

Threat Detection & Response

Korrelieren. Priorisieren. Reagieren.

Internetkriminelle rüsten auf und starten mit immer komplexeren, perfideren Maschen über jede beliebige Verbindung systematische Angriffe auf Ihr Netzwerk. Sicherheitssysteme müssen damit Schritt halten, indem sie sowohl netzwerk- und endpunktübergreifende Erkennungsfunktionen bereitstellen als auch die Möglichkeit zur Korrelation aller Ereignisaktivitäten bieten. Nur auf diese Weise lassen sich Maßnahmen zum lückenlosen Schutz des Netzwerks gezielt ergreifen. Threat Detection and Response (TDR) von WatchGuard setzt Security-Events im Netzwerk und am Endpunkt mit detaillierten Analysen zur Bedrohungslage in Verbindung. Dadurch können potenzielle Angriffe noch früher erkannt und bewertet werden. Sofortmaßnahmen zur Abwehr erfolgen rechtzeitig. Mit TDR können kleine und mittlere Unternehmen und die sie unterstützenden Managed Security Service Provider (MSSP) Angriffe durch hoch entwickelte Schadsoftware sicher abwehren – bevor geschäftskritische Daten oder die Produktivität des Unternehmens ernsthaft in Gefahr geraten.

Korrelation von Netzwerk- und Endpunkt-Ereignissen

ThreatSync ist die neue Cloud-basierte Engine von WatchGuard zur Korrelation und Bewertung von Bedrohungen. Mit ihrer Hilfe profitieren Unternehmen von einem erhöhten Sicherheitsbewusstsein sowie maximaler Reaktionsfähigkeit gegenüber Gefahren innerhalb des gesamten Netzwerks – bis zum Endpunkt. ThreatSync erfasst Ereignisdaten von der WatchGuard Firebox und dem WatchGuard Host Sensor und setzt diese mit aktuellen Cloud-basierten Informationen zur Bedrohungslage in Verbindung. Auf diese Weise ergibt sich ein solides Fundament für die Bewertung von Gefahren und das Ergreifen entsprechender Abwehrmaßnahmen.

Transparenz bis zum Endpunkt

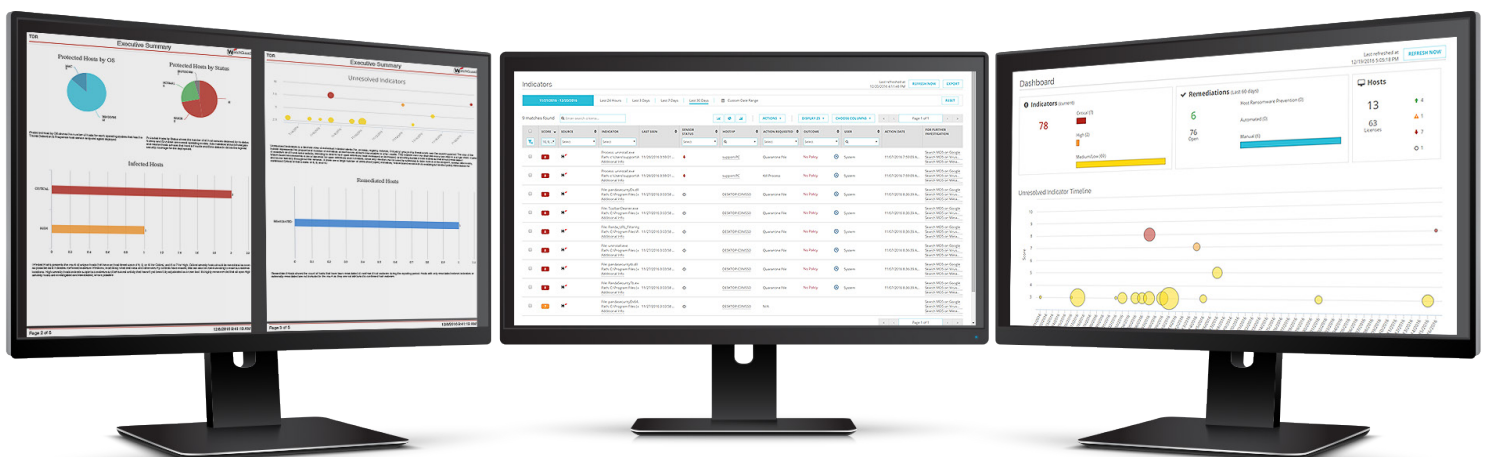
Der schlanke Host Sensor von WatchGuard überwacht und erkennt Bedrohungsaktivitäten in Ihrem Netzwerk. Die jeweiligen Informationen werden kontinuierlich an ThreatSync zur Korrelation und Bewertung gesendet. Daraus resultieren konkrete Handlungsanweisungen zur taktischen Bedrohungsabwehr. Die Host Sensoren werden zentral über die Cloud verwaltet, was MSSP und IT-Administratoren die Bereitstellung und Verwaltung von Host Sensoren an jedem beliebigen Ort der Welt ermöglicht.

