Schutz auch vor modernsten Cyber-Angriffen durch Korrelation

Jonas Spieckermann | Senior Sales Engineer
Jonas.Spieckermann@watchguard.com
WatchGuard Technologies Inc.


ena Decrypt0r 2.0
Ooops, your files have been encrypted!
German
Was geschah mit meinem Computer?
Ihre wichtigen Dateien sind verschlüsselt.
Viele Ihrer Dokumente, Fotos, Videos, Datenbanken und andere Dateien sind nicht mehr zugänglich, weil sie verschlüsselt wurden. Vielleicht sind Sie damit beschäftigt, einen Weg zu finden, um Ihre Dateien wiederherzustellen, aber verschwenden Sie nicht Ihre Zeit. Niemand kann Ihre Dateien ohne unseren Entschlüsselungsdienst wiederherstellen.
Kann ich meine Dateien wiederherstellen?
Sicher. Wir garantieren, dass Sie alle Ihre Dateien sicher und einfach wiederherstellen können. Aber du hast nicht genug Zeit.
Sie können einige Ihrer Dateien kostenlos entschlüsseln. Versuchen Sie jetzt, indem Sie auf <Decrypt> klicken.
Aber wenn du alle deine Dateien entschlüsseln willst, musst du bezahlen.
Sie haben nur 3 Tage, um die Zahlung einzureichen. Danach wird der Preis verdoppelt.
Auch wenn du nicht in 7 Tagen bezahlt hast, kannst du deine Dateien nicht für immer wiederherstellen.
Wir haben freie Veranstaltungen für Benutzer, die so arm sind, dass sie nicht in 6 Monaten bezahlen können.
Wie bezahle ich?
Die Zahlung wird nur in Bitcoin akzeptiert. Für weitere Informationen klicken Sie auf <About bitcoin>.
Payment will be raised on
6/1/2017 14:39:55
Time Left
Your files will be lost on
6/5/2017 14:39:55
Time Left
bout bitcoin
ow to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt


Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.

