SOPHOS
Security made simple.

Synchronized Security:

Branchenführende Abwehr, die koordinierter ist als moderne Angriffe

Heutzutage implementieren viele Unternehmen mehrere Schichten verschiedener Sicherheitsprodukte in ihrem Netzwerk und auf ihren Endpoints: host- und netzwerkbasierte Firewalls, Einrichtungen zur Überprüfung von Inhalten, Malware-Analyzer, Ereignis-Manager u.v.m. Diese „Defense-in-Depth"-Strategie soll vor bekannten und neuen Bedrohungen schützen. Die Idee dahinter: An irgendeinem Punkt der Angriffskette wird eines der Produkte in der Lage sein, den Angriff zu neutralisieren.

Einzelprodukte haben für sich genommen zwar ihre Daseinsberechtigung, jedoch hat eine solche „Silo-Architektur" entscheidende Nachteile. Erstens arbeiten die Produkte oft isoliert voneinander, d. h. Informationen werden nicht untereinander ausgetauscht. Dadurch wird eine wichtige Chance vertan: Firewalls und Endpoints könnten in Echtzeit Kontextinformationen auf Netzwerk- und Prozessebene austauschen, um so Infektionen zu isolieren und zu beseitigen.

Zweitens: Je weitreichender die „Defense-in-Depth"-Strategie eines Unternehmens ist, desto umständlicher wird die Verwaltung. Die Folge sind hohe Personalkosten, denn Warnmeldungen müssen manuell korreliert, verschiedene Bedienoberflächen verwaltet und Ereignisse überwacht werden. Auch die Performance kann beeinträchtigt werden, wenn mehrere Software-Agenten um Systemressourcen konkurrieren.

Drittens: Zwar wurden SIEM(Security Information and Event Management)-Tools entwickelt, um die Kommunikationslücken zwischen verschiedenen Einzelprodukten zu überbrücken. Die Hauptaufgabe solcher Tools besteht jedoch darin, Daten zentral und sinnvoll aufzubereiten. Die Möglichkeiten der Tools zum Extrahieren aussagekräftiger Informationen sind in der Regel begrenzt und vergangenheitsbezogen. Zudem müssen die Informationen zunächst von erfahrenen Mitarbeitern gründlich analysiert werden.

Die aktuelle Situation der meisten Unternehmen lässt sich gut an folgendem Beispiel illustrieren: Stellen Sie sich vor, Sie platzieren in und vor Ihrem Firmengebäude jeweils einen Wachmann. Die beiden erhalten jedoch keine Funkgeräte, mit denen sie kommunizieren könnten. Stattdessen erhalten die Wachleute die Anweisung, ihre Informationen getrennt voneinander an ein zentrales System zu senden. Dieses zentrale System wird von einer weiteren Person auf eingehende Informationen überprüft, die für die jeweils anderen Wachleute wichtig sein könnten. Gehen solche Informationen ein, werden diese jedem einzelnen Wachmann separat mitgeteilt. Erweitern Sie dieses Beispiel nun auf mehrere Gebäude mit einer Vielzahl von Wachleuten drinnen und draußen. Alle Wachleute schicken Ihre Informationen an ein zentrales System – ein System, das nicht kohärent erkennen kann, welcher Wachmann welche Nachricht sendet. Um das Ganze noch zu erschweren, probieren Angreifer immer neue Wege und Ablenkungsmanöver aus, um diese Patchwork-Abwehr zu überlisten.