Threat Intelligence auf Enterprise-Niveau

Bisher sind meist nur Konzerne mit großen Budgets und noch größeren Sicherheitsteams in den Genuss aktueller Informationen zur Bedrohungslage von Drittanbietern gekommen. Mit Threat Detection and Response macht WatchGuard diese Informationen allen zugänglich – Kunden können von den einschlägigen Sicherheitsvorteilen profitieren, ohne die damit verbundenen Aufwände und Kosten auf sich nehmen zu müssen.

Hoch entwickelter Schutz vor Ransomware

Host Ransomware Prevention (HRP) ist ein Ransomware-spezifisches Modul des WatchGuard Host Sensors. Auf Basis von Verhaltensanalysen sowie aktuellen Verzeichnissen der jeweils im Umlauf befindlichen Gefahren überprüft HRP eine Vielzahl von Merkmalen und ist somit in der Lage zu erkennen, ob ein Ereignis mit einem Ransomware-Angriff in Verbindung steht oder nicht. Auf diese Weise kann HRP bei ernsthaften Gefahren automatisch einen Ransomware-Angriff verhindern – noch bevor am Endpunkt eine Dateiverschlüsselung stattfindet.



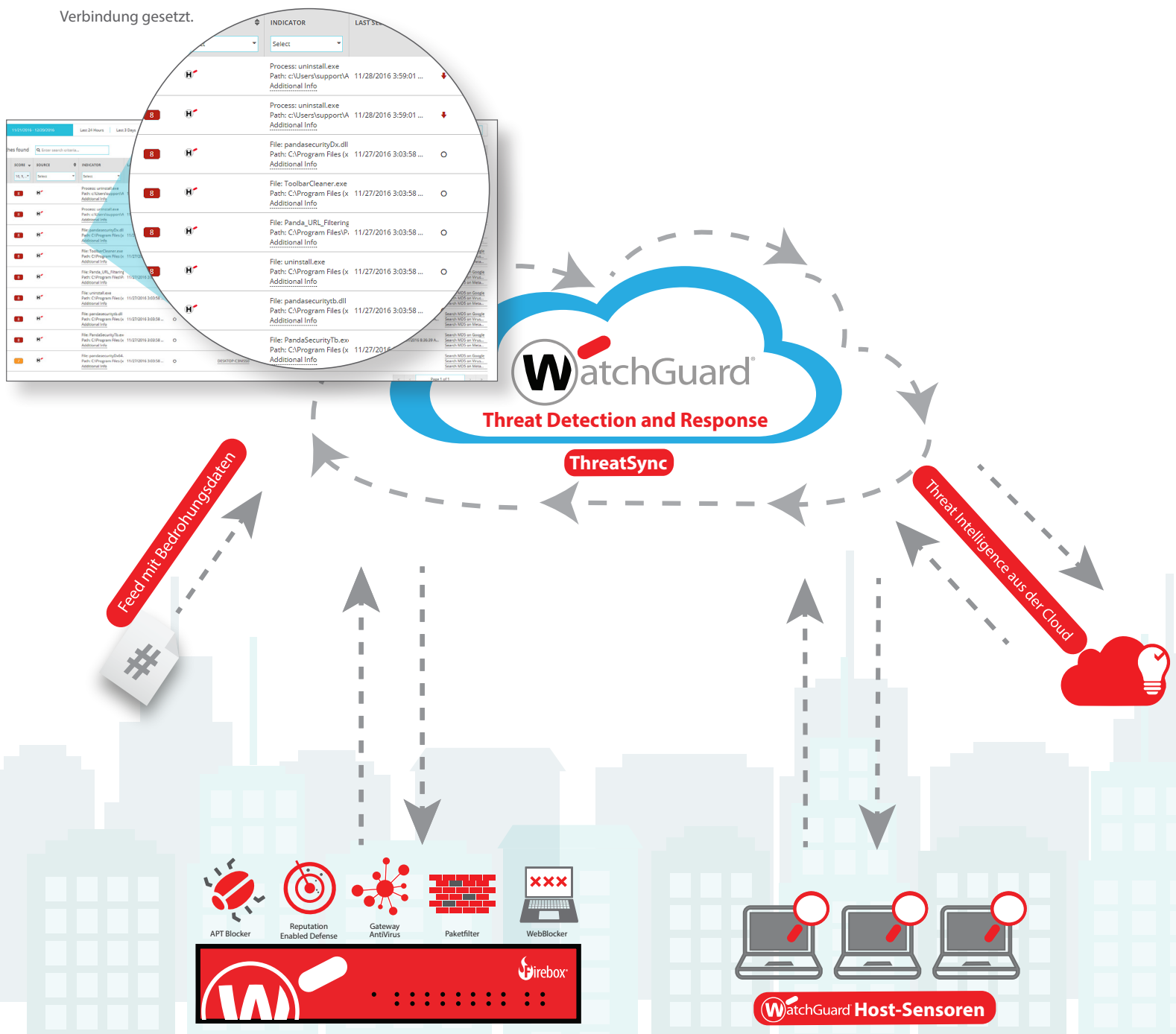
Mehr Sicherheit dank Korrelation

Mit ThreatSync, der neuen Cloud-basierten Engine zur Korrelation und Bewertung von Bedrohungen, profitieren Unternehmen von einem erhöhten Sicherheitsbewusstsein sowie maximaler Reaktionsfähigkeit gegenüber Gefahren innerhalb des gesamten Netzwerks – bis zum Endpunkt.

