Ende des Supports bedeutet nicht Ende der Sicherheit

Wie Trend Micro Ihre Server nach Support-Ende schützt und einen sicheren Übergang zu neuen Plattformen und in die Cloud ermöglicht

Einleitung

Das Ende des Supports (End of Support, EOS) für große Enterprise-Plattformen wie Microsoft® Windows® Server 2008 und 2008 R2 bedeutet erhebliche Herausforderungen für Unternehmen und andere Organisationen, deren tägliche Geschäftsabläufe von kritischen Applikationen abhängen. Als Microsoft zum Beispiel im Juli 2015 den Support für Windows 2003 eingestellt hat, führte dies zu Risiken für mehrere Millionen Server, die nur durch Migration auf eine neuere Plattform oder die Implementierung kompensierender Sicherheitskontrollen beseitigt werden konnten.[1] Im Januar 2020 steht nun der EOS von Windows Server 2008 und 2008 R2 bevor. Hacker wissen, dass Microsoft ab diesem Zeitpunkt keine weiteren Patches für Schwachstellen mehr veröffentlicht. Damit werden diese Systeme zu bevorzugten Angriffszielen. Unternehmen, die nach dem EOS eine nicht mehr unterstützte Plattform betreiben, müssen sich auf wachsende Risiken einstellen – denn im Laufe der Zeit werden Angreifer immer mehr Schwachstellen entdecken, für die niemals ein offizieller Patch bereitgestellt wird.

Dieses White Paper informiert über die Risiken für Unternehmen, die EOS-Plattformen wie Microsoft Server 2008 einsetzen. Außerdem werden die verfügbaren Optionen zur Adressierung dieser Risiken vorgestellt. Der Fokus liegt dabei auf dem Schutz von EOS-Plattformen mit Trend Micro™ Deep Security™, der Lösung vom Marktführer[2] bei Server-Sicherheit. Deep Security nutzt XGen™ Security und bietet eine generationsübergreifende Kombination mehrerer leistungsstarker und automatisierter Sicherheitskontrollen, mit denen EOS-Plattformen wie Windows 2008 weiterhin geschützt werden können. Unternehmen können somit ihren Übergangsprozess ganz nach den eigenen Anforderungen gestalten, die Lebensdauer von Legacy-Systemen und -Applikationen verlängern und kostenintensive Custom-Support-Vereinbarungen für Patches von Microsoft vermeiden. Deep Security schützt Systeme nicht nur bis zur Migration auf neuere Plattformen oder Public Cloud Services (Microsoft® Azure™, Amazon Web Services®, Google Cloud™), sondern auch darüber hinaus. Mit einer einzigen, effizienten Lösung schützen Organisationen ihre gesamte Hybrid Cloud.

1 Enterprise Strategy Group, Microsoft Windows Server 2003: The End is Nigh, Februar 2015
2 IDC, Worldwide Endpoint Security Market Shares, 2015: Currency Volatility Headwind, #US41867116, November 2016

DIE RISIKEN FÜR END-OF-SUPPORT-SYSTEME VERSTEHEN

Obwohl Microsoft für Windows Server 2003 einen eindeutigen EOS-Prozess definiert hatte, wurde die Plattform von vielen Organisationen über das offizielle Support-Ende hinaus eingesetzt. Beim EOS von Windows Server 2008 wird sich diese Situation wiederholen. Die Migration von Plattformen, die im Unternehmen extensiv genutzt werden, ist eine Herausforderung. Zu den am häufigsten genannten Hürden gehören begrenzte Zeit und Ressourcen sowie kritische Geschäftsanwendungen, die wahrscheinlich auch in Zukunft nicht migriert werden können. Organisationen benötigen daher eine Strategie für den ununterbrochenen Schutz verwundbarer EOS-Systeme.

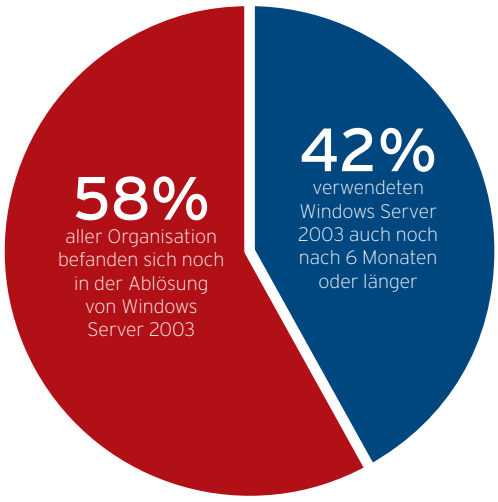
Denn durch den Einsatz von Systemen ohne Support entstehen Risiken, die nicht ignoriert werden dürfen. So verwenden zum Beispiel neuere Plattformen oftmals auch Programmcode ihrer Vorgänger. Ein Exploit wie **EternalRocks**, der die Microsoft SMB 1.0 Schwachstelle von Windows 2012 oder 2016 ausnutzt, betrifft damit unter Umständen auch ältere Systeme – für die aber im Gegensatz zu den neueren Plattformen kein Patch-Support mehr geleistet wird. Ohne aktuelle Updates der Betriebssysteme werden EOS-Systeme darüber hinaus zu Angriffsvektoren für Hacker.

