

NETZWERKSICHERHEIT

WIRKSAMER SCHUTZ VOR CYBERANGRIFFEN FÜR UNTERNEHMEN ALLER GRÖSSEN

AKTUELLE HERAUSFORDERUNGEN IM BEREICH CYBERSICHERHEIT

Unternehmen müssen sich vor komplexen, gezielten und gut getarnten Angriffen und Sicherheitsverletzungen schützen. Das ist nicht immer einfach:

- Cyberkriminelle nutzen raffinierte Angriffsmethoden, um Next-Generation-Firewalls, IPS und Antivirensoftware zu umgehen und bewegen sich oft monatelang unentdeckt in Unternehmensnetzwerken. (2015 vergingen im Durchschnitt 320 Tage bis die Eindringlinge entdeckt wurden, wobei die betroffenen Unternehmen oft erst durch Dritte von der Infiltration erfuhren.)¹
- Mehr als 68 % der Malware-Varianten wurden für Angriffe auf bestimmte Unternehmen entwickelt und 80 % werden nur einmal eingesetzt.² Deshalb sind signaturbasierte Sicherheitssysteme gegen gezielte Angriffe wirkungslos.
- Über 80 % der Warnmeldungen, die von signatur- und regelbasierten Sicherheitslösungen generiert werden, sind gegenstandslos³ und nehmen wichtige Ressourcen in Anspruch, die für die Bearbeitung der eigentlich kritischen Warnmeldungen benötigt würden.

Die von den modernen Unternehmen angestrebte digitale Transformation verschärft diese Herausforderungen noch, da sie die Angriffsfläche vergrößert:

- Im Jahr 2020 werden mehr als zwei Drittel der IT-Ausgaben von Unternehmen in Public-Cloud-Anwendungen fließen.⁴ Durch die Einführung cloudbasierter Lösungen nimmt der ein- und ausgehende Internetverkehr eines Unternehmens – und damit die potenzielle Angriffsgefahr – um 40 % zu.⁵ Doch auch dieses gesteigerte Datenverkehrsvolumen muss in vollem Umfang überwacht werden.
- In 96 % der Unternehmen werden inzwischen Geräte genutzt, die ein anderes Betriebssystem als Windows verwenden.⁶ Diese Geräte sind jedoch üblicherweise weniger stark gesichert.
- Für 40 % der Zweigstellen⁵ wurde eine direkte Internetverbindung eingerichtet, wodurch sich das Angriffsrisiko außerhalb des gut geschützten Hauptsitzes vergrößert.

VIER ANFORDERUNGEN AN CYBERSICHERHEITSLÖSUNGEN

Unternehmen aller Größen benötigen eine Lösung, die sie effektiv vor Angriffen schützt und das Risiko eines erfolgreichen Hackereintritts minimiert. Eine solche Lösung muss folgende Vorteile bieten:

1. Funktionen zur Erkennung und Abwehr von Bedrohungen, die von herkömmlichen Sicherheitssystemen nicht erfasst werden
2. Die Möglichkeit, rasch auf Sicherheitsvorfälle zu reagieren und deren Folgen einzudämmen

3. Die Fähigkeit zur kontinuierlichen Anpassung an die sich ständig ändernde Bedrohungslage
4. Verlässliche Skalierbarkeit und Flexibilität, wenn Ihr Unternehmen wächst oder sich der Bereitstellungsmodus von IT-Services ändert

FIREEYE NETWORK SECURITY

FireEye Network Security hilft Unternehmen aller Größenordnungen dabei, das Risiko kostspieliger Sicherheitsverletzungen zu senken. Die Lösung erkennt und stoppt komplexe, gezielte und im normalen Internet-Datenverkehr versteckte Angriffe unmittelbar. Bei ihren beiden Kernkomponenten handelt es sich um die MVX-Engine (Multi-Vector Virtual Execution™) und um IDA-Technologien (Intelligence-Driven Analysis). MVX ist eine signaturunabhängige, dynamische Analyse-Engine, die verdächtige Objekte untersucht und dadurch gezielte, getarnte und unbekannte Bedrohungen aufdeckt. Die IDA-Engines erkennen und blockieren schädliche Objekte anhand von Bedrohungsdaten aus verschiedensten Quellen: Sensoren, Angreiferbeobachtung und Incident-Response-Einsätzen.