ThreatSync kann Ereignisdaten im Netzwerk über die verschiedensten Sicherheitsdienste der Firebox ermitteln – beispielsweise APT Blocker, Reputation Enabled Defense (RED), Gateway AntiVirus und WebBlocker. Diese Ereignisse werden mit den Bedrohungsaktivitäten, die der WatchGuard Host Sensor identifiziert, sowie aktuellen Daten zur allgemeinen Bedrohungslage in Verbindung gesetzt.

Alle diese Informationen werden von ThreatSync analysiert, bewertet und entsprechend des Schweregrads eingeordnet. Die Rückmeldung spezifischer Handlungsanweisungen an den Host Sensor – wie beispielsweise die Aufforderung zur Isolierung von Dateien, zum Abbrechen von Prozessen oder Löschen von Registrierungswerten – erfolgt umgehend.

Mithilfe dieser spezifischen Technologie verkürzt sich nicht nur die Zeit der Gefahrenerkennung auf Basis maximaler Transparenz im Netzwerk und am Endpunkt. Letztendlich können dank nachhaltiger Bewertung passgenaue Gegenmaßnahmen ergriffen werden – effektiv und vor allem rechtzeitig.



Eine Appliance. Ein Paket. Total Security.

Threat Detection and Response ist Teil der WatchGuard Total Security Suite, die außerdem fortschrittliche Sicherheitslösungen wie APT Blocker, WebBlocker, Gateway AntiVirus, Intrusion Prevention Service and Reputation Enabled Defense beinhaltet.

Obwohl jede einzelne dieser Sicherheitslösungen für sich Schutz vor hoch entwickelten Bedrohungen bietet, profitieren Anwender am meisten, wenn die unterschiedlichen Sicherheitsfunktionen auf der Firebox ineinander greifen. Dadurch ergibt sich umfassende Sicherheit und maximale Effizienz – ganz ohne Leistungseinbußen.

