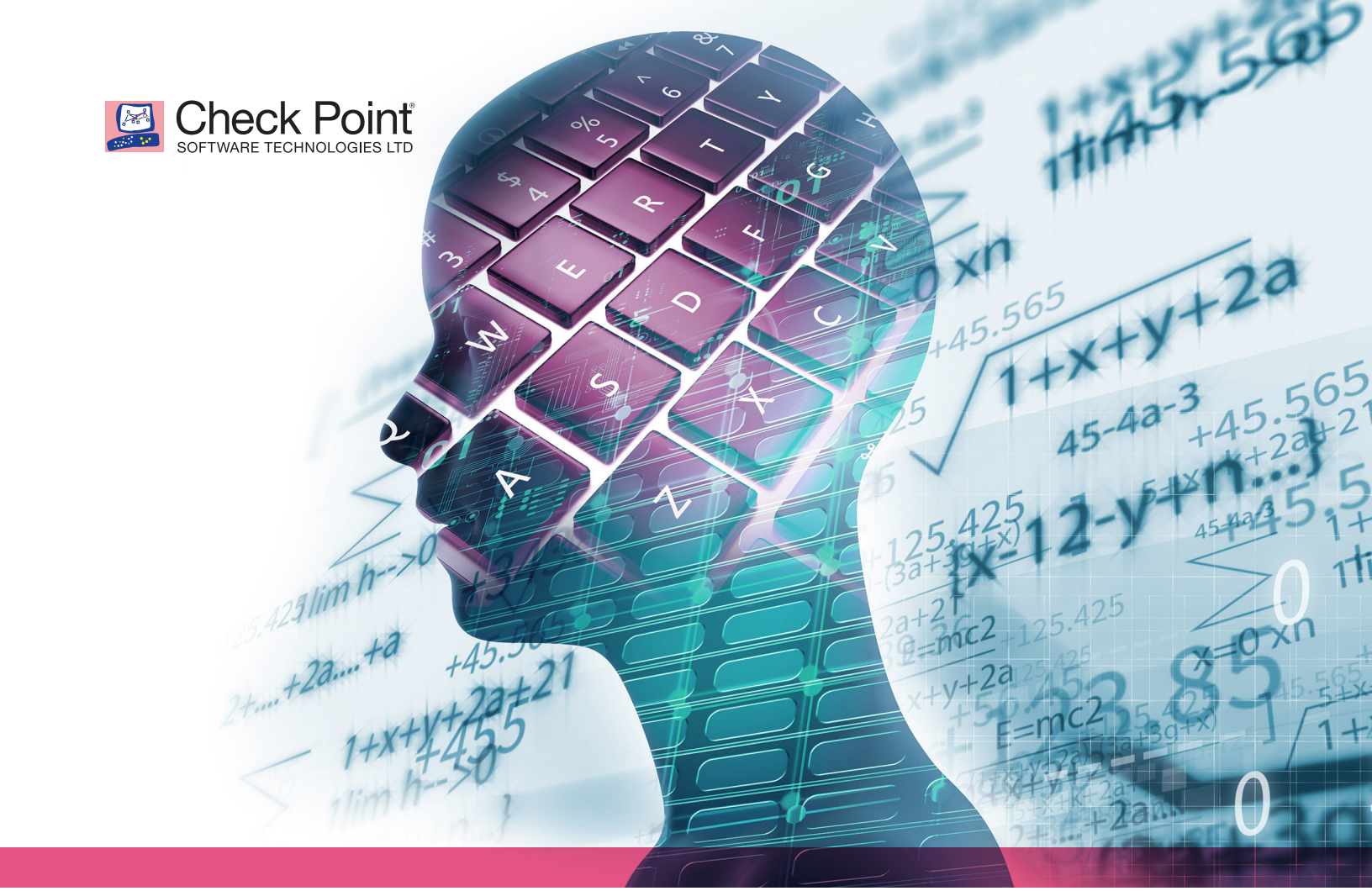
Check Point
SOFTWARE TECHNOLOGIES LTD



How Artificial Intelligence Helps Achieve the Best Cyber Threat Prevention Rates

Introduction

Cyber attacks continually evolve at an ever-increasing pace, making them much more sophisticated and dangerous compared to just a few years ago. Protecting against these advanced attacks requires advanced technologies. This paper explains how Check Point actively prevents today's sophisticated Fifth Generation cyber attacks by leveraging artificial intelligence in its security solutions.

