Best Practices – WatchGuard Firebox – Malware am Perimeter blocken

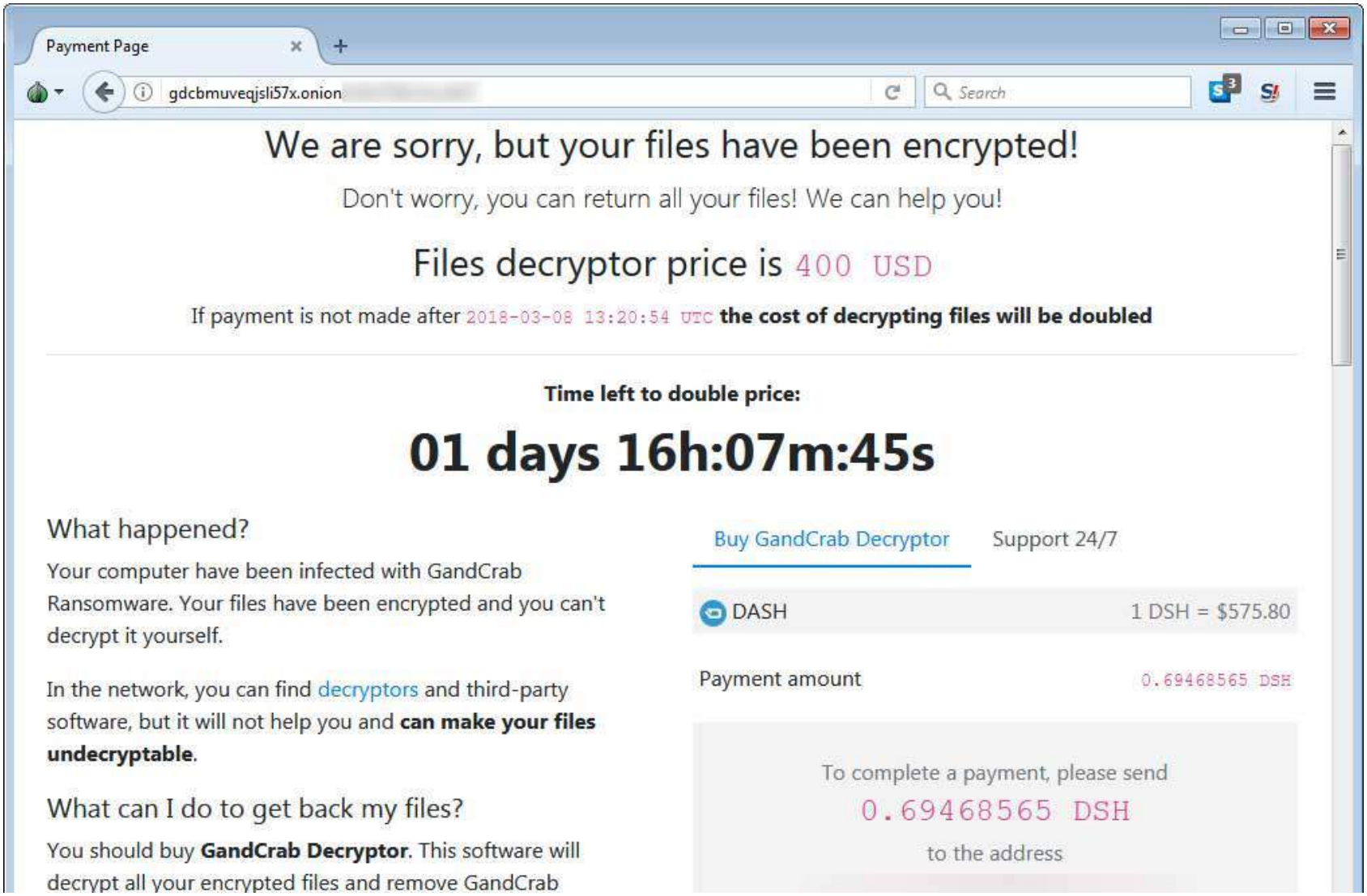
Thomas Fleischmann
Senior Sales Engineer, Central Europe
Thomas.Fleischmann@watchguard.com

Agenda

- Aktuelle Situation
  - Immer noch Ransonware !
- Lösungsansatz von WatchGuard
  - Multi-Layer Ansatz
- IntelligentAV
- APT Blocker und KI