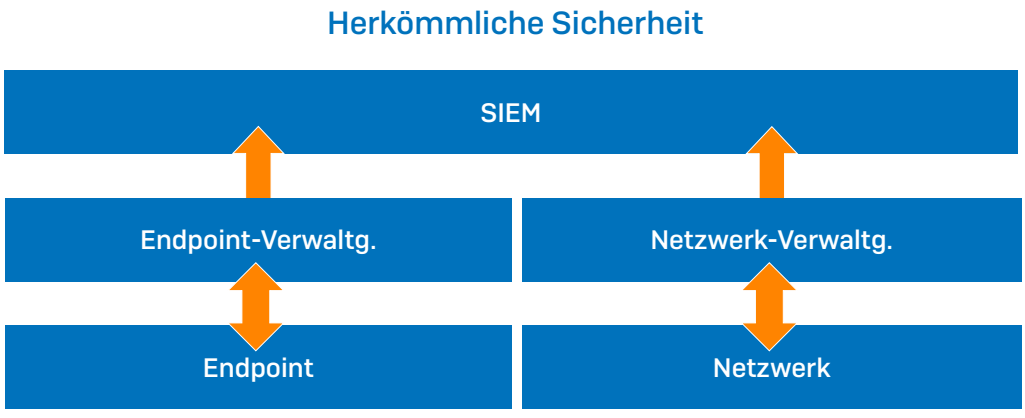


Abbildung 1: Herkömmliche Lösungen versuchen, Daten zu korrelieren und zu analysieren. Dazu sind Personal und spezielle Fachkenntnisse erforderlich, über die nur wenige verfügen.

Abwehr von gestern gegen Angriffe von heute

Bei frühen Cyberangriffen ging es den Angreifern oft vor allem darum, mit relativ einfachen Methoden Chaos zu stiften. Bei heutigen Angriffen geht es um weitaus mehr. Hinter ihnen stecken in der Regel finanzielle oder politische Motive. Ihre Taktiken sind ausgeklügelt, initiiert werden sie von Verbrechersyndikaten, Hacktivisten oder sogar Staaten. Mit überzeugend echt erscheinenden Phishing-Nachrichten bringen die Angreifer Enduser dazu, Zugangsdaten herauszugeben, Berechtigungen auszuweiten und Daten zu übertragen. Sie nutzen Schwachstellen in Software aus, bevor diese behoben werden können, sie infiltrieren Netzwerke mit speicherbasierter Malware und sie bewegen sich rasend schnell lateral vorwärts, wobei sie andere Systeme infizieren.

Die IT-Security-Branche hat Probleme, mit diesem Tempo Schritt zu halten, und so sind die Cyberkriminellen ihr oft einen Schritt voraus – dank Kommunikationen im Untergrund, untereinander ausgetauschten Techniken und Codes, anonymen Währungen, intelligenter, wandlungsfähiger Malware und gezielter Ausnutzung von Netzwerken vorinfizierter Geräte. Es gibt sogar voll funktionsfähige, intelligente, cloudbasierte Angriffs-Services, die praktisch von jedem in Anspruch genommen werden können – man kann auch von App Stores für kriminelle Aktivitäten sprechen – komplett mit Umsatzströmen zurück an die Programmierer im Falle eines erfolgreichen Angriffs.

Gleichzeitig übertragen Enduser immer mehr Daten in die Public Cloud, speichern Unternehmensdaten auf Privatgeräten und erwarten, auch außerhalb des Büros problemlos auf das Unternehmensnetzwerk zugreifen zu können – und zwar überall und jederzeit.

Die Flut moderner Bedrohungen stellt selbst die weltweit größten und innovativsten Unternehmen vor schier unüberwindbare Herausforderungen. Angriffe werden immer komplizierter und koordinierter. Die Einzelprodukte, die vor ihnen schützen sollen, arbeiten jedoch in den meisten Fällen immer noch isoliert voneinander. Gleichzeitig wächst die Angriffsfläche immer weiter, da Enduser Smartphones, Cloud-Anwendungen und verschiedene tragbare Geräte nutzen. Und IT-Abteilungen fehlen die finanziellen Mittel, um ihre Einzelprodukte entsprechend aufzustocken. Dem Ponemon Institute zufolge bleiben 74 % aller Datenpannen mehr als sechs Monate lang unbemerkt. Laut ESG Group sind 46 % aller Unternehmen zudem der Auffassung, dass sie nicht genügend auf Cybersecurity spezialisierte Mitarbeiter haben.

