FIREEYE™

WHITEPAPER

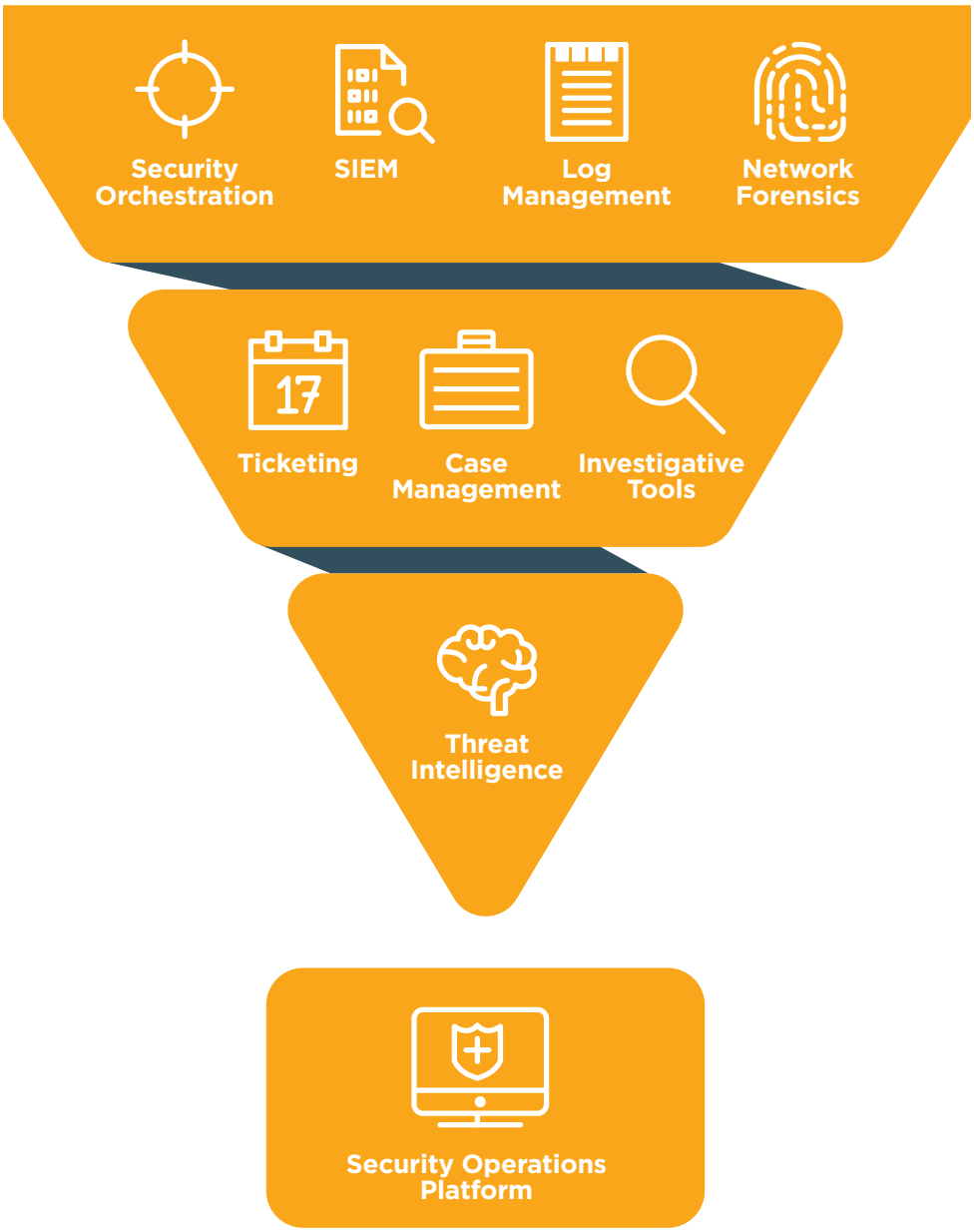
Sicherheitsmaßnahmen zentral verwalten

Konsolidierter Schutz für jedes Unternehmen

Ein neuer Ansatz für Ihre Sicherheitsmaßnahmen

Da derzeit fast täglich neue Cyberbedrohungen aufkommen, investieren viele Unternehmen verstärkt in Initiativen zur Stärkung ihrer Sicherheit. Die meisten Sicherheitsverantwortlichen haben erkannt, dass fast alle großen und kleinen Unternehmen früher oder später zum Ziel von Hackern werden, die Daten oder Geld stehlen oder die Geschäftsabläufe stören wollen. Doch der Aufbau einer effektiven Sicherheitsinfrastruktur ist schwierig – insbesondere für Unternehmen, denen nur begrenzte Ressourcen zur Verfügung stehen. Sie sind den gleichen Risiken ausgesetzt wie Großkonzerne von Weltrang, verfügen jedoch bei Weitem nicht über dasselbe Investitions- und Humankapital.

