DATENBLATT

FireEye

FireEye Endpoint Security

Mehrere Abwehr-Engines über einen einzigen Agenten für eine effektive Defense-in-Depth-Strategie

VORTEILE

- Vereitelt die Mehrzahl der Cyberangriffe auf Endpunkte Ihres Unternehmens.
- Erkennt und blockiert Angriffe und trägt so zur Schadensbegrenzung bei.
- Ermöglicht produktivere und effizientere Sicherheitsprozesse, da Ihre Teams nicht länger mit Warnmeldungen überschwemmt werden und sich auf echte Bedrohungen konzentrieren können.
- Minimiert die Auswirkungen auf die Nutzer, da nur ein Agent mit geringem Ressourcenbedarf nötig ist.
- Erleichtert die Einhaltung von Datenschutzstandards wie PCI-DSS und HIPAA.
- Kann On-Premises oder in der Cloud bereitgestellt werden.

Herkömmliche Lösungen für die Endpunktsicherheit wurden nicht für komplexe Bedrohungen oder Advanced Persistent Threats (APT) entwickelt und bieten daher keinen ausreichenden Schutz. Deshalb benötigen Unternehmen eine effiziente Lösung, die derartige Bedrohungen schnell analysiert und sofort Gegenmaßnahmen einleitet.

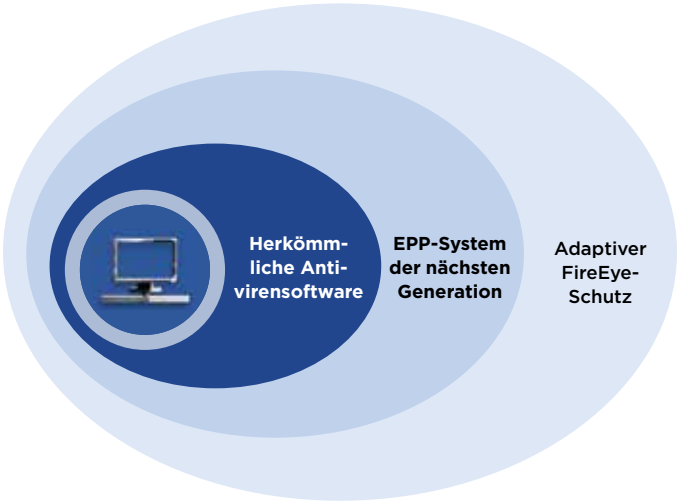
FireEye Endpoint Security erweitert die besten konventionellen Sicherheitslösungen um Technologie, Know-how und Bedrohungsdaten von FireEye, damit auch raffi-nierte Angriffe abgewehrt werden können. Dabei kommen vier verschiedene Engines zum Einsatz, die Bedrohungen effektiv identifizieren, eindämmen und eliminieren.

Zur Blockierung bekannter Malware wird eine signaturbasierte EPP-Engine (Endpoint Protection Platform) verwendet. Dagegen kommen bei der Erkennung von unbekannten und bisher signaturlosen Bedrohungen die lernfähigen, mit Erkenntnissen aus Incident-Response-Einsätzen gespeisten Schutzmechanismen von MalwareGuard zum Zug. Parallel dazu wird die Abwehr komplexer Bedrohungen durch eine Verhaltensanalyse-Engine mit EDR-Funktionen (Endpoint Detection and Response) unterstützt. Und schließlich beinhaltet Endpoint Security eine Echtzeit-IOC-Engine (Indicators of Compromise), die verborgene Gefahren anhand aktueller Bedrohungsdaten aus Incident-Response-Einsätzen aufdeckt. Diese Defense-in-Depth-Strategie trägt wesentlich zum Schutz wichtiger Daten auf den Endpunkten des Kundenunternehmens bei.

Doch auch mit den besten Schutzmaßnahmen sind Sicherheitsverletzungen nahezu unvermeidbar. Aus diesem Grund stellt Endpoint Security leistungsstarke Tools für eine effektive Reaktion bei minimaler Störung des Geschäftsbetriebs bereit. Damit können Sie ...