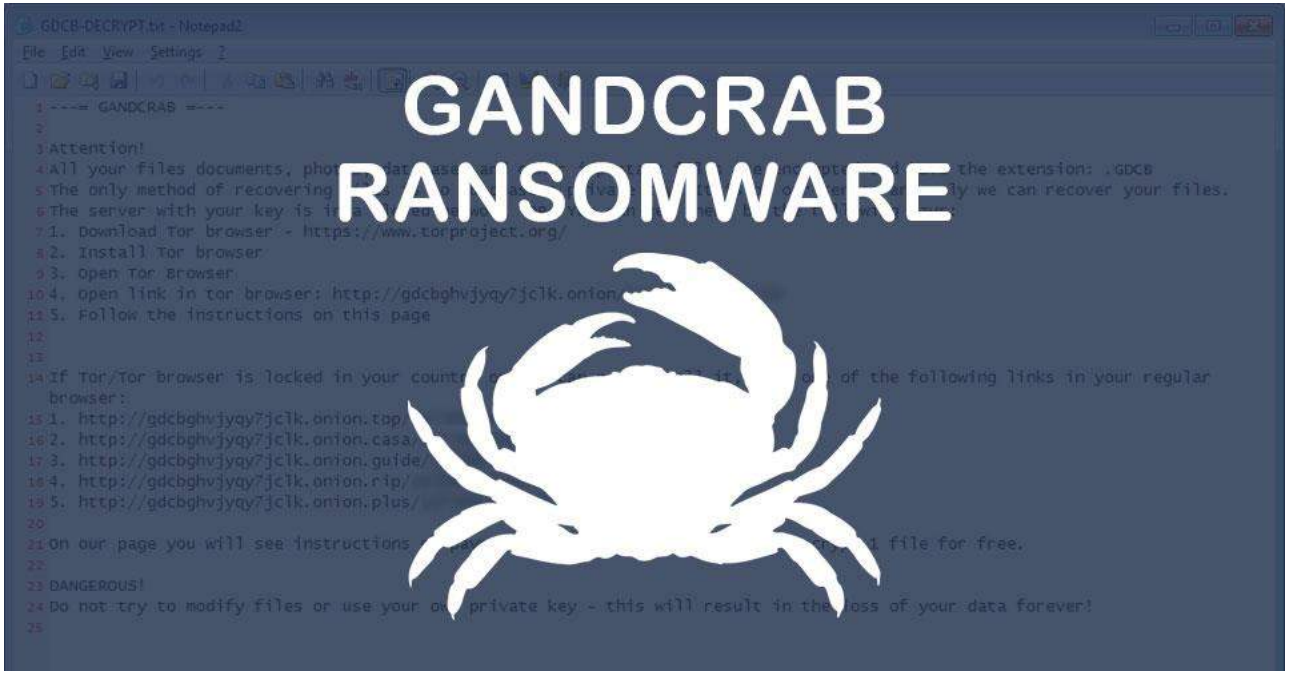
Aktuelle Situation

Aktuelle Situation



Aktuelle Situation

- Infektionsweg
  - Phishing Email
  - Passwortgeschütztes RAR-Archiv, in dem sich die Datei "Peter Reif – CV – Bewerbung – Arbeitsagentur.pdf.exe" befindet
  - Gleicher Angriffsart wie die Ransonware ColdenEye



Aktuelle Situation

- Infektion nicht nur über Phishing E-Mail, sondern als Download durch ***Vidar***:
  - relativ neuer, aber sehr vielseitiger Trojaner, der neben Dokumenten, Passwörtern, Browserverlauf und E-Mail-Daten sogar Daten in Software mit Zwei-Faktor-Authentifizierung auslesen kann.
  - Außerdem greift Vidar auch sogenannte Wallets an, also digitale Geldbeutel für Krypto-Währungen wie Bitcoin.
  - Lädt GrandGrab über sein C&C nach, sobald alle Daten abgeflossen sind.
- aktuelle Welle verbreitet sich über das Fallout Exploit Kit, das Sicherheitslücken im Flash Player und Windows Explorer ausnutzt.

Aktuelle Situation

Emotet und seine Freunde

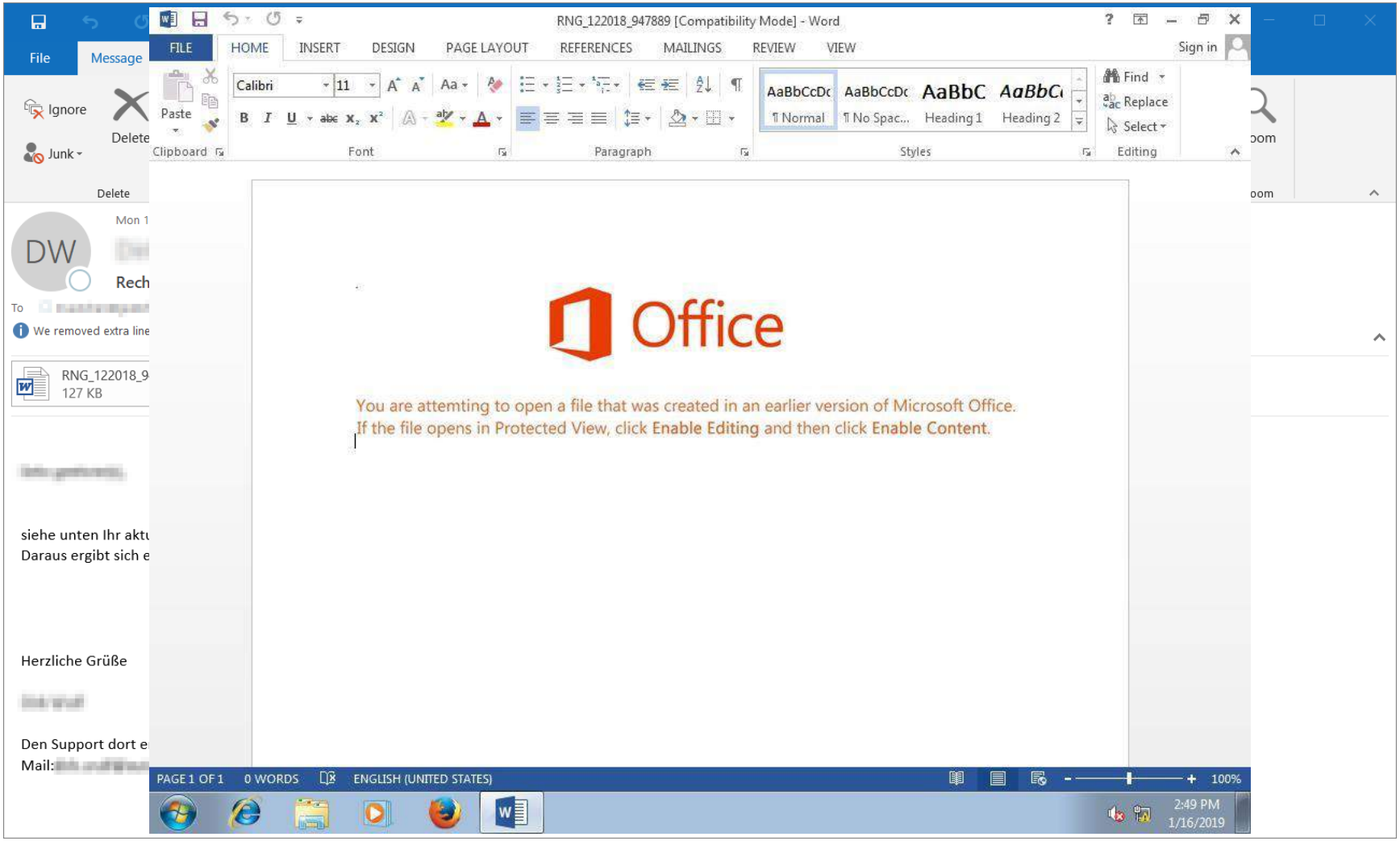
- Getarnt in einem Word-Dokument, dringt Emotet beim Ausführen der Datei in ein Unternehmensnetzwerk ein und kundschaftet dieses aus.
- Als „Türöffner“ lädt er den Banking-Trojaner TrickBot nach, der unter anderem Kontozugangsdaten kopiert.
- Diese Information gibt er an die Ransomware Ryuk weiter, die schließlich als letztes nachgeladen wird. Ryuk verschlüsselt nun alle im System befindlichen Dateien, die TrickBot und Emotet zuvor als sensibel bzw. wichtig eingestuft haben.

