WHITE PAPER

Harnessing the Power of Artificial Intelligence and Machine Learning with FortiNDR Solutions

Executive Summary

With the explosion of data and computing, adversaries and cybersecurity practitioners are harnessing the power of AI and ML to achieve their respective objectives. Fortinet applies AI and ML to its SecOps suite of solutions, including FortiNDR network detection and response and FortiNDR Cloud. Below, you'll find related use cases of how Fortinet uses AI and ML in these offerings, highlighting how the technologies solve common cybersecurity challenges and increase coverage related to detection and response.

AI and ML in Fortinet Cybersecurity Solutions

Fortinet uses AI and ML to solve common security operations center (SOC) challenges related to scale and time to detect. Fortinet also uses these capabilities to enhance detections in its own products in many ways, such as training different engines and neural networks for malware detections, profiling traffic on networks (FortiNDR, FortiNDR Cloud, and FortiWeb), analyzing network operations data (FortiAIOps), using GenAI with FortiAdvisor to interact with customers using natural language processing, and harnessing ML for face recognition in FortiCamera, to name a few.

What Makes Network Detection and Response Unique?

NDR is one cybersecurity solution that harnesses big data and uses ML to effectively model network traffic. NDR relies on processing raw network data and flows to capture the metadata of the network to surface attacks. As adversaries cannot escape the network, traces of activity are always left behind, whether malware lateral movement, deviation of traffic flow, abnormal application behavior, or the unusual upload of sensitive data. NDR solutions can conduct behavior-based analysis on the network, using AI and ML to determine if an action is potentially suspicious. This insight helps a human analyst better assess the situation and prioritize remediation.

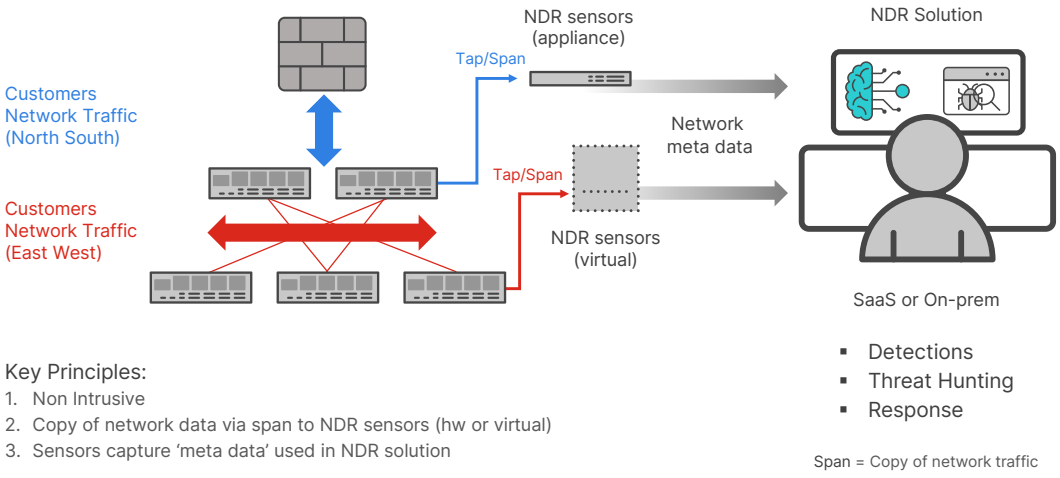


Figure 1: Architecture of a typical NDR solution

AI and ML Use Cases in the FortiNDR Product Family

Most mature NDR vendors will offer SaaS or cloud-based and on-premises solutions. Fortinet has deployment options for both FortiNDR Cloud (SaaS-based) and FortiNDR (on-premises). While many customers choose the SaaS or cloud-based deployment option, some industries need greater data sovereignty and have unique compliance requirements that necessitate an on-premises solution. Below are several examples, first of how FortiNDR on-premises, and then how FortiNDR Cloud solutions use AI and ML to enhance detection capabilities.

