Secure Endpoint

Alle Wege führen zum Endpunkt: Egal, wie Malware in die Umgebung eines Unternehmens gelangt, Angreifer versuchen letztlich die Endpunkte zu infizieren. Der Schaden kann vom Verlust eines einzelnen Endpunkts bis zur Lahmlegung der gesamten IT-Infrastruktur reichen. Daher bildet ein effektiver Endpunktschutz ein Eckpfeiler des Sicherheitskonzeptes eines jeden Unternehmens.

Ausgangslage

In Zeiten, in denen viele Mitarbeiter standortunabhängig arbeiten und Malware immer heimtückischer wird, schützen herkömmliche Antivirenprogramme Endgeräte nur unzureichend.

Lösung

Moderne Endpunktsicherheitslösungen werden mit Blick auf Security Operations entwickelt und bieten Funktionen, die zur Unterstützung der täglichen Sicherheitsabläufe erforderlich sind. Diese Funktionen bestehen aus:

1. **Prevention:** Nutzen von globalen Bedrohungsdaten, um bekannte Malware zu blockieren. Statische und dynamische Dateianalysen (Sandboxing), um neue Malware zu erkennen.
2. **Detection:** Kontinuierliche Überwachung von Datei- und Systemaktivitäten auf neue Bedrohungen. Rückwirkende Warnung mit dem gesamten aufgezeichneten Verlauf der Datei bis zum Eintrittspunkt, falls etwas Neues entdeckt wird.
3. **Response:** Liefern von umfangreichen Kontextinformationen, die bei der Untersuchung eines potenziellen Sicherheitsverstosses benötigt werden. Diese Hilfestellung ermöglicht die Priorisierung bei Wiederherstellung und Reaktionsplänen.

Wichtigste Erkenntnisse

1. Endpunktsicherheit ist kein Endspiel, sondern eine wichtige Komponente einer umfassenderen Sicherheitsarchitektur, die Netzwerk, Identität, Cloud und E-Mail miteinbezieht.
2. Die neue Normalität: Hybride Arbeit und verschlüsselter Verkehr bedeuten einen verstärkten Fokus auf Endpunktsicherheit (>90% der detektierten Malware kommt über einen verschlüsselten Kanal an).

Darum Security by Netcloud
Dank unserer Erfahrung in den Bereichen Cyber Defence und Incident Response beherrschen unsere Security Engineers die Disziplin Endpoint Security bis ins kleinste Detail.

Weitere Infos:

Cisco Secure Endpoint (Formerly AMP for Endpoints)

Endpoint Protection - Palo Alto Networks

Microsoft Defender for Endpoint

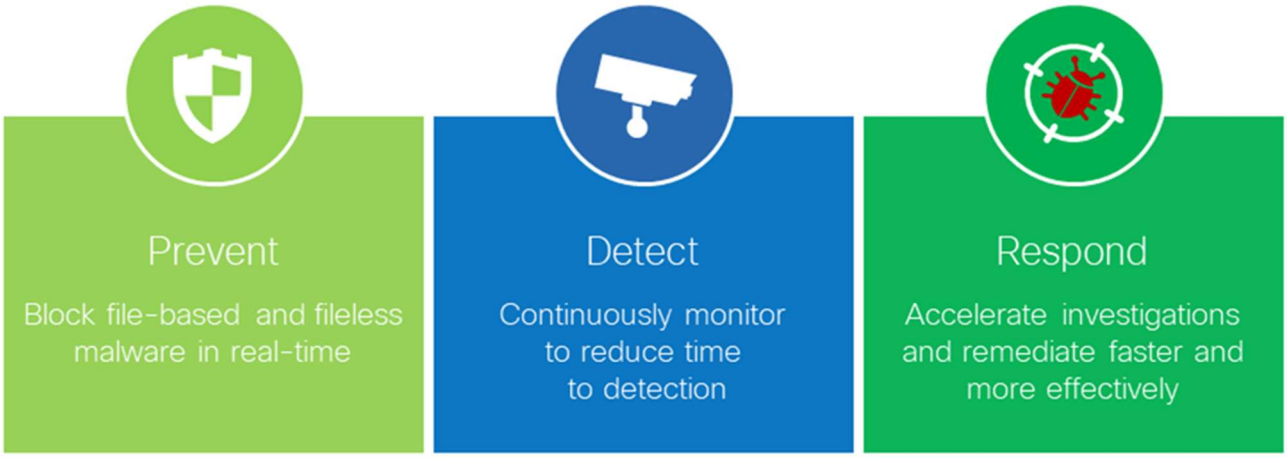

Abbildung 1: Bekämpfung des gesamten Lebenszyklus von moderner Malware – vor, während und nach einem Angriff.

Globale Bedrohungsdaten	- Sammlung und Teilen der neuesten Bedrohungsdaten durch Hersteller wie Cisco, Palo Alto und Microsoft. - Informationen werden genutzt, um komplexe Angriffe zu verstehen, zu priorisieren und abzuwehren.
Dynamische Malware-Analyse	- Analyse von Millionen von Malware-Beispielen jeden Monat. - Automatische Korrelation von Dateien, Verhalten, Telemetriedaten und Aktivitäten, um mit dieser Wissensbasis Malware schnell zu erkennen.
Kontinuierliche Überwachung	- Endpunktsicherheitslösungen wie Cisco Secure Endpoint, Palo Alto Cortex oder Microsoft Defender analysieren kontinuierlich Dateien und Datenverkehr auch nach der ersten Überprüfung.
Erkennung und Blockierung von Malware	- Analyse von Dateien am Eintrittspunkt, um bekannte und unbekannte Malware abzufangen und in Echtzeit zu blockieren.
Rückwirkende Sicherheit	- Im Falle eines Malware-Angriffs können die Security-Teams schnell nachvollziehen, was passiert ist. - Eindämmen von Malware indem verhindert wird, dass die Datei auf einem anderen Endpunkt erneut ausgeführt wird.
Erweitertes Sandboxing	- Automatische statische und dynamische Analyse von Dateien anhand von Hunderten von Verhaltensmerkmalen. - Aufdecken von heimlichen Bedrohungen und Unterstützung, um ausgeklügelte Angriffe zu verstehen, zu priorisieren und abzuwehren.