- innerhalb weniger Minuten Zehntausende Endpunkte auf bekannte und unbekannte Bedrohungen überprüfen,
- feststellen, welche Vektoren für den Hackerangriff auf den Endpunkt genutzt wurden,
- ermitteln, ob eine Bedrohung auf einem bestimmten Endpunkt aufgetreten ist, ob sie dort noch vorhanden ist und wohin sie sich ausgebreitet hat,
- den Verlauf und die Dauer der Infiltration von Endpunkten rekonstruieren und nachverfolgen sowie
- Endpunkte und Systeme identifizieren, die isoliert werden sollten, um eine weitere Ausbreitung im Netzwerk zu verhindern.

FLO



Manager denken häufig, dass jeder Virus gleich eine Katastrophe ist. Mit FireEye kann ich genau belegen, um welche Art von Bedrohung es sich gehandelt hat und wie wir sie erfolgreich bekämpft haben. Dass wir uns in Verdachtsfällen rasch Gewissheit verschaffen können, mindert den Druck auf alle Führungskräfte im Unternehmen.

– Michael Hennessy, Director Technology Services, Alpha Grainer Manufacturing, Inc

Wichtigste Features

- Die Implementierung eines einzigen Agenten mit vier Erkennungs-Engines ermöglicht eine optimale Bedrohungserkennung und -abwehr bei minimalem Konfigurationsaufwand.
- In Endpoint Security können alle Abläufe für die Bedrohungsanalyse und die Abwehr von Angriffen zu einem integrierten Workflow zusammengeführt werden.
- Die Lösung bietet vollständig integrierten Malware-Schutz basierend auf signaturbasierten Antivirussystemen, maschinellem Lernen, Verhaltensanalysen und der Überwachung von Endpunkten.
- Die Tools Triage Summary und Audit Viewer unterstützen die umfassende Untersuchung und Analyse auftretender Bedrohungen.

Weitere Features

- Enterprise Security Search unterstützt die schnelle Aufdeckung und Analyse verdächtiger Aktivitäten und möglicher Bedrohungen.
- Datenerfassungsfunktionen ermöglichen eine detaillierte Überprüfung und Analyse der Aktivitäten auf Endpunkten in einem spezifischen Zeitraum.
- Umfassende Transparenz erleichtert die schnelle Suche nach Bedrohungen sowie die Identifizierung und Einstufung akuter Gefahren durch Sicherheitsteams.
- Effektive Erkennungs- und Abwehrfunktionen beschleunigen die Identifizierung, Untersuchung und Isolierung infizierter Endpunkte und die Einleitung von Gegenmaßnahmen.
- Für die schnelle Analyse und Unterbindung verdächtiger Aktivitäten auf Endpunkten steht eine benutzerfreundliche Oberfläche zur Verfügung.

Unterstützte Betriebssysteme und Umgebungen	
Windows	XP SP3, 2003 SP2, Vista SP1 und höher, 2008, Win7, 2012, 8, 8.1, 10, Server 2016
Mac	OS X 10.9 und höher
Linux	Red Hat Enterprise Linux (RHEL) Versionen 6.8 und höher, 7.2 und höher CentOS Versionen 6.9 und höher, 7.4 und höher

Bereitstellungsoptionen: physische oder virtuelle On-Premises-Appliance oder FireEye-Cloudservice

Mehr Informationen zu FireEye erhalten Sie unter: **www.FireEye.de**

Telecom Liechtenstein AG
Schaanerstrasse 1
9490 Vaduz / Liechtenstein
security@telecom.li
+423 237 90 90

Über FL1

Als erster konvergenter Full-Service-Provider Liechtensteins ergänzt FL1 damit sein Portfolio sowie sein strategisches Geschäftsfeld um Managed Security Services der nächsten Generation. Im Mittelpunkt steht die zeitnahe Erkennung von Risiken für die Sicherheit der IT von Unternehmen und Behörden als Solution oder als Managed Service. Basis dafür ist eine hochmoderne, eigenentwickelte Technologie- plattform mit welcher Kunden ihr Cyber Defence Centre (CDC) aufbauen können oder die in Kombination mit Security-Analyseexperten, bewährten Prozessen und Best Practices als CDC as a Service zur Verfügung steht.