Selbst wenn man einmal von den Kosten absieht, ist zu bedenken, dass der Kauf einer neuen Appliance oder das Abonnement eines neuen Service nur in den seltensten Fällen zu den Verbesserungen führt, die die Käufer sich davon erhofft hatten. Die Erweiterung der Sicherheitsinfrastruktur um zusätzliche Punktlösungen führt oft zu mehr Komplexität, einem steigenden Personalbedarf, zusätzlichen fehleranfälligen manuellen Arbeitsschritten und möglicherweise sogar einem größeren Gesamtrisiko, wenn die neuen Sicherheitsmaßnahmen nicht korrekt implementiert werden. Neue Produkte weisen bei der Erfüllung dieser dringenden, bereits bekannten Kundenanforderungen einen überraschenden Nachholbedarf auf.



Glücklicherweise setzt sich inzwischen jedoch eine holistischere Herangehensweise durch.

Cybersicherheitsplattformen
Eine Sicherheitsplattform ist eine innovative Lösung für die Verwaltung komplexer Sicherheitsinfrastrukturen und fungiert als Kontrollzentrum für das Security Operations Center (SOC). Sicherheitsplattformen ermöglichen die Konsolidierung und Automatisierung vorhandener Sicherheitsmaßnahmen, sodass Sicherheitsteams Bedrohungen schneller und kosteneffizienter abwehren können. Doch nicht alle Lösungen sind gleich.

Beispielsweise versuchen die Anbieter von SIEM-Lösungen (Security Information and Event Management), ihre Produkte als Konsolen für das zentralisierte Sicherheitsmanagement zu repositionieren, obwohl dies nur begrenzte taktische Vorteile bietet. Durch den Einsatz einer solchen SIEM-basierten Sicherheitsplattform steigt die Zahl der eingehenden Warnmeldungen, ohne dass Kontextanalysen oder Automatisierungsfunktionen zur Verfügung stehen. Das macht die Arbeit der SOC-Analysten eher schwerer statt einfacher.

Dieses Whitepaper untersucht die wichtigsten Features einer Sicherheitsplattform und nennt einige Kriterien, die bei der Auswahl eines Anbieters unbedingt beachtet werden sollten. Auch wenn eine innovative Plattform letztlich kein Ersatz für erstklassige Sicherheitstechnologien, -prozesse und -experten sein kann, ermöglicht sie Unternehmen doch den Aufbau einer Sicherheitsinfrastruktur, die wesentlich effizienter sowie einfacher zu verwalten ist und dadurch letztlich stärkeren Schutz bietet.

Transparenz
Mit Transparenz ist die Fähigkeit eines Unternehmens gemeint, Angriffe zu erkennen, zu melden und ihre Auswirkungen abzuschätzen. Darüber hinaus bedeutet Transparenz auch, dass die Verantwortlichen wissen, welchen Bedrohungen ihr Unternehmen ausgesetzt ist und von welchen Gefahren das größte Risiko ausgeht. Ohne Transparenz kann es keine effektive Sicherheit geben, da „tote Winkel“ in der IT-Infrastruktur erhebliche Probleme verursachen können.

Da sich die IT-Umgebungen und Netzwerke moderner Unternehmen ständig weiterentwickeln, können jederzeit neue tote Winkel entstehen. Unter anderem müssen mittlerweile die Zugangspunkte für Zulieferer und Tochtergesellschaften sowie zahlreiche weitere Verbindungen überwacht werden, die es bis vor Kurzem noch nicht gab.

Auch durch die Nutzung von Cloud-Infrastrukturen können neue Schwachstellen und tote Winkel entstehen. Wenn Unternehmen geschäftskritische Prozesse und vertrauliche Daten in die Cloud verlagern, wo das zentralisierte Management von Anmeldedaten und Konfigurationen schwierig sein kann, wird auch der Schutz der Daten notwendigerweise komplexer.