74 %

aller Datenpannen bleiben 6 Monate oder länger unbemerkt.

46 %

aller Unternehmen haben nicht genügend auf Cybersecurity spezialisierte Mitarbeiter.

Synchronized Security – eine einfache Lösung für ein komplexes Problem

Erstmals können Endpoint und Network Protection als ein integriertes Sicherheitssystem agieren. Dieses System setzt sich aus branchenführenden Produkten zusammen, die über eine zentrale Oberfläche verwaltet werden und bidirektional Echtzeit-Informationen austauschen, um automatisch auf Bedrohungen reagieren zu können.

Synchronized Security: Branchenführende Abwehr, die koordinierter ist als moderne Angriffe

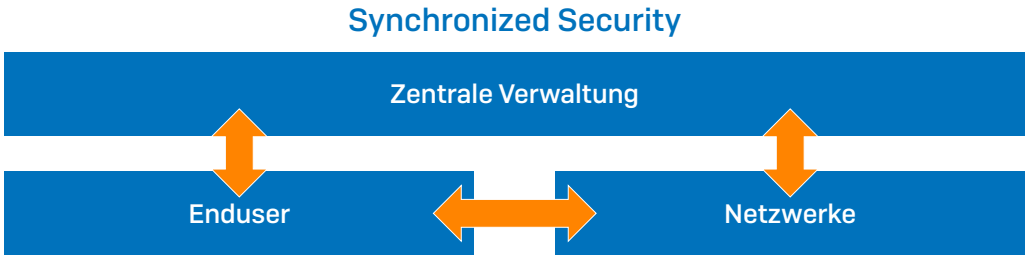


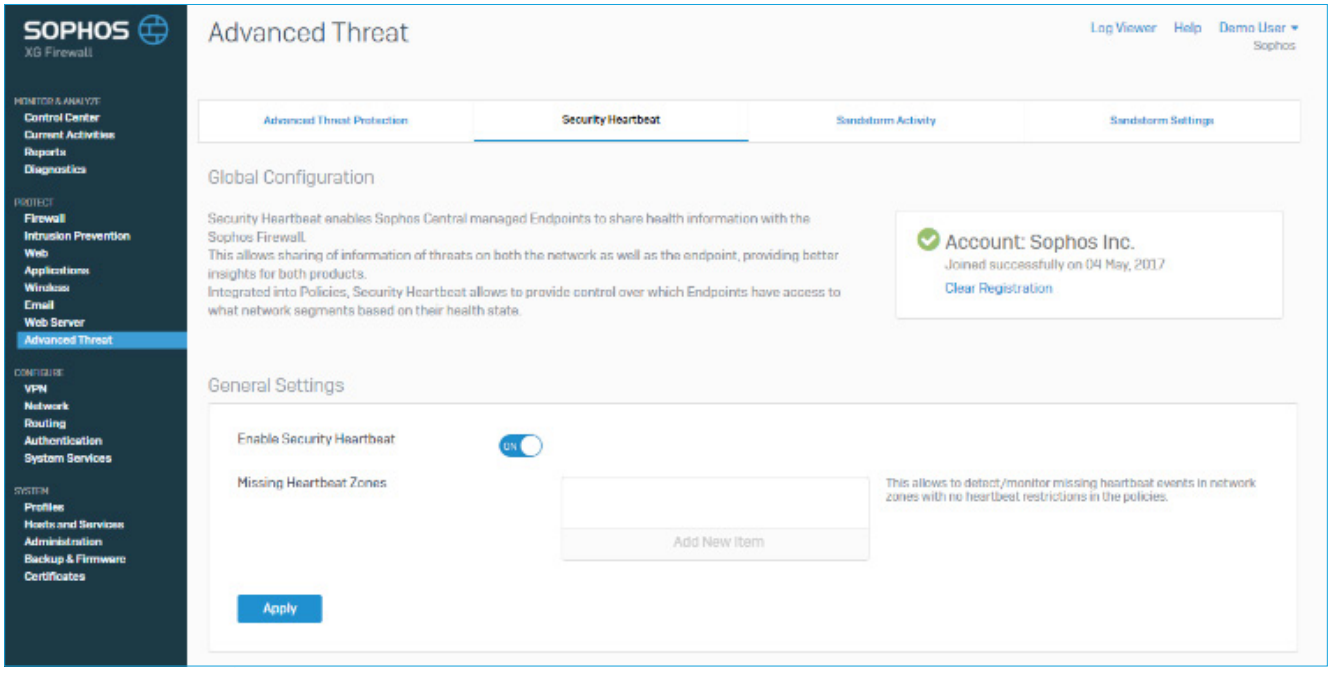
Abbildung 2: Synchronized Security vereinfacht und zentralisiert die Kommunikation und Verwaltung.

