FireEye

Wie Sie neuartigen Angriffen auf Ihr Netzwerk Paroli bieten

Erkennen Sie Bedrohungen, die anderen Lösungen entgehen

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 bleiben oft monatelang unbemerkt. (In Unternehmen, die durch Dritte auf Angreifer aufmerksam gemacht wurden, geschah das 2015 im Durchschnitt 320 Tage nach dem ersten Eindringen.)[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 gegenstandslos[3] und nehmen wichtige Ressourcen in Anspruch, die für die Bearbeitung der eigentlich kritischen Warnmeldungen benötigt würden.

Die von 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] Doch durch die Nutzung cloudbasierter Lösungen nimmt der ein- und ausgehende Internetverkehr eines Unternehmens– und damit die potenzielle Angriffsgefahr – um 40% zu.[5] Deshalb darf der höhere Durchsatz das Sicherheitsniveau nicht senken.
- In 96% der Unternehmen werden inzwischen Geräte genutzt, die ein anderes Betriebssystem als Windows verwenden.[6] Diese Geräte wurden bislang meist weniger stark gesichert.
- Für 40% der Zweigstellen[5] 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 Hackereinbruchs minimiert. Eine solche Lösung muss folgende Vorteile bieten:

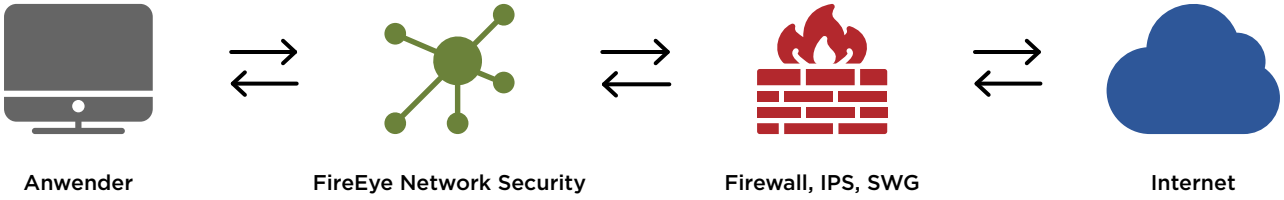
1. Funktionen zur Erkennung und Abwehr von Bedrohungen, die von herkömmlichen Sicherheitssystemen nicht erfasst werden
2. Rasche Reaktion auf Vorfälle und effektive Eindämmung ihrer Folgen
3. Kontinuierliche Anpassung an die sich ständig ändernde Bedrohungslage
4. Verlässliche Skalierbarkeit und Flexibilität, 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. Ihre Kernkomponenten sind die MVX- (Multi-Vector Virtual Execution™) und IDA-Engines (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-Einsätze.

FireEye Network Security ist in verschiedenen Baugrößen 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.

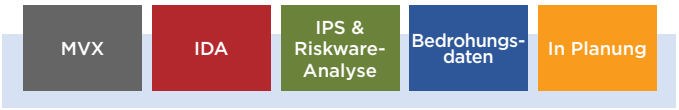
1 FireEye, Februar 2016: M-Trends 2016.
2 Joshua Goldfarb, 19. September 2016: „Detection Innovations“
3 Ponemon Institute, Januar 2015: „The Cost of Malware Containment“
4 Forrester, September 2016: „The Public Cloud Services Market Will Grow Rapidly to $236 Billion in 2020“
5 IDC, Februar 2016: „Communication 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“

Abbildung 1: Typische Konfiguration – 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-Engines erkennen Angriffe zuverlässig 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.
- **Aufschlussreiche Einblicke:** Die Warnmeldungen von FireEye Network Security beinhalten konkrete 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.



NEU
- **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.

NEU
- **Distributed Network Security:** Mit Network Smart Nodes und dem gemeinsam genutzten MVX-Dienst wird das gesamte Unternehmen geschützt.
  - **Network Smart Node:** physische oder virtuelle Appliances, die an Internetzugangspunkten installiert werden, um verdächtige Aktivitäten zu identifizieren und zu blockieren.

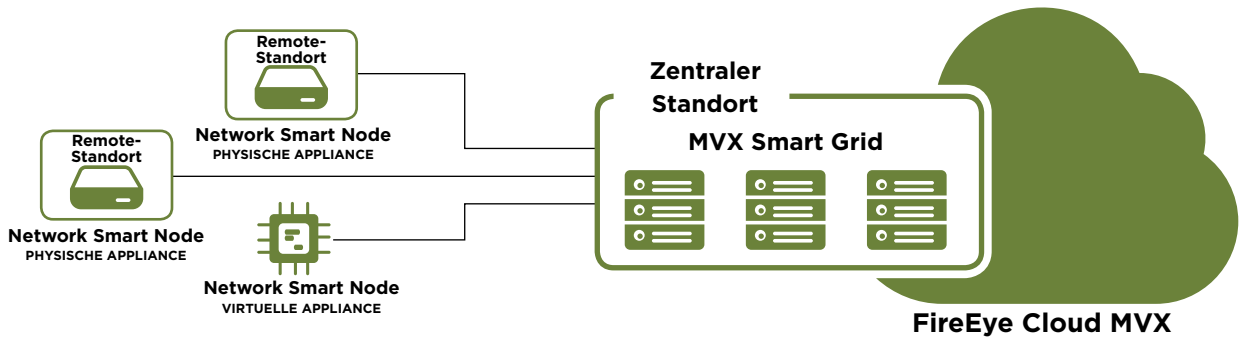


Abbildung 1: Distributed Network Security

Tabelle 1: Bereitstellungsoptionen für FireEye Network Security

	Integrierte Appliance	Network Smart Node	MVX Smart Grid Network SmartNodes erforderlich	FireEye Cloud MVX Network SmartNodes erforderlich
FireEye Network Security für mittlere bis große Unternehmen	On-Premises	Physisch oder virtuell	On-Premises und verteilt	Cloudbasiert und verteilt
FireEye Network Security Essentials für kleine und mittlere Unternehmen	On-Premises	Physisch oder virtuell	Nicht verfügbar	Cloudbasiert und verteilt

- **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.

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.

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 Consulting[7] 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 können durch folgende Vorteile dauerhaft Kosten eingespart werden:

- 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 erfolgreichste[8] Lösung zum Schutz vor komplexen Angriffen, die derzeit auf dem Markt verfügbar ist:

- Seit 2013 hat FireEye mehr aktive Zero-Day-Angriffe erfasst 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 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.

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"

Tabelle 2: Die Vorteile von FireEye Network Security im Überblick

Funktion	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
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
NEU **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
Reichweite	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

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, Inc.

FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye fungiert als nahtlose und skalierbare Erweiterung der Sicherheitsumgebung seiner Kunden 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 hat mehr als 6.600 Kunden in 67 Ländern, darunter über 45 Prozent der Forbes-Global-2000-Unternehmen.

FireEye®