Why Artificial Intelligence Is So Important in Cybersecurity

Traditional security solutions are based on a single detection engine, or a combination of several engines that are built on logic that uses signatures and rules-based analysis. While these methods are important for fast detection of many known threats – as well as some unknown ones – they are limited in scale and capability.

The velocity of malware evolution, an increasing number of devices and technologies that need protection, and a huge amount of data to process all combine to make it impossible for human-created models to give comprehensive, up-to-date protection. Therefore, relying solely on traditional detection engines leaves organizations exposed to incredibly damaging attacks.

Check Point overcomes this challenge by incorporating artificial intelligence into its unified, multi-layered security architecture. By doing so, the company provides an ever-improving, intelligent system that doesn't just detect, but actively prevents complex, sophisticated attacks.

Incorporating AI in All Four Stages of the Adaptive Security Cycle

Each stage of the adaptive security cycle (predict, prevent, detect, and respond) is a decision point worthy of AI models. Check Point's vision is to incorporate AI models throughout the entire cycle and across the entire IT infrastructure, to shorten response times and enhance security.

Why Predict?

Today's attacks spread fast across organizations' networks and between organizations, causing severe damage very quickly. Therefore, predicting attacks before they strike is critical.

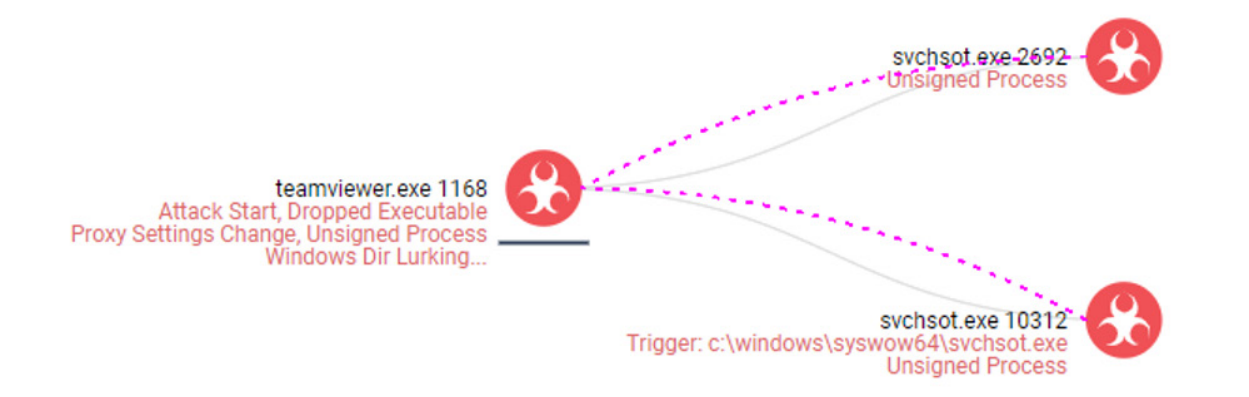
Check Point uses several AI models to improve attack prediction. These models are integrated in all the SandBlast products (Network, Agent and Mobile), CloudGuard products (SaaS, IaaS and Dome9) and in ThreatCloud.

For example, SandBlast Agent Behavioral Guard is one of SandBlast Agent's prediction engines, and leverages SandBlast Agent Forensics to effectively and uniquely identify the behavior of new, unknown malware and enable accurate classification of malware families. The engine combines behavioral signatures created by Check Point researchers with an AI model that analyzes behavioral patterns to detect and identify malware. This unique combination of generic signatures and AI-model validation enables the activation of signatures that couldn't be activated previously because of high false positive rates. By incorporating AI validation, Check Point technology ignores 99% of suspicious behaviors and accurately prevents only genuine attacks.

CASE STUDY: SandBlast Agent Predicts an Unknown Cryptominer

Attackers frequently use look-alike process names as a camouflage technique (Mitre ATT&CK™ Technique: Masquerading). However, even legitimate processes sometimes use look-alike process names as well. Therefore, classifying an event as malicious based only on the name similarity could lead to many false alerts – and lead to genuine threats being missed. Check Point has developed a unique AI engine that evaluates the behavior of the process and then classifies it.

In this example, Sandblast Agent detected a look-alike process in one of Check Point's customers' endpoint devices. At this point the process was not yet known as malicious. The Behavioral Guard AI engine then evaluated the process's behavior and classified it as a cryptominer malware, at which point the attack attempt was prevented.



