Detecta Security Overview

Detecta
ENTERPRISE DATABASE MONITORING

Preserving the confidentiality and integrity of your information is one of Detecta's highest priorities.
This document summarizes the key measures we take in ensuring your data is always protected. Detecta maintains a deep culture of security and utilises an iterative approach in designing and improving security procedures and controls.

We continuously analyze the effectiveness of our security policies to ensure we are providing optimal protection for our customers.

Data Center Security

Detecta's offsite data center provides 24/7/365 video surveillance, pin based locks, strict personnel access controls and detailed visitor entry logs. Unattended access is not allowed. • All entry is logged.
Only authorised members of the Koda team are able to access the data centre facility.

Customer Data Protection

All data is classified as confidential and treated as such. Inbound and outbound low-level logical firewalls ensure that data cannot be leaked between Detecta networks. All data is encrypted on the Detecta servers. Sensitive production data is never migrated or used outside of the production network. Client data is stored only on the Detecta production repository and associated production back ups. Only meta data related to monitored SQL Server instances is stored within the Detecta repository, there is no application data captured by the tool.

Hardened Operating System

Detecta runs on hardened Linux servers. Externally exposed critical patches are addressed within 24 hours.

Secure Connections

All connections to Detecta are secured via SSL/TLS. Any attempt to connect over HTTP is redirected to HTTPS.

Remote Access

Access to the Detecta production environment is restricted to users authenticated within the Koda VPN. The Koda VPN is a network restricted to employees for Koda Technology Ltd. Access to the Detecta Staging and development environments is restricted to users with access to the Koda VPN environment Access to the Koda VPN requires a user to be authenticated by the Koda security team and a password to be used.

Application Security

Koda utilizes secure development best practices that integrate security reviews throughout design, prototype and deployment. All code associated with the Detecta application is managed within a version control tool. Changes to the Detecta code base are made to the Detecta staging environment where thorough testing takes place prior to release to production The Detecta application utilises a test driven development methodology, here tests are written prior to application code being written, the test suite is run automatically as the code base is compiled.

Penetration Security

Umbrella, the Koda infrastructure partner implement and manage a DDoS solution that ensures the Detecta application is protected from external denial of service attacks. The infrastructure on which the Detecta application runs is protected by both physical and software firewall solutions. Detecta has undergone a rigorous third-party conducted penetration test which it passed successfully.

Business Continuity

Detecta customer data is backed up continuously and protected with strong encryption on disk. Backups are transferred offsite over SSH and properly deleted after 12 months.

Contact Detecta at support@detecta.io

www.detecta.io