CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Endpoint Protection

Definition Endpoint Protection

Endpoint Data Protection ist eine gängige Maßnahme zum Überwachen und Kontrollieren von Datenübertragungen eines Netzwerkes nach innen und außen. Diese Maßnahme wird in Unternehmen und Behörden getroffen, um den ungewollten Datenabfluss zu verhindern und sich somit gegen Datenschutzverletzungen zu schützen.

Kernkomponenten

Antivirus und Antimalware:

- **Definition:** Software-Tools, die darauf ausgelegt sind, bekannte Malware zu erkennen, zu blockieren und zu entfernen. Sie nutzen häufig Signaturen, um bekannte Bedrohungen zu identifizieren.
- **Funktionsweise:** Durchsucht Dateien, Anwendungen und E-Mails auf bekannte Bedrohungen, basierend auf einer ständig aktualisierten Datenbank von Malware-Signaturen.
- **Beispiel:** Echtzeit-Scanning und automatische Updates, um Schutz gegen die neuesten Bedrohungen zu bieten

Kernkomponenten

Firewalls und Intrusion Prevention Systems (IPS):

- **Firewalls:** Überwachen den ein- und ausgehenden Netzwerkverkehr und blockieren unautorisierte Zugriffe basierend auf vordefinierten Sicherheitsregeln.
- **Beispiel:** Konfigurierbare Firewall-Regeln, die den Zugriff auf bestimmte Ports und IP-Adressen einschränken.

- **Intrusion Prevention Systems:** Analysieren den Netzwerkverkehr, um Angriffe zu erkennen und zu verhindern, bevor sie Schaden anrichten.
- **Beispiel:** Erkennung und Blockierung von Netzwerkangriffen in Echtzeit durch Analyse des Verkehrs auf Anomalien.

Kernkomponenten

Endpoint Detection and Response (EDR):

- **Definition:** Sicherheitslösungen, die fortschrittliche Bedrohungen auf Endpunkten erkennen, untersuchen, darauf reagieren und sie abwehren.
- **Funktionsweise:** Nutzt kontinuierliches Monitoring und Sammlung von Endpunkt-Daten, um verdächtige Aktivitäten zu identifizieren und darauf zu reagieren.
- **Beispiel:** Automatische Alarme bei verdächtigem Verhalten, Bereitstellung detaillierter Analysen für Untersuchungen und automatisierte Reaktionen auf Vorfälle.

Kernkomponenten

Sandboxing und Verhaltensanalyse:

- **Sandboxing:** Isoliert potenziell schädliche Programme in einer sicheren Umgebung, um ihr Verhalten zu analysieren, ohne das Host-System zu gefährden.
- **Beispiel:** Ausführung und Bewertung unbekannter Anhänge in einer virtuellen Umgebung, um Schadsoftware zu identifizieren, bevor sie Schaden anrichten kann.

Kernkomponenten

Sandboxing und Verhaltensanalyse:

- **Verhaltensanalyse:** Erkennt Malware und fortgeschrittene Bedrohungen durch Analyse des Verhaltens von Anwendungen und Prozessen, anstatt sich auf Signaturen zu verlassen.
- **Beispiel:** Identifizierung von Zero-Day-Angriffen und fortschrittlicher Malware durch Erkennung von Anomalien im Verhalten von Endpunkten.

Traditionelle Ansätze

Signaturbasierte Erkennung:

- Nutzt eine Datenbank bekannter Malware-Signaturen für die Erkennung von Bedrohungen. Effektiv gegen bekannte Malware, aber nicht gegen neue oder veränderte Bedrohungen.

Beispiel:

- Antivirus-Software, die tägliche Updates der Signaturdatenbank erfordert.

Moderne Ansätze

Heuristische Analyse:

- Erkennt Malware durch Analyse des Verhaltens und der Eigenschaften von Dateien, um unbekannte oder modifizierte Bedrohungen zu identifizieren.

Cloud-basierte Analysen:

- Nutzt die Cloud für eine umfassendere Bedrohungsanalyse und -erkennung, indem sie auf globale Bedrohungsintelligenz und Echtzeit-Daten zurückgreift.

Beispiel:

- EDR (Endpoint Detection and Response) Systeme, die verdächtige Aktivitäten auf Endpunkten überwachen und darauf reagieren.

Maschinelles Lernen und KI in der Endpoint Protection

Maschinelles Lernen:

- Ermöglicht es Sicherheitssystemen, aus früheren Bedrohungen zu lernen und zukünftige Angriffe effektiver zu erkennen und zu blockieren.

Beispiel:

- Automatische Erkennung von Phishing-Versuchen durch Analyse von E-Mail-Merkmalen und Vergleich mit bekannten Phishing-Indikatoren.

Maschinelles Lernen und KI in der Endpoint Protection

Künstliche Intelligenz (KI):

- Nutzt komplexe Algorithmen zur Analyse großer Datenmengen, um Muster zu erkennen, die auf potenzielle Sicherheitsbedrohungen hinweisen.

Beispiel:

- KI-gestützte Sicherheitsplattformen, die in der Lage sind, Zero-Day-Angriffe zu erkennen, indem sie Abweichungen von normalen Verhaltensmustern identifizieren.