The behaviors marked in red are the Behavioral Guard AI model features.

The generic signature combined with the AI model, predicts the attack and prevents it.

Why Prevent?

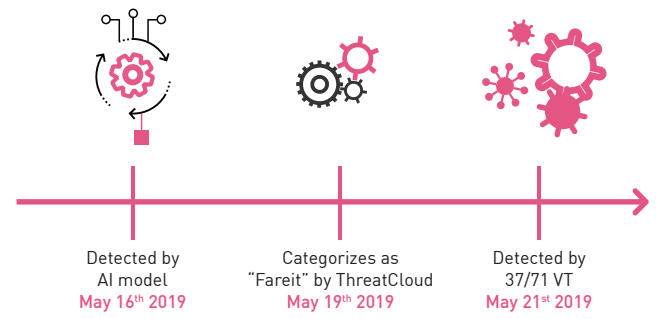
Check Point's approach to cybersecurity focuses on threat prevention because it is less costly to prevent an attack, than to detect and remediate it after it has breached the network and caused damage. This is why Check Point has invested heavily in developing threat prevention AI engines.

Check Point's unique technology incorporates AI models in the prevention decision point across the entire IT infrastructure. All SandBlast (Network, Agent and Mobile) and CloudGuard (SaaS, IaaS and Dome9) solutions use AI to prevent attacks before they enter an organization. This is how Check Point is able to achieve the best prevention across the industry in dozens of independent third-party tests.

For example, Cloud Guard SaaS's sophisticated anti-phishing AI engine differentiates between a clean email and a malicious phishing email by analyzing more than 300 parameters, including the language used, in every incoming email. Based on the different parameters, the anti-phishing AI engine provides a verdict (phishing, spam or clean). CloudGuard SaaS blocks all malicious emails from reaching the designated recipient mailbox. Another example is SandBlast Network's sandbox solution AI engine outlined in the case study below.

CASE STUDY: SandBlast Network Prevents a New Variant of the Fareit Trojan

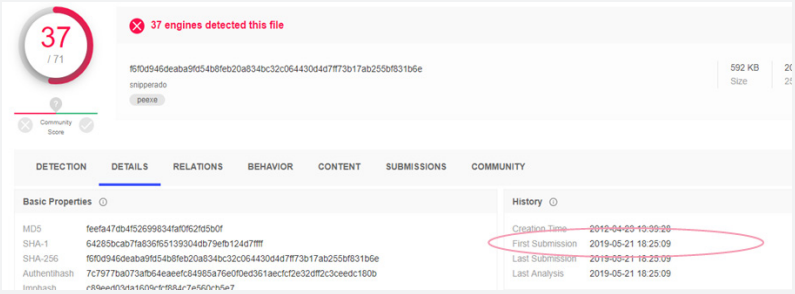
Fareit is a Trojan that has been in the wild since 2012. Its variants typically steal users' sensitive information such as passwords, FTP accounts and other credentials stored in web browsers. Fareit was detected by Check Point's dynamic emulation AI model, five days before it was first seen in Virus Total.



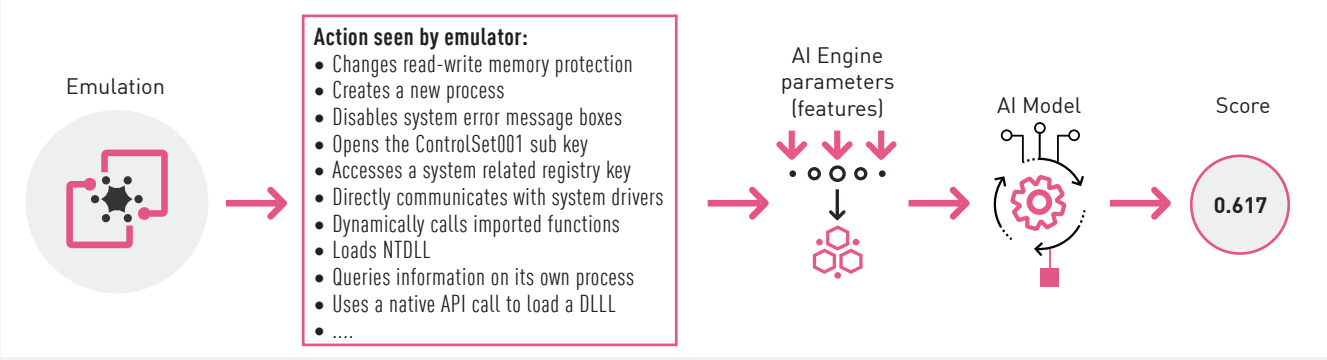
First detection on May 16th at 12PM (IST) as seen in Check Point's data lake:

