DriveLock Endpoint Detection & Response: Maximises your security, helps detect and resolve incidents

With the increase of digitalisation and heightened corporate defence measures, cybercriminals are looking to evolve by employing more targeted and sophisticated cyber tactics. Comprehensive prevention measures are crucial. However, it does not offer one hundred percent protection. When criminals infiltrate your system, you need to be able to identify this by recognising their behaviour, observing them, and reacting before any critical damage is done.

Cyber threats have become increasingly severe in recent years. Many companies have recognised this, and are improving their defensive measures. However, it's an ongoing race against cybercriminals who are employing increasingly targeted and sophisticated cyber tactics.

While prevention plays an important role in making organisations more resistant to attacks, "detection" capabilities are critical for identifying ongoing attacks that may have bypassed the prevention measures. There is now a consensus among experts that 100% protection is neither practical nor possible. Instead, an organisation must deal with the eventuality that an attacker will succeed in penetrating its network. When this happens, the organisation should be informed at all times about the activities occurring at the endpoints in order to avoid costly damages. Comprehensive protection requires the prevention, detection and response measures to be constantly adapted in order to react appropriately to various security breaches.

Boost your defences when other controls fail with DriveLock's Endpoint Detection & Response

Transform your security strategy from taking preventative measures to actively detecting and responding to threats. To increase IT security, you need functions that actively monitors and sends alerts when an "intrusion" has occurred.

These features are supported by DriveLock's Endpoint Detection & Response (EDR). Our solution collects data on the endpoints of your systems while being undetectable by attackers. Using this data, IT (security) personnel in your company can identify anomalies and react accordingly. This can be through sending out alerts or triggering a response (e.g. manually or automatically terminating processes or isolating a computer in the network).

Endpoint Detection & Response (EDR) Benefits:

- + EDR ALLOWS FOR A FULL COVERAGE PREVENTION STRATEGY
- + CONTINUOUS REAL-TIME MONITORING ON END POINTS
- + AUTOMATES ROUTINE TASKS IN YOUR IT SECURITY
- + DETECTS AND AVOIDS DANGERS BEFORE THEY CAUSE CRITICAL DAMAGE
- + CAN BE INTEGRATED WITH OTHER SYSTEMS, SUCH AS SIEM, FOR FURTHER PROCESSING
- + INTEGRATED COMPONENT OF THE DRIVELOCK ZERO TRUST PLATFORM WITH PREVENTION AND DISCOVERY MODULES

Cyber Threats - Status Quo

- + > 50% OF COMPANIES WORLDWIDE ARE THE TARGET OF AN ATTACK
- + AVERAGE TOTAL COST OF CYBER ATTACKS IN 2020 WAS € 3.86 MILLION WORLDWIDE
- + SOURCES OF THREAT TYPICALLY FROM INSIDER ACTIONS OR EXTERNAL ATTACKS
- + DIGITISATION LESSENS CORPORATE BOUNDARIES
- + LEGAL REGULATIONS (GDPR)

Identification of live attacks

The EDR platform collects information relating to...

Processes being run

Files being acressed

Devices being connected

Programs being startet

Type of access occurring over the network to an endpoint

logon attempts that are performed

Uncovering abnormal behavior

User privileges being used

Any changes to the endpoints´ baseline

Advantages of DriveLock EDR in detail

The DriveLock solution impresses through endpoint monitoring, analysis support and automated responses, thus fulfilling your prevention measures strategy:

- **Monitoring activity on the endpoint without impairments**

  DriveLock EDR enables the real-time monitoring of endpoint activity - without interfering with an attack already in progress.

- **Incident response and forensic investigation**

  DriveLock EDR gives IT security teams and forensic investigators the information they need to conduct their analysis. You can automate alerts and also trigger defensive responses like shutting down certain processes.

- **Support for the clean-up and fixing of problems**

  Our EDR solution enables more effective clean-up and remediation after an attack.

Flexible response options

You can configure responses in the DriveLock Policy. They are either executed ad-hoc (automatically) when an alert event occurs, or triggered centrally by an administrator.

DriveLock offers the following response options, including:

- Execution of remote actions on the endpoints
- Change of group membership to control policies
- Evaluation of user behaviour (User Score)
- Determination of unsafe computers (Computer Score)
- Launch of a security awareness campaign

DriveLock - Features

+ BOTH DRIVELOCK AND SYSTEM EVENTS ARE DETECTED, CORRELATED AND EVALUATED ON ENDPOINTS
+ RESPONSE OPTIONS ARE CONFIGURABLE AND HIGHLY FLEXIBLE
+ AUTOMATION OF WARNING MESSAGES AS WELL AS DEFENSIVE REACTIONS SUCH AS THE SHUTDOWN OF CERTAIN PROCESSES
+ THREATS AND ALERTS BASED ON THE MITRE ATT&CK® FRAMEWORKS
+ EASY CONFIGURATION, ROLLOUT AND ADMINISTRATION OF EDR RULES
+ STATE-BASED SECURITY INCIDENTS CAN BE VIEWED CENTRALLY
+ WEB-BASED INTERFACE FOR DETECTION AND THREAT SEARCHES
+ OFFLINE ENDPOINT DETECTION & RESPONSE

DriveLock: Expert in IT and data security for more than 20 years

The German company **DriveLock SE** was founded in 1999 and is now one of the leading international specialists for cloud-based endpoint and data security. The solutions include measures for a prevention, as well as for the detection and containment of attackers in the system.

DriveLock is Made in Germany, with development and technical support from Germany.

DriveLock
DriveLock SE • Germany • France • Australia • Singapore • Middle East • USA
sales@drivelock.com • www.drivelock.com