DATENBLATT

FireEye Network Security

Wirksamer Schutz vor Cyberangriffen für mittelgroße und große Unternehmen

Überblick

FireEye Network Security ist eine effektive Cybersicherheitslösung, die komplexe, gezielte und im Internetverkehr versteckte Angriffe in Echtzeit aufdeckt und abwehrt und damit das Risiko kostspieliger Sicherheitsverletzungen senkt. Zudem liefert FireEye Network Security binnen weniger Minuten konkrete Beweise, verwertbare Daten und Handlungsempfehlungen für die effektive Behebung der aufgedeckten Sicherheitsvorfälle. Mit FireEye Network Security können Unternehmen sich effektiv vor Bedrohungen schützen – unabhängig davon, ob diese eine Schwachstelle in Windows, Apple OS X oder einer bestimmten Anwendung ausnutzen, ob der Hauptsitz oder eine Niederlassung angegriffen wird und wie gut die Bedrohung in dem umfangreichen eingehenden Internetdatenverkehr versteckt ist, der in Echtzeit überwacht werden muss.

Die Kernkomponenten der Lösung sind die MVX-Engine (Multi-Vector Virtual Execution™) und IDA (Intelligence-Driven Analysis).

Bei MVX handelt es sich um eine signaturunabhängige, dynamische Analyse-Engine, die das Netzwerk auf verdächtigen Verkehr prüft und so Angriffe erkennt, die konventionelle signatur- und regelbasierte Sicherheitssysteme umgehen. Mehrere kontextbezogene, auf dynamischen Regeln basierende ML-, KI- und Korrelations-Engines erkennen Angriffe mithilfe von Informationen zu Technologien, Angreifern und Opfern sowohl in Echtzeit als auch rückwirkend und wehren sie ab. Gleichzeitig greift FireEye Network Security auf ein herkömmliches IPS (Intrusion Prevention System) zurück, das bereits bekannte Angriffsmuster mithilfe eines konventionellen Signaturabgleichs erkennt.

FireEye Network Security ist in verschiedenen Formfaktoren bzw. als Service mit unterschiedlichen Bereitstellungs- und Leistungsoptionen erhältlich. Die Lösung wird normalerweise an der Schnittstelle zum Internet hinter den gängigen Netzwerksicherheitslösungen wie Firewalls der nächsten Generation, IPS und Secure Web Gateways (SWG) installiert. FireEye Network Security ergänzt diese Lösungen durch die rasche und zuverlässige Erkennung bekannter und unbekannter Bedrohungen. Es zeichnet sich insbesondere durch eine niedrige Anzahl an Fehlalarmen aus und versetzt Sicherheitsteams so in die Lage, effizient und effektiv auf jede Warnung zu reagieren.

Abbildung 1: Typische Konfiguration – Netzwerksicherheitslösungen

Leistungsmerkmale	Vorteile
Aufdeckung	
Zuverlässige Erkennung komplexer, gezielter und gut getarnter Cyberangriffe	Minimierung des Risikos kostspieliger Sicherheitsverletzungen
Modulare, skalierbare Sicherheitsarchitektur	Investitionsschutz und Unterstützung von Wachstumsphasen
Konsistenter Schutz für alle Internet-Zugangspunkte, auch in Umgebungen mit verschiedenen Betriebssystemen	Zuverlässiger Schutz für alle Gerätetypen im gesamten Unternehmen
Optionen für die integrierte oder verteilte, physische oder virtuelle sowie die unternehmensinterne oder cloudbasierte Bereitstellung	Flexibilität zur Anpassung an die individuellen Anforderungen und Ressourcen verschiedenster Unternehmen
Abgleich mehrerer Angriffsvektoren mit Daten aus Email Security und Content Security	Überwachung großer Angriffsflächen
Abwehr	
Unmittelbare Blockierung von Angriffen für Netzwerkverbindungen mit Bandbreiten von 250 Mbit/s bis 10 Gbit/s	Echtzeit-Schutz gegen gut getarnte Angriffe
Einblicke in verschlüsselten Datenverkehr	In Appliances integrierte Unterstützung für TLS 1.3-Entschlüsselung ohne zusätzliche Lizenzkosten verfügbar
Reaktion	
Niedriger Anteil von Fehlalarmen, Riskware-Kategorisierung und -Einordnung in das MITRE ATT&CK-Framework	Geringere Kosten für das Herausfiltern von unzuverlässigen Warnmeldungen
Unmittelbarer Übergang zur Untersuchung und Validierung von Warnmeldungen, ihrer Isolation auf dem betroffenen Endpunkt und der Einleitung geeigneter Gegenmaßnahmen	Automatisierung und Vereinfachung von Sicherheitsworkflows
Ausführungsnachweise und verwertbare Bedrohungsdaten	Schnellere Priorisierung und Behebung der aufgedeckten Sicherheitsvorfälle