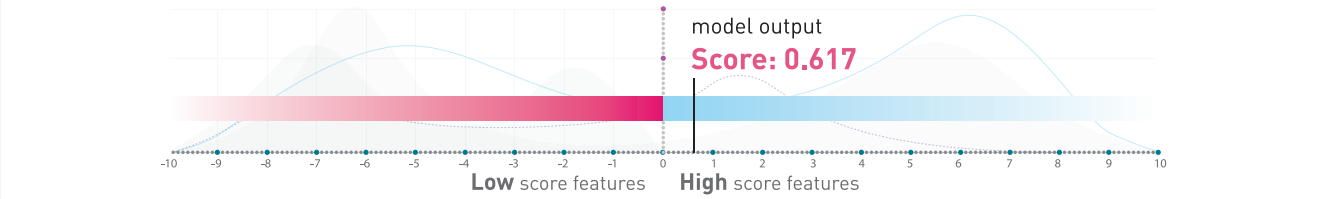
Time	cadet_score	buffy_raw_score
May 16th 2019, 12:00:30.068	0.617	0.6129

First seen by Virus Total on May 21st at 6PM (IST):



The following diagram illustrates the detection flow of Fareit attack by Check Point's AI model:





Check Point Threat Emulation is a sandboxing technology integrated within both on-premise networks and in the cloud. The solution incorporates an AI model that evaluates the actions taken by an executable file during run time. The model's output is a score that is used by Threat Emulation to determine whether the file is malicious. If the model decides that the file is malicious, SandBlast Network will then block the file and prevent the attack. The AI model is responsible for 50% of Check Point's Threat Emulation detections.

Detection Prevents Damage

Organizations today should assume that they will eventually be compromised at some point. Even if an organization is equipped with the most comprehensive, state-of-the-art security products, the risk of being breached cannot be completely eliminated. Detecting and automatically blocking the attack at an early stage can prevent damage.

Therefore, detection and prioritization remain important. Check Point uses AI to detect incidents in various engines and automatically block the attack. For example, SandBlast Mobile performs an AI-based analysis of a system using various techniques. Check Point analyzes the reputation of an application, including its behavior, metadata and its similarity to any other malicious applications. These testing models are trained based on comprehensive analyses of millions of applications that have been collected since 2013. The result is an excellent detection rate that allows both damage prevention and the fastest possible remediation when needed.

Half of the applications blocked by SandBlast Mobile were detected exclusively by the Mobile AI model and were unknown and undetected by other vendors. The following "Agent Smith" case study demonstrates how early detection of an attack can prevent damage.

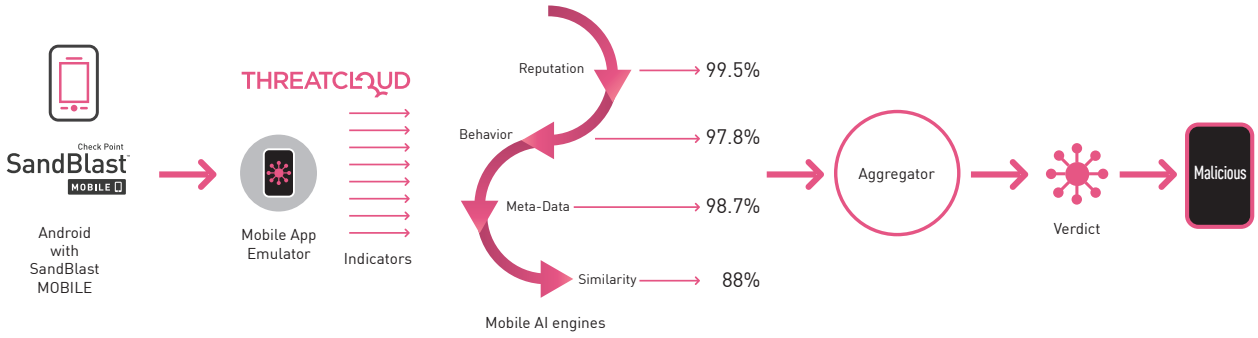
CASE STUDY: "Agent Smith" Core Malware Detection

"Agent Smith" is a campaign discovered by Check Point's mobile threat researchers. The campaign infected approximately 30 million devices for financial gain. Disguised as a Google-related app, the core part of the malware exploits various known Android vulnerabilities and automatically replaces multiple installed apps on the device with malicious versions.

