Sicherheitsbarrieren einreißen:

Korrelation schafft maximale Sicherheit

Dezentral aufgestellte Unternehmen mit mehreren Zweigstellen sowie kleine und mittlere Unternehmen mit einer Belegschaft im niedrigen zweistelligen Bereich haben eins gemein: Häufig gibt es Lücken in ihren Sicherheitsdaten, bedingt durch disparate Lösungen und Umgebungen. Diese Sicherheitsbarrieren stellen ein großes Problem für die IT dar; die logische Verknüpfung und Zuordnung von Daten zwischen der Unternehmenszentrale und den Zweigstellen oder inkompatible Lösungen für das Netzwerk und die Endpunkte gerät zur Geduldsprobe.

Typische Sicherheitsbarrieren

1

Angesichts der weiterhin zunehmenden Sicherheitsbedrohungen für Organisationen jeder Größenordnung lassen sich zielgerichtete Sicherheitsmaßnahmen beobachten. Darunter fällt das Hinzufügen problemspezifischer Lösungen zur bestehenden Infrastruktur – auch wenn kein Datenaustausch stattfindet. Dadurch können Barrieren zwischen disparaten Sicherheitslösungen im Unternehmen entstehen.

2

Dezentral aufgestellte Unternehmen leiden mitunter unter Inkonsistenzen zwischen der Sicherheit in der Firmenzentrale und der in den Niederlassungen. Mehrere Sicherheitsstufen sind für diese Organisationen sinnvoll, können aber immer noch eine Barriere für IT-Teams schaffen, mehrere Sicherheitssysteme und Standorte verwalten zu müssen.