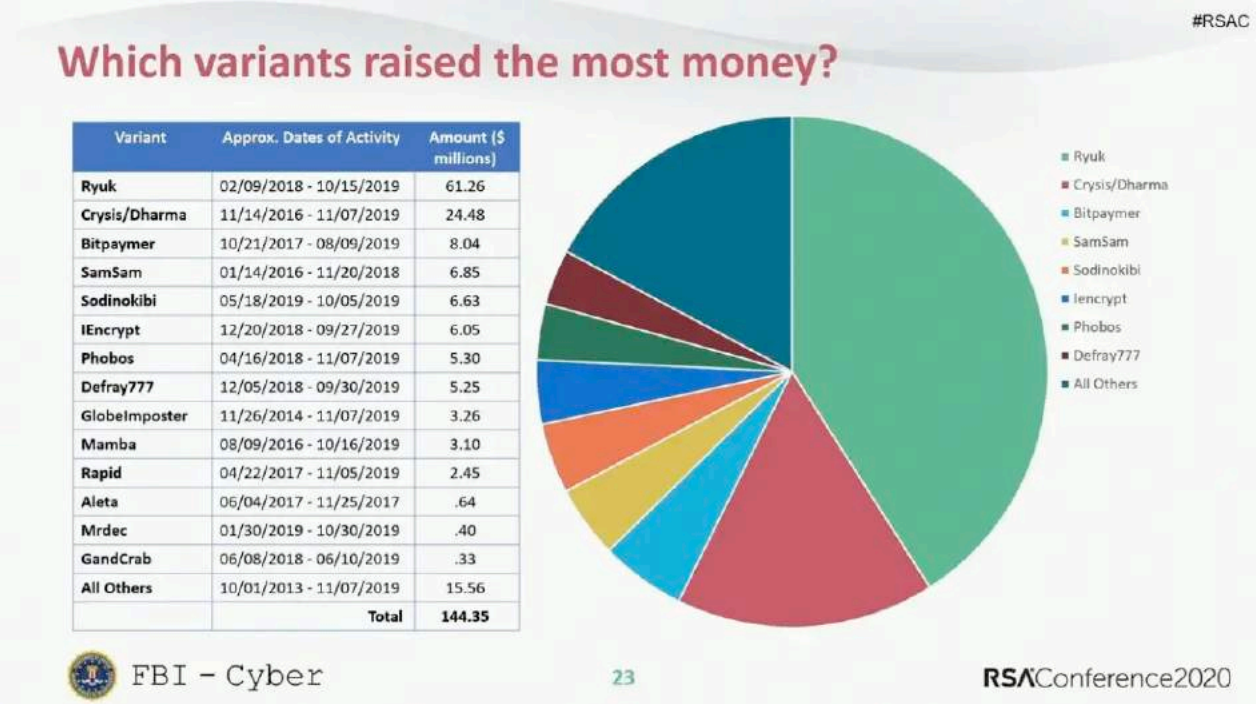

ALL YOUR PERSONAL FILES ARE ENCRYPTED
All your data (photos, documents, database, ...) have been encrypted with a private and unique key generated for this computer. It means that you will not be able to access your files anymore until they're decrypted. The private key is stored in our servers and the only way to receive your key to decrypt your files is making a payment.
The payment has to be done in Bitcoin to a unique address that we generated for you. Bitcoins are a virtual currency to make online payments. If you don't know how to get Bitcoins, you can google "How to Buy Bitcoins" and follow the instructions.
YOU ONLY HAVE 4 DAYS TO SUBMIT THE PAYMENT! When the provided time ends, the payment will increase to 5 Bitcoins. Also, if you don't pay in 7 days, your unique key will be destroyed and you won't be able to recover your files anymore.
To recover your files and unlock your computer, you must send 1.2 Bitcoin (500$), to the next Bitcoin address:
Click Here to Show Bitcoin Address
WARNING!
DO NOT TRY TO GET RID OF THIS PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTIONS.
If above bitcoin address didn't work use default address to decrypt data(17XajvHHeWbfKfNwnS7sHRMAEXvQUUGNd)


PETYA
Start
Payment
FAQ
Support
English
Your computer has been encrypted
The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.
The price will be doubled in:
6 days 13 hours 43 minutes 10 seconds
Start the decryption process

Verhinderte Angriffe in Europa

https://www.secplicity.org/threat-landscape/?s=2020-01-01&e=2020-03-17&type=all&region=emea

Warum finden so viele Cyber-Angriffe statt?



Variant	Approx. Dates of Activity	Amount ($ millions)
Ryuk	02/09/2018 - 10/15/2019	61.26
Crysis/Dharma	11/14/2016 - 11/07/2019	24.48
Bitpaymer	10/21/2017 - 08/09/2019	8.04
SamSam	01/14/2016 - 11/20/2018	6.85
Sodinokibi	05/18/2019 - 10/05/2019	6.63
IEncrypt	12/20/2018 - 09/27/2019	6.05
Phobos	04/16/2018 - 11/07/2019	5.30
Defray777	12/05/2018 - 09/30/2019	5.25
GlobeImposter	11/26/2014 - 11/07/2019	3.26
Mamba	08/09/2016 - 10/16/2019	3.10
Rapid	04/22/2017 - 11/05/2019	2.45
Aleta	06/04/2017 - 11/25/2017	.64
Mrdec	01/30/2019 - 10/30/2019	.40
GandCrab	06/08/2018 - 06/10/2019	.33
All Others	10/01/2013 - 11/07/2019	15.56
	Total	144.35

https://www.heise.de/security/meldung/FBI-Ransomware-Opfer-zahlten-ueber-140-Millionen-4675780.html

Den Herausforderungen sicher entgegentreten

Malware Schutz auch außerhalb des Firmennetzwerks

Zusammenführung der erfassten Vorkomnisse aus Netzwerk- und Endgerätesicht zum Schutz des gesamten Unternehmens.