Dank einfachem Management lässt sich das Framework problemlos einrichten und verwalten – ohne zusätzliche Analysten und Ereignis-Manager. Erkennungs-, Isolierungs- und Bereinigungsergebnisse werden im Falle eines Angriffs innerhalb von Sekunden – nicht innerhalb von Stunden oder Tagen –neutralisiert. Das Ergebnis ist besserer Schutz, der außerdem auch kosten- und zeiteffizienter ist.

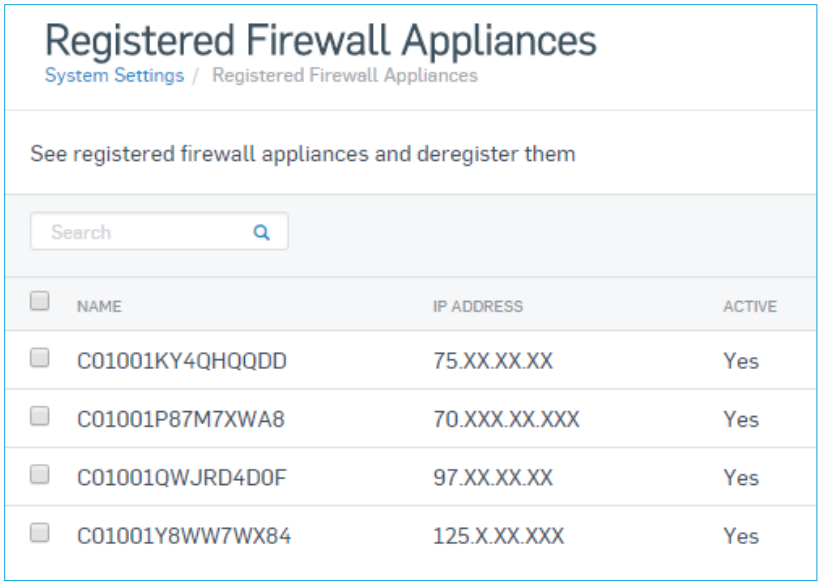
	Synchronized Security	Herkömmliche Sicherheit
Informationen	Übergreifend verfügbar	Isoliert
Korrelation	Automatisiert	Manuell und teilweise automatisiert
Erkennung unbekannter Bedrohungen	Kontextgestützt	Nicht kontextgestützt
Reaktion auf Vorfälle	Sehr gezielt	Unpräzise
Zusätzliche Investitionen in Produkte und Personal	--	Erheblich
Verwaltung	Einfach und zentral	Kompliziert und auf Silo-Infrastruktur basierend

Tabelle 1: Eigenschaften von Synchronized Security im Vergleich zu herkömmlicher IT-Security

Die Kommunikation zwischen Firewalls und Endpoints wird durch den Sophos Security Heartbeat ermöglicht – einem einfach bereitzustellenden Feature, das einen sicheren bidirektionalen Kanal aufbaut, der von der cloudbasierten Sophos Central Management-Konsole gesteuert wird.