FireEye Network Security ist in mehreren Formfaktoren sowie mit unterschiedlichen Bereitstellungsoptionen 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.

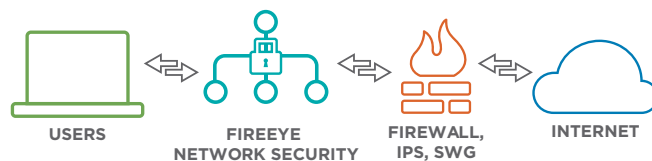


ABBILDUNG 1: TYPISCHE IMPLEMENTIERUNG DER NETZWERKSICHERHEITSLÖSUNGEN

FireEye Network Security bietet kleinen, mittleren und großen Unternehmen, die sich vor Sicherheitsverletzungen schützen wollen, die folgenden Vorteile:

- **Präzise Bedrohungserkennung:** Die MVX und die IDA-Technologien erkennen Angriffe mit hoher Genauigkeit und generieren nur eine geringe Quote von Fehlalarmen. Sie decken Zusammenhänge zwischen Ereignissen aus verschiedenen Datenströmen und auf diversen Bedrohungsvektoren auf.

Dadurch bieten sie Schutz vor mehrstufigen Angriffen, die von anderen Sicherheitslösungen nicht erfasst oder nicht abgewehrt werden können.

- **Unmittelbarer, zuverlässiger Schutz:** Bei der Inline-Implementierung werden eingehende Exploits und Malware automatisch abgewehrt und ausgehende Callbacks über verschiedene Protokolle unterbunden. Bei Nutzung der Hochverfügbarkeitsoption bleibt der Schutz auch dann bestehen, wenn eine Netzverbindung oder ein Gerät ausfällt.
- **Praxistaugliche Informationen:** Die Warnmeldungen von FireEye Network Security beinhalten verwertbare und kontextbezogene Daten, die von unseren erfahrenen Experten zusammengestellt wurden und es Ihnen ermöglichen, Angriffe rasch abzuwehren, Gegenmaßnahmen zügig zu priorisieren und Bedrohungen schnell einzudämmen.
- **Einspeisung von Bedrohungsindikatoren:** Die Nutzung des STIX-Formats (Structured Threat Intelligence eXpression) ermöglicht die Einspeisung von Bedrohungsdaten aus beliebigen Quellen in die IDA-Engines.
- **Erweiterbare Architektur** Dank des speziellen Designs der Software und des Systems können diverse Technologien zur Bedrohungsabwehr als Softwaremodule implementiert und bereitgestellt werden.



- **Umfassender Schutz:** Es werden diverse Umgebungen unterstützt, zum Beispiel die gängigsten Microsoft Windows- und Apple OS X-Betriebssysteme, sowie über 140 unterschiedliche Dateitypen und Tausende Kombinationen von Betriebssystemen, Service Packs und Anwendungen. Dadurch lassen sich Infrastrukturen verschiedenen Zuschnitts schützen.
- **Integration in die Prozesse zur Bedrohungsabwehr:** Mithilfe der Funktionen zur Validierung von Warnmeldungen, zur Kategorisierung von Riskware und zur extrem schnellen Paketerfassung mit anschließender Analyse können die Prozesse zur Bearbeitung von Warnmeldungen gestrafft und automatisiert werden.

DIE PERFEKTE LÖSUNG FÜR IHR UNTERNEHMEN

FireEye Network Security ist für einen Datendurchsatz von bis zu 8 Gbit/s ausgelegt und unterstützt flexible, skalierbare Bereitstellungsmodelle. Dadurch wird die Lösung auch den Anforderungen und Budgets mittlerer und großer Unternehmen gerecht.

- **Integrated Network Security:** Bereitstellung in Form einer eigenständigen, All-in-one-Hardware-Appliance, die mithilfe des MVX-Dienstes einen einzelnen Internetzugangspunkt sichert.
- **Distributed Network Security:** Mit Network Smart Nodes und dem gemeinsam genutzten MVX-Dienst wird das gesamte Unternehmen geschützt.
 - **Network Smart Nodes:** physische oder virtuelle Appliances, die an Internetzugangspunkten installiert werden, um verdächtige Aktivitäten zu identifizieren und zu blockieren.
 - **MVX Smart Grid oder FireEye Cloud MVX:** unternehmensintern installierter oder cloudbasierter MVX-Dienst, der tief greifende Analysen durchführt, um komplexe Angriffe aufzudecken und den Sicherheitsteams ein effizienteres Arbeiten zu ermöglichen