Erweiterte Schutzfunktionen sind nötig gegen immer fortschrittlichere Angriffe

Multi-Faktor Authentifizierung ist erforderlich

Zero-day Malware und APTs sind weit verbreitet

Schutz vor Ransomware ist ein bedeutender Baustein

Ein mehrschichtiger Sicherheitsansatz

1. Gateway Antivirus

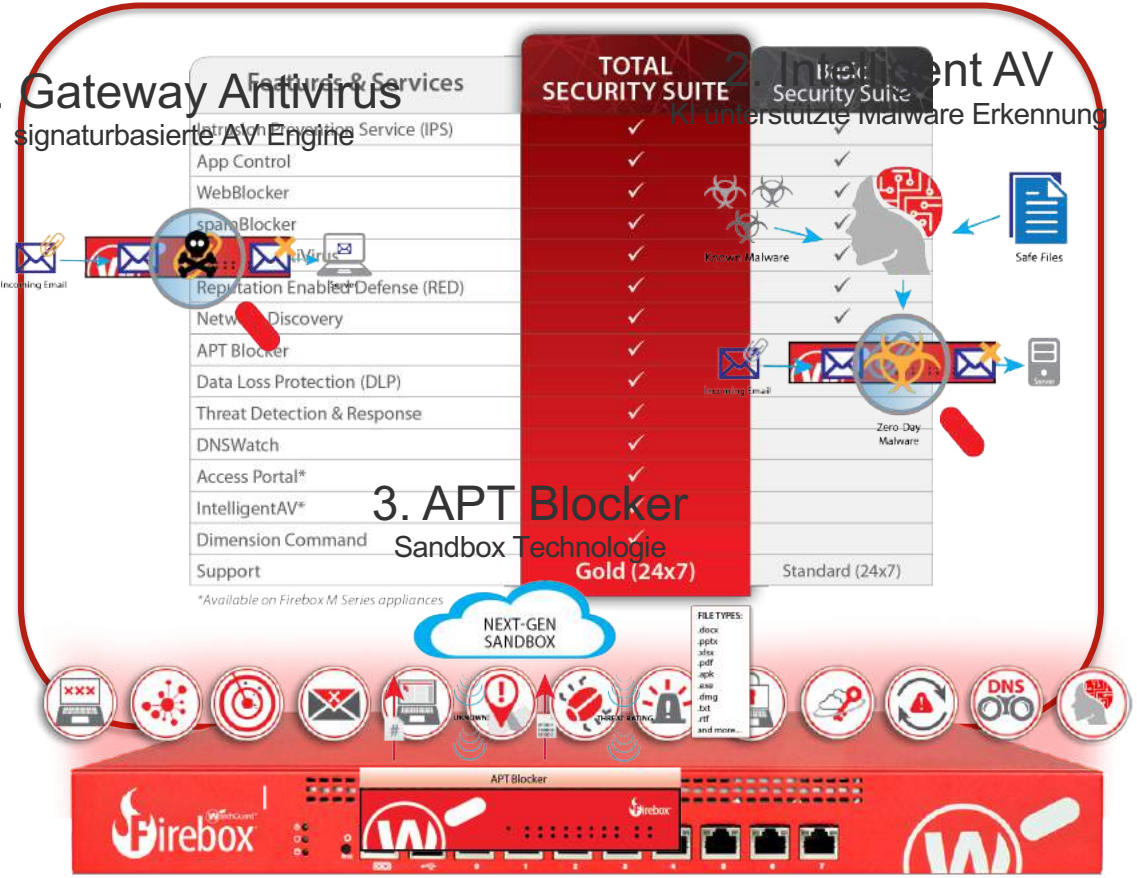
signaturbasierte AV Engine

2. Intelligent AV

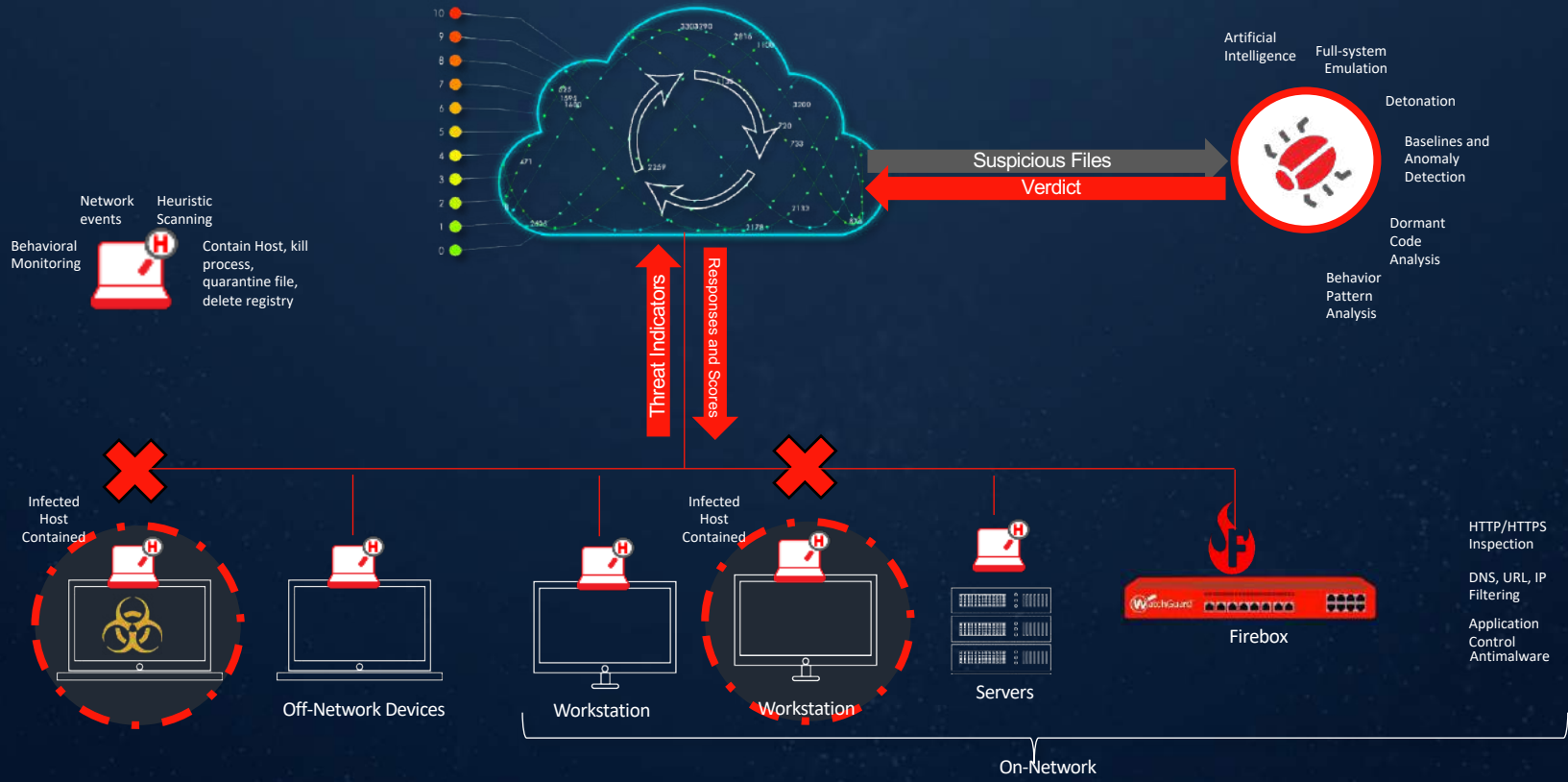
KI unterstützte Malware Erkennung

3. APT Blocker

Sandbox Technologie

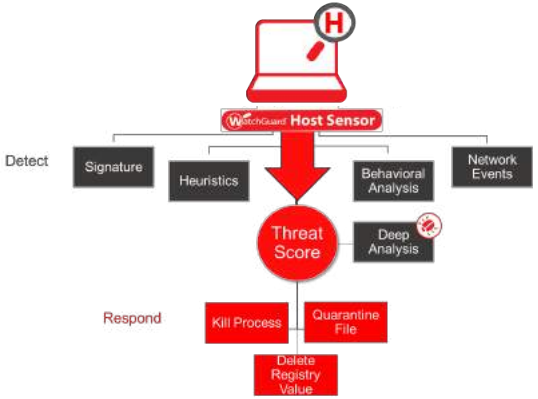


Threat Detection & Response