Für die Einrichtung müssen Sie lediglich Ihre Sophos Central Admin Zugangsdaten im Bereich „Security Heartbeat“ der Sophos XG Firewall Oberfläche eingeben. Anschließend erscheint die Firewall in Sophos Central und alle über Sophos Central verwalteten Computer beginnen, eine Heartbeat-Verbindung an verbundene Firewalls zu senden. Verbundene Firewalls senden zudem einen Heartbeat zurück an die Computer.



Computer verbinden sich automatisch mit der nächstgelegenen Firewall und Firewalls überprüfen eingehende Verbindungsanfragen von Computern, um sicherzustellen, dass diese über Sophos Central geschützt werden. Im Gegenzug verifizieren auch die Computer die Firewall, indem sie überprüfen, ob deren Sicherheitsinformationen mit Sophos Central übereinstimmen. Alles funktioniert automatisch: keine komplexen Regeln, Konfigurationen oder Updates.

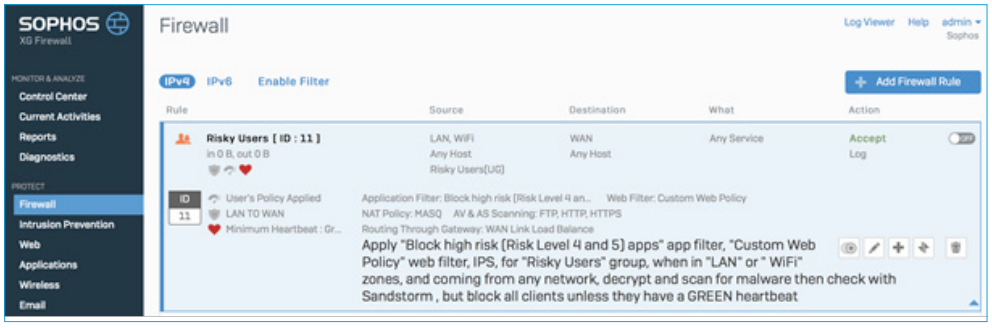
Sophos Security Heartbeat Widget im XG Firewall Dashboard

Synchronized Security in Aktion: Die Grundlagen

Durch die Verbindung zwischen Firewall- und Endpoint-Clients beginnen Informationen zur Systemintegrität über Sophos Central von den Endpoints zur Firewall zu fließen. Im Dashboard der XG Firewall zeigt das Sophos Security Heartbeat Widget den Integritätsstatus aller Sophos-Central-verwalteten Endpoints an. Systeme, auf denen unerwünschte Anwendungen ausgeführt werden oder bei denen eine Infektion vorliegt, werden hier als gelb oder rot angezeigt. Auf rote Anzeigen sollte sofort reagiert werden, gelbe Anzeigen weisen auf ein Risiko hin, sind jedoch weniger dringlich.

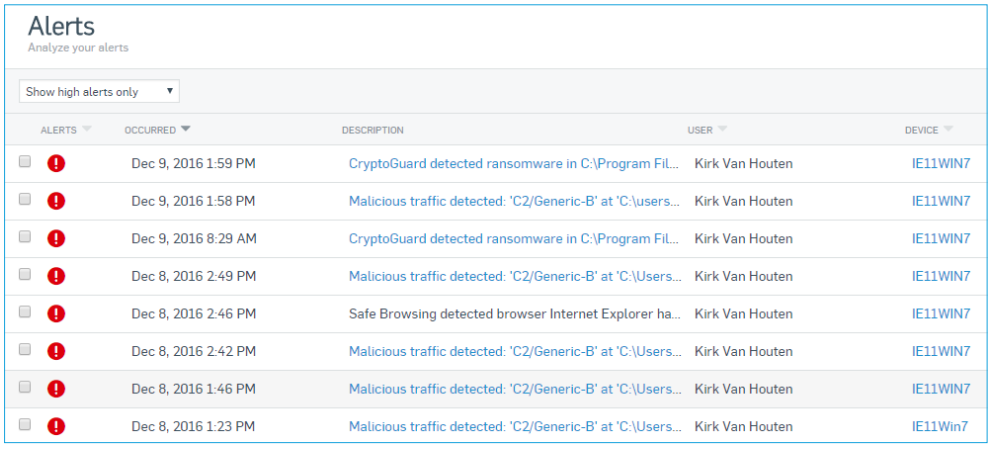
Um je nach Sicherheitsstatus unterschiedliche Maßnahmen zu ergreifen, können Firewall-Regeln eingerichtet werden. Beispielsweise können Sie