Aktuelle Situation

Besonderheiten bei diesen Trio:

- Das besonders Hinterlistige an *Ryuk* ist allerdings, dass es neben der Verschlüsselung wichtiger Daten im gleichen Zuge alle hiervon existierenden Sicherheitskopien löscht und somit die Wiederherstellung erheblich erschwert.
- Die geforderte Summe richtet sich zudem nach dem Wert, den TrickBot als derzeitigen finanziellen Verfügbarkeitsrahmen des Unternehmens ausmachen konnte.

Aktuelle Situation



Aktuelle Situation

Q3 2018 Overall Malware Trends:

- **40,265 Fireboxes** reported to the Firebox Feed in Q3. A 1% increase quarter-on-quarter (QoQ) and **34.6% increase year-over-year (YoY)**. We are pleased to see the number of reporting boxes continue to grow and ask customers to continue opting in to this data sharing.
- GAV services worked significantly harder this quarter compared to last, blocking **14,343,015 malware variants; a 34% increase QoQ, yet 36% decrease YoY.**
- **APT Blocker** contributed more this quarter as well, **blocking 3,574,901 additional threats**. This represents a **13% increase QoQ** and, more significantly, a **14% increase YoY**.
- However, despite the growth in APT Blocker hits, the comparably larger increase in GAV detection **lowered our zero day malware percentage to 28.9%**. That is a **22.7% decrease from Q2 (37.4%)**, but a **4% increase YoY**.
- To summarize, we saw a **23% QoQ increase in malware overall**.

Aktuelle Situation

New Dynamic ISR Threat Landscape Page

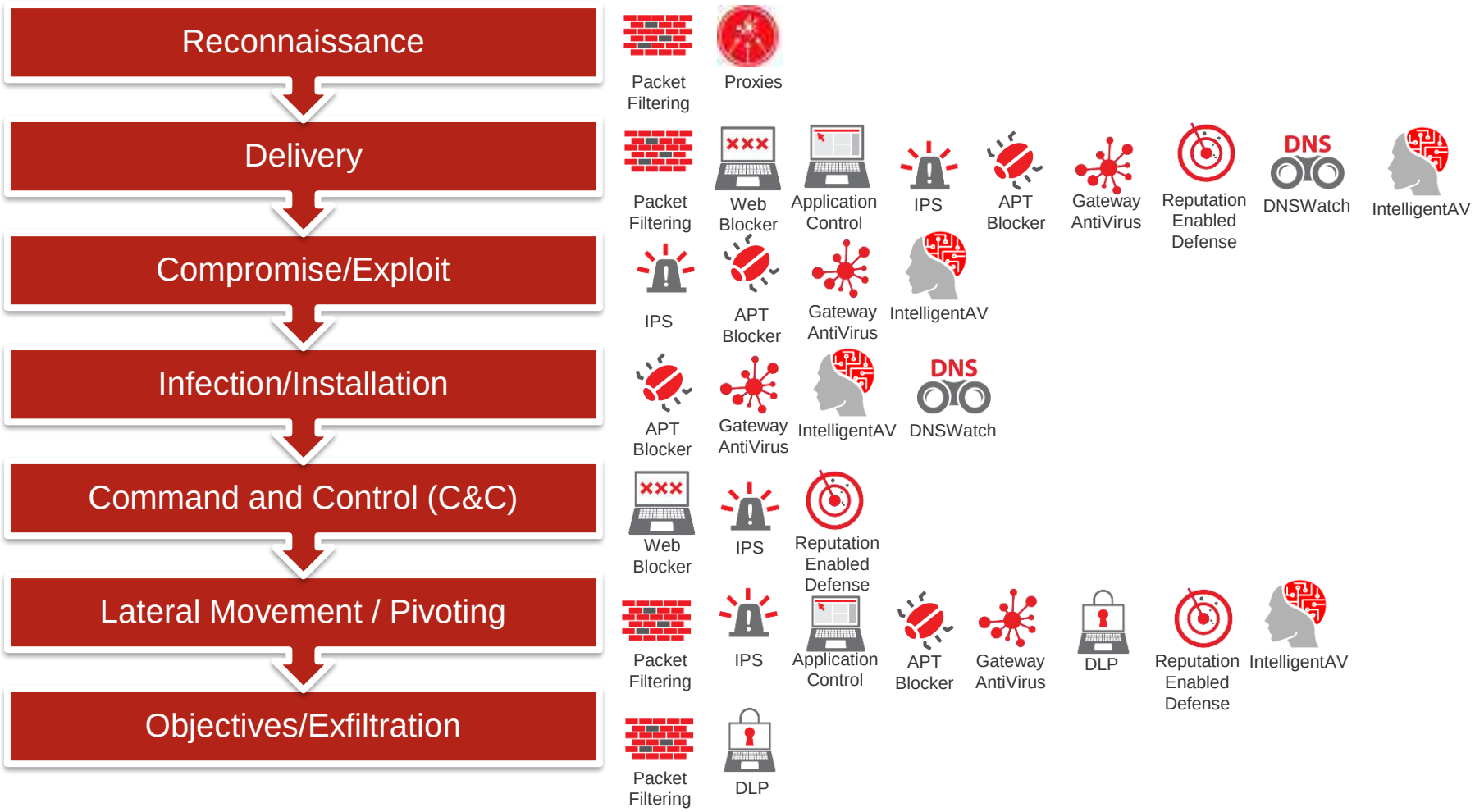
1. Dynamic date ranges
2. Filter by region or country
3. Filter by malware / network attacks

