COMINTELLI®

WHITE PAPER

Security in Intelligence2day® SaaS

IN A WORLD THAT MOVES FAST | YOU NEED TO RUN WITH IT.

CONTENTS

1 INTRODUCTION 2

2 Application Security 3

3 Back-end Security 6

4 Security and Penetration Tests 7

5 Policies 8

1 INTRODUCTION

Never before have people and organizations been subjected to extortion on such a massive scale as they are today. In recent years, cyber-criminals have emerged targeting innocent users with a wide range of malware and theft of data.
Securing data is therefore a top priority for Comintelli. Therefore, some of the largest multinational companies in the world entrust us with their information. Security is all about protecting corporate information and assets from intruders, thieves, and vandals. This includes coping with spyware, viruses, and firewall vulnerabilities.
To address these concerns, this White Paper describes how Intelligence2day® implements security, respects your privacy, and protects every bit of your data!
Intelligence2day® focus on data ownership, data retention, privacy, and integration, as well as the traditional triad of security: confidentiality, integrity, and availability.

This Whitepaper covers the Google Cloud Platform. There is a separate Whitepaper for the hosted service and on-premises installations S-132-F.

2 Application Security

2.1 Single Sign On

We recommend Single sign on as the first option for login. It both enables centralized user management and ensures that passwords meet the company's minimum password requirements.

Intelligence2day® supports idp initiated SAML 2.0, which is the most used standard today. A user types the email address and is redirected to the idp for verification. The user is redirected back with SAML that contains encrypted information and certification that the user has been validated. In intelligence2day® this information is validated for authenticity and the user is logged in. The idp address is stored in a cookie, and the next time the user wants to login this process is automatic and the email-address is not needed.

2.2 Form Login

Each Intelligence2day® user is identified with a unique username and password. Adopting a good personal password policy is the most important barrier to unauthorized access. Some recommended password properties are:

- At least ten characters
- Upper- and lower-case characters
- Numeric and special characters

To make passwords more complex, our recommendation is that a password is built on a sentence.

Intelligence2day® has a password complexity verification build in, that ensures that the minimum requirements are fulfilled.

Intelligence2day® does not allow users to use a password previously used with the system.

To minimize the risk of automated intrusion attempts, Intelligence2day® temporary locks users account after six failed login attempts from a specific IP address. The user may login again after one hour, or earlier if an Administrator manually re-enables login.

Intelligence2day® does not store users' passwords. Instead, an encrypted fingerprint value (password hash) is stored.
Password hashes utilizes a stronger-than-typical version of Password-Based Key Derivation Function (PBKDF2) with 100.000 iterations of the SHA algorithm. This implementation of

PBKDF2 ensures that the two pieces of the data, the password submitted and the hash value that's stored on the Intelligence2day® server are thoroughly protected.

No one, including super-admins and developers can retrieve a lost password. Instead, a time limited "reset password" link can be sent out to users to reset their login credentials.

An optional two factor authentication can be activated. With this option turned on, a time limited link is provided via email after successful authentication.

2.3 Military-Grade Encryption

By default, Intelligence2day® uses TLS 1.3 protocol with 256-bit AES encryption to protect data in transit. No user data, including log-in information, is sent through unencrypted public channels.

Data encryption keys are managed by Comintelli and are not shared with customers.

2.4 Data Validation

Uploaded images are validated with the expected MIME type and feeds downloads removes embedded scripts to protect readers against malicious content.

2.5 Obfuscated URL Parameters

Links presented to users for example in search results and email alerts does not expose predictable data parameters such as users' IDs or article IDs.

2.6 Session Management

Each user accessing Intelligence2day® is working within a private session scope on a Server. A session refers to all the connections that a single client might make to a server while viewing any pages associated with a given application. Sessions are specific to both the individual user and the application. As a result, every Intelligence2day® user has a separate session scope with access to individual session variables. Session variables are used for storing e.g., language preferences, custom settings, articles, and reports during authoring.

Session variables are regenerated at every login, and to avoid session attacks, session identifiers are rotated. When the session terminates, for example the user logs off or closes the browser, the session information is cleared. Intelligence2day® automatically logs off an inactive user after 8h.

2.7 Data Storage

Intelligence2day® stores data in NoSQL and SQL databases and other information storage systems such as the search index and as files on the server disks. The information in Intelligence2day® is located outside the web server's reach. This means that access to content such as articles, reports, files etc. is always safely protected by the security layer. Data is always encrypted both at rest and in transit both when transferred between backend systems and to the user's browser.

2.8 Server Disclosure

Error messages do not include sensitive data such as physical paths and system information.

2.9 Activity Logging and Traceability

Activities are logged in Intelligence2day®. This includes Article changes (creation, modification, and deletion), failed login attempts and emailing information from Intelligence2day®. Logfiles are consolidated to a central log management system, Stackdriver.

2.10 Encryption of Application Variables

When initializing Intelligence2day® it reads basic values for what data sources to use,, installation -file and -information paths. All these values are safely stored in an encrypted format.

2.11 Data segmentation

Different customers data is logically segmented with a GUID identifier that guarantees data and information always resides within the customer realm.