Computern mit gelbem Status den Zugriff aufs Internet prinzipiell erlauben, den Zugriff auf Seiten, die sensible Unternehmensinformationen enthalten könnten (z. B. Salesforce oder Dropbox), hingegen sperren. Bei einem roten Status können Sie den Internet-Zugang der betroffenen Systeme komplett sperren und, sofern Sie unser Dateiverschlüsselungsprodukt SafeGuard lizenziert haben, die Dateischlüssel entziehen, bis die Systeme wieder über einen grünen Status verfügen. Ist der Status wieder grün, wird der Internet-Zugriff automatisch wiederhergestellt und die Dateischlüssel werden wieder ausgegeben.



Firewall-Regel in der Oberfläche der XG Firewall verwehrt riskanten Benutzern den Netzwerkzugriff, sofern diese sich nicht in einem sicheren Zustand befinden

Die Sophos XG Firewall kann auch erkennen, ob ein ehemals sicherer Endpoint Netzwerkverkehr generiert, ohne einen Heartbeat zu senden. Ein fehlender Security Heartbeat kann darauf hindeuten, dass die Anti-Malware-Software des Endpoints von einem Eindringling manipuliert oder deaktiviert wurde. In einem solchen Fall wird der Endpoint vom übrigen Netzwerk isoliert, bis die Bereinigung erfolgt ist und der Heartbeat wiederhergestellt wurde.
Dank Security Heartbeat werden betroffene Systeme klar identifiziert – in der Oberfläche der XG Firewall und in der Oberfläche von Sophos Central Admin. Der Computername, der angemeldete Benutzer und der Prozessname, der einen Warnhinweis ausgelöst hat, werden angezeigt, sodass Bedrohungen schneller erkannt, analysiert und beseitigt werden können. In herkömmlichen Silo-Infrastrukturen kann es Stunden oder Tage dauern, an diese Informationen zu gelangen, da dem Ermittler lediglich die vorübergehende IP-Netzwerkadresse vorliegt, um dem Problem auf den Grund zu gehen.



Seite mit roten Warnhinweisen in Sophos Central Admin

Synchronized Security – mehr Sicherheit für Server

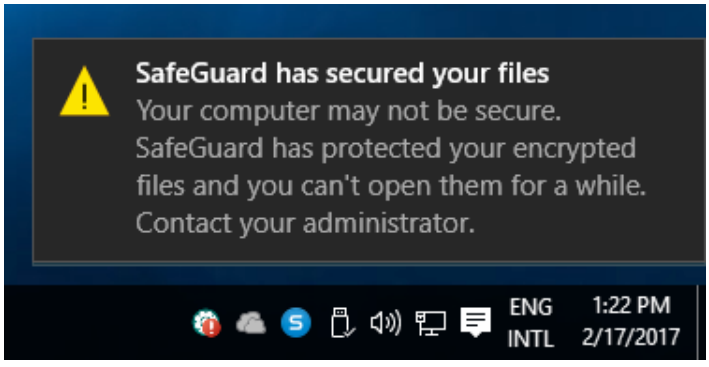
Auf Servern sind die wertvollsten Daten von Unternehmen gespeichert. Sie sind daher lukrative Ziele für Malware-Autoren und sollten unbedingt vor direkten Angriffen geschützt werden. Darüber hinaus müssen jedoch auch laterale Bewegungen von Enduser-Computern abgewehrt werden, die mit den Servern verbunden sind.