Artificial neural networks and supervised machine learning

FortiNDR (on-premises) is equipped with patented artificial neural networks (ANN) to scan and analyze files on the network in real time. Few NDR solutions in the market scan the files from raw traffic and inform users what malware attacks are happening in their network. Most solutions only offer post-attack recovery recommendations. The benefits of using ANN versus traditional detection technology like antivirus software include:

- Reducing the time needed to detect, as no signature matching is required. FortiNDR ANN is trained by FortiGuard Labs experts to identify specific ransomware types, such as CoinMiner Banking Trojan.
- ANN's learning ability and its automatic adaptation to malware variants on network. ANN can compare similarities between suspicious files, drawing a conclusion about whether the new file poses a risk to the network.
- The ability to add detection timing and connections to the evaluation criteria. As a result, FortiNDR can determine if an infected user spreads malware to another and whether there are connections between these hosts. This helps analysts determine the origin of an attack.
- Other self-learning capabilities based on customer traffic to further detect malware anomalies for both clean and malicious files.

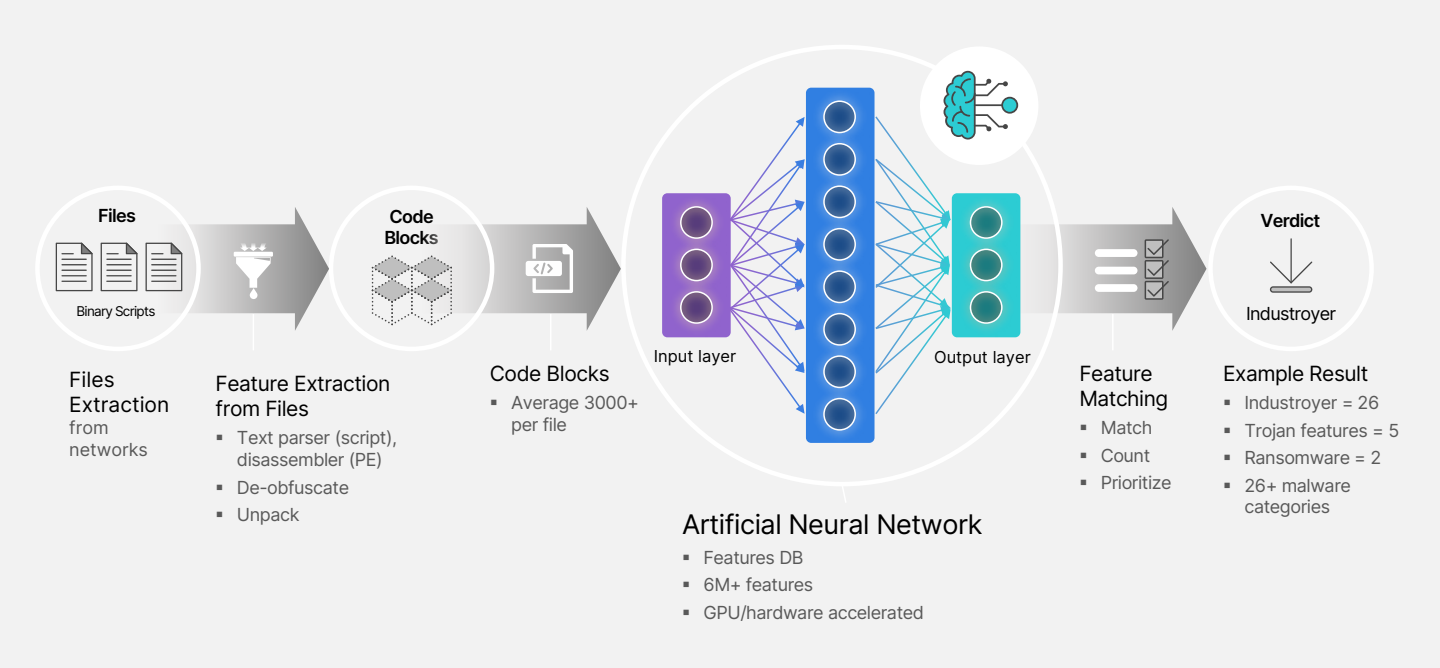


Figure 2: FortiNDR ANN

One-class support vector machines and unsupervised ML

A second example of how FortiNDR (on-premises) uses ML is related to traffic profiling. When capturing raw network traffic, FortiNDR uses a One-Class Support Vector Machine (SVM) to model traffic, form a baseline, and identify instances that deviate significantly from that baseline. The One-Class SVM is an unsupervised ML algorithm that requires training by feeding different types of clean and malicious files to it, baselines customers' traffic using a specified time interval to learn the "norm" to form the baseline, and detects deviations from that baseline. This analysis includes different network characteristics such as IP addresses, geolocations, application behavior, and ports. Different ML profiles or patterns can be built for different network segments in the FortiNDR configuration. For example, a critical server on a bank's network should only communicate with selected hosts via well-defined ports and application behavior. If any deviations are detected, FortiNDR will alert us of this activity. While the activity might not be a legitimate attack, it can be classified as suspicious traffic that warrants investigation.