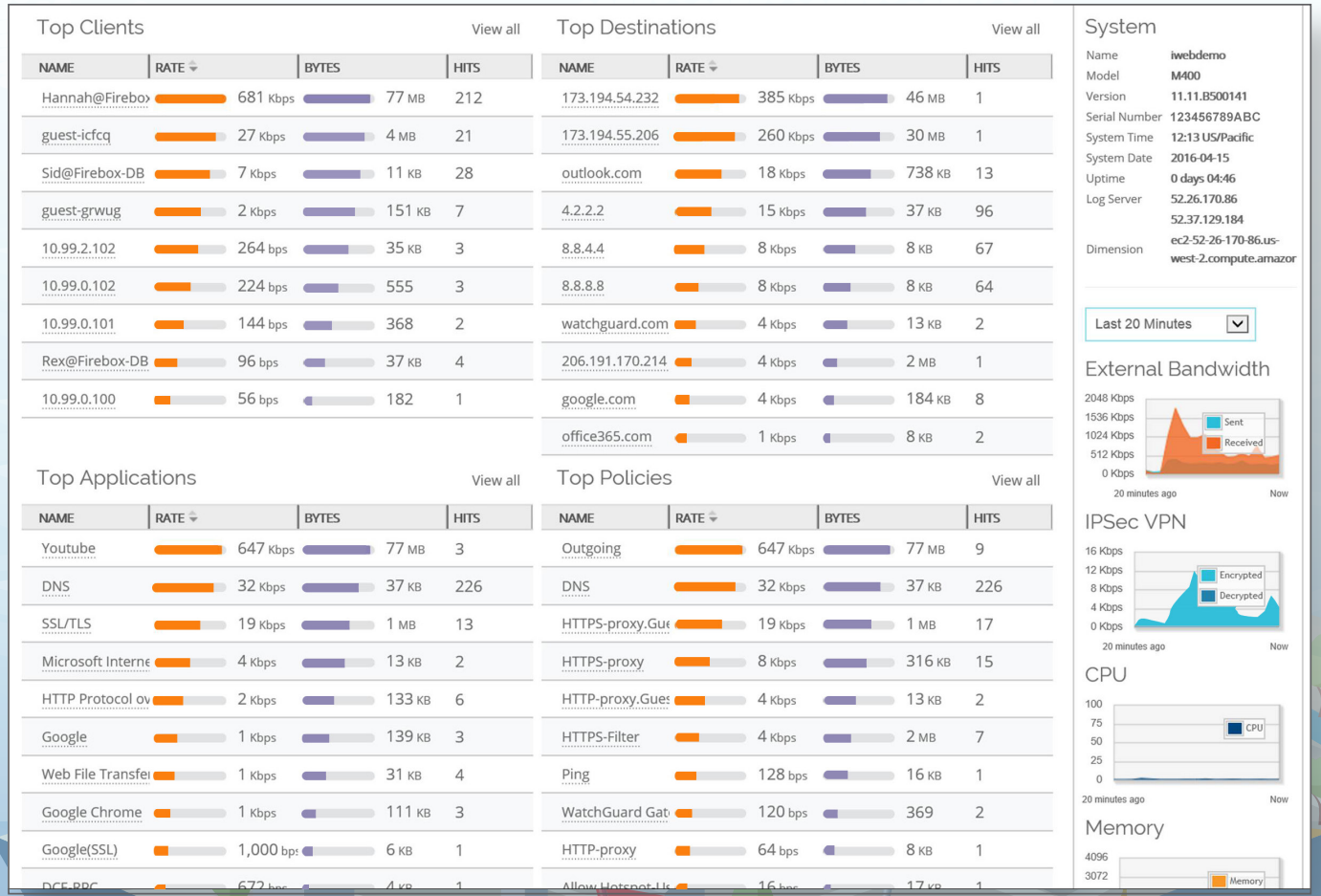
3

Remote-Mitarbeiter sind besonders anfällig für Bedrohungen, da sie sich nur selten hinter der Firewall befinden. Fehlt es bei diesen Remote-Geräten an Transparenz, werden sie zum leichten Ziel für Hacker, die in Ihr Netzwerk eindringen möchten.

Das Netzwerk als Ausgangspunkt

Das Netzwerk bietet eine Fülle an Sicherheitsdaten. Wer Einblick in Muster zu ungewöhnlichen oder gesperrten Datenbewegungen und Besuchen bösartiger oder bedrohter Websites gewinnt und Botnets und andere Bedrohungen zu erkennen vermag, hat schon viel für den Schutz des Unternehmens erreicht. Außerdem muss erfasst werden, welche Geräte mit dem Netzwerk verbunden sind, damit nur jene mit der entsprechenden Berechtigung und den richtigen Sicherheitsrichtlinien Zugriff erhalten.

Wenn Sie wissen, was in Ihrem Netzwerk passiert, können Sie daraus auch den Datendurchsatz und nutzungsbasierte Leistungsparameter ableiten. Das Wissen darüber, welche Benutzer für was die meiste Bandbreite beanspruchen, spielt bei der Steuerung von Leistungsengpässen eine entscheidende Rolle.

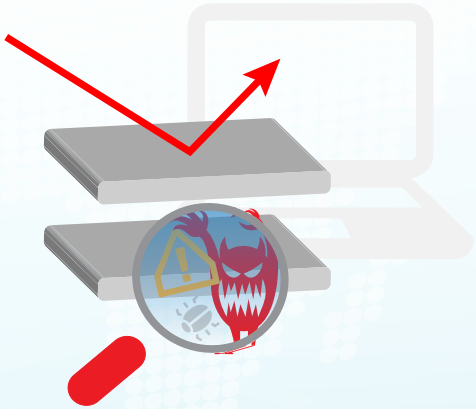


Netzwerk

Verlagerung zum Endpunkt

Transparenz an den Endpunkten beginnt damit, dass Sie Ihre Geräte kennen und für deren angemessenen Schutz sorgen. Außerdem müssen Sie wissen, ob bestimmte Nutzer besonders gefährdet oder bereits infiziert sind.

Es gibt in Wahrheit **zwei Visualisierungsstufen** für den Schutz des Endpunkts:
Bekanntes sperren und **Unbekanntes erkennen**.