Auswahl der richtigen Endpoint Protection Lösung

- Erkennungsrate
  - Berücksichtigung von unabhängigen Testergebnissen und Benchmarks
- Systemleistung
- Bewertung der Ressourcennutzung und des Einflusses auf die Endbenutzererfahrung
- Einfachheit der Installation, Konfiguration und des täglichen Managements
- Zugänglichkeit des Supports und Qualität der Dokumentation.
- Kompatibilität mit bestehenden Betriebssystemen und Anwendungen innerhalb der Organisation
- Kosten der Lösung im Vergleich zu den gebotenen Funktionen und dem Schutzniveau

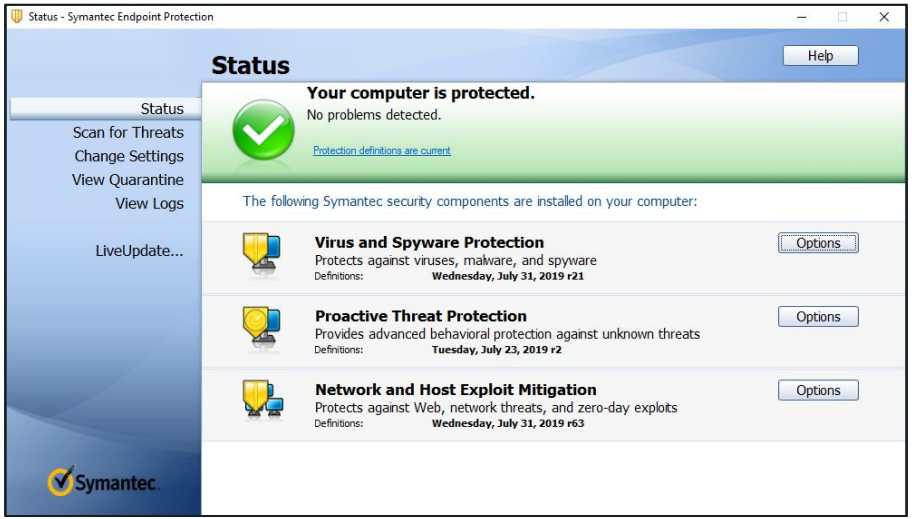
Gängige Endpoint Protection Lösungen

Symantec Endpoint Security (Broadcom):

- **Fortschrittlicher Bedrohungsschutz:**
  Nutzt maschinelles Lernen und Verhaltensanalyse
- **Intrusion Prevention:**
  Schützt vor Netzwerkbedrohungen
- **EDR-Fähigkeiten:**
  Bietet tiefgreifende Untersuchungen und Reaktionen auf Sicherheitsvorfälle
- **Zero-Day-Bedrohungserkennung:**
  Starke Leistung bei der Erkennung unbekannter Bedrohungen

Gängige Endpoint Protection Lösungen

Symantec Endpoint Security (Broadcom):



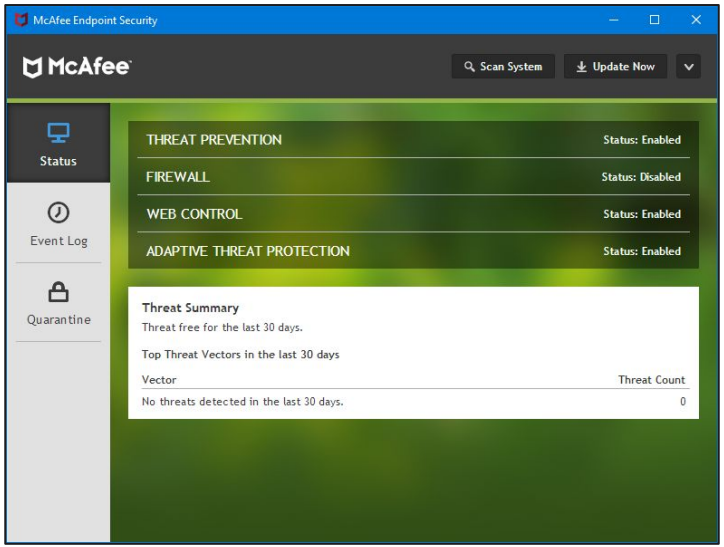
Gängige Endpoint Protection Lösungen

McAfee Endpoint Security:

- **Kombinierter Schutz:**
  Verbindet traditionelle und fortschrittliche Verteidigungsmechanismen
- **Cloud-Management:**
  Ermöglicht einfache Bereitstellung und Verwaltung
- **Integration:**
  Arbeitet nahtlos mit anderen McAfee-Produkten für einen koordinierten Sicherheitsansatz

Gängige Endpoint Protection Lösungen

McAfee Endpoint Security:



Gängige Endpoint Protection Lösungen

Microsoft Defender for Endpoint:

- **Integration ins Windows-Ökosystem:**
  Bietet tiefgreifenden Schutz für Windows-Geräte
- **Breites Spektrum an Sicherheitstechnologien:**
  Nutzt Verhaltenssensoren und maschinelles Lernen
- **Automatisierte Sicherheitsmaßnahmen:**
  Effektive Anomalieerkennung und Reaktion

Gängige Endpoint Protection Lösungen

CrowdStrike Falcon:

- **Cloud-native Architektur:**
  Bietet Echtzeitschutz mit leichtem Agenten
- **Künstliche Intelligenz und IOAs:**
  Stoppt Malware und malware-freie Angriffe durch Verhaltensanalyse
- **Leichte Agentenarchitektur:**
  Minimiert die Auswirkungen auf die Endpunkt-Leistung

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm