FIREEYE™

DATENBLATT

FireEye Endpoint Security

Incident-Response-Erfahrungen helfen, weitere Angriffe zu stoppen

HIGHLIGHTS

- Vereitelt die meisten Cyberangriffe auf Endpunkte
- Erkennt und blockiert Angriffe und trägt so zur Schadensbegrenzung bei
- Steigert die Produktivität und Effizienz der Sicherheitsprozesse durch weniger, aber verlässlichere Warnmeldungen
- Minimiert die Auswirkungen auf die Benutzer mit nur einem Agenten mit geringem Ressourcenbedarf
- Unterstützt die Erweiterung von Schutz und Funktionalität durch das Herunterladen zusätzlicher Module
- Erleichtert die Einhaltung von Datenschutzstandards wie PCI-DSS und HIPAA
- Kann On-Premises oder in der Cloud bereitgestellt werden

Jeden Tag gibt es einen neuen Cyberangriff, eine neue Schwachstelle oder ein neues Ziel für Ransomware. Sicherheitsteams fällt es immer schwerer, sich über sämtliche Bedrohungen auf dem Laufenden zu halten, die die Benutzer, die Daten und das geistige Eigentum ihres Unternehmens gefährden könnten, und sie erhalten nicht immer die Hilfe, die sie benötigen. Auch die zahlreichen Tools, die sie nutzen, sind bei der Reaktion auf Vorfälle oft eher hinderlich als hilfreich, weil sie nicht ordentlich zusammenarbeiten und mehr irrelevante als nützliche Informationen liefern. Zudem verfügen die installierten Systeme vielerorts nicht über die erforderliche Funktionalität, um komplexe Bedrohungen zu erkennen und abzuwehren.

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. Es basiert auf einem Defense-in-Depth-Modell: Eine modulare Architektur mit standardmäßig verfügbaren Algorithmen kann durch zusätzlich heruntergeladene Module ergänzt werden, um die Infrastruktur noch besser zu schützen, mehr Bedrohungen zu erkennen und abzuwehren und die Endpunktsicherheit zu verwalten.

Bekannte Malware wird von einer signaturbasierten EPP-Engine (Endpoint Protection Platform) blockiert. 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. Zur Abwehr von Exploits, die Schwachstellen in gängigen Browsern und anderen Softwareprodukten ausnutzen, setzt ExploitGuard eine Engine zur Verhaltensanalyse ein, die derartige Exploits erkennt und ihre Ausführung verhindert. Darüber hinaus entwickelt FireEye kontinuierlich neue Module zur Erkennung und schnelleren Abwehr neu aufkommender Angriffstechniken und Bedrohungen. So unterbindet Process Guard beispielsweise das Ausschleusen von Anmeldedaten.

