DATENBLATT

FireEye Endpoint Security

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

HIGHLIGHTS

- 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. Für wirklich effektiven Endpunktschutz benötigen Unternehmen eine Lösung, die derartige Bedrohungen schnell analysiert und sofort Gegenmaßnahmen einleitet.

FireEye Endpoint Security vereint die besten Funktionen konventioneller Sicherheitslösungen mit der modernsten Technologie, der Expertise und den Bedrohungsdaten von FireEye für effektiven Schutz vor aktuellen Bedrohungen. Dabei kommen vier verschiedene Engines zum Einsatz, die Bedrohungen effektiv identifizieren, eindämmen und eliminieren.

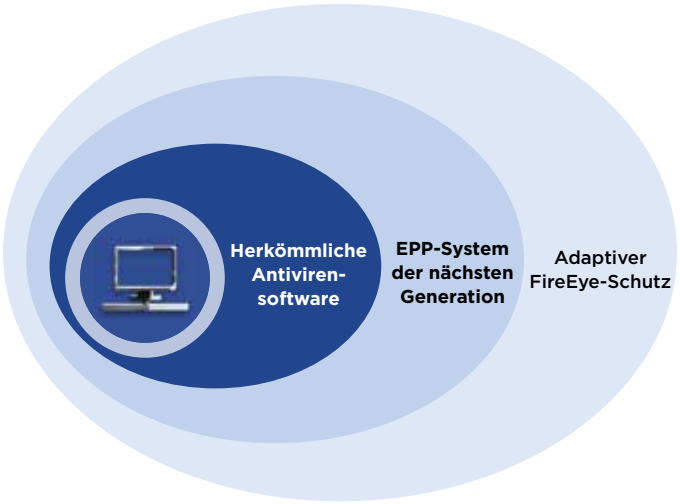
Zur Blockierung bekannter Malware wird eine signaturbasierte EPP-Engine (Endpoint Protection Platform) verwendet. Dagegen kommen bei der Erkennung von unbekannten und bisher signaturlosen Bedrohungen die lernfähigen, mit Erkenntnissen aus Incident-Response-Einsätzen gespeisten Schutzmechanismen von MalwareGuard 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.

IT spielt eine strategische Rolle bei der effektiven Ausbildung unserer Studierenden. Mit FireEye Endpoint Security können wir sicherstellen, dass unsere IT-Ressourcen verfügbar, funktionstüchtig und sicher sind. Das ist für die Realisierung unserer Zielsetzungen unerlässlich.

James D. Perry II
Chief Information Security Officer, University of South Carolina



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

- Minimiert den Konfigurationsaufwand und optimiert die Bedrohungserkennung und -abwehr mit vier Engines in einem einzigen Agenten.
- 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

ICSA labs CERTIFIED ANTI-VIRUS

vb 100 VIRUS virusbtn.com

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

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035, USA
+1 408 321 6300/+1 877-FIREEYE (347 3393)
info-dach@FireEye.com

© 2020 FireEye, Inc. Alle Rechte vorbehalten. FireEye ist eine eingetragene Marke von FireEye, Inc. Alle anderen Marken, Produkte oder Servicenamen sind Marken oder Dienstleistungsmarken der jeweiligen Eigentümer.
EP-EXT-DS-DE-DE-000018-04

Über FireEye, Inc.
FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye erweitert die Sicherheitskapazitäten seiner Kunden nahtlos und skalierbar und bietet über eine einheitliche Plattform die weltweit anerkannten Beratungsdienste von Mandiant®, innovative Sicherheitstechnologien und Bedrohungsdaten an, die denen staatlicher Sicherheitsbehörden in nichts nachstehen. Mit diesem Ansatz übernimmt FireEye die Verantwortung für die Vorbereitung von Kundenunternehmen auf die Erkennung und Abwehr von Cyberangriffen.

FIREEYE