DEMO TIME:

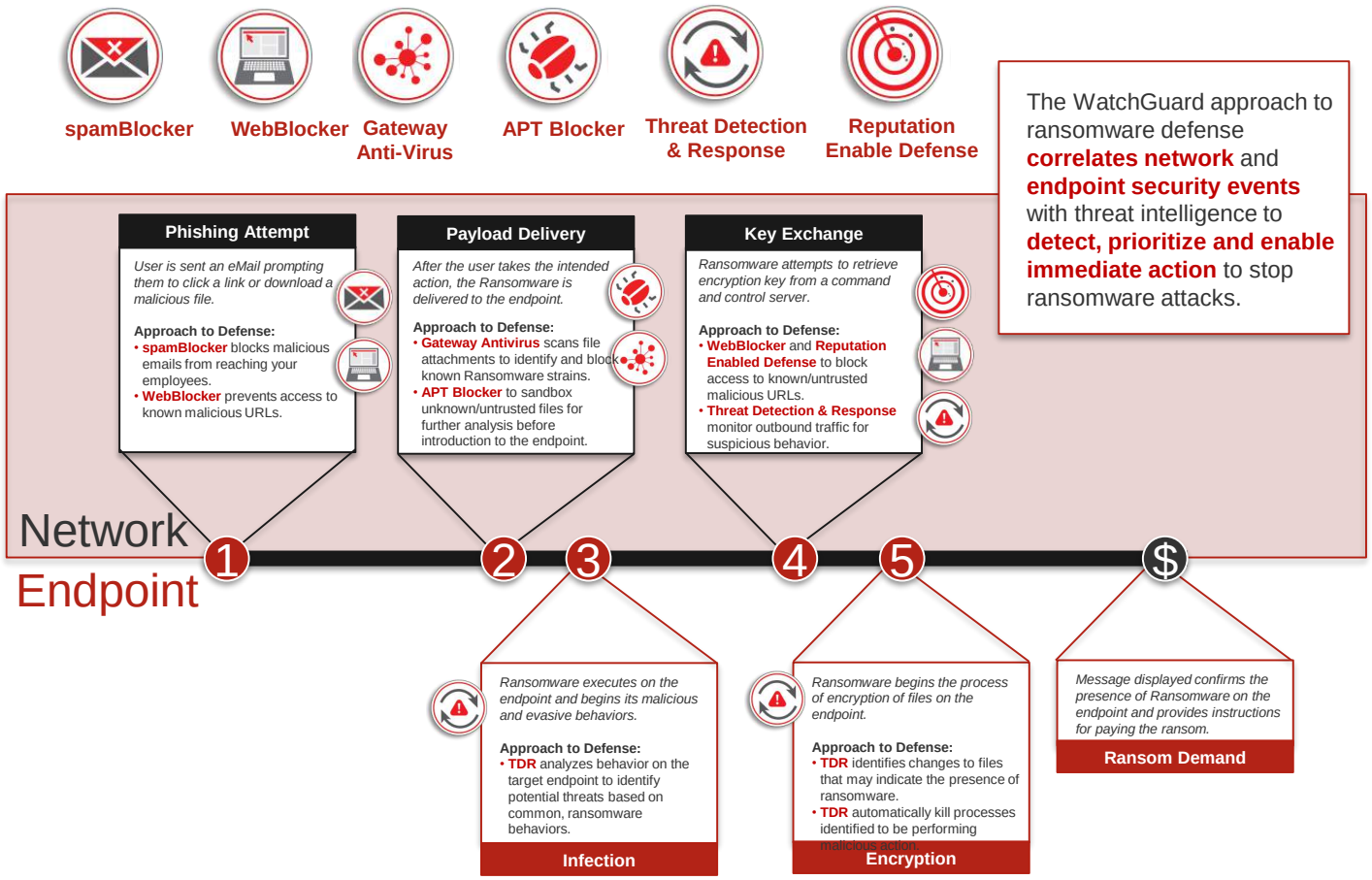
https://www.secplicity.org/threat-landscape/

Lösungsansatz von WatchGuard

WatchGuard **Breaks** the KillChain



WatchGuard Firebox UTM mit der Total Security Suite schützt gegen alle 5 Stufen eines Ransomware-Angriffs



The WatchGuard approach to ransomware defense **correlates network** and **endpoint security events** with threat intelligence to **detect, prioritize and enable immediate action** to stop ransomware attacks.

WatchGuard bietet die umfassendste Ransomware-Lösung für kleine und mittlere Unternehmen

Basic Security

spamBlocker

Real-time, continuous, and highly reliable protection from spam and phishing attempts. WatchGuard spamBlocker is so fast and effective, it can review up to 4 billion messages per day, while providing effective protection regardless of the language, format, or content of the message.

WebBlocker

In addition to automatically blocking known malicious sites, WatchGuard WebBlocker delivers granular content and URL filtering tools to block inappropriate content, conserve network bandwidth, and increase employee productivity.

Gateway Anti-Virus

Leverage our continuously updated signatures to identify and block known, ransomware, spyware, viruses, trojans, worms, rogueware and blended threats – including new variants of known viruses. At the same time, heuristic analysis tracks down suspicious data constructions and actions to make sure unknown viruses don't slip by.