Check Point's AI engines detected this malware before the campaign was first discovered, and before the command and control sites were known to be malicious.

The core malware was detected by three of Check Point's AI engines, each of them looking at a different type of indicator. For example, one model receives the application's code as an input and returns a verdict based on the code flow analysis. The engines that detected this malware work independently, which means that even if some of the indicators do not appear in some variants of the malware, it will still be detected by the other engines.

Detecting the malware prevented damage, as "Agent Smith" was detected before it replaced the applications with malicious versions.



SandBlast Mobile uploads every installed application to the cloud for evaluation. In the cloud, several engines are inspecting the application; some of them based on AI. Each of the AI models calculates the probability of the application to be malicious. The aggregator model decides, based on those probabilities, and a pre-defined threshold, whether the application is malicious, risky or benign. In this case, the application was successfully identified as malicious.

Respond: The Need for Speed

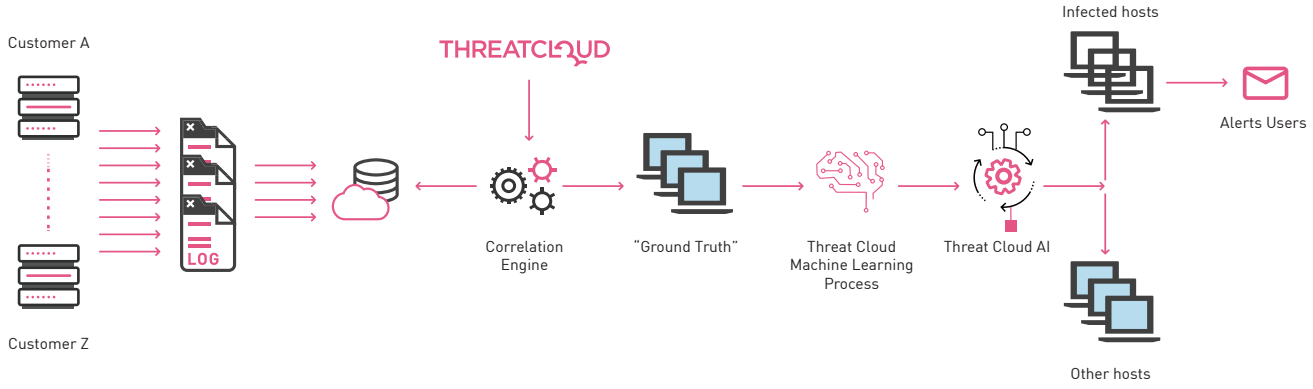
Responding to an attack quickly and accurately can remediate damage or even prevent it completely. Check Point uses AI for several stages of the response process – such as victim identification, alerts elimination, and attack classification. Check Point generates specific, actionable alerts that quicken response and remediation time.

CASE STUDY: ThreatCloud AI Identified Several Dozen Infected Hosts

ThreatCloud AI sifts through log entries and distills actionable events from them. In this case, a company that provides IT services to critical government institutes contacted Check Point after receiving tens of thousands of alerts regarding allegedly malicious activities reported by a non-Check Point solution.

ThreatCloud AI provided an accurate list of 25 infected devices. The devices were then cleaned before the malware caused any damage.

The concept behind ThreatCloud AI is to create a machine that is capable of making a decision with the sophistication and accuracy of a cybersecurity researcher. The machine makes a decision in seconds, while the security researcher could spend weeks just researching a single type of threat. ThreatCloud AI will then point the customer to the top events in their network that need immediate attention. The system correlates suspicious and malicious events from multiple sources, thus recognizing an infection behavior and identifying the infected hosts. An actionable report is immediately sent by email to the customer, allowing quick remediation.

