



# DETECTION & RESPONSE

Maximize your security through detection, prediction and remediation of incidents

The screenshot displays the DriveLock security dashboard. The main view is 'Threats', which includes two bar charts: one for 'State' (Active, Closed, Resolved) and another for 'Severity' (Information, Warning, Critical). Below the charts is a table of alerts with columns for Severity, State, Date of creation, and Description. A detailed view of an alert is shown on the right, titled 'HYPERSECURE Platform Component'. This view includes fields for Date of creation, Severity, Computer name, User name, and Comment. It also features a 'Responses' table and a 'Properties' section with detailed information about the incident, including the computer name (NB-BLN-1001), category (Hijack Execution Flow: DLL Side-Loading (T1574)), date of creation (4/21/2023, 3:05:07 PM), severity (Critical), and a comment describing the attack: 'Loading of MS Defender related DLLs from non-default directories may be an attempt to sideload arbitrary DLL. Adversaries may execute their own malicious payloads by side-loading DLLs. Similar to DLL Search Order Hijacking, side-loading involves hijacking which DLL a program loads. MITRE-ID: T1574. Tactic: Persistence'.

TEST TODAY – BE HYPERSECURE TOMORROW

Find out which use cases are most important for your company.

LEARN MORE

Free 30-day trial – no obligations



Contact our experts

DRIVELOCK.COM



# DETECTION & RESPONSE



**Maximize your security through detection, prediction and remediation of incidents.**

## YOUR CHALLENGES

One hundred percent protection against cyber attacks does not exist, despite comprehensive preventive measures. If an attack is successful, you need to detect and respond as quickly as possible.

You want to strengthen your defenses for when other controls fail.

You want to monitor activity on your endpoints in real time.

You are missing automated alerts and flexible response capabilities.

You need support for cleanup and remediation.

## OUR SOLUTION

Complete your prevention measures with DriveLock Risk & Compliance.

DriveLock as well as system events are detected, correlated and evaluated in real time.

Response options are configurable.

Automated alerts as well as defensive responses, such as shutting down certain processes.

Threat and alert notifications based on the Mitre Att&ck® framework.

Easy configuration, rollout and administration of rules.

## YOUR BENEFITS

- 1 Monitor activity on the endpoint without degradation
- 2 Support for cleanup and remediation of problems
- 3 Potential security breaches are predicted
- 4 Incident alerts and forensic investigations