Mit bestehenden Antivirenlösungen, die sich auf Signaturen stützen, lassen sich bekannte Bedrohungen wirksam sperren. Diese Schutzstufe kann jedoch oft Lücken aufweisen, da Patches nur wöchentlich bzw. nach Bedarf aktualisiert werden.

Die Erkennung unbekannter Bedrohungen ist etwas komplizierter. Es gibt diverse Lösungen, die sich verschiedener Ansätze bedienen, um zu bestimmen, ob ein Ereignis eine Bedrohung darstellt. Visualisierung am Endpunkt ist immer wichtig – ob bei der Verfolgung der Heuristik, Verhaltensanalysen oder Änderungen an Dateien, Prozessen und Verzeichnissen. Ohne diese Daten sind Unternehmen gegenüber Malware und Ransomware extrem gefährdet.

Besser informiert mit Bedrohungsanalysen

Gartner definiert Bedrohungsanalysen (engl. Threat Intelligence) als *„evidenzbasierte Kenntnisse, einschließlich Kontext, Mechanismen, Indikatoren, Implikationen und umsetzbare Handlungsempfehlungen, zu einer bestehenden oder aufkommenden Bedrohung für Vermögenswerte, die zum Treffen informierter Entscheidungen als Reaktion auf diese Bedrohung herangezogen werden können."*

Bitte was? Im Grunde geht es bei Bedrohungsanalysen um das Zusammentragen sämtlicher Daten zu einem bestehenden oder kürzlich erfolgten Bedrohungsschlag, um potenzielle Opfer zwecks Abwehr möglicher Schäden gezielt zu informieren. Klingt kompliziert und zeitaufwändig. Man sollte es kaum glauben, aber es gibt tatsächlich Anbieter, die das wollen, einen Haufen Geld dafür kassieren und ihr Angebot hauptsächlich an große Konzerne richten.

Es gibt unzählige kostenlose Feeds zu aktuellen Bedrohungen, aber wir wissen: Man kriegt, was man bezahlt. Kostenlose Feeds zu Bedrohungsanalysen werden meist nicht regelmäßig aktualisiert. Sie laufen also Gefahr, eine heute oder in den letzten Tagen entdeckte Bedrohung noch nicht zu kennen. Zudem funktionieren Feeds für die intelligente Gefahrenerkennung auf Enterprise-Niveau am besten in Kombination, sind aber für kleine und mittlere Unternehmen zu teuer.

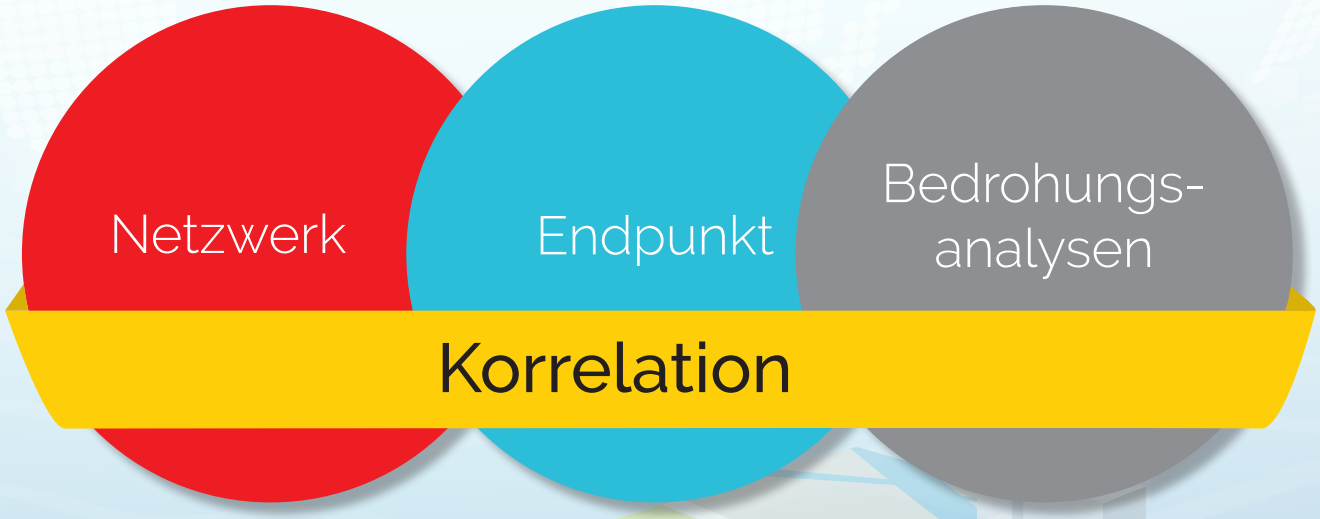
Bedrohungsanalysen sind jedoch ein wichtiges Element bei der Abwehr der stets wachsenden Anzahl an Bedrohungen, denen diese Unternehmen ausgesetzt sind. Diese Websites werden nahezu in Echtzeit aktualisiert und liefern hochpräzise Daten zu bekannten Bedrohungen, die Unternehmen massiv schädigen können.