Zur Verbesserung der Transparenz sollte eine Cybersicherheitsplattform Sicherheitsverletzungen schnell erkennen, Schwachstellen proaktiv aufdecken und alle sicherheitsrelevanten Daten zusammentragen und zueinander in Beziehung setzen, um den Sicherheitsverantwortlichen zu helfen, Angreifern immer einen Schritt voraus zu sein.

Angriffe zeitnah aufdecken
Selbstverständlich ist jedes Unternehmen daran interessiert, Angriffe möglichst effektiv zu verhindern und abzuwehren. Doch da die Angreifer bei der Ausnutzung technologischer und menschlicher Schwachstellen immer gewiefter werden, lassen sich nicht alle Sicherheitsverletzungen vermeiden. Die entscheidende Frage lautet also: Wie schnell kann ein erfolgreicher Hackereinbruch aufgedeckt werden? Der weltweite Medianwert für die Zeit zwischen der Infiltration durch die Hacker und der Erkennung der Bedrohung (Verweildauer) ist mit 99 Tagen immer noch sehr lang, sodass Angreifer genug Zeit haben, um sensible Daten zu stehlen und anschließend die Spuren ihrer Aktivitäten zu verwischen.[1]

Deshalb muss eine Sicherheitsplattform vor allem die zügige Abwehr von Bedrohungen erleichtern. Sie sollte die Verantwortlichen in die Lage versetzen, die Funktionsweise der von den Angreifern verwendeten Malware nachzuvollziehen, die mit dem Hackereinbruch verbundenen Risiken und Schäden rasch abzuschätzen und die gewonnenen Erkenntnisse in die verschiedenen Komponenten der Sicherheitsinfrastruktur einzuspeisen, um deren Effektivität zu steigern. Außerdem sollte sie die Aufdeckung von Sicherheitsverletzungen innerhalb weniger Minuten – statt in Stunden oder gar Tagen – ermöglichen, da jede Minute einer Sicherheitsverletzung inzwischen mehrere Hundert (oder sogar Tausend) US-Dollar an Kosten verursacht.

Aussagekräftige Warnmeldungen
Moderne Unternehmen müssen in der Lage sein, echte Bedrohungen aus einer Flut von Warnmeldungen herauszufiltern. Sicherheitsteams erhalten im Schnitt 17.000 Malware-Warnmeldungen pro Woche, von denen nur 19% als zuverlässig eingestuft und nur 4% genauer untersucht werden. Im Umkehrschluss bedeutet das eine große Zahl an Fehlalarmen, die nicht nur Zeit, sondern auch Geld kosten. Die Zeit, die ein Unternehmen benötigt, um auf ungenaue oder falsche Warnmeldungen zu reagieren, kann jährliche Kosten in Höhe von 1,27 Millionen US-Dollar verursachen.[2]

Warnmeldungen ohne entsprechende Kontextinformationen erschweren Sicherheitsanalysten die Entscheidungsfindung. Eine effektive Sicherheitsplattform bringt Bedrohungen zum Vorschein und analysiert sie. Zudem automatisiert sie die Validierung von Warnmeldungen und eliminiert Fehlalarme. So können die Sicherheitsteams schneller gegen die wirklich wichtigen Bedrohungen vorgehen, die sonst allzu oft in der Flut der Warnmeldungen untergehen.

Angreiferaktivitäten analysieren und prognostizieren
Die Effizienz herkömmlicher signaturbasierter Produkte hat in den letzten Jahren stark abgenommen. Dieser Rückgang ist der beste Beweis dafür, dass Angreifer nun in der Lage sind, Schadprogramme so abzuändern, dass sie nicht mit signaturbasierten Erkennungsmethoden identifiziert werden können. Zudem ist er ein Hinweis darauf, dass die Angreifer allmählich weniger Malware verwenden und verstärkt auf den Diebstahl von Zugangsdaten und andere Angriffsmethoden setzen, für die kein Schadcode benötigt wird.[3]

Aus diesem Grund muss eine Sicherheitsplattform auch unbekannte Bedrohungen erkennen können, um effektiven Schutz zu bieten. Sie sollte das Verhalten der Angreifer mithilfe ausgereifter Analyseverfahren modellieren und so die Grundlage für die Erkennung künftiger Angriffe schaffen. Bei der Erfassung und Kodifizierung der Angreiferaktivitäten müssen Analysefunktionen, Bedrohungsdaten und bei der Angriffsabwehr gesammelte Erfahrungen ineinandergreifen. Deshalb sollten Sicherheitslösungen mehr als nur maschinelles Lernen und Analysen von Anwenderverhalten (User Behavior Analytics, UBA) bieten: Sie sollten den Analysten dabei helfen,

1 FireEye (2017). „M-Trends 2017: A View from the Front Lines“.
2 Ponemon Institute (Januar 2015). „The Cost of Malware Containment“.
3 Joshua Goldfarb (26. Oktober 2016). „20 Endpoint Security Questions You Never Thought to Ask“.