Der Betrieb ungeschützter EOL-Systeme verursacht zudem Risiken, die über einzelne Plattformen hinausgehen. Ein kompromittierter Server reicht oftmals aus, um das gesamte Netzwerk anfällig zu machen für Hacker-Angriffe, Datenverluste und Malware (Ransomware, Crypto-Mining-Attacken und viele weitere mehr). Ohne einen wirksamen Aktionsplan wird es außerdem unmöglich sein, die Compliance mit Regularien (DSGVO, PCI DSS, HIPAA etc.) und Rahmenwerken (SANS/CIS Top 20 Critical Security Controls, NIST 800-53 etc.) zu gewährleisten.

SICHERHEIT VOR, WÄHREND UND NACH DER MIGRATION

Unternehmen müssen sich grundsätzlich auf die Ablösung von EOS-Plattformen vorbereiten. In der Realität treffen Planungen aber oftmals auf begrenzte Budgets oder technische Einschränkungen. Deshalb benötigen Organisationen die Option, EOS-Systeme nach eigenem Zeitplan schrittweise abzulösen und währenddessen den Schutz dieser Systeme auf kosteneffiziente Weise aufrechtzuerhalten. Unabhängig vom konkreten Migrationsplan - zu Windows Server 2016 oder 2019, zu Microsoft Azure oder einer anderen führenden Cloud-Umgebung wie AWS – müssen Sicherheitslösungen in der Lage sein, nicht nur die Anforderungen von EOS-Systemen zu adressieren, sondern auch von neueren Umgebungen, inklusive Containern und Hybrid-Cloud-Bereitstellungen. Aus der Sicherheits- und auch aus der Betriebsperspektive ist dies ein entscheidender Faktor, der von Unternehmen bei der Prüfung der zur Verfügung stehenden Optionen unbedingt berücksichtigt werden sollte.

Neun Monate nach Support-Ende



Quelle: Osterman Research, April 2016

Die Ablösung kann einige Zeit in Anspruch nehmen, daher sollten sich Planungen über den gesamten Zeithorizont und den vollständigen Migrationsprozess erstrecken. Neun Monate nach dem offiziellen EOS von Windows 2003 ergab eine Branchenumfrage, dass immer noch viele betroffene Server in Betrieb waren. Für die vollständige Transition zu einer neuen Plattform oder in die Cloud benötigten Unternehmen noch erheblich mehr Zeit, so die Umfrage.

WEITERVERWENDUNG EINER END-OF-SUPPORT-PLATTFORM: WAS IST ZU TUN?

Sobald Plattformen wie Windows Server 2008 und Server 2003 den EOS-Termin erreichen, können verschiedene Optionen verfolgt werden. Im Rahmen der Planungen müssen die verschiedenen positiven und negativen Aspekte dieser Optionen abgewogen werden. Obwohl dabei jede Organisation die jeweiligen Kosten und Risiken für sich selber beurteilen muss, gibt es doch ein paar eindeutige Favoriten.

1. STATUS QUO: BEREITSTELLUNG UNVERÄNDERT LASSEN

Es gibt immer die Option, alle Risikoanalysen beiseite zu lassen und gar nichts zu tun. Damit entstehen dann natürlich auch keine Kosten für die Migration oder zusätzliche Sicherheitskontrollen. Allerdings sind die Risiken, die von Systemen ohne Patch verursacht werden, für Organisationen nicht vertretbar. EOS-Systeme wie Windows Server 2008 und Windows 2003 sind bevorzugte Ziele für Angreifer, denn sie öffnen unter Umständen einen Pfad in das Unternehmen. Das Schadenspotenzial ist hier immens, daher wird diese nicht empfehlenswerte Option hier auch nur der Vollständigkeit halber aufgeführt. Unternehmen sollten vielmehr einen der anderen verfügbaren Ansätze prüfen, die Sicherheit und Kosteneffizienz verbinden.

2. CUSTOM-SUPPORT-VEREINBARUNGEN MIT DEM PLATTFORMHERSTELLER

Microsoft bietet Kunden unter Umständen erweiterte oder Custom-Support-Vereinbarungen für Windows Server 2008, sodass diese Plattformen weiterhin mit Notfall-Sicherheitspatches versorgt werden. In der Regel sind solche Vereinbarungen aber sehr kostenintensiv (oftmals mehr als 200.000 US-Dollar pro Jahr). Viele Kunden suchen daher nach alternativen Methoden zur Risikominimierung, während andere resignieren und sich mit dem gesteigerten Risiko abfinden. Darüber hinaus unterliegen die verlängerten Sicherheitsupdates möglicherweise Bedingungen, wie zum Beispiel Software Assurance (SA) oder Subscription-Lizenzen.

