

DATENBLATT

FireEye Helix

Erkennungsfunktionen und Bedrohungsdaten von Weltklasse für moderne Sicherheitsteams



HIGHLIGHTS

- Erkennung komplexer Bedrohungen:** Die Kombination von über 600 Sicherheitstools von FireEye und anderen Anbietern ermöglicht eine detaillierte Übersicht über die Sicherheitslage, die durch kontextbezogene Bedrohungsdaten und Analysefunktionen noch verbessert wird.
- Schadensbegrenzung:** Die von erfahrenen Experten entwickelte Lösung ermöglicht die Koordinierung und Automatisierung von Sicherheitsprozessen und unterstützt dadurch schnellere Reaktionen auf Bedrohungen.
- Umfassende Einblicke in alle Angriffsvektoren und die aktuelle Bedrohungslage:** Mit der SIEM-Lösung der nächsten Generation können Sie alle sicherheitsrelevanten Daten zusammenführen, um sich einen detaillierten Überblick über die Bedrohungen und Schwachstellen in Ihrer gesamten On-Premises-Infrastruktur und allen Cloud-Umgebungen zu verschaffen.

Einleitung

Cybersicherheit war nie eine größere Herausforderung als heute. Da fast täglich neue Bedrohungen bekannt werden, sehen sich Unternehmen gezwungen, in immer neue Sicherheitslösungen zu investieren und immer mehr IT-Sicherheitsexperten einzustellen. Dieses reaktive Vorgehen führt dazu, dass die Komplexität der Sicherheitsinfrastruktur rasant zunimmt, wodurch wiederum eine weitere Schwachstelle entsteht, die von Angreifern ausgenutzt werden kann. Moderne Sicherheitsmaßnahmen – für komplexe ebenso wie für von Natur aus übersichtliche Umgebungen – erfordern einen umfassenden, grundlegenden Ansatz. Mit FireEye Helix können Unternehmen das Fundament dafür schaffen.

Die cloudbasierte SaaS-Sicherheitsplattform FireEye Helix ermöglicht das Management aller Sicherheitsvorfälle – von der ersten Identifizierung einer Bedrohung bis zur Abwehr. Mithilfe der bereitgestellten Bedrohungsdaten sowie durch die Integration sämtlicher Sicherheitstools und deren Erweiterung um Orchestrierungs- und SIEM-Funktionen der nächsten Generation lässt sich das volle Potenzial bestehender Sicherheitslösungen erschließen. FireEye Helix wurde von Sicherheitsexperten für Sicherheitsexperten entwickelt und bietet Sicherheitsteams unter anderem leistungsstarke Funktionen für das Management von Warnmeldungen sowie für die Bedrohungssuche, die Analyse und forensische Untersuchung von Angriffen und die Berichterstellung.

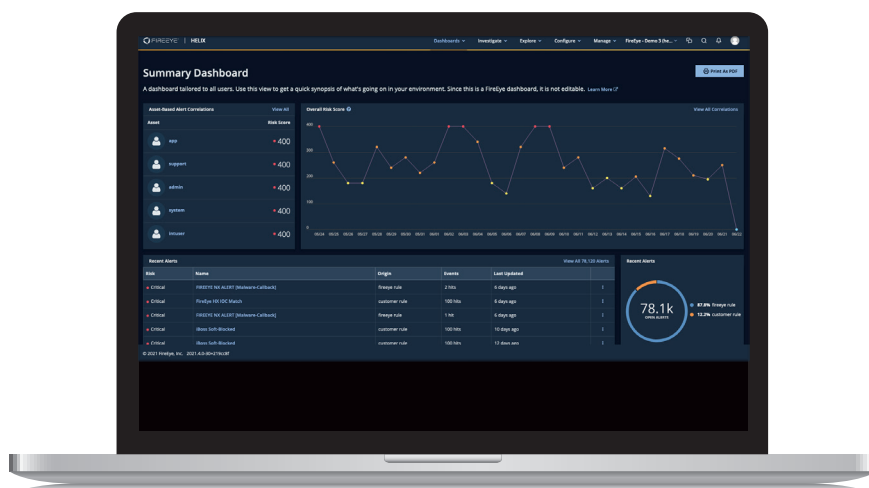


Abbildung 1: Die übersichtliche Konsole bietet aktuelle Informationen über die Sicherheitslage auf einen Blick.

● ● ●
**FireEye Helix:
 Funktionen**



Erkennung von Sicherheitsvorfällen durch Abgleich der Daten aus verschiedenen Tools



Bereitstellung kontextbezogener Bedrohungsdaten für fundierte, effiziente Entscheidungsprozesse



Zusammenführung von Sicherheitsdaten und Konsolidierung der Infrastruktur



Bedrohungsdaten

Sie erhalten Daten und Informationen über erfasste Cyberbedrohungen, die Sie anreichern und analysieren können.



SIEM der nächsten Generation

Ausgefeilte Nutzer- und Verhaltensanalysen verbessern die Bedrohungs- und Schwachstellenerkennung.



SOAR (Security Orchestration and Automation)

Playbooks, die von unseren erfahrenen Experten erstellt wurden, ermöglichen automatisierte Prozesse für die Reaktion auf Bedrohungen.



Analysen des Anwender- und Objektverhaltens (User and Entity Behavior Analytics, UEBA)

Die Kombination aus Warnmeldungen und maschinellen Lernalgorithmen ermöglicht Ihnen, Aktivitäten zu identifizieren, die auf eine Insider-Bedrohung, eine Ausbreitung im Netzwerk oder einen Angriff in der Endphase hinweisen.



Workflow-Management

Automatische und manuelle Workflows erleichtern die Organisation, Zuordnung, Abstimmung und Durchführung der einzelnen Schritte bei der Untersuchung von Vorfällen.



Compliance-Berichte

Die bereitgestellten Dashboards und Widgets zur visuellen Zusammenfassung, Darstellung und Analyse der wichtigsten Informationen lassen sich einfach an Ihre spezifischen Anforderungen anpassen.

So erhalten Sie FireEye Helix

FireEye Helix ist beim Kauf von Abonnements für FireEye-Lösungen erhältlich. Die Plattform ist mit allen Technologien von FireEye und den bereits installierten Sicherheitsprodukten anderer Anbieter kompatibel. Wenn Ihr Unternehmen wächst und sich verändert, können Sie FireEye-Lösungen ohne Beeinträchtigung des Geschäftsbetriebs neu konfigurieren, hinzufügen oder erweitern.

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 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.