Reputation Enable Defense

A powerful, cloud-based web reputation service that aggregates data from multiple feeds to provide real-time protection from malicious sites and botnets, while dramatically improving web processing overhead.

Total Security

APT Blocker

APT Blocker uses an award-winning next-generation sandbox to detect and stop the most sophisticated attacks including ransomware, zero day threats, and other advanced malware designed to evade traditional network security defenses.

ThreatSync

Security data collected from the Firebox and WatchGuard Host Sensor at the endpoint is correlated by enterprise-grade threat intelligence to detect, prioritize and enable immediate action against ransomware attacks.

DNSWatch

Using aggregated threat intelligence, DNSWatch prevents people from interacting with malicious content, collects data about attempted attacks, and presents users with educational materials to prevent future attacks.

IntelligentAV

IntelligentAV leverages AI to better defend against continuously evolving zero day malware. While signature-based AV solutions are only able to detect known threats, IntelligentAV makes it possible to predict threats months before they are released.

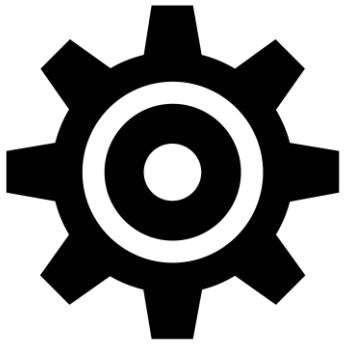

IntelligentAV

Wie unterscheidet sich KI von der menschlichen Intelligenz?