> 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

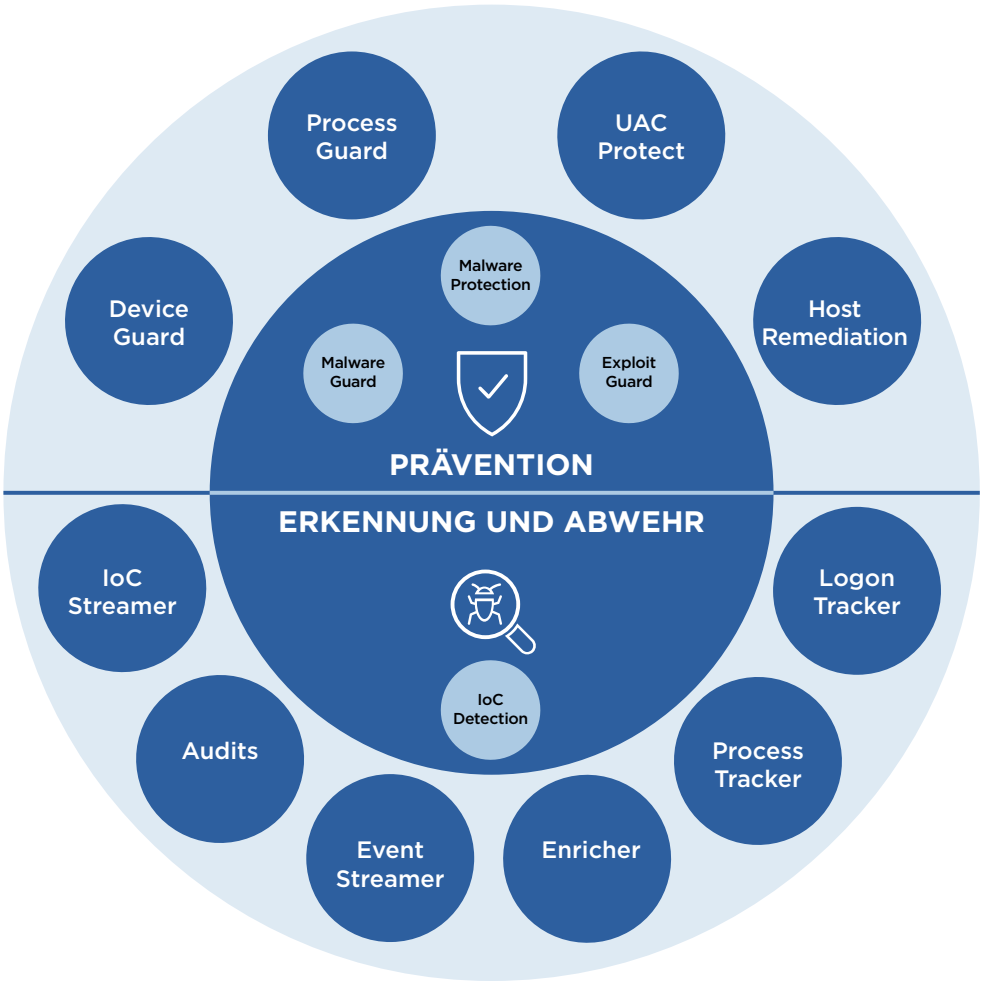
Doch auch mit den besten Schutzmaßnahmen sind Sicherheitsverletzungen nahezu unvermeidbar. Aus diesem Grund stellt Endpoint Security leistungsstarke Funktionen für eine effektive Reaktion bei minimaler Störung des Geschäftsbetriebs bereit, unter anderem zur Bedrohungserkennung und -abwehr an Endpunkten (EDR) und zur Echtzeitsuche nach Gefahrenindikatoren (IOCs), die von den Incident-Response-Teams von Mandiant bereitgestellt werden. Darüber hinaus können Sie mit den Tools von FireEye:

- innerhalb weniger Minuten Zehntausende Endpunkte auf bekannte und unbekannte Bedrohungen überprüfen,
- feststellen, welche Vektoren für einen Angriff auf einen 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, und
- den Verlauf und die Dauer der Infiltration von Endpunkten rekonstruieren und nachverfolgen.

Moderne Bedrohungen beschränken sich in der Regel nicht auf einen Endpunkt allein und können daher nicht erfolgreich mit Gegenmaßnahmen bekämpft werden, die sich nur auf einen Endpunkt konzentrieren. Stattdessen müssen alle Geräte, die von der Bedrohung betroffen sein könnten, in Echtzeit identifiziert und die Abwehrmaßnahmen auf all diesen Geräten koordiniert werden. Endpoint Security ist eine Komponente von FireEye Helix XDR und als solche nahtlos mit anderen Technologien und Services von FireEye verknüpft, um auch die raffiniertesten Bedrohungen effektiv zu erkennen und abzuwehren.

Abbildung 1:

Kern-Engines (innen) und optionale Module (außen) von FireEye Endpoint Security



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

- Ein zentraler Agent mit Defense-in-Depth 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 Malware-Schutz basierend auf Antivirusfunktionen, maschinellem Lernen, Verhaltensanalysen, Gefahrenindikatoren (IOCs) und der Überwachung von Endpunkten.
- Endpoint Security ermöglicht als Komponente von FireEye Helix XDR die Reaktion auf alle für eine Infrastruktur gefährlichen 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	Windows 7, 8, 8.1, 10 Server 2008R2, 2012R2, 2016, 2019
Mac	10.9 bis 10.15, 11
Linux	RHEL 6.8 bis 6.10, 7.1 bis 7.7, 8 bis 8.2 CentOS 6.9 bis 6.10, 7.1 bis 7.7 sowie 8 SUSE 11.3, 11.4, 12.2 bis 12.5 sowie 15 Open SUSE 15.1, 15.2 Ubuntu 12.04, 14.04, 16.04, 18.04, 19.04, 20.04, 20.10 Amazon Linux AMI 2018.3, AM2 Oracle Linux 6.10, 7.6, 8 (1 und 2)

Deployment-Optionen: physische oder virtuelle On-Premises-Appliance oder FireEye-Cloud-Service

SE Labs AAA Enterprise Endpoint Protection Jan-Mar 2021 · AV comparatives Approved Business Security Dec 2020 · vb100 Feb 2021 VIRUS virusbtn.com · OPSWAT. Access Control Certification Anti-Malware Gold

AV-TEST · MITRE · VirusTotal

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

Über FireEye

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™