2.12 Access Groups

Access to information in Intelligence2day® is controlled by a user's access group belonging. A user will be able to read certain information depending on the access groups he or she belongs to.

2.13 Article Attachments

Files that are attached to an article are stored in a safe, dedicated filesystem and are separated from the web server.

2.14 Cookies

A cookie is a file on a user's computer or cache memory.
Intelligence2day uses cookies to, for example, maintain user sessions, provide protection against Cross-Site Request Forgery (CSRF), enable Single Sign on and to analyze and track application usage. The cookies do not contain any personal information and no personal information about the use of Intelligence2day is shared with other parties. Users must consent to the cookies to be able to log in to Intelligence2day.
Read the full policy at: https://comintelli.com/privacy-policy/

2.15 Software Security Measures

Intelligence2day® includes an application firewall against Cross-site scripting (XSS), SQL Injection, Cross Frame Scripting and Unvalidated http Redirects and Forwards when interacting with the system.
Login is protected with tokens for Cross-Site Request Forgery (CSRF)
3rd party java scripts are being actively maintained with security patches.

The application is regularly Vulnerability tested to guarantee that new and updated functionality does not contain vulnerabilities.

3 Back-end Security

3.1 Locked-up Network Perimeter

The network containing the Intelligence2day® application is protected by redundant load balancers with firewall functionality. Comintelli® proactively monitors and analyses firewall and system logs to identify unusual traffic patterns, potential intrusion attempts and other security threats. Intelligence2day® also uses reliable network monitoring and alerting systems.

3.2 Physical and Environmental Measures

The Intelligence2day® server environment is hosted by
In the Google Cloud Platform and managed by Comintelli with
Rackspace as back-end support.
Both Google and Rackspace are ISO 27001:2005 and Safe Harbor certified organization that provides cloud facilities with 24-hour physical security. They also adhere to SSAE16 Type II SOC1, SOC2 (Security and Availability Only), and SOC3. Comintelli does not have any formal certificates but align with the relevant ISO standards.

3.3 Systems Management

To minimize the risks of unauthorized access to the back-end several security mechanism are in place. is maintained exclusively through a VPN connection and in addition using SSH to a Bastion host that provides a single point of fortification.

Only authorized personnel are allowed to access the servers. Personal user accounts are used to trace actions. Customer Data may only be accessed by Comintelli personnel on request by a customer and only to help solve problems related to the system. Comintelli applies the principle of least privileges, which translates to giving a user account only those privileges which are essential to that user's work.

The only permitted method for remote server access is encrypted connectivity. Authentication policy for remote access employs strong complexity requirements. Minimum authorized access is provided with clear segregation of duties and formal request processes for the extension of access and/or changes to access requirements are established.

3.4 Software Updates

Servers Operating Systems are frequently updated with security patches and bug fixes.

3.5 Secure Socket Layer (SSL) Encryption

Intelligence2day® back-end traffic communicates over encrypted channels with exception for storing data in the usage statistics database.

3.6 Server redundancy

The Intelligence2day® is designed for high availability and is both redundant and is automatically scalable to meet current demands.

4 Security and Penetration Tests

Each released edition of Intelligence2day® is undergoing Penetration Testing to find vulnerabilities that an attacker could exploit. The tests include various scenarios for Cross Site Scripting (XSS) attacks, SQL & CSS injection attacks, cross-site request forgery (CSRF) and malicious user input.

Comintelli aims to comply with the Open Web Application Security Project (OWASP). OWASP is an online community that produces methodologies, documentation, tools, and technologies to improve web application security.
protocols for the vulnerability tests are available on request.

5 Policies

Comintelli has been a trusted software provider since 1999 with tens of thousands of users in many successful organizations. Comintelli´s Security and IT policy governs the conduct of all our employees, including

- IT security and general data / Information protection
- Business Continuity Management and Disaster Recovery
- Personal Data
- Computers and related peripherals equipment
- Data-communications (e-mail, Internet accounts, Internet access, telephone subscriptions)
- Office equipment (copiers, faxes, telephones)
- Electrical issues (Electrical outlets, Power supply)
- Crime prevention (burglar alarm, locks for doors and windows)

The Policies are available at https://comintelli.com/termsandpolicies/

ABOUT COMINTELLI

Comintelli is a Swedish software company which sells Intelligence Software that converts unstructured Big Data content into organized, digestible information for decision-making.

The award-winning solution Intelligence2day® acts as an insight engine to help customers make faster and more confident decisions.

Founded in 1999 and with extensive intelligence experience, Comintelli continues to develop user-friendly solutions that shortens Time-To-Insights.

,

For more information, please contact:
Phone: +46-8-663 76 00, US/Canada: 1-800-485-6402
E-mail: contact@comintelli.com

Web: www.comintelli.com | www.intelligence2day.com

Comintelli makes no warranties, either expressed or implied, in this document. Information in this document is subject to change without notice. The entire risk of the use or the results of the use of this document remains with the user. No part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means or for any purpose without the expressed written permission by Comintelli. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.