

ESET DYNAMIC THREAT DEFENSE



What it is

ESET Dynamic Threat Defense (EDTD) is a cloud-based sandboxing technology that adds a powerful layer of security to your existing ESET endpoint protection.

EDTD detects and analyzes never-before-seen threats to protect against ransomware, targeted attacks, advanced persistent threats (APTs), zero-days and other sophisticated malware.

EDTD will automatically identify a suspicious program, execute it in a secure sandbox and analyze it, then block it if it's malicious—all before the malware can reach your network, endpoints or users.

Why you need it

- **Advanced threats designed to spread ransomware and other attacks** proliferate as criminals seek new ways to circumvent security for huge financial rewards. With ~\$1.5 trillion in cybercrime revenues annually and cybercriminals earning upwards of \$166,000 per month, developing APTs and malware becomes more lucrative.
- **Blocking these threats requires a behavioral approach to detection.** While endpoint protection calculates what a file might do, EDTD runs it in a real operating system with AI and machine learning to uncover its true purpose.
- **Combining the intelligence of ESET Endpoint Security's layered protection** with fast, cloud-based sandboxing keeps your business armed against advanced threats and leaves day-to-day operations uninterrupted.

Key benefits

- Fully cloud-based technology, able to analyze files in under five minutes
- Vital layer of security on top of endpoint protection and mail security to shield against new advanced threats
- Simple setup and management via ESET Security Management Center
- Analyzes files from web browsers, mail clients, compressed files and removable media

\$3.92M: Global average total cost of a single data breach in 2019

(IBM Security Cost of a Data Breach Report 2019)

\$1.42M: Average cost to a company of lost business due to data breach

(IBM Security Cost of a Data Breach Report 2019)

51% of data breaches in 2019 were caused by malicious attacks (as opposed to human error)

(IBM Security Cost of a Data Breach Report 2019)

* "Into the Web of Profit: Understanding the Growth of the Cybercrime Economy," by Dr. Michael McGuire.