# ***Endpoint Security***

Endpoint security detection is the method by which an organization is able to detect and respond to malicious activities right at their entry point which are the connected devices of the organisation**.** This early detection helps prevent most of the damage the malware could cause to the organisation if it otherwise had penetrated deeper into the IT infrastructure of the organisation.

Usually, endpoint security is a security system that consists of security software, located on a centrally managed and accessible server or gateway within the network, in addition to client software being installed on each of the endpoints (or devices). The server authenticates logins from the endpoints and also updates the device software when needed. While endpoint security software differs by vendor, you can expect most software offerings to provide antivirus, antispyware, firewall and also a host intrusion prevention system.

In most cases, continuous monitoring of every packet of data in each endpoint is required where the incoming data is compared with the existing knowledge base of known threats so that an alarm can be raised. This demands the use of Machine Learning and Deep Learning models. Since we know that the accuracy of these AI models will be as good as the quantity and quality of data we train them upon, there exists some products like Cisco AMP for example, which has its Machine Learning models trained with data that relate to file based attacks collected through Cisco Talos which provides data from around 10 million endpoints and 1.5 million samples of malware each day. This leads to better monitoring on the endpoints and increases the accuracy of predictions that our AI model can do.

Also, Machine learning is used in Endpoint Detection and Response (EDR) as it helps to identify new type of attacks with complex behaviour. In contrast to traditional approaches based on static rules, machine-learning-based EDR may be able to detect attacks sooner, potentially interrupting more complex action chains that would result in further compromise.

Another example that we have referred to deals with the use of Deep Learning in the place of Machine Learning. Deep learning has consistently outperformed other machine learning models, including random forest, k-means clustering, or Bayesian networks, but requires vast amounts of data and computational power to build an effective model.

FireEye's deep learning model (CNN) detects malware by analysing the raw bytes of a windows executable file.

Typically, endpoint security software will include these key components:

1. Machine-learning classification to detect zero-day threats in near real time
2. Advanced antimalware and antivirus protection to protect, detect, and correct malware across multiple endpoint devices and operating systems
3. Proactive web security to ensure safe browsing on the web
4. Data classification and data loss prevention to prevent data loss and exfiltration
5. Integrated firewall to block hostile network attacks
6. Email gateway to block phishing and social engineering attempts targeting your employees
7. Actionable threat forensics to allow administrators to quickly isolate infections
8. Insider threat protection to safeguard against unintentional and malicious actions
9. Centralized endpoint management platform to improve visibility and simplify operations
10. Endpoint, email and disk encryption to prevent data exfiltration

**References:**


- Cisco – Machine Learning and Security

  (https://www.youtube.com/watch?v=JaJ8ikPj3RA)

- Cisco - How Cisco Endpoint Security uses machine learning to stop advanced threats

  (https://www.youtube.com/watch?v=2RvKvkYCSc4)

- What are Deep Neural Networks Learning About Malware?

  (https://www.fireeye.com/blog/threat-research/2018/12/what-are-deep-neural-networks-learning-about-malware.html)

- https://www.webopedia.com/TERM/E/endpoint_security.html

- https://www.mcafee.com/enterprise/en-in/security-awareness/endpoint.html#:~:text=Endpoint%20security%20is%20the%20practice,the%20cloud%20from%20cybersecurity%20threats

- https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/451ResearchExpandingMLApplicationsontheEPReport.pdf

- https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/endpoint-survey-report.pdf

- https://www.rsa.com/content/dam/en/white-paper/endpoint-detection-and-response.pdf