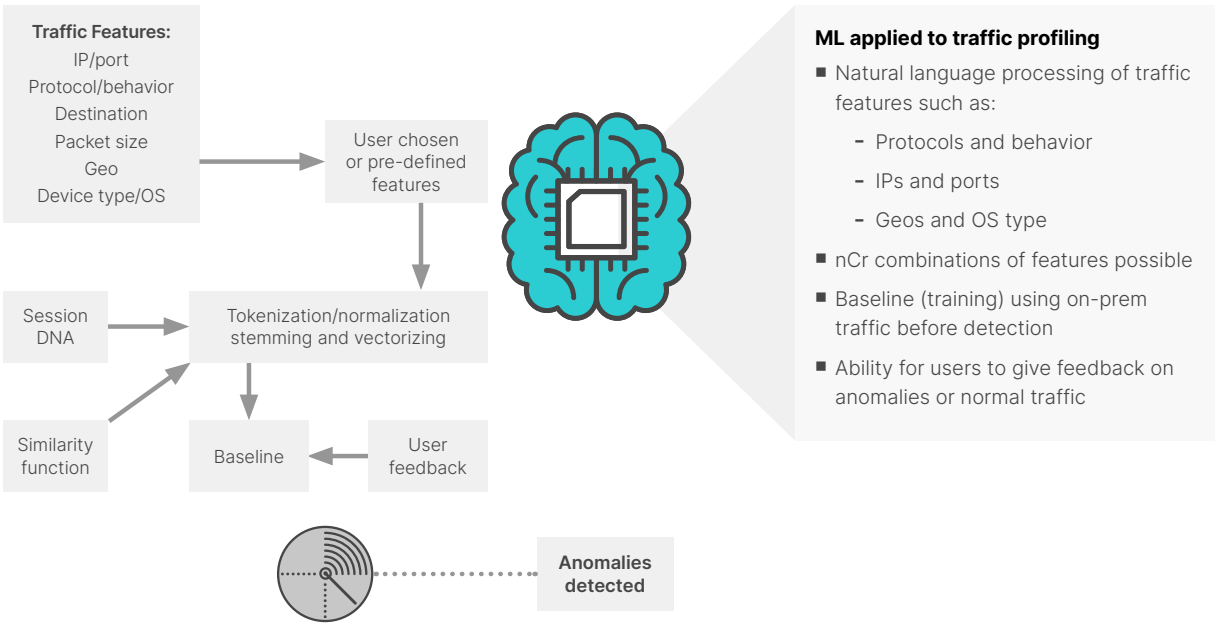


Figure 3: FortiNDR and ML applications for traffic profiling

FortiNDR Cloud Examples of AI/ML Use

FortiNDR Cloud, a SaaS NDR offering from Fortinet, captures customers' network data. This data is then sent to FortiCloud for detection, modeling, and threat hunting. The SaaS architecture provides an opportunity to harness cloud computing to scale in speed, training, and analysis.

There are numerous advantages to leveraging cloud computing, AI, and ML, such as:

- Autoscaling compute when required, moving away from on-site compute constraints
- Cross-domain data leveraging multiple datasets
- Sharing detection models across verticals
- Comparing observations across verticals to draw more accurate conclusions
- Analyzing large amounts of data and applying ML to datasets
- Rapid deployment with SaaS-based ML solutions

In 2023, FortiNDR Cloud:

- Analyzed 11T network events
- Recorded 146M observations
- Triggered 463K detections
- Had < 1% customer-reported false-positive rate

The following section outlines detections and observations in FortiNDR Cloud, as well as how AI and ML assist with detecting anomalies in a customer's network.