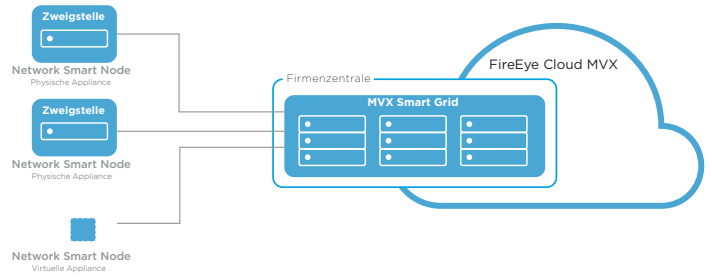


ABBILDUNG 2: DISTRIBUTED NETWORK SECURITY

FireEye Network Security Essentials bietet kleinen und mittleren Unternehmen kostengünstige, integrierte und verteilte Bereitstellungsmodelle mit einer Bandbreite zwischen 10 Mbit/s und 2 Gbit/s.

	BEREITSTELLUNGSOPTIONEN			
	Integrierte Appliance	Network Smart Node	MVX Smart Grid NETWORK SMART NODES ERFORDERLICH	FireEye Cloud MVX NETWORK SMART NODES ERFORDERLICH
FireEye Network Security für mittlere bis große Unternehmen	On-Premise	Physisch oder virtuell	On-Premise und verteilt	Cloud-basiert und verteilt
FireEye Network Security Essentials für kleine und mittlere Unternehmen	On-Premise	Physisch oder virtuell	Nicht verfügbar	Cloud-basiert und verteilt

TABELLE 1: BEREITSTELLUNGSOPTIONEN FÜR FIREEYE NETWORK SECURITY

RASCHE AMORTISIERUNG

FireEye Network Security wurde sowohl für die Anforderungen von Unternehmen mit nur einem Standort als auch für die Anforderungen von Unternehmen mit mehreren Standorten entwickelt. Die Lösung minimiert das Risiko einer Sicherheitsverletzung und amortisiert sich in kürzester Zeit.

Laut einem kürzlich veröffentlichten Bericht von Forrester Consulting⁷ können Kunden von FireEye Network Security eine Rendite von 152 % in drei Jahren sowie die Amortisierung ihrer ursprünglichen Investition in nur 9,7 Monaten erwarten. Zudem bietet die Lösung die folgenden Vorteile, die dauerhafte Kosteneinsparungen ermöglichen:

- die Entlastung von Sicherheitsexperten, die sich dann auf die Abwehr tatsächlich stattfindender Angriffe konzentrieren können
- die optimale Nutzung getätigter Investitionen durch den gemeinsam genutzten MVX-Dienst und eine Vielzahl an Leistungsoptionen für die genaue Anpassung der Bereitstellung an spezifische Anforderungen
- die langfristige Nutzung der angeschafften Sicherheitslösungen durch die Möglichkeit zur nahtlosen Skalierung, wenn die Anzahl der Standorte wächst oder das Volumen des Internetverkehrs zunimmt
- Investitionssicherheit durch die Möglichkeit zur kostenlosen Migration von einer integrierten zu einer verteilten Bereitstellung
- die Minimierung zukünftiger Investitionskosten durch eine modulare und erweiterbare Architektur

WAS SPRICHT FÜR FIREEYE NETWORK SECURITY?

Die FireEye MVX-Engine ist die erfolgreichste⁸ Lösung zum Schutz vor komplexen Angriffen, die derzeit auf dem Markt verfügbar ist:

- Seit 2013 hat FireEye mehr praktisch erfolgreiche Zero-Day-Angriffe aufgedeckt als alle anderen Lösungen zusammen.
- Im Jahr 2016 führte Frost & Sullivan FireEye als unumstrittenen Marktführer auf und bezifferte den Marktanteil des Unternehmens auf 56 % - mehr als die nachfolgenden zehn Anbieter zusammen.⁹
- FireEye Network Security hat zahlreiche Auszeichnungen gewonnen, unter anderem vom 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.