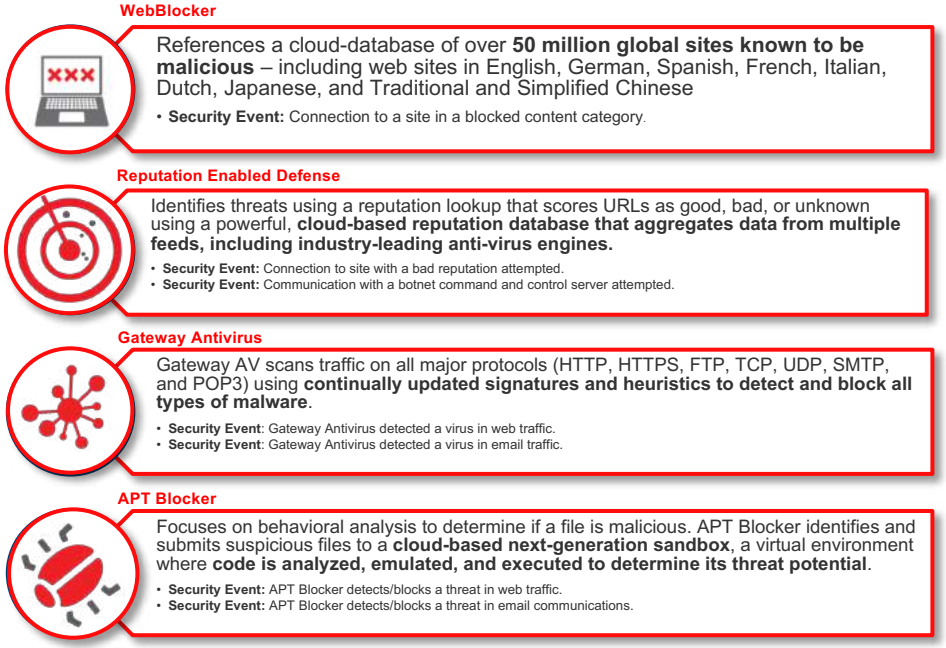
Host Sensor

- Überwacht und erkennt gefährliche Aktivitäten am Endgerät.
- Sendet die Host Sensor Events regelmäßig an TDR ThreatSync zur Beurteilung und Korrelation mit Netzwerk-Events.
- Potentiell schädliche Dateien und Prozesse werden zur Detailanalyse an den APT Blocker übergeben.
- Automatische Gegenmaßnahmen sind über Kill Process, Quarantine File, Delete Registry Value und Contain Host möglich.
- Schützt Systeme in- und außerhalb des Firmen-Netzwerks.



WatchGuard Firebox und TDR