Technische Vorteile

Zuverlässige, praxistaugliche Bedrohungserkennung und -informationen

FireEye Network Security nutzt verschiedene Analysemethoden, um Angriffe zuverlässig zu erkennen und den Anteil der Fehlalarme gering zu halten:

- Die **MVX-Engine** (Multi-Vector Virtual Execution™) erfasst Zero-Day-Exploits, Multi-Flow-Angriffe und andere gut getarnte Angriffe mithilfe einer dynamischen, signaturunabhängigen Analyse in einer sicheren, virtuellen Umgebung. Durch die Identifizierung bisher vollkommen unbekannter Exploits und Malware können Angriffe bereits in den ersten Phasen des Angriffszyklus gestoppt werden.
- **Mehrere, dynamische ML-, KI- und Korrelations-Engines** führen aufgrund der in Tausenden von Stunden von Incident-Response-Einsätzen gesammelten Erfahrungen kontextbezogene, regelbasierte Analysen von Echtzeitinformationen durch, um gut getarnte, gezielte und andere spezifische Angriffe zu erkennen und erfolgreich abzuwehren. Sie identifizieren schädliche Exploits, Malware, Phishing-Angriffe und Datenaustausch mit Command-and-Control-Servern. Dadurch können sie Aktivitäten in allen Angriffsphasen aufdecken und die Akteure daran hindern, Geräte zu infiltrieren und unter ihre Kontrolle zu bringen. Verdächtiger Netzwerkverkehr wird extrahiert und an die MVX-Engine zur Analyse weitergeleitet.
  Die Engines erkennen nicht nur clientseitige, sondern auch serverseitige Bedrohungen, die Ausbreitung im Netzwerk und Datenverkehr, der auf eine Ausschleusung gestohlener Daten hinweist.
- Die von FireEye Network Security generierten Warnmeldungen beinhalten konkrete verwertbare und kontextbezogene Daten, damit Teams umgehend auf Bedrohungen reagieren sowie diese priorisieren und eindämmen können. Zudem können erkannte Bedrohungen in das MITRE ATT&CK-Framework eingeordnet werden, um Kontextdaten zu gewinnen.

Unmittelbarer, zuverlässiger Schutz

FireEye Network Security bietet unter anderem folgende flexible Bereitstellungsmodi:

- Out-of-Band-Überwachung über TAP/SPAN, Inline-Überwachung sowie Inline mit aktiver Abwehr. Bei der Bereitstellung im Inline-Abwehrmodus werden eingehende Exploits und Malware automatisch abgewehrt sowie ausgehende Verbindungen über verschiedene Protokolle unterbunden. Dagegen werden im Inline-Überwachungsmodus lediglich Warnmeldungen generiert, wenn eine Bedrohung erkannt wird. Die Verantwortlichen des Unternehmens entscheiden dann, welche Gegenmaßnahmen angemessen sind. Im Out-of-Band-Schutzmodus löst FireEye Network Security TCP-Resets aus, um TCP- und HTTP-Verbindungen zu blockieren.
- Ausgewählte Modelle bieten aktive Hochverfügbarkeit, damit auch bei Netzwerk- oder Geräteausfällen zuverlässiger Schutz gewährleistet wird.