3. ISOLATION

Ein Ansatz zum Risikomanagement von EOS-Software wie Windows Server 2008 besteht darin, die betroffenen Systeme für Hacker schwer erreichbar zu machen. Die Isolation der Systeme in separaten Netzwerken oder VLANS bzw. die Segmentierung mittels Netzwerk- oder Host-basierten Firewalls etabliert eine weitere Schutzschicht, die Hacker bei einem Angriff überwinden müssen – wenn sie zu diesem Mehraufwand bereit sind und sich nicht lieber einfachere Ziele suchen. Für essentiell wichtige Geschäftssysteme ist eine Netzwerkisolation aber vielleicht gar nicht praktisch machbar. Denn wenn EOS-Systeme schwer zu erreichen sind, können sie oftmals auch nicht mehr effizient genutzt werden. Dieser Ansatz kann daher zwar für einen kleinen Prozentsatz der eingesetzten Server sinnvoll sein, führt aber in den meisten Szenarien nicht zu praxistauglichen Lösungen.

4. SYSTEMHÄRTUNG

Das Härten von Systemen wie Windows Server 2008 oder 2008 R2 (z.B. durch Entfernung nicht benötigter Services, Deaktivierung verwundbarer Service-Versionen wie SMB 1.0, Anwenderkonten) ist ein guter Ansatz zur Risikominimierung. Autorisierte Anwender benötigen aber immer noch Zugang zum System. Aus Business-Gründen ist daher die Einschränkung von Anwenderkonten unter Umständen nicht praktikabel.

Für Windows Server 2008 sollten Organisationen die eingebauten Richtlinien für Software-Einschränkungen nutzen, die als globale Richtlinien durchgesetzt werden können. Dies minimiert das Risiko, dass Applikationen fehlerhafte Kommandos ausführen. Das ist keine triviale Aufgabe, aber hilft dabei, Server vor Angriffen via Applikationen zu schützen. Alleine reicht diese Maßnahme allerdings nicht aus, sie muss immer mit zusätzlichen Sicherheitsvorkehrungen kombiniert werden.
Das Härten durch Abschaltung oder Entfernung nicht benötigter Services und Ports ist kein einfacher Vorgang. Dies gilt umso mehr, wenn Business-Applikationen konzipiert wurden, um auf Universal-Betriebssystemen mit verschiedenen Services und Ports (z.B. RPC Ports, Web Services) zu laufen. Es besteht die sehr reale Gefahr, dass das Härten die Applikation unbrauchbar macht. Die Beschränkung von Applikations-Ports kann außerdem dazu führen, dass Stateful Packet Filter Firewalls ineffektiv werden, da viele Applikationen nach Bedarf Ports dynamisch zuweisen.

5. EINSATZ ZUSÄTZLICHER SICHERHEITSKONTROLLEN

Um potenzielle Schwachstellen in EOS-Systemen wie Windows Server 2008 zu adressieren, können zusätzliche Sicherheitskontrollen implementiert werden, die Angriffe identifizieren und abwehren. Host-basierte Lösungen sind hierfür ideal geeignet, da Perimeter-Lösungen einfach keinen effektiven Schutz für jeden einzelnen Server bereitstellen können. Dies gilt insbesondere im Kontext moderner Rechenzentren und der Hybrid Cloud. Zu den wichtigen Host-basierten Sicherheitskontrollen, die jedes Unternehmen erwägen sollte, gehören:

- Intrusion Detection and Prevention (IDS/IPS) zum Schutz vor Netzwerk-Angriffsvektoren, wie zum Beispiel der Apache Struts 2 Schwachstelle, die zum katastrophalen Equifax-Sicherheitsvorfall geführt hat.
- Integritätsüberwachung für Systemdateien, Registry-Einstellungen und andere kritische Applikationsdateien, um sicherzustellen, dass ungeplante oder verdächtige Aktivitäten identifiziert werden.
- Malware-Schutz, inklusive Anti-Malware und Verhaltensanalysen zur Abwehr neuer Malware-Formen, insbesondere Ransomware und Crypto-Mining-Angriffe.

Da multiple Sicherheitskontrollen erforderlich sind, besteht der empfohlene Ansatz in der Implementierung einer Lösung, die alle Kontrollen in einem einzigen Produkt kombiniert und zentral verwaltet werden kann. Außerdem sollte gewährleistet sein, dass dieselbe Lösung auch für neue Bereitstellungen geeignet ist, unabhängig von Server-Umgebung (Windows oder Linux) und Bereitstellungsansatz (physisch, virtuell, Cloud und/oder Container).