Im Falle eines Angriffs kann Sophos Server Protection die XG Firewall über eine Änderung des Integritätsstatus benachrichtigen. Zu diesem Zeitpunkt kann die Firewall den Server sowohl vom Internet als auch von anderen Systemen im Netzwerk isolieren, um das Abschöpfen von Daten und eine Verbreitung der Infektion zu verhindern. Eingehende Verbindungen zum Server werden von der Firewall abgelehnt und der Server wird vor anderen Geräten im Netzwerk verborgen („Destination Heartbeat"). Nach erfolgter Bereinigung können der Netzwerkzugriff und die Sichtbarkeit des Servers automatisch wiederhergestellt werden.

Mit der bidirektionalen Kommunikation zwischen Firewalls, Servern und Endpoints sorgt Sophos Synchronized Security für eine sofortige Koordination und wehrt auf diese Weise selbst besonders raffinierte Angriffe ab. Außerdem spart die automatische Identifizierung und Isolierung von Servern auf Grundlage des Sophos Security Heartbeat auch wertvolle Zeit beim Reagieren auf Sicherheitsvorfälle. In Kombination mit der kontinuierlichen Durchsetzung von Heartbeat-Richtlinien lässt sich ein kompromittiertes System effektiv isolieren – sowohl eingehend als auch ausgehend.

Ein neues Konzept: Synchronized Encryption

Die Verschlüsselung von Dateien war bislang ein umständlicher Prozess – sowohl für Administratoren, die die Verschlüsselung einrichten mussten, als auch für Enduser, die mit der Verschlüsselung arbeiten mussten. Sophos SafeGuard Encryption bietet nun jedoch ein neues Konzept für die Sicherheitsstrategien von Unternehmen: Alle Dateien werden standardmäßig verschlüsselt. Bevor eine Datei auf einem Gerät entschlüsselt werden darf, erfolgt zunächst eine Überprüfung des Benutzers, der Anwendung und des Sicherheitsstatus. Nur Anwendungen, die als sicher eingestuft wurden, dürfen unverschlüsselte Daten aufrufen, sodass Malware keine Chance hat, auf sensible Daten zuzugreifen. Der gesamte Vorgang ist transparent für den Enduser: Inhalte werden sofort bei ihrer Erstellung verschlüsselt und bleiben verschlüsselt, wenn sie innerhalb des Unternehmens ausgetauscht oder auf Cloud-Sites hochgeladen werden. Optional kann mit nur einem Klick ein Passwortschutz für den externen Austausch eingerichtet werden.



Nachricht, dass SafeGuard während eines Angriffs Dateischlüssel entzogen hat

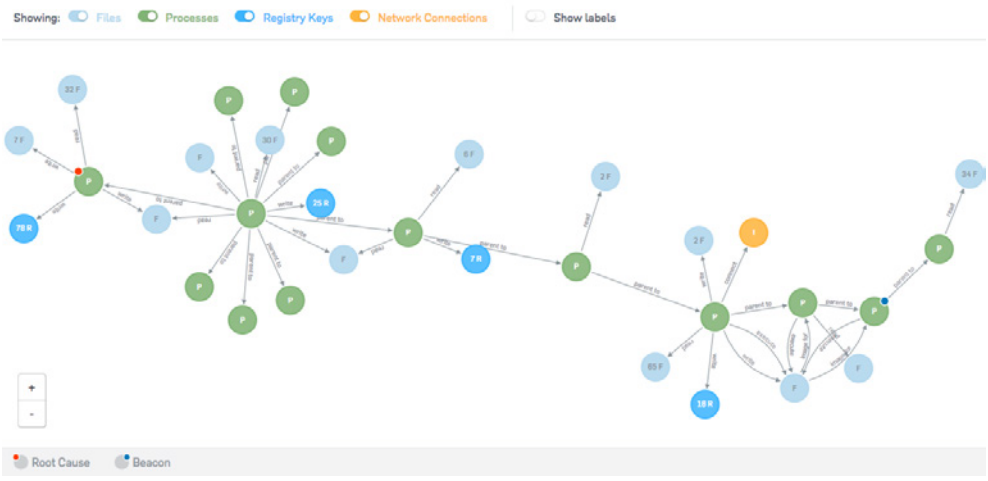
Sophos SafeGuard Encryption ist vollständig Synchronized-Security-kompatibel. Wenn ein Sophos-geschützter Endpoint der XG Firewall meldet, dass er angegriffen wurde, isoliert die Firewall nicht nur den Endpoint vom