Bedrohungen zu priorisieren, zu isolieren und die richtige Strategie zur Abwehr und Schadensbehebung zu wählen.

Reaktion

Da die Medien immer häufiger von Cyberangriffen berichten, ist nun auch außerhalb der Sicherheitsbranche allgemein bekannt, dass die Reaktion auf einen Angriff genauso wichtig ist wie der Schutz davor. Effiziente und effektive Gegenmaßnahmen basieren auf qualitativ hochwertigen Warnmeldungen, einer sorgfältig nach Prioritäten geordneten Liste mit den anstehenden Aufgaben sowie präzisen Analysen und einem lückenlosen Fallmanagement. Auch wenn es vielleicht auf den ersten Blick scheint, dass kleinere Unternehmen nicht unbedingt einen reibungslosen Workflow benötigen, sprechen die einschlägigen Daten eine andere Sprache. Letztes Jahr benötigten Unternehmen durchschnittlich 82 Tage, um einen komplexen Angriff einzudämmen und den entstandenen Schaden zu beheben.[4]

Um die Effizienz der Sicherheitsteams zu steigern, sollte eine Sicherheitsplattform alle Sicherheitsprozesse integrieren und Bedrohungsdaten zur Verbesserung der Angriffsabwehr sowie Funktionen für das Fallmanagement bereitstellen.

Integration aller Tools, Komponenten und Prozesse

Eine gute Plattform sollte es Ihren Sicherheitsteams ermöglichen, schneller von der Prüfung von Warnmeldungen zur Schadensbehebung überzugehen. Die Reaktionsgeschwindigkeit hängt typischerweise davon ab, wie schnell Sicherheitsteams eine Warnmeldung interpretieren können. Logdateien, die Warnmeldungen aus mehreren Quellen enthalten, ohne dass diese durch relevante Kontextinformationen ergänzt oder miteinander abgeglichen und in Zusammenhang gebracht werden, sind so gut wie wertlos. Eine moderne Plattform steigert die Reaktionsgeschwindigkeit, indem sie Logdateien mit Bedrohungsdaten und Analysen anreichert, um neue Bedrohungen aufzudecken. Auf diese Weise kann eine gut konzipierte Plattform viel mehr sein als nur das Bindeglied zwischen den Komponenten der Sicherheitsinfrastruktur.

Datengestützte Angriffsabwehr

Zuverlässige Bedrohungsdaten sind ein wichtiger Bestandteil einer ausgereiften Sicherheitsinfrastruktur. Sie nützen jedoch nichts, wenn sie nicht direkt in allen Komponenten der Sicherheitsinfrastruktur angewandt werden können. Anders gesagt: Bedrohungsdaten, die nicht oder nur mit großer Mühe zum Schutz des Unternehmens eingesetzt werden können, sind wertlos. Deshalb sollten die Bedrohungsdaten der Sicherheitsplattform immer kontextbezogen und relevant sowie speziell auf das Unternehmen und die aktuell zu bekämpfende Sicherheitsverletzung zugeschnitten sein. Außerdem ist es von Vorteil, wenn sie von den Sicherheitsteams bei Bedarf angefordert werden können, falls die Analysten mehr Unterstützung bei der Untersuchung eines Vorfalls benötigen.

Tools für das Fallmanagement

Bedrohungen werden oft von einzelnen Mitarbeitern im SOC erkannt. Trotzdem sind an der Vorfallsuntersuchung und den anschließenden Gegenmaßnahmen meistens mehrere Teammitglieder beteiligt, die zugeteilte Aufgaben erledigen, Berichte erstellen und vertrauliche Informationen untereinander austauschen müssen. Leider bieten herkömmliche Projektmanagement- und Kommunikationstools oft nicht die Funktionen, die SOC-Teams zur Koordinierung ihrer Aufgaben benötigen. Eine Sicherheitsplattform sollte den Teams nutzerfreundliche Tools bereitstellen, mit denen sie die zu erledigenden Aufgaben verteilen und verfolgen, die Aufgabenliste verwalten und sich untereinander austauschen können, um das Problem möglichst effizient zu lösen.