DER BESTE ANSATZ: EINE BEWÄHRTE SICHERHEITSLÖSUNG

Das Härten der Server, inklusive Verwendung der in Windows eingebauten Richtlinien für Software-Beschränkungen, leistet unzweifelhaft einen Beitrag zur Risikominimierung. Wenn aber der Plattformhersteller keine Schwachstellen mehr identifiziert und per Patch schließt, benötigen Organisationen auf jeden Fall zusätzliche Sicherheitskontrollen. Es werden permanent neue kritische Schwachstellen entdeckt, die adressiert werden müssen – auch wenn der Plattformhersteller keine Patches mehr liefert.

Trend Micro™ Deep Security™ bietet den erforderlichen Schutz. Deep Security beinhaltet leistungsstarke und automatisierte Sicherheitskontrollen, die von vielen Tausend Organisationen auf der ganzen Welt eingesetzt werden, um mehrere Millionen physische, virtuelle und Cloud-Server zu schützen – inklusive Server, die EOS-Plattformen wie Windows Server 2008 verwenden. Die Lösung von Trend Micro stellt die benötigte kritische Funktionalität bereit, die Organisationen eine sichere Transition ermöglicht. Ohne unnötige Risiken oder Kosten können Unternehmen damit selber bestimmen, wie und wann sie eine Migration durchführen.

TREND MICRO DEEP SECURITY

Deep Security bietet eine generationsübergreifende Kombination mehrerer Sicherheitstechnologien, die einen nahtlosen Schutz von Server- und Applikations-Workloads in physischen, virtuellen, Cloud- und Container-Umgebungen ermöglichen. Die Bereitstellung erfolgt über einen einzigen, schlanken Agenten sowie auf der Hypervisor-Ebene mit VMware NSX für zusätzliche Effizienz. Eine zentrale Sicherheitskonsole sorgt für ein konsolidiertes Management. Deep Security wurde für die Automation von Sicherheitsaufgaben konzipiert und reduziert sowohl manuelle Eingriffe als auch den Verwaltungsaufwand durch automatisierte Bereitstellung, Richtlinien-Management und ein umfangreiches Set von RESTful APIs.

Deep Security umfasst bewährte Netzwerk-Sicherheitskontrollen, die Schwachstellen (z.B. Apache Struts 2 oder die Microsoft SMB Schwachstelle, über die sich WannaCry verbreitete) in kritischen Systemen abschirmen, bis ein Patch verfügbar ist und implementiert werden konnte. Auf diesem Weg können auch EOS-Systeme vor und während der Migration umfassend geschützt werden.

WAS DEEP SECURITY MACHT UND WARUM DAS WICHTIG IST

Deep Security ist eine Host-basierte Sicherheitslösung, die leistungsstarke und automatisierte Sicherheitskontrollen über einen einzigen Agenten bereitstellt. Sie beinhaltet die empfohlenen Schlüsselfunktionen zum Schutz von Systemen am Support-Ende, wie zum Beispiel Windows Server 2008, 2008 R2 und Windows XP. Während der Migration reduzieren Organisationen mit Deep Security sowohl Risiken als auch Kosten in physischen, virtuellen, Cloud- und Container-Bereitstellungen. Auf Basis der engen Integration mit VMware schützt Deep Security darüber hinaus auch Virtual Desktop Infrastructures (VDI). Dazu gehören auch VDIs, in denen EOS-Systeme wie Windows XP zum Einsatz kommen.

NETZWERKSICHERHEIT: SERVER UND APPLIKATIONEN ABSCHIRMEN

Die Netzwerk-Sicherheitskontrollen von Deep Security können Unternehmensserver vor bekannten und unbekannten Schwachstellen abschirmen, inklusive neuer kritischer Schwachstellen wie Bluekeep und älterer Schwachstellen wie Apache Struts 2, Shellshock und Heartbleed, die auch heute noch für viele Systeme eine Bedrohung darstellen.

Deep Security setzt Intrusion Detection and Prevention (IDS/IPS)-Funktionalität ein und beinhaltet mehrere Tausend bewährter Sicherheitsrichtlinien für Netzwerkdatenverkehr der Schichten 2 bis 7. Auf Basis der Bereitstellungsumgebung lassen sich diese Richtlinien automatisch durchsetzen, um Netzwerk-gerichtete Systeme ohne Patch und Unternehmensanwendungen zu schützen. Als Verteidigungsschicht gegen neue Angriffe gewährleistet der Netzwerkschutz von Deep Security, dass Server vor Schwachstellen abgeschirmt sind, über die sich ansonsten Infektionen im Rechenzentrum oder in der Hybrid Cloud ausbreiten könnten.

