne aktuelle Patches stellt ein erhebliches Risiko dar – insbesondere bei kritischer Software wie Windows Server 2008, die von potenziellen Angreifern immer weiter auf Schwachstellen untersucht wird. Allein in der ersten Hälfte des Jahres 2019 wurden mehr als 150 neue Schwachstellen für Windows Server 2008 identifiziert. Trend Micro hilft dabei, die Risiken beim Weiterbetrieb von Windows 2008 zu minimieren, und gewährleistet umfassenden Schutz während und nach der Transition zu einer neuen Plattform.

Chancen für Channel-Partner

- Verkauf von Hybrid-Cloud-Sicherheits-software (Virtuelles Patching, Systemsicherheit, Anti-Malware)
- Services für die Bereitstellung
- Sicherheits- und Compliance-Consulting
- Monitoring oder Managed Security Services

Relevante Produkte

- Trend Micro™ Deep Security™

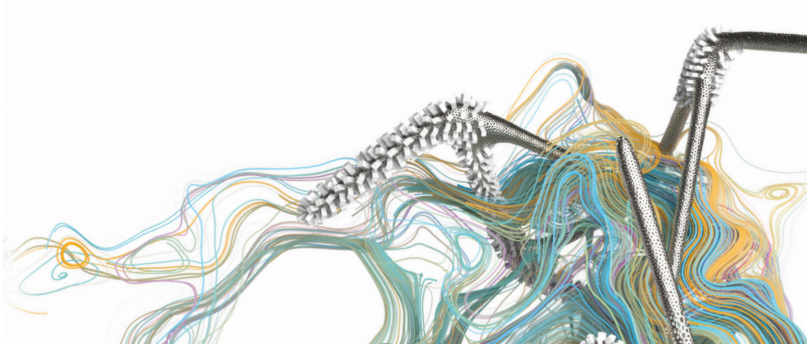
Ideales Kundenprofil

Große bis mittlere Unternehmen mit:

- Microsoft 2008 Server Umgebungen, die bis zum Support-Ende nicht migriert werden
- Budget-Begrenzungen, die Microsoft Custom-Support-Vereinbarungen ausschließen
- Erfahrungen aus dem Support-Ende von Windows 2003, 2000 oder XP

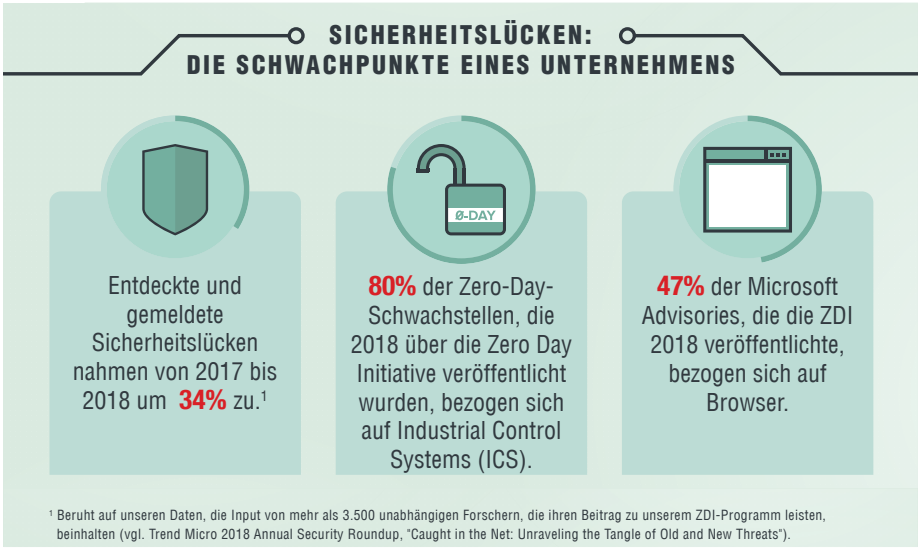
Zielgruppe beim Kunden

- Director / Manager Data Center Operations
- Director / Manager Cloud Engineering / Operations
- Director / Manager IT / Security
- Enterprise-Architekt



Für die Cloud oder kritische Workloads, die aufgrund von zeitlichen, budgetären oder technischen Begrenzungen nicht sofort migriert werden können, bietet Deep Security den benötigten Schutz vor neuen Schwachstellen durch:

- **Virtuelles Patching:** Intrusion Detection and Protection (IDS/IPS) schirmt Workloads auf neuen und End-of-Service-Plattformen (EOS) automatisch durch einen virtuellen Patch ab. Kunden können somit ihre Systeme schützen, bis die Transition geplant und durchgeführt ist.



- **Systemsicherheit:** Deep Security verfügt über eingebaute Kontrollen für die Systemsicherheit, darunter Echtzeit-Integritätsüberwachung, Applikationskontrolle und Log-Inspektion. Ungeplante oder bösartige Änderungen an Windows Server 2008 werden schnell erkannt und dem Sicherheitsteam per Alarm gemeldet.
- **Malware-Schutz:** Fortschrittliche Funktionen zur Malware-Abwehr, inklusive Verhaltensanalysen und Machine Learning, bieten Schutz vor Ransomware, Crypto-Mining-Angriffen und anderer bösartiger Software.