Vielseitiger und umfassender Schutz

FireEye Network Security bietet zuverlässigen Schutz für viele der derzeit verwendeten Netzwerkumgebungen:

- Unterstützung der meisten gängigen Versionen von Microsoft Windows und Apple Mac OS X
- Analyse von mehr als 160 verschiedenen Dateitypen, darunter PEs (Portable Executables), aktive Webinhalte, Archive, Abbildungen sowie Java-, Microsoft- und Adobe-Anwendungen und Multimedia-Dateien
- Ausführung verdächtiger Netzwerkpakete in zahlreichen Umgebungen mit unterschiedlichen Kombinationen aus Betriebssystem, Service Pack, IoT-Anwendungstyp und Anwendungsversion
- Schutz vor ausgefeilten Angriffen und komplexer Malware, die sich mit signaturbasierten Erkennungsmethoden nicht leicht aufdecken lassen, darunter Webshell-Uploads, über vorhandene Webshells ausgeführte Befehle, Ransomware und Krypto-Mining-Malware

Überprüfte und priorisierte Warnmeldungen

Neben der Erkennung von Angriffen wird die FireEye MVX-Technologie auch zur Überprüfung der Warnmeldungen konventioneller signaturabhängiger Sicherheitsvorkehrungen und zur Identifizierung und Priorisierung kritischer Bedrohungen eingesetzt:

- Wenn die von einem IPS (Intrusion Prevention System) generierten Warnmeldungen von der MVX-Engine überprüft werden, sinkt der Arbeitsaufwand für die Priorisierung der verbleibenden Warnmeldungen, da IPS oft viele Fehlalarme generieren.
- Mit der Kategorisierung von Riskware kann zwischen kritischen Sicherheitsverletzungen und unerwünschten, aber weniger gefährlichen Vorfällen (z. B. durch Adware und Spyware) unterschieden werden, um die Reaktion auf die verschiedenen Warnmeldungen zu priorisieren.

Integration in den Reaktionsworkflow

FireEye Network Security kann für die Automatisierung von Reaktionsworkflows bei Warnmeldungen ergänzt werden:

- **FireEye Central Management** gleicht die Warnmeldungen von FireEye Network Security und FireEye Email Security ab, um ein Gesamtbild des Angriffs zu erstellen und Abwehrregeln zu definieren, die eine Ausbreitung verhindern.
- **FireEye Network Forensics** ist mit FireEye Network Security verknüpft und bietet eine detaillierte Paketerfassung einschließlich Warnmeldungen und ermöglicht gründliche Untersuchungen.
- **FireEye Endpoint Security** identifiziert und prüft von FireEye Network Security erkannte Gefährdungen und isoliert diese, um die Eindämmung und Schadensbehebung an den betroffenen Endpunkten zu ermöglichen.

Flexible Bereitstellungsoptionen

FireEye Network Security bietet verschiedene Bereitstellungsoptionen für unterschiedliche Unternehmensanforderungen und -budgets:

