

E GAMBIT ENDPOINT DETECTION & RESPONSE [EDR]



- ✓ **Intrusion detection and response**
- ✓ **Traceability**
- ✓ **Real-time alerts**

eGambit EDR Solution meets regulatory requirements while detecting real-time threats and enhancing your information system security.

In case of **personal data breach**, the General Data Protection Regulation (GDPR) requires processing personal data companies to notify **the competent supervisory authority** within **72 hours** after awareness. When the personal data breach is likely to result in a high risk to data subject's rights and freedoms, the data controller shall communicate the personal data breach to the data subject without undue delay.

Companies must hold a **data breach detection plan** and regularly evaluate **security practices effectiveness**. They must maintain an **internal security breach record**, the remediation measures taken and the data subjects concerned likely consequences.

As workstations and servers' volume widens, it raises exposure for potential attacks. eGambit EDR agent monitors, detects and isolates infected workstations before damage.

Hackers target workstations and servers due to its volume; software and potential human vulnerabilities profusion.

Because eGambit EDR collects and analyzes a large amount of event logs it is able to detect the most vulnerable targets and issue an alert.

eGambit EDR Solution is essential to ensure your network, information system and personal data contained therein security.

eGambit EDR Solution's privacy by design measures:

Collecting, archiving and processing log and data encryption;

eGambit EDR Solution and your computer system secure interactions: via VPN and encryption algorithm;

Exported data secure back-up to ensure their availability and access in case of incident;

Frontend secure connection with triple authentication lock;

Collected and analyzed data fast and efficient localization.