Humans

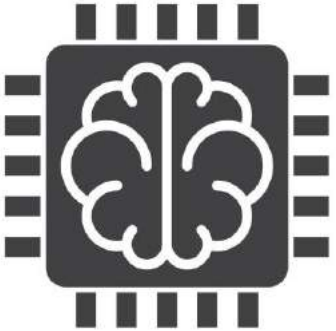
Learn From Experience

Traditional Programming



Follow Instruction

AI/ML

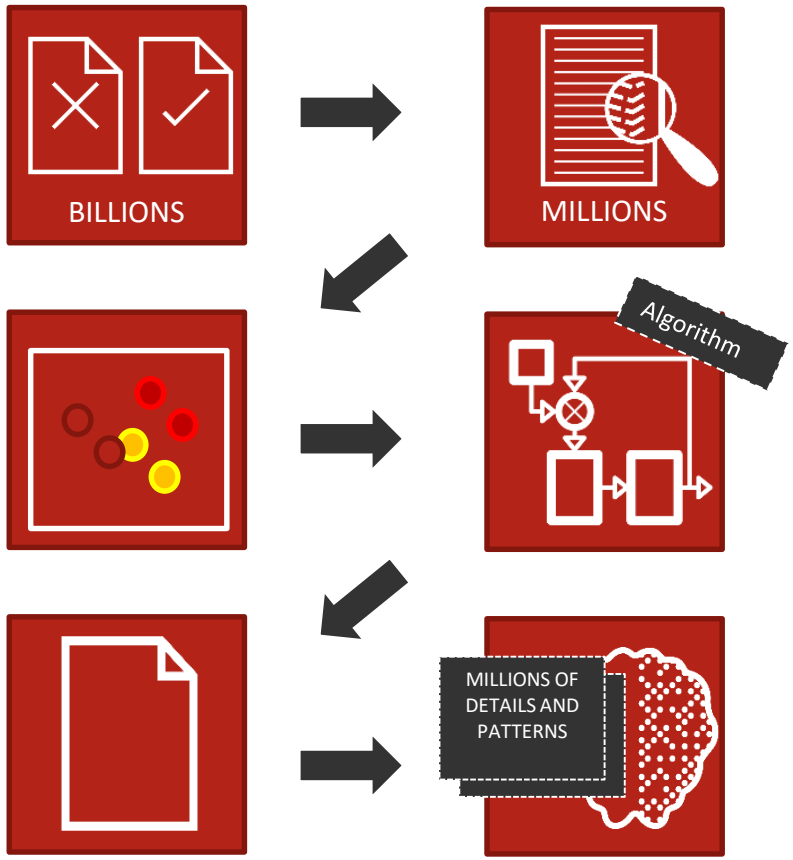


Learn From Data

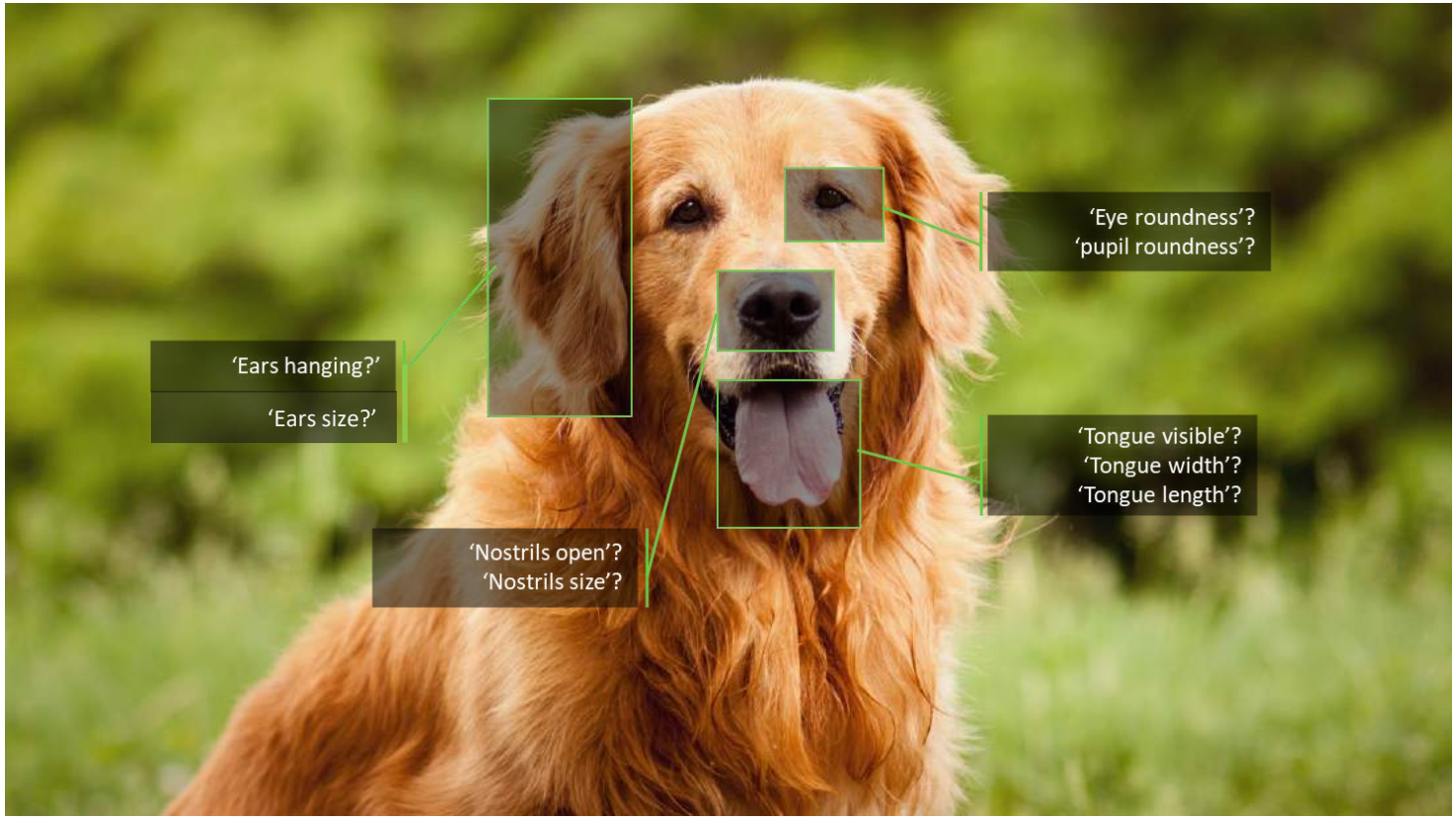
Maschinelles Lernen ist der Prozess der Verwendung historischer Daten zur Entwicklung eines Vorhersagealgorithmus für zuvor nicht gesehene Daten.

Artificial Intelligence in Firebox: Defense in Depth

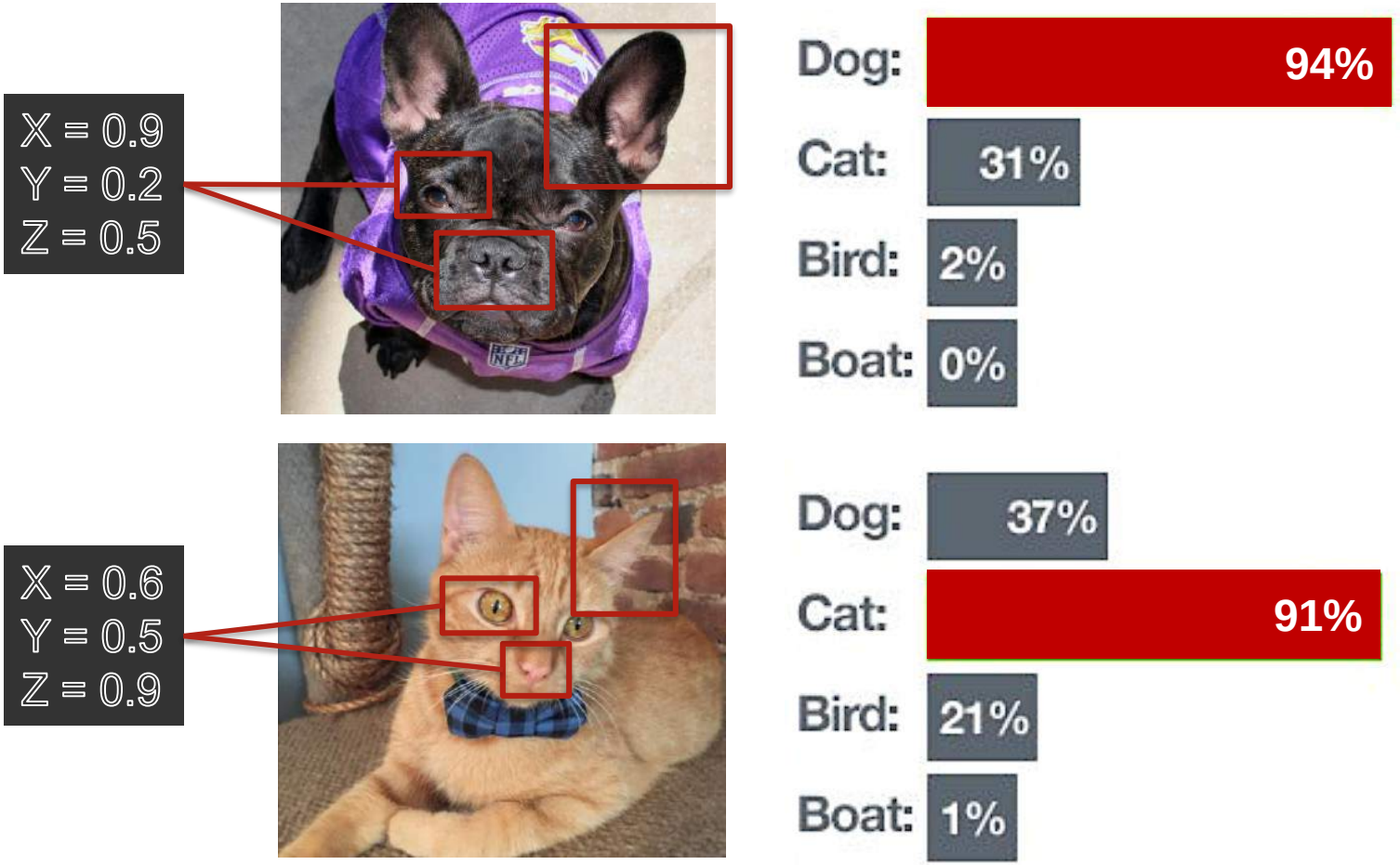
- Neue Modelle ca. alle 6-8 Monate
- False Positive Rate sinkt mit jedem neuen Modell
- **Keine** Cloud benötigt
- **Keine** Signaturen benötigt