Detections and observations

Detections on FortiNDR Cloud are considered high-fidelity, low false-positive events. A well-designed NDR solution should:

- Not generate too many false positives
- Provide customers with the ability to tune detections to minimize noise

One of the key benefits of a SaaS-based solution such as FortiNDR Cloud is the ability to leverage cloud computing and apply ML on a next-generation data management solution. Another advantage is that the solution maintains network metadata for at least 365 days at a lower cost, which is important for customers for threat hunting, as well as applying ML techniques to the larger dataset over time to aid in detecting anomalies.

Different ML algorithms generate “observations” in the FortiNDR Cloud solution, which models normal and malicious traffic in various ways. There are more than 60 observations currently available in FortiNDR Cloud, with the Fortinet engineering team adding new observations regularly. ML is applied to identify anomalous behavior and generate observations. These models are built on the network metadata observed, a unique capability of the Fortinet NDR solution.

Below are a few examples of how ML is applied to identify anomalous behavior and generate observations. These ML models are built on the network metadata observed, a unique capability of the Fortinet NDR solution.

Detections	Observations
Based on well-known rules and signatures detected in traffic	ML-based with traffic modeling
High fidelity, low false positives	Varying levels of confidence
Ability to tune	Continuously learn and fine-tune
Example: Log4J attack	Example: Suspicious large data upload

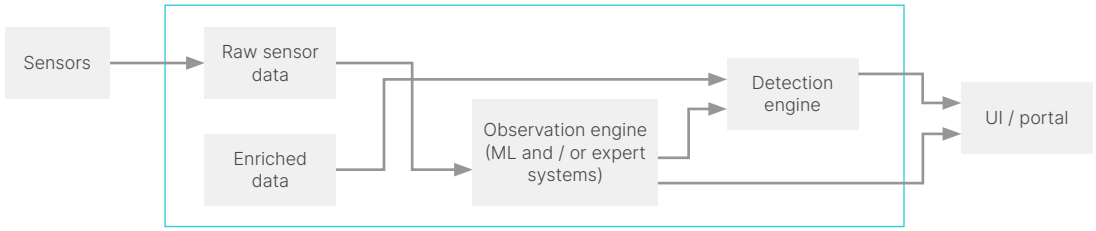


Figure 4: Detections and observations data process flow

Detecting exfiltration attempts based on supervised learning

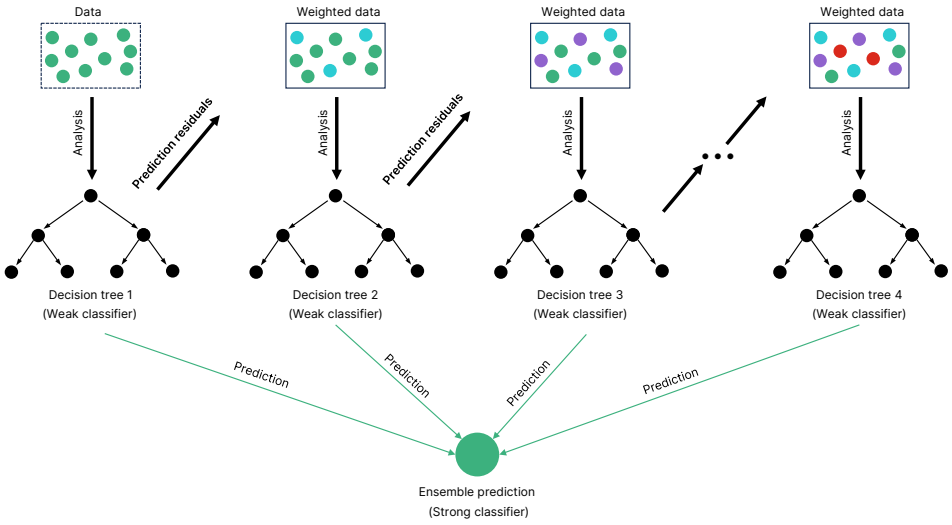
One of the characteristics of a breach is a large or unusual amount of data being transferred out of an organization’s network. This is covered in MITRE ATT&CK Technique TA0010.