Korrelation fügt das Puzzle zusammen

Für den Schutz Ihres Unternehmens brauchen Sie zuverlässige Daten aus dem Netzwerk, vom Endpunkt und aus Feeds zu Bedrohungsanalysen. Werden diese Daten jedoch isoliert voneinander betrachtet, ist es schwer zu erkennen, was vor sich geht. Die Kunst ist, alle Teile zusammenzufügen. Das Zauberwort lautet Korrelation.

Korrelation sorgt für zusätzliche Visualisierung aus diesen verschiedenen Quellen. Wenn sämtliche Ereignisdaten an einem Ort zusammengetragen werden, erhalten Organisationen umsetzbare Einblicke und können informiert reagieren. Durch das Analysieren und Priorisieren dieser Informationen ist die IT für zielgerichtete Reaktionen auf die Bedrohungen, die die Sicherheit oder geschäftliche Produktivität am meisten gefährden, optimal gerüstet. Das ist gerade für Organisationen mit begrenzten zeitlichen und personellen Ressourcen wichtig; diese können die Zeit bis zur Erkennung senken und effiziente, effektive Maßnahmen zur Bekämpfung der schlimmsten Bedrohungen ergreifen.

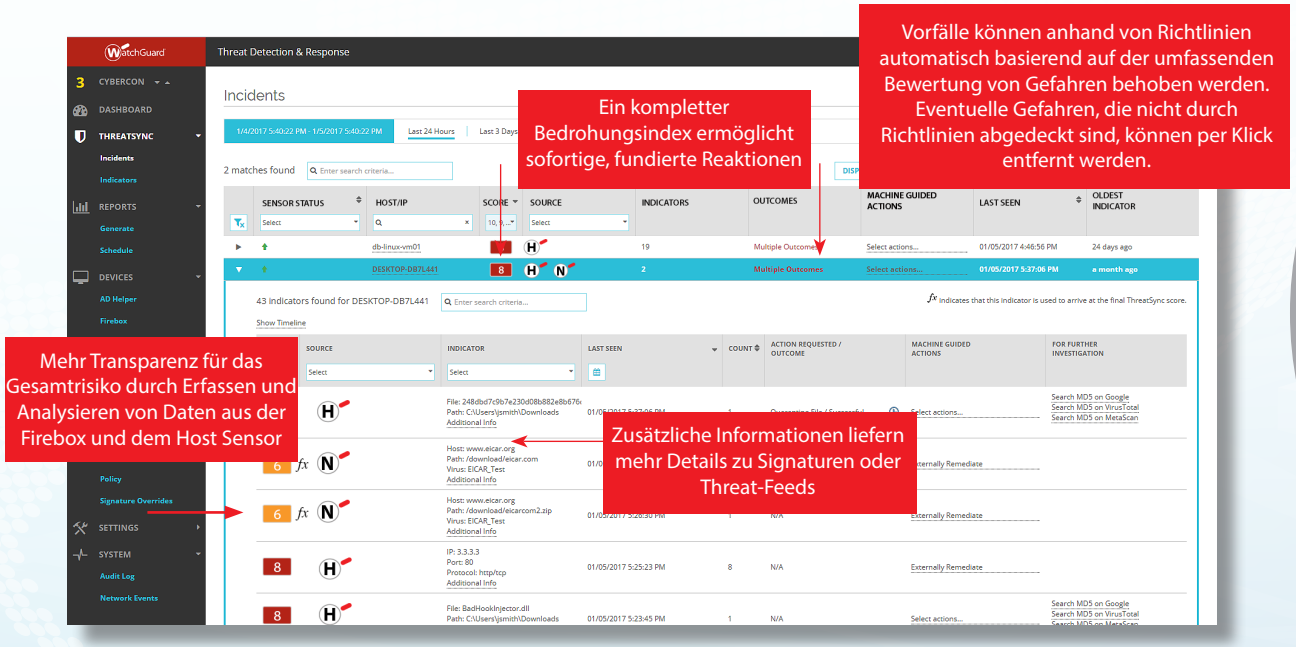
Korrelation



Korrelieren, priorisieren, reagieren – mit WatchGuard

Wenn Korrelation so toll ist, wie kommt's, dass Sie noch nichts davon gehört haben? Gute Frage, ernsthaft. Die Antwort ist einfach: Korrelation ist keine einfache Sache. Die Automatisierung ist dabei besonders knifflig.

Nicht so mit Threat Detection and Response (TDR). Der neue Sicherheitsdienst aus dem Hause WatchGuard bietet kleinen, mittelständischen und dezentral aufgestellten Unternehmen Korrelationsfunktionen auf Enterprise-Niveau.