Produkt	Support	TOTAL SECURITY	Basic Security
Stateful Firewall	✓	✓	✓
Mobile VPN	✓	✓	✓
VPN zwischen Standorten	✓	✓	✓
Anwendungsproxies	✓	✓	✓
Intrusion Prevention Service (IPS)		✓	✓
App Control		✓	✓
WebBlocker		✓	✓
spamBlocker		✓	✓
Gateway AntiVirus		✓	✓
Reputation Enabled Defense (RED)		✓	✓
Network Discovery		✓	✓
APT Blocker		✓	
Data Loss Protection (DLP)		✓	
Dimension Command		✓	
Threat Detection & Response		✓	
Support	Standard (24x7)	Gold (24x7)	Standard (24x7)

Firebox-Modell	Enthaltene Host Sensoren
T10	5
T30	20
T50	35
T70/M200	60
M300	150
M400/M440/M500/ M4600/M5600	250
XTMv S	20
XTMv M	50
XTMv L	150
XTMv DC	250

Sie benötigen weitere Host Sensoren?

Die Anzahl der Host Sensoren pro Appliance ist festgelegt – je nachdem, welche Firebox der M- oder T-Serie oder welche XTMv-Appliance bei Ihnen zum Einsatz kommt. Weitere Host Sensoren sind bei Bedarf über ein Upgrade-Paket erhältlich.

Zusatz-Optionen Host Sensor
10 Host Sensoren
25 Host Sensoren
50 Host Sensoren
100 Host Sensoren
250 Host Sensoren
500 Host Sensoren

Threat Detection und Response beinhaltet je nach eingesetztem Appliance-Modell eine feste Anzahl an Host Sensoren. Weitere Host Sensoren können beliebig erworben und der Gesamtanzahl, die dem Kunden jeweils zur Verfügung steht, hinzugefügt werden.

Skalierbare Sicherheit einfach umgesetzt

Mithilfe von Threat Detection and Response ergeben sich ganz neue Möglichkeiten, IT-Sicherheit passgenau umzusetzen und zu skalieren. Der Cloud-basierte Dienst erleichtert Administratoren die schnelle Bereitstellung von Host Sensoren innerhalb ihrer gesamten Organisation. Die Erstellung von Richtlinien und die Abwehr von Bedrohungen erfolgt per Mausklick.

TDR lässt sich leicht skalieren und wächst so mit Ihrem Unternehmen mit. Jede TDR-Instanz wartet abhängig von der eingesetzten Appliance mit einer festen Anzahl von Host Sensoren auf. Mit Upgrade-Paketen lassen sich jedoch jederzeit weitere Host Sensoren hinzufügen, um die jeweiligen organisatorischen Anforderungen exakt abdecken zu können.

Zeit und Ressourcen sind für Ihr Unternehmen wertvoll. Wenn Ihnen die Verwaltung Ihrer Sicherheitsdienste in den eigenen Reihen zu aufwendig ist, bietet Ihnen unser weitreichendes Netzwerk aus MSSP-Partnern die Möglichkeit, die täglichen Routine-Aufgaben einem kompetenten Partner zu übertragen – während Sie selbst voll und ganz in den Genuss der Vorteile von Threat Detection and Response kommen.



Erfahren Sie mehr über Threat Detection and Response. Weitere Informationen zum neuesten Sicherheitsdienst erhalten Sie auf unserer Website www.watchguard.com/TDR.

Los geht's

WatchGuard verfügt über eines der größten Partnernetzwerke der Branche. Neben den klassischen Vertriebspartnern umfasst dieses auch zahlreiche Service Provider. Für den Einstieg empfehlen wir einen Besuch unserer Webseite. Dort finden Sie den passenden Partner für Ihr Unternehmen. Selbstverständlich können Sie uns auch direkt ansprechen. Wir beantworten gerne alle Fragen und vermitteln Ihnen den Kontakt zu einem Partner, der Ihren Anforderungen optimal gerecht wird.

- Besuchen Sie die Seite „Händler finden“, um einen Vertriebspartner in Ihrer Nähe auszumachen: <http://www.watchguard.com/de/wgrd-international/find-a-reseller>
- Sprechen Sie mit einem unserer eigenen Sicherheitsexperten: <http://www.watchguard.com/de/wgrd-international/contact-us>

Über WatchGuard

WatchGuard Technologies gehört zu den führenden Anbietern im Bereich Netzwerksicherheit. Mehr als 75.000 Unternehmen weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung insbesondere kleine bis mittlere sowie dezentral aufgestellte Unternehmen vom Einsatz profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington verfügt WatchGuard über Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.com.