FortiNDR Cloud applies supervised ML using a light gradient boosting model (GBM) to detect suspicious outbound data quantity transfer, detecting unusually large uploads related to exfiltration attempts. LightGBM ML framework has the following characteristics:

- Faster training speed and higher efficiency
- Lower memory usage
- Better accuracy
- Support of parallel, distributed, and GPU learning
- Capable of handling large-scale data

The ML model used by detection exfiltration is a tree-based model trained against synthetic exfiltration attempts. There are two models: one is a classification model to identify if exfiltration is occurring, utilizing close to 50 features, including max, mean, median, and standard deviation of incoming and outgoing bytes to identify outliers. The other is a regression model that estimates how much of the traffic is exfiltration.

Once the models are built and trained by normal and anomalous datasets, FortiNDR Cloud can apply the same model to new customer traffic and it will work instantly. No additional training or baseline data is required.



Gradient-boosted decision trees are a machine learning technique for optimizing the predictive value of a model through successive steps in the learning process.

FortiNDR leverages this technique to detect suspicious outbound traffic (exfiltration).

Figure 5: LightGBM boosting tree algorithm applied on suspicious outbound traffic

ML to detect encrypted malicious botnet activity

A second example of ML applications in FortiNDR Cloud is the ability to detect encrypted command and control (C2) outbound attempts within a customer's environment. The solution detects known indicators of compromise, such as a well-known set of botnet servers or URLs related to ransomware campaigns. FortiGuard Labs Applied Threat Research (ATR) team further studies the behavior of such connections and applies different ML models—one example is SK Learn Classifier—to model different features within the malicious traffic, such as:

- Beaconing frequency of botnets
- HTTP headers or user agent strings
- Certificates and their characteristics used for SSL encryption
- How long the connection lives
- JA3 client and server headers
- Number of bytes or packets transferred in connection

Using this technique, FortiNDR Cloud can build an accurate model of malicious C2 behavior. In general, C2 networks are not static and constantly change. Attackers couple dynamic C2 activity with machine-generated Domain Generated Algorithms to avoid detections.

The benefit of having this C2 supervised learning model when new traffic is observed on network is that if any of the traffic from the C2 model is routed to a new and unknown destination, FortiNDR Cloud will alert on this anomaly to determine if an SSL C2 is observed. The confidence of the observations will depend on how well the traffic profile fits into the model. This model also gets refined over time as the FortiGuard Labs team detects and identifies additional IOCs as new threats are discovered.

Once users are prompted with SSL C2 observations, SOC analysts can conduct further threat hunting on FortiNDR itself based on the internal query language (IQL) query language, or through other offerings that are part of the Fortinet Security Fabric platform, such as FortiEDR endpoint detection and response, FortiGate Next-Generation Firewalls, or FortiSIEM to further triage the attack.

Figure 6: Modeling of malicious botnet behavior

FortiNDR Cloud: Combining unsupervised and supervised learning

The example above examines how FortiNDR Cloud detects botnet communication using SSL data, but botnets can also communicate via HTTP using redirects. To detect this activity, FortiNDR Cloud relies on a similar method for detecting SSL C2 to detect HTTP C2 behavior. Leveraging a PageRank unsupervised learning model, FortiNDR Cloud evaluates the trustworthiness of various webpages while modeling traffic. For example, adversaries can create spoofed domains to redirect botnet C2 traffic via HTTP to avoid detections. FortiNDR Cloud evaluates these redirected webpages using the PageRank algorithm to measure how trusted (or new) the webpages are. Once evaluated, FortiNDR Cloud inputs these measures into an additional supervised HTTP learning model for further analysis. This showcases how Fortinet combines the power of unsupervised and supervised learning to allow FortiNDR Cloud to determine if observed HTTP connections exhibit botnet C2 behavior and qualify for a new detection.

FortiNDR Solutions Deliver Unique Advantages

FortiNDR and FortiNDR Cloud are two solutions that truly apply ML and AI, whether on-premises or a SaaS-based cloud solution. This ongoing application of ML and AI helps identify anomalies, as adversaries always leave traces of activity on the network. NDR solutions offer unique capabilities to security teams as they conduct investigations and perform threat hunting. They can be combined with other Fortinet Security Fabric platform offerings to create a comprehensive solution to secure any network.

Visit our website for more information.

August 5, 2024 11:44 PM
2635871-0-0-EN