ThreatSync, das Cloud-basierte Scoring- und Korrelationsmodul von TDR, analysiert Bedrohungsdaten aus der Firebox, an Endpunkten installierte WatchGuard Host Sensors und externe Feeds zu Bedrohungsanalysen. Die Eingangsdaten werden anschließend von ThreatSync analysiert, um einen umfassenden Bedrohungsindex auf Grundlage des Schweregrads einzelner Bedrohungen zu erstellen und danach geeignete Abwehrmaßnahmen zu ergreifen. Malware entwickelt sich laufend weiter und verdächtige Anzeichen können Frühwarnungen bisher noch nicht identifizierter Malware sein. Dank der engen Integration mit WatchGuard APT Blocker können die verdächtigen Dateien nun zur tiefgreifenden Analyse und Neubewertung in eine Cloud-Sandbox der nächsten Generation gesendet werden.

Das Beste daran: Threat Detection and Response ist Bestandteil der Total Security Suite und erfasst sogar Daten von anderen Advanced Security Services in der Suite, einschließlich APT Blocker, WebBlocker und Reputation Enabled Defense (RED). WatchGuard ist der einzige UTM-Anbieter, der all diese Sicherheitsdienste in einem Angebot vereint. Einmalig sind auch die stabilen Korrelationsfunktionen für Unternehmen jeder Größenordnung.

Korrelieren.
Priorisieren. Reagieren.

Threat Detection and Response (TDR) von WatchGuard bietet kleinen, mittelständischen und dezentral aufgestellten Unternehmen Korrelationsfunktionen auf Enterprise-Niveau. Wann immer Sie ein Problem vermuten: Branchenführende Lösungen beleuchten Ihren Endpunkt, erkennen und korrelieren Bedrohungen und schützen Ihre wichtigsten Vermögenswerte.

WatchGuard® Technologies, Inc. gehört zu den weltweit führenden Anbietern von integrierten multifunktionellen Business-Sicherheitslösungen, die Hardware auf Industriestandard mit führenden Sicherheitslösungen und richtlinienbasierten Managementtools intelligent vereinen. WatchGuard liefert Hunderttausenden von Unternehmen weltweit benutzerfreundlichen Schutz auf Enterprise-Niveau.

Weitere Informationen finden Sie unter **WatchGuard.com/TDR**.