Maschinelles Lernen: Ein allgemeines Beispiel



Feature Classification

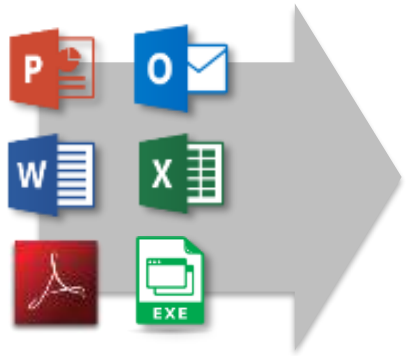


Probleme mit herkömmlichen Ansätzen zum Schutz vor Malware

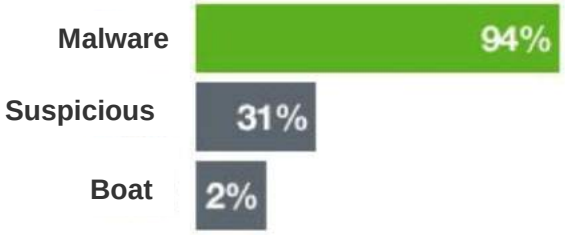
- Computer eignen sich gut zum Analysieren großer Datensätze und zur Erkennung von Mustern. Menschen sind es nicht
- Viele Sicherheitsmodelle, wie signaturbasierte Techniken und White- / Blacklist-Methoden, sind methodisch und reaktionsbasiert
- Polymorphe Malware und Evasive Malware führt regelmäßig zu Problemen mit althergebrachten Vorgehensweisen bei Malware

Künstliche Intelligenz bei der Identifizierung von Malware

Ein menschlicher Malware-Analyst kann sich die Eigenschaften von 10 - 30 Dateien ansehen, um die Schädlichkeit einer Datei zu ermitteln, wohingegen Machine Learning (ML) Tausende, wenn nicht Millionen von Funktionen gleichzeitig berücksichtigt



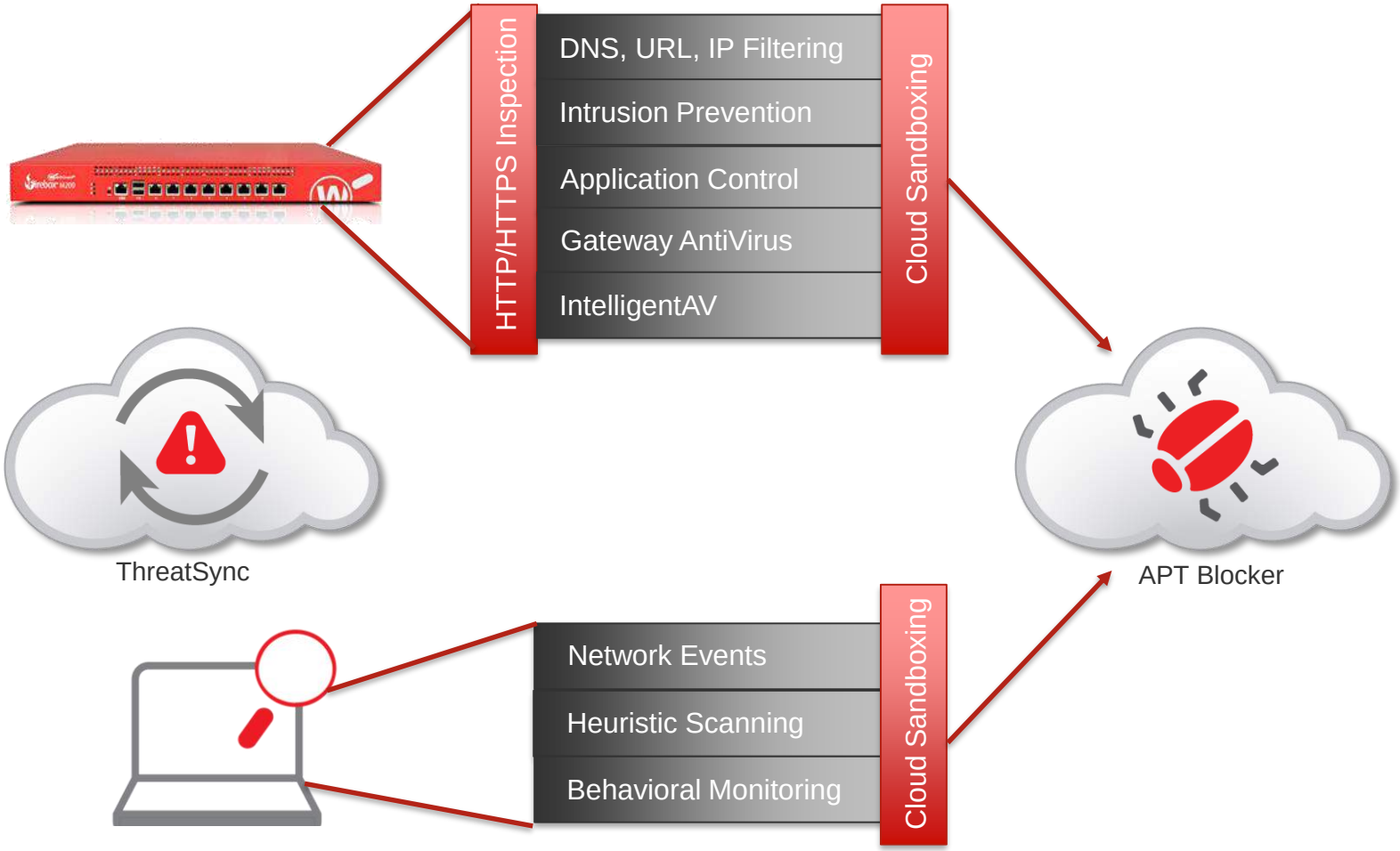
DOS Header
NT Header
File Header
Section Headers
Export Directory
Import Directory
Resource Directory
Relocation Directory
Debug Directory
Packer Used
Compiler Type
Compiler Language
File size
PE size
Image section headers
Functions called
Kernel hooks
Image Paths
Image Resource Directory
Bitmaps
Icons
Strings
RCData
Version Info…




```
lea     rcx,[rdi+20h]
mov     qword ptr [rdi+10h],r13
lea      rdx,[rsp+258h]
or       r9,0FFFFFFFFFFFFFFFFh
xor      r8d,r8d
mov     word ptr [rcx+8],r13w
mov     ebx,r14d
```