Heartbleed April 2018

Suche nach CVE-2014-0160 ergab 140.602 Treffer am 18.4.2018

Top-Länder

1. USA
2. China
3. Deutschland
4. Frankreich
5. Russische Föderation
6. Republik Korea
7. Kanada
8. Italien
9. Großbritannien
10. Japan

Der Schutz erstreckt sich auf das zugrundeliegende Betriebssystem und auf verbreitete Unternehmensanwendungen, die auf den Servern bereitgestellt werden. Deep Security umfasst sofort einsatzbereiten Schwachstellenschutz für Hunderte Applikationen, inklusive Datenbank-, Web-, Email- und FTP-Servern. Darüber hinaus bietet Deep Security Zero-Day-Schutz: Sowohl für bekannte Schwachstellen, für die kein Patch verfügbar ist, als auch für unbekannte Schwachstellen. Bei letzteren kommen Smart Rules mit Verhaltensanalysen und selbstlernenden Verfahren zum Einsatz, die eine Blockade neuer Bedrohungen ermöglichen.

Die Deep Security Sicherheitsregeln für Web-Applikationen bieten Schutz vor den häufigsten Web-Angriffen, inklusive SQL-Injection, Cross-Site-Scripting und anderen Schwachstellen in Web-Applikationen. Bis die entsprechenden Code-Fixes abgeschlossen sind, werden diese Schwachstellen zuverlässig abgeschirmt. Sicherheitsregeln sorgen für Protokoll-Konformität und nutzen heuristische Analysen zur Identifikation bösartiger Aktivitäten. Um kritische Fälle (zum Beispiel die laterale Ausbreitung von Bedrohungen im Rechenzentrum) zu adressieren, umfasst Deep Security auch robuste Regeln, mit denen sich potenziell bösartige Aktivitäten erkennen und blockieren lassen. Für Organisationen, die Container einsetzen, übernimmt die Deep Security IPS Engine das Scanning des gesamten Container-Verkehrs inklusive Inter-Container-Datenverkehr (Ost-West). Angriffe und laterale Ausbreitungsversuche können so proaktiv erkannt und verhindert werden.

Angriffe

Angreifer versuchen, über das Netzwerk eine Schwachstelle auf Betriebssystem- oder Applikationsebene auszunutzen

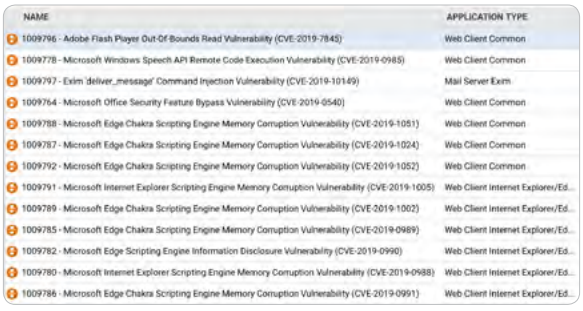
Netzwerkschutz

Deep Security blockiert Angriffe auf Netzwerkebene und schirmt Server vor neuen und bestehenden Bedrohungen ab

Ganze Hybrid Cloud

Deep Security schützt Applikationen und Workloads in physischen, virtuellen, Cloud- und Container-Umgebungen

Eine eingebaute, bi-direktionale Firewall hilft bei der Durchsetzung von IPS-Regeln. Diese Firewall unterstützt die Kontrolle der Kommunikation über Ports und Protokolle, die für den korrekten Server-Betrieb erforderlich sind. Alle anderen Ports und Protokolle werden blockiert. Dadurch wird das Risiko eines unautorisierten Zugriffs auf Bereitstellungen minimiert, die EOS-Server wie Windows Server 2008 oder 2003 umfassen. Darüber hinaus unterstützt die Host-Firewall Unternehmen bei der Compliance mit DSGVO, PCI DSS, HIPAA und anderen Regularien. Dies gilt insbesondere in Cloud-Umgebungen, in denen kein Zugriff auf Firewall-Logs von Netzwerkereignissen möglich ist.