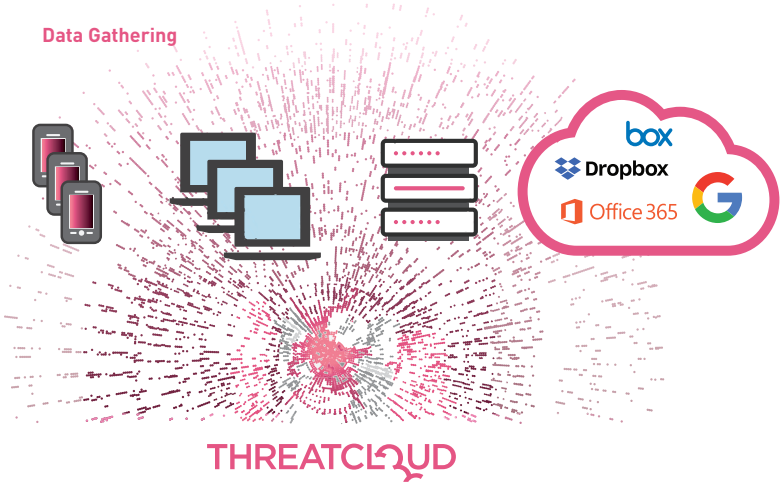


What Makes Check Point's Models So Effective?

Check Point's models are effective at preventing attacks thanks to the vast amount of real-world data of known threats, and domain experts who develop, train, and validate the models.

Real Data

Check Point trains its models using millions of valid samples that come from customers. Hundreds of thousands of new data samples are labeled automatically every day, based on internal and external cyber intelligence. Check Point records production feeds and uses them to train the next model on even newer data. This process never stops, yielding an ever-improving system.



Domain Experts

Defining suitable features for each data type and correctly labeling the data is key to the process of building an effective model and requires substantial domain expertise. The collaboration of Check Point's security experts with Check Point's data scientists makes the value of the models stronger.

Trustworthy Ground Truth

Check Point has developed a proprietary labeling methodology that delivers an equitable balance between high detection rates and low false positives.

Unique Feature Set

Check Point's data scientists evaluate a huge amount of data and carefully select a unique set of features that deliver industry-leading detection rates.

Data Enrichment

Enriching real-time data with proprietary intelligence from campaign research and other sources, improves the accuracy and efficiency of the models.

Integration of Several Algorithm Approaches

Check Point uses a number of algorithm approaches on the same input to improve the accuracy.

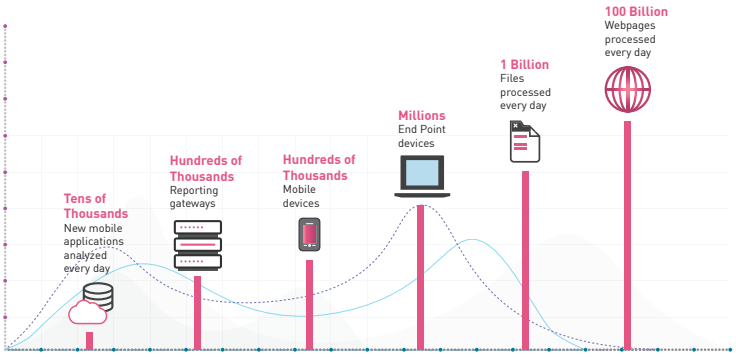
Real-Time Prevention

The Check Point approach incorporates an AI model in the production environment in order to prevent attacks before they cause damage. Using AI models in production protects customers from both known and unknown attacks.

Check Point ThreatCloud

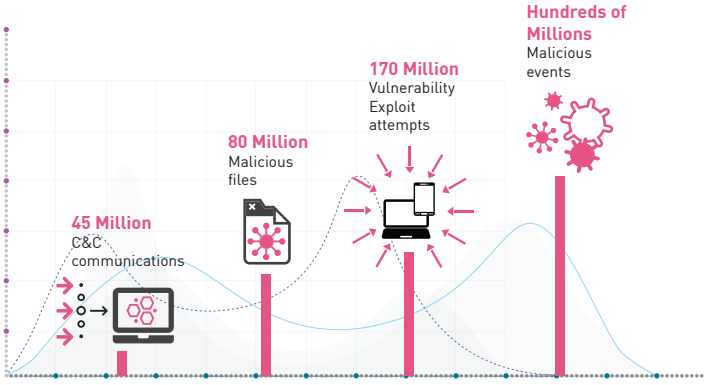
ThreatCloud is a collaborative knowledge base that delivers real-time dynamic security intelligence to Check Point's security solutions. ThreatCloud's knowledge base is dynamically updated using feeds from a vast network of global threat sensors, attack information from gateways around the world, and Check Point research labs. The resulting up-to-the-minute security intelligence is shared across the entire product line.