Steigerung der Effizienz der Mitarbeiter

Angesichts der sich verschärfenden Bedrohungslage müssen die Unternehmen offene Stellen im Bereich Cybersicherheit so schnell wie möglich besetzen. Allerdings übersteigt die Nachfrage das Angebot an qualifizierten Kandidaten bei Weitem. In den USA sind derzeit mehr als 209.000 Stellen für Sicherheitsexperten nicht besetzt und die Zahl der entsprechenden Jobangebote ist in den letzten fünf Jahren um 74% gestiegen.[5] Außerdem müssen viele Unternehmen feststellen, dass ihr Budget nicht ausreicht, um rund um die Uhr ein voll besetztes Sicherheitsteam vorzuhalten. Für die meisten Unternehmen sind der finanzielle und zeitliche Aufwand für die Bearbeitung der Warnmeldungen herkömmlicher Systeme durch Analysten angesichts der aktuellen Ressourcenknappheit nicht wirklich vertretbar. Die entsprechenden manuellen Prozesse sind ineffizient und fehleranfällig und beinträchtigen sowohl die Sicherheit als auch die Mitarbeitermotivation. Deshalb ist eine Sicherheitsplattform nötig, die diese zeitraubenden Routineaufgaben automatisieren kann.

Gesamtbetriebskosten

Es gibt vermutlich kein anderes Thema in der Cybersicherheitsbranche, das so ausführlich und oft besprochen wird wie die Gesamtbetriebskosten. Unternehmen nehmen bei der Evaluation von Produkten oft einen direkten Preisvergleich vor. Daran ist prinzipiell nichts auszusetzen — auch wenn die Produkte völlig verschieden sind. Schließlich steht jeder Euro, der für die Cybersicherheit ausgegeben wird, nicht mehr für die Realisierung anderer Unternehmensziele zur Verfügung, sodass Unternehmen verschiedene Prioritäten gegeneinander abwägen müssen.

Wenn man bedenkt, dass der Schutz wertvoller Ressourcen weiterhin ein Hauptkostenfaktor sein wird, ermöglicht eine etwas differenziertere Herangehensweise an die Gesamtbetriebskosten eine breiter gefasste, strategischere Diskussion über das Thema Cybersicherheit. Mit diesem Ansatz verschaffen Sie sich einen umfassenderen Überblick über die Kosten und Vorteile, die eine Sicherheitsplattform mit sich bringt.

Aufwendungen

Typischerweise achten die Verantwortlichen im Vorfeld einer Neuanschaffung am meisten auf die Investitions- und Abonnementkosten der entsprechenden Hardware und Software sowie auf den finanziellen Aufwand für Upgrades, Implementierung und Wartung. Doch bei dieser scheinbar einfachen und logischen Herangehensweise werden redundante Komponenten und ineffiziente Bereiche der Infrastruktur oft übersehen. Diese entstehen durch parallel betriebene Tools mit denselben Funktionen, voneinander isolierte, wartungsintensive Punktlösungen, häufige Upgrades und längere Ausfallzeiten infolge der steigenden Komplexität.

Eine effektive Sicherheitsplattform integriert eine Vielzahl verschiedener Komponenten, darunter Tools zum Schutz Ihres Netzwerks, Ihrer Endpunkte und Ihrer E-Mails, SIEM-Systeme und Orchestrierungslösungen sowie Funktionen für die Logdateiverwaltung und Forensik. Die Plattform sollte Sie zudem dabei unterstützen, Ihre Infrastruktur durch die

4 Ponemon Institute (März 2016), „The State of Malware Detection and Prevention“
5 Ariha Setalvad (31. März 2015), „Demand to fill cybersecurity jobs booming”

Integration oder Entfernung vorhandener Punktlösungen zu straffen und dadurch Kosten einzusparen.

Betriebskosten
Wenn ein Unternehmen eine Anwendung gekauft oder einen Service abonniert hat, entstehen neben diesen Investitionskosten auch Betriebskosten. Letztere schließen unter anderem Ausgaben für die Anwerbung, Einarbeitung und Schulung qualifizierter Mitarbeiter und neuer Talente ein, die den Betrieb der erweiterten Sicherheitsinfrastruktur unterstützen. In den meisten Unternehmen gelten derartige Kosten als unvermeidbar.