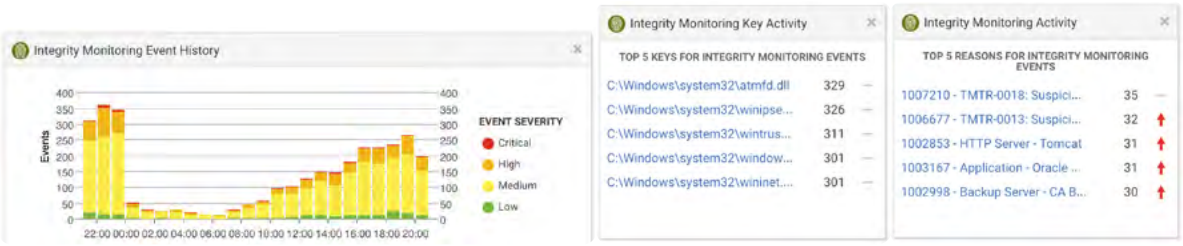
NAME	APPLICATION TYPE
1009796 - Adobe Flash Player Out-Of-Bounds Read Vulnerability (CVE-2019-7845)	Web Client Common
1009778 - Microsoft Windows Speech API Remote Code Execution Vulnerability (CVE-2019-0985)	Web Client Common
1009797 - Exim 'deliver_message' Command Injection Vulnerability (CVE-2019-10149)	Mail Server Exim
1009764 - Microsoft Office Security Feature Bypass Vulnerability (CVE-2019-0540)	Web Client Common
1009788 - Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-1051)	Web Client Common
1009787 - Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-1024)	Web Client Common
1009792 - Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-1052)	Web Client Common
1009791 - Microsoft Internet Explorer Scripting Engine Memory Corruption Vulnerability (CVE-2019-1005)	Web Client Internet Explorer/Ed...
1009789 - Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-1002)	Web Client Internet Explorer/Ed...
1009785 - Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-0989)	Web Client Internet Explorer/Ed...
1009782 - Microsoft Edge Scripting Engine Information Disclosure Vulnerability (CVE-2019-0990)	Web Client Internet Explorer/Ed...
1009780 - Microsoft Internet Explorer Scripting Engine Memory Corruption Vulnerability (CVE-2019-0988)	Web Client Internet Explorer/Ed...
1009786 - Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-0991)	Web Client Internet Explorer/Ed...

Laterale Ausbreitung erkennen und stoppen

Systemsicherheit: Integritätsüberwachung

Zu den Sicherheitskontrollen von Deep Security gehört unter anderem auch die Integritätsüberwachung. Große Mengen von Telemetriedaten werden analysiert, um Organisationen in Echtzeit vor unerwarteten Änderungen an Betriebssystemen und Applikationen zu warnen. Überwacht werden zum Beispiel Dateien, Verzeichnisse, Registry-Schlüssel, Prozesse, Anwender-Aktivitäten und weitere häufige Angriffsziele. Die Regeln ermöglichen zudem einen Container-spezifischen Schutz, um Angriffe gegen bereitgestellte Container, die Container-Plattform (z.B. Docker) oder Orchestrierungswerkzeuge (z.B. Kubernetes) zu identifizieren.

Im Fall von EOS-Systemen gibt es meist große Bereiche des Betriebssystems und der Applikationen, an denen keine Veränderungen mehr vorgenommen werden sollten. Mithilfe der Integritätsüberwachung können Unternehmen schnell verstehen, was geändert wurde und warum. Außerdem wird die Erkennung von Vorfällen und potenziellen Indicators of Compromise (IOC) unterstützt. Integritätsüberwachung bietet spezialisierte Regeln, die von den Trend Micro Teams für Threat Research and Incident Response entwickelt werden. Deep Security erkennt und meldet Hunderte potenzieller Indicators of Compromise (IOC), bei einer geringen Anzahl falscher Positivmeldungen. Zu den identifizierten Angriffen gehören unter anderem Flamer, Gauss, Duquu, Confiker und viele weitere. Durch diese Alarme können Angriffe von Incident Response Teams schneller erkannt und einfacher mit einer spezifischen Bedrohung in Verbindung gebracht werden.



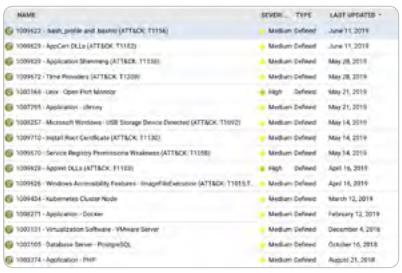
Zentrales Dashboard informiert sofort über bösartige Änderungen an sensiblen Dateien und Applikationen

Schutz vor Malware

Deep Security bietet umfangreiche Funktionalität zur Abwehr von Malware, inklusive Anti-Malware, Verhaltensanalysen und Web Reputation. Unternehmen können damit physische, virtuelle, Cloud- und Container-Workloads vor einem breiten Bedrohungsspektrum schützen, darunter Ransomware, Crypto-Mining-Angriffe, Viren, Spyware, Wümer und Trojaner. Die Integration mit den globalen Sensoren des Trend Micro™ Smart Protection Network™ sorgt für stets aktuelle Bedrohungsinformationen, zusätzlich unterstützt von der weltweit führenden Trend Micro Bedrohungs- und Schwachstellenforschung.