DIE VORTEILE VON FIREEYE NETWORK SECURITY IM ÜBERBLICK

Feature	Vorteil
Funktionen zur Erkennung und Abwehr von Bedrohungen, die von herkömmlichen Sicherheitssystemen nicht erfasst werden	
Signaturunabhängige Bedrohungserkennung (MVX)	Erkennt mehrstufige, polymorphe, Multi-Flow-, Zero-Day-, Ransomware- und andere Angriffe
Echtzeit- und nachträgliche Erkennung	Erkennt bekannte und unbekannte Bedrohungen in Echtzeit und rückwirkend
Abgleich mehrerer Angriffsvektoren	Automatisiert die Validierung und Blockierung von Angriffen über mehrere Vektoren hinweg
Unterstützung verschiedener Betriebssysteme, Anwendungen und Dateitypen	Unterstützt heterogene Endpunktumgebungen für zahlreiche unterschiedliche Anwendungen
Abgesicherter Hypervisor	Schützt vor Umgehungstechniken
Rasche Reaktion auf Vorfälle und effektive Eindämmung ihrer Folgen	
Inline-Abwehr in Echtzeit	Wehrt Angriffe unmittelbar ab
Integrierte Sicherheitsprozesse	Ermöglicht den direkten Übergang von der Erkennung zur Untersuchung und Abwehr
Hochverfügbarkeit	Bietet robuste Sicherheit
Signaturabhängige IPS-Erkennung und weniger Fehlalarme	Überprüft Warnmeldungen schnell und automatisch, sodass der manuelle Arbeitsaufwand reduziert wird
Erkennung und Kategorisierung von Riskware	Identifiziert kritische und weniger gefährliche Malware, sodass die gefährlichsten Varianten zuerst bekämpft werden können
Verwertbare, kontextbezogene Bedrohungsdaten	Beschleunigt die Eindämmung komplexer Bedrohungen dank detaillierter Informationen zum Angriff und den Angreifern

Feature	Vorteil
Kontinuierliche Anpassung an die sich ständig ändernde Bedrohungslage	
Weltweiter Austausch von Bedrohungsdaten in Echtzeit	Bezieht zuverlässige Bedrohungsdaten, mit denen sich bislang unbekannte Angriffe stoppen und Abwehrmaßnahmen beschleunigen lassen
Bedrohungsdaten im STIX-Format* aus eigener Quelle und von Drittanbietern	Ermöglicht die Einspeisung der Gefahrenindikatoren von FireEye und Drittanbietern in die STIX-kompatiblen IDA-Engines
Strategische Bedrohungsdaten	Unterstützt die vorausschauende Bewertung von Änderungen der Bedrohungslage und eine proaktive Sicherheitsstrategie
Verlässliche Skalierbarkeit und Flexibilität, wenn Ihr Unternehmen wächst oder sich der Bereitstellungsmodus von IT-Services ändert	
Unterstützte Bandbreiten	10 Mbit/s - 8 Gbit/s
Abdeckung	Von einem Standort bis zu Tausenden Standorten (bei verteilter Bereitstellung)
Unterstützte Formfaktoren	Physisch, virtuell oder cloudbasiert
Bereitstellungsoptionen	Integrated Network Security und Distributed Network Security mit Network Smart Nodes und MVX-Service

Lesen Sie mehr darüber, wie Sie Ihr Unternehmen mit der äußerst präzisen, adaptiven und skalierbaren Lösung von FireEye vor Cyberangriffen schützen können.

- [1 FireEye, Februar 2016: M-Trends 2016.](#)
- [2 Joshua Goldfarb, 19. September 2016: Detection Innovations.](#)
- [3 Ponemon Institute, Januar 2015: The Cost of Malware Containment.](#)
- [4 Forrester, September 2016: The Public Cloud Services Market Will Grow Rapidly to \\$236 Billion in 2020.](#)
- [5 IDC, Februar 2016: Communication Service Provider Adoption of SD-WAN Technology and Its Impact to MPLS VPN Services.](#)
- [6 JAMF Software, 2015: 2015 Survey: Managing Apple Devices in the Enterprise.](#)
- [7 Forrester, Mai 2016: The Total Economic Impact Of FireEye.](#)
- [8 IDC, 2015: Worldwide Specialized Threat Analysis and Protection Market Shares.](#)
- [9 Frost & Sullivan, September 2016: Network Security Sandbox Market Analysis](#)

FireEye, Inc.
 1440 McCarthy Blvd. Milpitas, CA 95035, USA
 +1 408 321 6300/+1 877-FIREEYE (347 3393)/info@FireEye.com

www.FireEye.de