Kommunikation zu **Domains und IP Adressen**, die bekanntermaßen schädlich sind, können ein Indikator für **vorhandene Infektionen** sein. WatchGuard Firebox steigert die Erkennungsrate mit **TDR,** durch die **automatische Korrelation** von Netzwerk-Verhalten und **sicherheitskritischen Vorfällen,** die durch WatchGuard's Security Services erkannt werden.

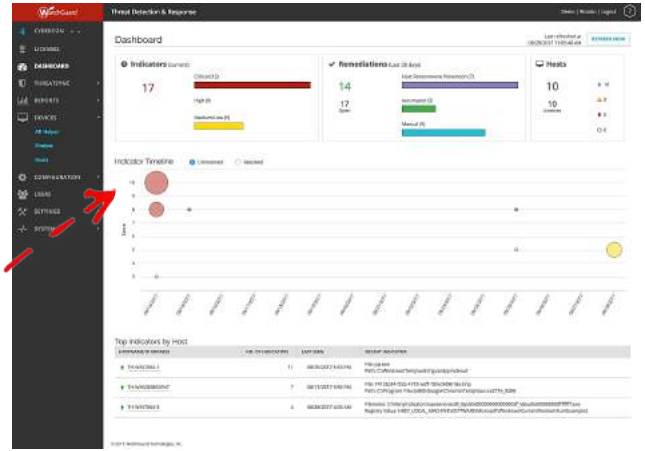


Korrelation - Threat Detection & Response

Für Hier und zum Mitnehmen:

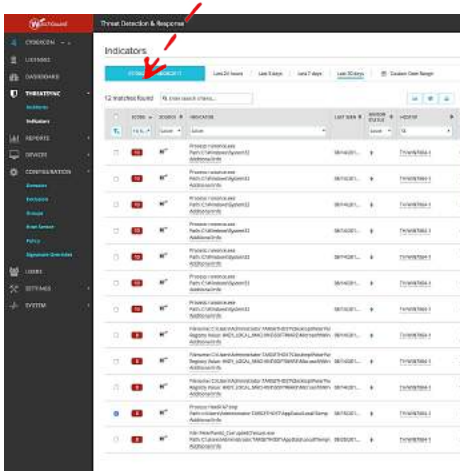
Ganzheitliche Betrachtung durch Integration der Endpoints