- **Integrated Network Security:** eine All-in-one-Hardware-Appliance mit integriertem MVX-Dienst zum Sichern des Internet-Zugangspunkts an einem Standort. FireEye Network Security ist eine verwaltungsfreundliche Plattform ohne Client, die in kurzer Zeit einsatzbereit ist, ohne dass Regeln oder Richtlinien definiert oder Feineinstellungen vorgenommen werden müssen.
- **Distributed Network Security:** erweiterbare Appliances mit zentral genutztem MVX-Dienst zur Sicherung von Internet-Zugangspunkten im Unternehmen.
  - **Network Smart Nodes:** physische oder virtuelle Appliances, die den Internetverkehr analysieren, um schädlichen Verkehr zu identifizieren und abzuwehren und verdächtige Aktivitäten über eine verschlüsselte Verbindung an den MVX-Dienst für eine detaillierte Analyse weiterzuleiten.
  - **MVX Smart Grid:** unternehmensintern installierter, zentraler und flexibler MVX-Dienst, der transparente Skalierbarkeit, integrierte N+1-Fehlertoleranz und automatisiertes Load Balancing bietet.
  - **FireEye Cloud MVX:** von FireEye gehostetes MVX-Dienstabonnement, mit dem der Datenschutz über Analysen des Verkehrs auf dem Network Smart Node gewährleistet wird. Nur verdächtige Objekte werden über eine verschlüsselte Verbindung an den MVX-Dienst weitergeleitet, wo sie später umgehend gelöscht werden, falls sie sich bei der Analyse als harmlos erweisen.
  - **Zuverlässiger Schutz, On-Premises oder in der Cloud:** FireEye Network Security ist sowohl auf unternehmensinternen physischen und virtuellen Geräten als auch in öffentlichen Clouds (Amazon und Azure) verfügbar.

Abbildung 2: Ausgewählte Appliances für Integrated Network Security: NX 2550, NX 3500, NX 5500, NX 10550

Abbildung 3:

Modelle für eine verteilte Bereitstellung von Network Security

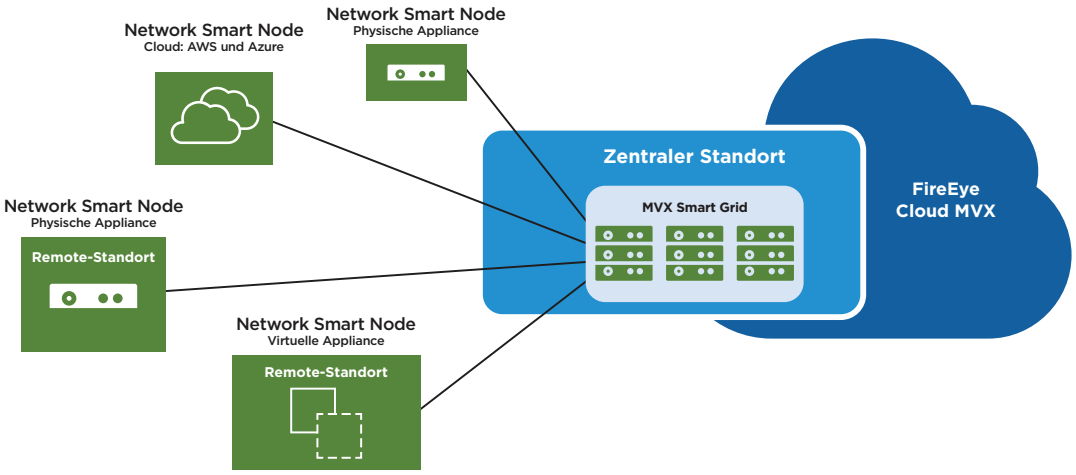

Abbildung 4:

Modulare Komponenten von FireEye Network Security

Herausragende Leistung und Skalierbarkeit

FireEye Network Security bietet verschiedene Leistungsoptionen für den Schutz von Internet-Zugangspunkten in den Zweigstellen und am Hauptsitz des Kundenunternehmens:

Dank der skalierbaren Architektur von MVX Smart Grid und FireEye Cloud MVX kann der MVX-Service Umgebungen jeder Größe unterstützen – von einem einzigen bis zu Tausenden von Network Smart Nodes.

