Cognitive Machine Reading Plus Security Information

ANTWORKS™

Organisations today are facing increasing pressure to secure and protect data to ever higher standards. There is widespread concern regarding data privacy and security. New regulations require organisations to ensure they are taking this issue seriously. The potential penalties for data breaches are significant, not to mention the damage to trust and reputation of the company brand.

When it comes to the privacy and security of data, there is nothing more important to us at AntWorks and we invest heavily in security. AntWorks have been independently certified to the international standard for information security, ISO 27001.

We comply with numerous global privacy laws, including the US, Canada, EU & Asia Pacific. AntWorks is certified compliant for both the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) through a third-party risk management consulting firm. AntWorks' policies, procedures, and technologies are validated by many of the world's most security-conscious organisations, including many of the largest financial services and insurance firms.

Security

Cognitive Machine Reading (CMR) Plus uses the client's database - wherever it resides within the organisation. During processing, data is encrypted and stored in a secured database for a short period. This requirement depends based on the client's retention requirements before sending data downstream for processing.

Data Encryption

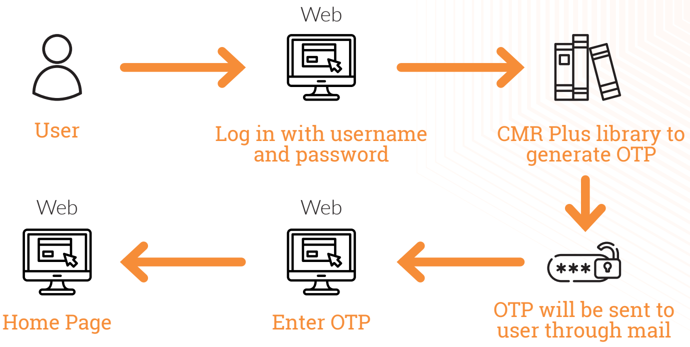
Encryption is fundamental to modern security. All sensitive information is encrypted with Advanced Encryption Standard (AES). AntWorks uses AES256 which is the longest and provides the strongest level of encryption which complies with the US government requirements for sensitive data. All connections are protected by Transport Layer Security (TLS). AntWorks uses TLS1.2 which is another federal requirement.

Customers also have the option to encrypt some custom fields before they are saved in the database, and mask their contents based on the access permissions assigned. This is a complex area and one that AntWorks recommends further discussion around, as encryption as a technology imposes certain limitations and impacts some application functionality.

Authentication and Identification

CMR Plus ensures that passwords are secure and routinely changed. Standard login to CMR Plus is via a unique username and password encrypted with strong cryptography. CMR Plus can generate and send email-based One Time Password (OTP) for authentication. OTP's are timebound and cannot be used once expired. Role-based access controls and two-factor authentication can be implemented for identity verification to add another layer of protection.

Two Factor Authentication

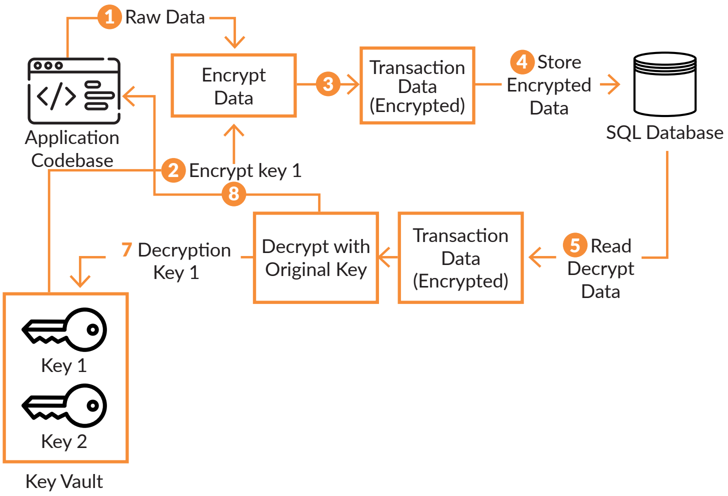

User
Web
Log in with username and password
CMR Plus library to generate OTP
OTP will be sent to user through mail
Web
Enter OTP
Web
Home Page

Network Security

Defence in depth is provided by internal firewalls that segregate the application and database tiers. Primary and secondary firewall monitors all ingress. AntWorks' internal application and database servers themselves are hardened to industry and vendor best-practice guidelines and continuously monitored to detect any changes.

Security Key Management

CMR Plus can be integrated with the client's hardware security module and/or key management service. It accommodates predefined key rotations. CMR Plus automatically keeps the previous version of keys to use for decryption of data encrypted under an old version of a key. All new encryption requests against a key are encrypted under the newest version of the key.



Organisational Security and How We Operate Internally

At AntWorks, our commitment to security, privacy, reliability, and trust is adopted by the entire company. There is an over-arching Information Security Policy supported by processes and procedures which form the ISO 27002 Certified Information Security Management System (ISMS). Our employees receive information security and privacy training, defined by our Enterprise Security Policy. Employees that handle sensitive data receive additional training specific to their roles before access is given. Access is strictly limited to only those who require it, and this is reviewed regularly.

Vulnerability Assessment and Penetration Testing

When it comes to security, AntWorks welcomes 3rd party experts to conduct Vulnerability Assessment and Penetration Testing (VAPT). If requested, AntWorks can provide VAPT reports to clients, generated every quarter. This provides our clients with valuable insights about AntWorks' security standards and risk management.

Threat Monitoring

Sophisticated threat monitoring tools such as IDS, IPS and SIEM are used to capture and detect and prevent malicious events, threats and intrusion attempts. State-of-the-art intrusion detection systems are used to detect common types of attacks, which means that every network in the production environment is monitored continually for potentially malicious network traffic. Application and database activity are monitored with security event management tools to proactively alert operators to potential internal and external threats.

Security Development Life Cycle

AntWorks has a clearly defined secure software development lifecycle (SSDLC) to ensure all changes and releases to our software are carried out in a secure, controlled manner. The SSDLC includes design, development, testing and release phases with security considered at all stages. Changes to the application are strictly controlled and versioned in our source code control system. Releases are announced in advance and scheduled to provide the least impact for the customer.

Vulnerability Assessment and Penetration Testing is conducted on a thick client and web module level in accordance with Open Web Application Security Project (OWASP) Top 10. AntWorks meets OWASP compliance standards to minimise common risks and provide more secure code.

Threat modelling, a core element of SSDLC, is regularly conducted as per industry standard to protect confidentiality, integrity and availability of the solution and data. AntWorks distinguishes hotspots from vulnerabilities using SonarQube to target always-actionable security vulnerabilities at the code construct level.

Conclusion

Providing a secure experience enables our clients to feel confident utilising our products. Security is just another important aspect for us to provide excellent customer service. AntWorks understands the different factors when it comes to data access, privacy and security and offers our customers peace of mind in providing one of the most secure software available today.

Contact us at Hello@Ant.Works to answer any additional questions or to schedule a demo.