Netzwerk, sondern entfernt auch die SafeGuard-Dateischlüssel von diesem Computer. So werden alle Daten, die ggf. abgeschöpft werden, für die Angreifer unbrauchbar. Sobald der sichere Status des Endpoints wiederhergestellt wurde, darf dieser wieder auf das Netzwerk zugreifen und er erhält wieder Schlüssel. Der gesamte Vorgang – von der Isolierung über die Bereinigung bis hin zur Wiederherstellung – läuft automatisch und innerhalb weniger Sekunden ab, nicht innerhalb von Stunden oder Tagen wie bei Angriffen gegen ein Patchwork von Einzelprodukten.

Der Ursache eines Angriffs auf den Grund gehen

Die automatische Isolierung, Bereinigung und Wiederherstellung von Synchronized Security und der bidirektionale Security Heartbeat revolutionieren zweifellos die IT-Security-Branche. Um zukünftige Angriffe abwehren zu können, sind aber auch einfach verwertbare Analysen vergangener Angriffe von entscheidender Bedeutung.

Die Ursachenanalyse in Sophos Intercept X liefert eine detaillierte, forensikbasierte Darstellung des Infektionswegs eines Angriffs – mit Informationen über betroffene Dateien, Prozesse und Registry-Schlüssel. Dazu gibt sie Empfehlungen, wie ein solcher Angriff in Zukunft verhindert werden kann.

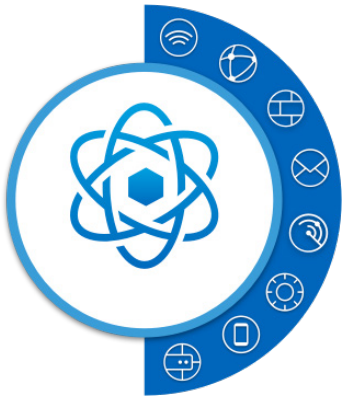


Ursachenanalyse in Sophos Intercept X

Dank der Ursachenanalyse können Sie nachvollziehen, wie die Malware in Ihr System gelangt ist und was die Malware getan hat, bevor sie entdeckt und entfernt wurde. Außerdem können Sie sicherstellen, dass die Malware komplett entfernt wird, und Maßnahmen treffen, um ähnliche Angriffe in Zukunft zu vermeiden.

Synchronized Security: Einfach bessere IT-Security

Synchronized Security ist ein branchenführendes Sicherheitssystem, das Ihren Abwehrmaßnahmen ermöglicht, so koordiniert zu agieren wie die Angriffe, vor denen sie schützen. Synchronized Security kombiniert eine intuitive Security-Plattform mit preisgekrönten Produkten, die aktiv zusammenarbeiten, um komplexe Bedrohungen zu blockieren und Sie optimal zu schützen – mit automatischer Reaktion auf Vorfälle sowie Echtzeit-Transparenz und -Kontrolle.



Im Gegensatz zu separaten Einzelprodukten, deren Komplexität mit jeder zusätzlichen Schutzschicht zunimmt, wird Synchronized Security mit jeder weiteren Sophos-Lösung leistungsstärker.

Mehr erfahren und selbst testen unter

www.sophos.de/synchronized

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

2017-05 WP-DE (NP)

SOPHOS