An diesem Beispiel wird einmal mehr ersichtlich, wie sich ein erhöhter Zeit- und Personalaufwand schließlich in steigenden Betriebskosten niederschlägt und warum dieser Gesichtspunkt im Rahmen eines Auswahl- und Anschaffungsprozesses unbedingt berücksichtigt werden sollte. Daher sollten die Verantwortlichen bei der Evaluation von Sicherheitsplattformen besonders auf folgende Features achten:

- Einheitliche Verwaltungsfunktionen, die ein möglichst breites Spektrum an Sicherheitstools abdecken und so den zeitlichen und finanziellen Aufwand für die Einarbeitung und Schulung ihrer Mitarbeiter senken
- Moderne Erkennungsfunktionen, die die Flut der eingehenden Warnungen eindämmen und echte Bedrohungen schnell identifizieren
- Leistungsstarke Orchestrierungs- und Untersuchungsfunktionen, die Sicherheitsteams in die Lage versetzen, sich verstärkt auf wertschöpfende Aufgaben zu konzentrieren

Durch Automatisierung lässt sich der Aufwand für die Validierung von Warnmeldungen und andere manuelle Routineprozesse auf ein Minimum reduzieren. Zu viele Sicherheitsexperten verbringen bis zu 80% ihrer Zeit mit solchen Aufgaben, die langfristig demotivierend wirken und die Betroffenen häufig zur Abwanderung veranlassen. Wenn diese Routineaufgaben jedoch automatisch von einer Sicherheitsplattform erledigt werden, können sich die Mitarbeiter auf Aufgaben konzentrieren, die deutlich ansprechender und zudem für das Unternehmen wichtiger sind: die Suche nach Bedrohungen, den Schutz vor Gefahren und – falls dennoch ein Angriff stattfindet – die Abwehr und Schadensbehebung.

Außerdem sollte die Sicherheitsplattform die Prozesse des Sicherheitsteams in Form von Regeln erfassen und automatisieren, damit sichergestellt ist, dass die etablierten Best Practices trotz einer gewissen Mitarbeiterfluktuation weiterhin eingehalten werden.

Dies ist umso wichtiger, da sich die Abwanderung von Mitarbeitern negativ auf die Aufrechterhaltung des Sicherheitsbetriebs auswirkt. Erstklassiges Sicherheitspersonal im Unternehmen zu halten, ist genauso schwer, wie es zu finden. Die Einstellung eines Mitarbeiters ist normalerweise gut planbar – eine Kündigung jedoch meist nicht. Deshalb stellt jede Abwanderung eine Gefahr für die Kontinuität aller Sicherheitsmaßnahmen dar. Aus diesem Grund sollte eine Sicherheitsplattform dafür sorgen, dass alle Teammitglieder ihren Qualifikationen entsprechende Aufgaben zugewiesen bekommen und die zu ihrer Erledigung erforderlichen Informationen und Tools zur Hand haben. So lässt sich die Personalabwanderung so gering wie möglich halten.

Tabelle 1: Sicherheitsplattformen – Checkliste unverzichtbarer Features

Verbesserte Transparenz	
Erkennung von Sicherheitsverletzungen innerhalb von Minuten	✓
Konsolidierung und Priorisierung der wichtigsten Warnmeldungen	✓
Vorhersage von Angreiferaktivitäten	✓
Schnellere Reaktion	
Verwaltung der gesamten Infrastruktur über eine zentrale Konsole	✓
Kontextinformationen zur Verbesserung der Abwehrmaßnahmen	✓
Funktionen für das Fallmanagement	✓
Kostenoptimierung	
Senkung der Investitionskosten	✓
Steigerung der Mitarbeitereffizienz	✓
Aufrechterhaltung der Sicherheitsprozesse	✓

Fazit
Eine moderne Sicherheitsplattform bietet vielen Unternehmen enorme Vorteile. Genau wie bei jeder Kaufentscheidung sollten die Unternehmen auch hier von den Anbietern absolute Klarheit verlangen, um die Funktionen jeder infrage kommenden Lösung genau beurteilen zu können. Nur unter diesen Bedingungen können die Verantwortlichen auch ohne das enorme Budget eines Großkonzerns für eine ausgereifte Sicherheitsinfrastruktur sorgen.

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
(+1 877 347 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 unterstützt FireEye Kundenunternehmen bei der Vorbereitung auf die Erkennung und Abwehr von Cyberangriffen.

FIREEYE