Den Überblick behalten und Abhilfe schaffen

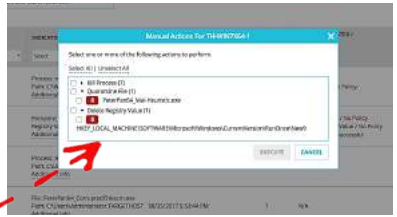


Schneller Überblick zu Bedrohungsaktivitäten im gesamten Unternehmen

Die Gefahr beurteilen



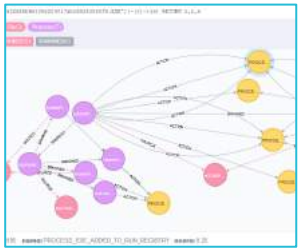
Beseitigung zahlreicher Bedrohungen



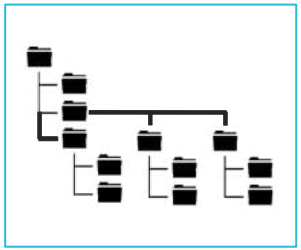
Schutz vor Ransomware

Host Ransomware Prevention verhindert die Ausführung von Ransomware bevor eine schädliche Verschlüsselung stattfindet. Somit können Ransomware Angriffe gestoppt werden bevor ein Schaden entsteht.

Malicious Behaviors Prevented



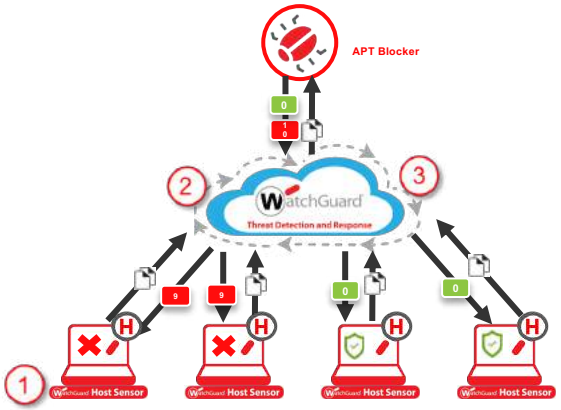
Unique Decoy Directory Honeypot

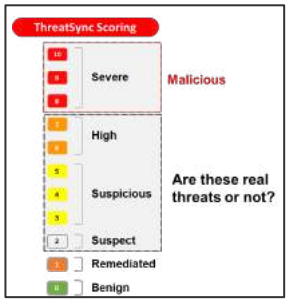


Integration des APT Blockers

Die Integration des APT Blockers ermöglicht eine weitreichende Analyse der potentiell gefährlichen Vorfälle in einer Cloud-basierten Sandbox. Nach Feststellung einer Gefahr kann eine automatische Bereinigung erfolgen.

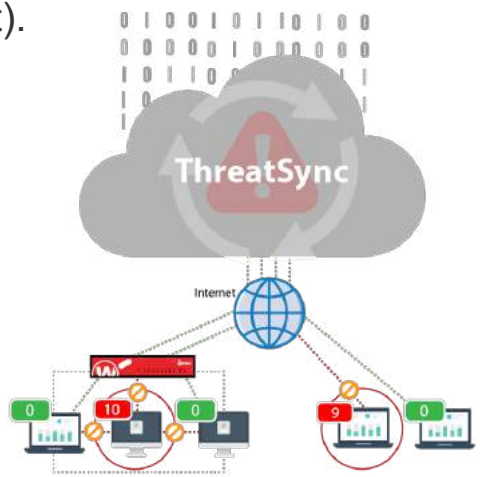
1. Suspicious files sent from the host sensor to APT Blocker via ThreatSync.
2. APT Blocker executes the malware and analyzes its behavior.
3. If APT Blocker discovers a threat, ThreatSync will automatically update the threat score to guide response.





Host Containment

- Infizierte Hosts werden im Netzwerk isoliert (Containment).
- Verhindert eine interne Verbreitung von Malware.
- Auch außerhalb der geschützten Netzwerke kann Contain Host genutzt werden.
- Netzwerk-Zugriff wird automatisiert freigegeben, wenn die Bereinigung erfolgreich war.



Live Demo
Threat Detection & Response

Vielen Dank!

Jonas Spieckermann | Senior Sales Engineer
Jonas.Spieckermann@watchguard.com
WatchGuard Technologies Inc.