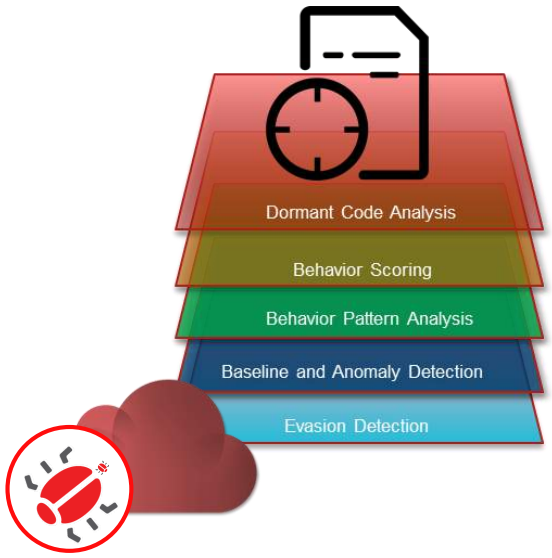

APT Blocker

Die WatchGuard Unified Security-Plattform



Verkürzte Erkennungszeit

APT Blocker nutzt die KI während des umfassenden Inspektionsprozesses, um eine umfassende Analyse von Dateien durchzuführen, für die normalerweise ein Team qualifizierter Sicherheitsanalytiker Hunderttausende von Verhaltensmerkmalen durchleuchten muss, um die bösartige Absicht zu ermitteln

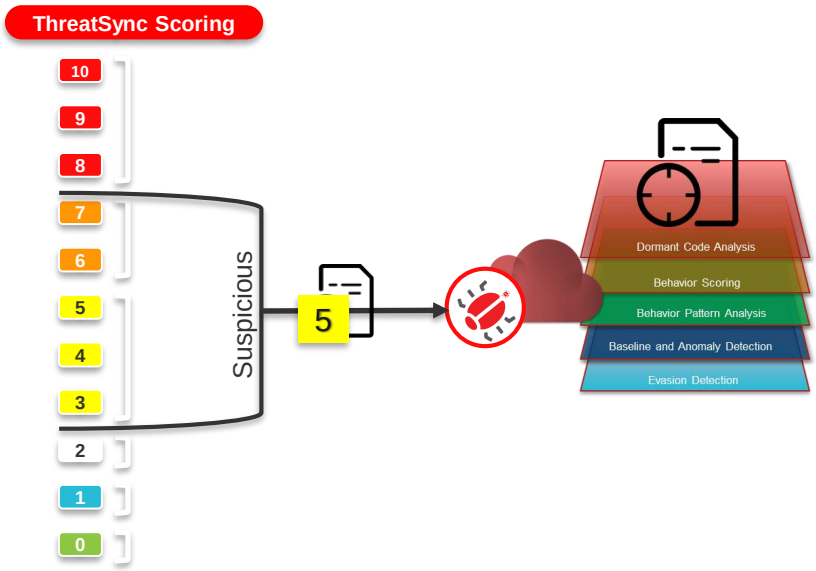


APT Blocker uses self-learning artificial intelligence throughout the deep inspection process to:

- Detect evasive malware by encouraging detonation
- Analyze, attribute and score dormant code
- Analyze, weight and score individual behaviors
- Develop baselines and perform anomaly detection
- Determine if a file is malicious or clean based on a final analysis of behavioral patterns

Reduzierte Reaktionszeiten und automatisierte Bedrohungsabwehr

ThreatSync verwendet AI in Verbindung mit APT Blocker, um die Erkennung von unbekannten Bedrohung zu erleichtern und die Abwehr zu automatisieren.



1. With a foundation of AI, ThreatSync is regularly trained on thousands of malicious and benign files.

2. ThreatSync is able to automate the classification of suspicious files, and determine which should be sent to APT Blocker

3. APT Blocker will automatically return results to ThreatSync for automated remediation

Total Security Suite: mit AI built-in, in 3 Ebenen

Der „Vorhersagevorteil“ ist die Fähigkeit von ML-Modellen in TSS, die Malware von morgen mit den heutigen Machine-Learning-Modellen zu verhindern

Features & Services	TOTAL SECURITY SUITE	Basic Security Suite
Intrusion Prevention Service (IPS)	✓	✓
App Control	✓	✓
WebBlocker	✓	✓
spamBlocker	✓	✓
Gateway AntiVirus	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Protection (DLP)	✓	
Threat Detection & Response	✓	
DNSWatch	✓	
Access Portal*	✓	
IntelligentAV*	✓	
Dimension Command	✓	
Support	Gold (24x7)	Standard (24x7)

**Available on Firebox M Series appliances*