SCHUTZ VON MICROSOFT LEGACY-PLATTFORMEN: WARUM TREND MICRO?

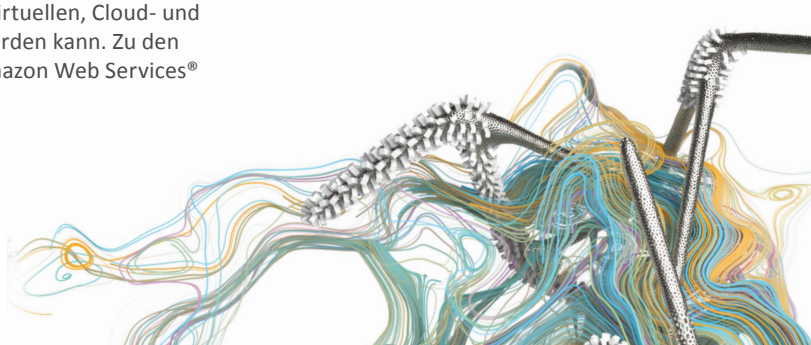
Tausende Unternehmen und Organisationen auf der ganzen Welt vertrauen beim Schutz mehrerer Millionen Server auf Trend Micro Deep Security. Die bewährte Sicherheitsplattform unterstützt Kunden dabei, die bevorstehenden Risiken für Windows 2008 Systeme zu minimieren. Trend Micro Deep Security bietet:

Plattform mit umfassender Sicherheitsfunktionalität

In einer einzigen Lösung vereint Deep Security ein breites Funktionsspektrum, inklusive Netzwerk-Sicherheitskontrollen (Virtuelles Patching / IPS, Firewall und Web-Reputation), Systemsicherheit (Integritätsüberwachung, Log-Inspektion und Applikationskontrolle) sowie Malware-Schutz.

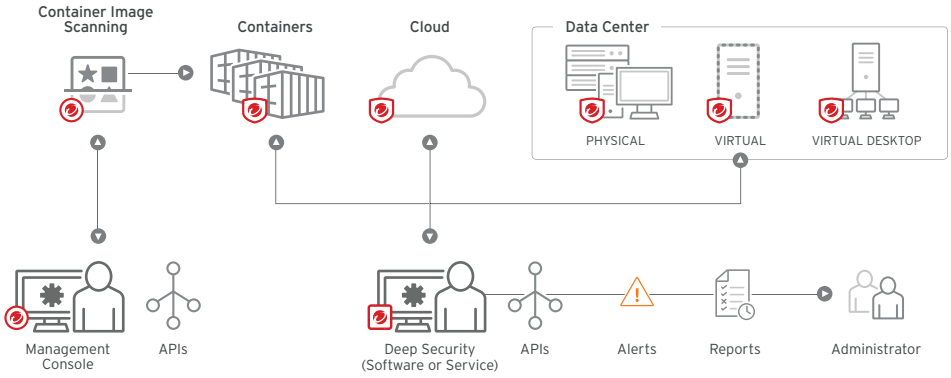
Optimierte Sicherheit reduziert Kosten und Komplexität

Deep Security ermöglicht End-to-End-Sicherheit, die in physischen, virtuellen, Cloud- und Container-Umgebungen automatisch bereitgestellt und verwaltet werden kann. Zu den Vorteilen gehören die Integration und Optimierung für VMware®, Amazon Web Services® (AWS), Microsoft Azure™, Google Cloud™, Docker und Kubernetes.



Nahtlose Migration auf neue Plattformen

Mit Deep Security können Unternehmen eine sichere Transition planen und durchführen. Kunden können sich darauf verlassen, dass ihre Workloads und Applikationen automatisch durch virtuelles Patching geschützt sind – bis zur Migration auf eine neuere Plattform und darüber hinaus.



ANSÄTZE FÜR KUNDENGESPRÄCHE

- Setzt Ihr Unternehmen derzeit Microsoft Windows 2008 Server ein?
- Haben Sie eine Strategie für den Schutz dieser Server nach dem Support-Ende?
- Welche Auswirkungen erwarten Sie für Ihr Unternehmen, wenn Microsoft keine Patches mehr bereitstellt?
- Prüfen Sie aktuell Strategien für die Migration auf neuere Plattformen oder die Cloud?
- Werden Sie alle Workloads bis zum Support-Ende migrieren können?
- Welche Konsequenzen hatte das Support-Ende von Windows 2003 für Ihr Unternehmen?
- Wie viel Zeit wird in der Regel für den Patch-Rollout auf Systemen benötigt?

Zusätzliche Ressourcen

- Trend Micro Webseite zu **virtuellem Patching**
- Trend Micro Webseite zur **Sicherheit von End-of-Support-Systemen**
- Trend Micro Webseite zu **Sicherheitslösungen für die Hybrid Cloud**

Securing Your Connected World