Formfaktor	Durchsatz
Integrated Network Security	50 Mbit/s bis 5 Gbit/s
Physischer Network Smart Node	50 Mbit/s bis 10 Gbit/s
Virtueller und Public-Cloud-Network Smart Node	50 Mbit/s bis 8 Gbit/s

Mehrwert und Vorteile

FireEye Network Security bietet sowohl Unternehmen mit einem Standort als auch Unternehmen mit mehreren Standorten zahlreiche Vorteile:

Minimierung des Risikos von Sicherheitsverletzungen

FireEye Network Security ist eine äußerst effektive Cybersicherheitslösung zur …

- Unterbindung gezielter und gut getarnter Angriffe: Cyberkriminelle werden daran gehindert, das Unternehmensnetzwerk zu infiltrieren und dort wertvolle Daten zu stehlen oder den Geschäftsbetrieb zu stören.
- Eindämmung und Abwehr von Angriffen: Die Lösung liefert forensische Beweise und praxistaugliche Bedrohungsdaten, ermöglicht Inline-Abwehrmaßnahmen und unterstützt automatisierte Notfallprozesse.
- Behebung von Schwachstellen und Sicherheitslücken in der Infrastruktur des Unternehmens: An den Hauptstandorten und in den Zweigstellen werden Komponenten mit diversen Betriebssystemen und Anwendungen kontinuierlich geschützt.

Rasche Amortisierung

Laut einem von Forrester Consulting veröffentlichten Bericht[1] können Nutzer von FireEye Network Security mit beträchtlichen Einsparungen rechnen und dadurch eine Rendite von 152 Prozent in drei Jahren realisieren sowie die Amortisierung ihrer ursprünglichen Investition in nur 9,7 Monaten erwarten. Im Einzelnen bietet FireEye Network Security folgende Vorteile:

- Sicherheitsteams können sich auf tatsächliche Angriffe konzentrieren und so die Betriebskosten senken.
- Die Lösung fördert die optimale Nutzung getätigter Investitionen durch den gemeinsam genutzten MVX-Dienst und eine Vielzahl an Leistungsoptionen für die genaue Anpassung der Sicherheitsinfrastruktur an spezifische Anforderungen.
- Dank der nahtlosen Skalierbarkeit kann der Schutz auf neue Standorte ausgedehnt und an steigende Traffic-Volumen angepasst werden. Das ermöglicht zukunftsorientierte Investitionsstrategien.
- Die Möglichkeit zur kostenlosen Migration von einem integrierten zu einem verteilten Bereitstellungsmodell bietet Investitionssicherheit.
- Die modulare und erweiterbare Architektur minimiert künftige Investitionskosten.

1 Forrester (Mai 2016), „The Total Economic Impact Of FireEye"

Auszeichnungen und Zertifizierungen
Das Produktportfolio von FireEye Network Security hat bereits zahlreiche staatliche und Industriepreise erhalten:

- Bei der Naval Information Warfare Systems Command (NAVWAR) Artificial Intelligence Cybersecurity Challenge 2020 belegte FireEye den ersten Platz.[2]
- Ebenfalls 2020 zeichnete KuppingerCole FireEye mit dem Leadership Compass for Network Detection and Response aus.[3]
- Im selben Jahr stufte Forrester FireEye als großen Anbieter für Netzwerkanalysen und -transparenz ein.[4]
- Im Jahr 2018 führte Frost & Sullivan FireEye als unumstrittenen Marktführer auf und bezifferte den Marktanteil des Unternehmens auf 46 Prozent – mehr als die nachfolgenden zehn Anbieter zusammen.[5]
- FireEye Network Security wurde unter anderem gemäß den Common Criteria, FIPS 140-2 und SOC 2 zertifiziert.
- FireEye Network Security hat zahlreiche Auszeichnungen gewonnen, unter anderem von SANS Institute, SC Magazine und CRN.
- FireEye Network Security war die erste nach dem US Department of Homeland Security Safety Act zertifizierte Sicherheitslösung auf dem Markt.

2 FireEye (6. Januar 2021), Naval Information Warfare Systems Command (NAVWAR) Awards, FireEye: 1. Platz bei Network Threat Detection Challenge
3 KuppingerCole (10. Juni 2020), Leadership Compass Network Detection and Response
4 Forrester (23. Juni 2020), Now Tech: Network Analysis and Visibility, 2. Quartal 2020
5 Frost & Sullivan (5. Juli 2018): „Advanced Malware Sandbox (AMS) Solutions Market", Globale Prognose bis 2022

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™