Once an unknown, zero-day attack is detected by one of ThreatCloud's sensors, ThreatCloud distributes the attack's indicators to all sensors across the network in real time, and the attack becomes known and will be prevented. Therefore, once any of Check Point's AI engines detects an unknown attack, it immediately becomes known to all Check Point's customers.



ThreatCloud is a major source of data used by Check Point's data scientists to train, test and improve AI models. It handles hundreds of billions of requests every day, of which millions are malicious.

ThreatCloud is constantly leveraging AI to provide unique intelligence. For example, ThreatCloud has an AI-based reputation service that handles tens of millions of requests per day. The service predicts the risk of indicators such as domains, URLs, IPs and provides a rich feed of unique malicious indicators. Half of the malicious indicators observed by Check Point are detected uniquely by this service.ThreatCloud holds records of tens of millions of malicious web sites, and files and updates millions of records every day.



Check Point Infinity

Check Point Infinity is the only fully consolidated cybersecurity architecture that protects businesses and IT infrastructures against mega cyber attacks across all networks, endpoint, cloud and mobile. The Infinity architecture delivers the highest threat prevention in the industry, with the best NSS Labs test scored over the past four years. The AI engines take a major role in those excellent results, as seen in this document.

AI Engines Employed Across the Infinity Architecture

Check Point has built dozens of AI models over the past few years. The models are integrated in the SandBlast and CloudGuard solutions and in ThreatCloud. The models integrated in SandBlast and CloudGuard solutions are improving the detection and prevention engines, while the models integrated in ThreatCloud are enriching the intelligence.

	Adaptive Security Stage in which the Model Is Used				Product Using the Model				
Model Type	**Predict**	**Detect**	**Prevent**	**Respond**	**SandBlast Network**	**SandBlast Mobile**	**SandBlast Agent**	**Cloud Guard**	**Threat Cloud**
INTELLIGENCE									
Machine generated signatures	✓	✓	✓		✓		✓		✓
Anonymizer detection model	✓	✓	✓	✓	✓				
Internal intelligence model	✓	✓	✓	✓	✓	✓	✓	✓	✓
External intelligence model		✓	✓	✓	✓	✓	✓	✓	✓
Reputation service	✓	✓	✓	✓	✓	✓	✓	✓	✓
STATIC ANALYSIS									
Static analysis of executable files	✓	✓	✓	✓	✓		✓	✓	
Fast Static analysis of applications	✓	✓	✓	✓		✓			
Deep Static analysis of applications	✓	✓	✓	✓		✓			
Fast Static analysis of documents	✓	✓	✓	✓	✓	✓	✓	✓	
Deep Static analysis of documents	✓	✓	✓	✓	✓	✓	✓	✓	
Static analysis of emails	✓	✓	✓	✓	✓			✓	
Disassembled code analyzer	✓	✓	✓	✓	✓	✓			
Document macros analyzer	✓	✓	✓	✓	✓				
Static analysis of Javascript Files	✓	✓	✓	✓			✓		
Malware static classification model	✓	✓	✓	✓	✓	✓	✓	✓	✓
DYNAMIC BEHAVIORAL ANALYSIS									
Dynamic behavioral analysis of executable files	✓	✓	✓	✓	✓		✓	✓	
Dynamic behavioral analysis of documents	✓	✓	✓	✓	✓	✓	✓	✓	
Dynamic behavioral analysis of applications	✓	✓	✓	✓		✓			
Malware dynamic behavioral classification model	✓	✓	✓	✓	✓	✓	✓	✓	✓
CORRELATION AND ELIMINATION MODELS									
Machine based incidents correlation				✓	✓	✓	✓	✓	✓
Machine validated signatures				✓			✓		
Executable files detection accuracy model	✓	✓	✓	✓	✓		✓	✓	
Documents detection accuracy model	✓	✓	✓	✓	✓	✓	✓	✓	
Application detection accuracy model	✓	✓	✓	✓		✓			

Conclusion

There is a limit to the ability of human-created logic to cope with the sheer diversity and velocity of attacks. In order to constantly improve Check Point's excellent detection and prevention rate, Check Point has developed dozens of artificial intelligence engines and incorporated them in critical decision points across Check Point products. Check Point domain experts are constantly defining suitable features and labeling data for each engine. They use a vast amount of data for training, testing and validating the models, and the data is enriched with Check Point's unique intelligence. The solutions integrate several algorithm approaches on the same input. The result of all of this, is the industry's leading prevention rate for both known and unknown attacks.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com