Automatisierte Abschirmung von Schwachstellen

Deep Security kann konfiguriert werden, um automatisch Systeme zu scannen und passende Sicherheitsregeln einzusetzen. Durch den System-Scan wird identifiziert, welche der vielen Tausend verfügbaren IDS/IPS-Regeln für optimierten Schutz verwendet werden sollten. Dabei werden Faktoren wie Betriebssystemversion, Service Pack, Patch Level und installierte Applikationen in die Entscheidung einbezogen. Genau wie die Regeln für Systemsicherheit gewährleisten auch die Intrusion-Prevention-Regeln eine proaktive Analyse und Blockade von Container-spezifischem Datenverkehr, um Container auf allen Ebenen zu schützen. Mittels Richtlinien können Routine-Scans für Systeme eingerichtet werden (z.B. wöchentlich), um potenzielle neue Schwachstellen zu erkennen und automatisch abzuschirmen. Aktivierte Regeln werden bei Bedarf sofort nahtlos durchgesetzt, sodass die entsprechenden Systeme geschützt sind und Notfall-Patching überflüssig wird. Dies gilt für neu entdeckte Schwachstellen wie Bluekeep und Oracle WebLogic, aber auch für ältere Schwachstellen wie Shellshock und Heartbleed. Für EOS-Systeme wie Windows 2008 und Server 2003, bei denen keine Patches mehr zu erwarten sind, ist dies ein kritischer Schutzmechanismus.

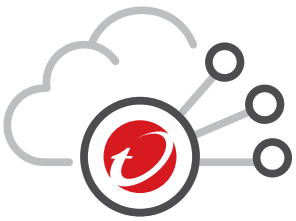


Eingebaute Funktionen für Erkennung und Meldung potenzieller Kompromittierung

Führende Threat Intelligence

Ein dediziertes Team aus Sicherheitsexperten überwacht die Bedrohungslage 24x7 und versorgt Deep Security mit kontinuierlichen Updates, um aktuellsten Schutz für Kunden zu gewährleisten. Das Monitoring erstreckt sich auf verschiedene Quellen für neu entdeckte Schwachstellen sowie auf Daten, die direkt aus den globalen Bedrohungsforschungszentren von Trend Micro stammen. Trend Micro Research erhält außerdem Informationen von der Zero Day Initiative™ (ZDI), dem weltweit größten, herstellerneutralen Bug-Bounty-Programm. Die Initiative arbeitet mit mehr als 3.500 externen Bedrohungsforschern zusammen, die neue Schwachstellen an Trend Micro melden. Seit 2007 ist die ZDI weltweit führend in der Entdeckung von Schwachstellen. Allein im Jahr 2018 wurde mehr als 1.400 Schwachstellen identifiziert.

Zusätzliche Informationen kommen von den mehr als 150 Millionen Endpunkten, die vom Trend Micro Smart Protection Network geschützt werden. Diese Informationen werden verwendet, um neue Bedrohungen zu identifizieren und zu korrelieren, sodass wirksame Regeln zum Schutz gefährdeter Systeme generiert werden können. Im Fall von Heartbleed und Shellshock konnte Trend Micro so innerhalb von 24 Stunden nach Bekanntwerden einen Schutz bereitstellen. Mit Deep Security waren Server somit sofort abgesichert. Bei der im März 2017 veröffentlichten SMB 1.0 Schwachstelle wurde ebenfalls in weniger als 24 Stunden ein Schutz bereitgestellt - Monate vor dem nachfolgenden Angriff auf die Schwachstelle durch WannaCry. Schon vor dem Support-Ende von Windows Server 2003 konnten zudem mit Deep Security Schwachstellen im Betriebssystem abgeschirmt werden, für die kein Patch zur Verfügung stand. Aufgrund des kurz bevorstehenden EOS (drei Wochen) hatte sich Microsoft entschieden, für eine bekannte Schwachstelle keinen Patch mehr zu entwickeln.



Globales Sensor-Netzwerk

Sammelt mehr Informationen aus mehr Quellen
- 250M+ Sensoren
- 8 Milliarden Bedrohungsabfragen täglich

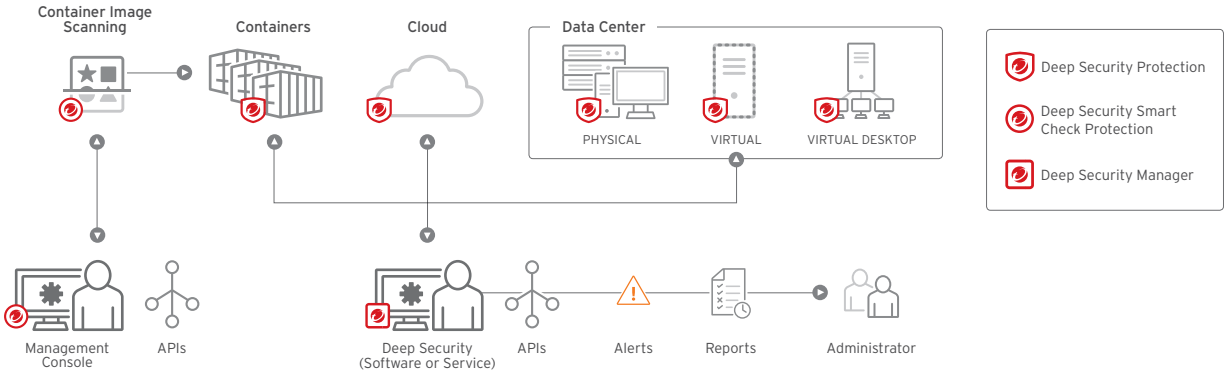
Globale Threat Intelligence

Analysiert Bedrohungen schneller und akkurater
- 450+ interne Bedrohungsexperten und 3.500 externe Schwachstellenforscher in der ZDI
- 24/7 Monitoring

Proaktiver Schutz

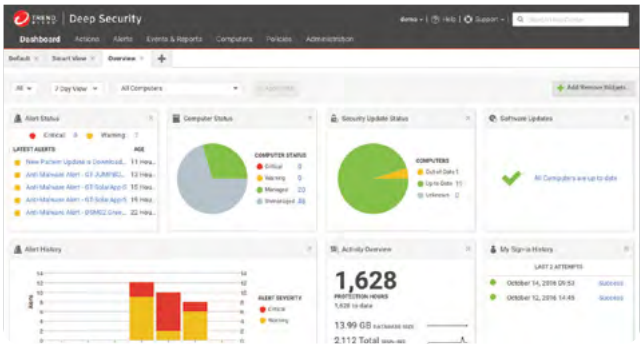
Blockiert Realworld-Bedrohungen früher
- Führende Schwachstellenforschung, Veröffentlichung von 1.400+ Schwachstellen in 2018 über die Zero Day Initiative
- Schnelle Reaktion auf neue Bedrohungen wie Bluekeep, Apache Struts, WannaCry und Heartbleed
- 18 Millionen neue Bedrohungen identifiziert und täglich 180 Millionen blockiert

Sicherheit in der Hybrid Cloud kontrollieren



Warum Trend Micro?

In diesem Whitepaper wurde vorgestellt, wie Deep Security mit einem breiten Spektrum integrierter Sicherheitskontrollen dafür sorgt, dass auch EOS-Systeme wie Windows Server 2008 umfassend geschützt sind. Die Lösung ist als Software-as-a-Service sowie über die Marketplaces von AWS und Azure verfügbar. Sie kann für alle physischen, virtuellen, Cloud- und Container-Umgebungen übergreifend eingesetzt werden. Deep Security ermöglicht damit ein optimiertes Management und konsistente Sicherheit vor, während und nach der Migration auf neue Systeme und Infrastrukturen. Die breite Plattformunterstützung und die enge Integration mit führenden Plattformanbietern gewährleisten vereinheitlichte Sichtbarkeit und Sicherheit über Hybrid- und Multi-Cloud-Umgebungen hinweg.



Zentrales Dashboard bietet vollständige Sichtbarkeit aller Sicherheitskontrollen

Organisation auf der ganzen Welt vertrauen auf Trend Micro beim Schutz ihrer Rechenzentren und Hybrid-Cloud-Bereitstellungen. Die automatisierte Schwachstellenabschirmung von Deep Security schützt Workloads auf neuen und EOS-Plattformen. Darüber hinaus wird Trend Micro nicht nur von Kunden und Partnern, sondern auch von renommierten Marktforschern als ein Marktführer betrachtet. In sieben Jahren nacheinander wurde Trend Micro von IDC als führend nach Marktanteilen eingestuft. Darüber hinaus erfüllt Trend Micro nach eigener Analyse alle acht von Gartner definierten, zentralen Sicherheitskontrollen für Cloud-Workloads.

Fazit: Es gibt einen sicheren Weg voran für EOS-Systeme

Falls Sie nicht mehr unterstützte Systeme wie Windows Server 2008 oder 2003 einsetzen, machen Sie sich wahrscheinlich Gedanken darüber, wie Workloads und Daten auf diesen Systemen nach dem Support-Ende konsistent und kosteneffizient geschützt werden können. Mit dieser Herausforderung sind Sie nicht allein, denn viele Unternehmen werden Windows 2008 nach dem EOS in der einen oder anderen Weise weiterverwenden. Aufgrund der Komplexität einer Migration der Unternehmensserverplattform ist ein mehrteiliger Ansatz für den Schutz von EOS-Systemen empfehlenswert. Dazu gehört die Verwendung der von Microsoft bereitgestellten integrierten Richtlinien für Software-Beschränkungen in Kombination mit zusätzlichen Sicherheitskontrollen.

TREND MICRO™
Securing Your Connected World