נספח טכנולוגיה

Logbox solution is based on international leading technologies that provide excellent security, availability, reliability, performance and exceptional usability – all this at minimal cost, commitment and risk

- Easy to start because our modern technology, enabling easy to use SaaS products, means customers can be up and running in minutes without requiring complex implementation or upfront fees
- Easy to own because our software-as-a-service (SaaS) solutions don't require IT support or dedicated hardware, and new features are upgraded automatically
- Easy to use without specialized technical skills or significant training because of our intuitive and simple software interface.

Microsoft Windows® Azure™ Platform

The Windows Azure platform empowers partners to embrace cloud computing, database as a service technology, and on demand computing with a simple, reliable and powerful online web services technology.

Logbox is built, hosted and secured at the Microsoft Windows Azure datacenters
Learn more: Microsoft Windows® Azure™ Platform

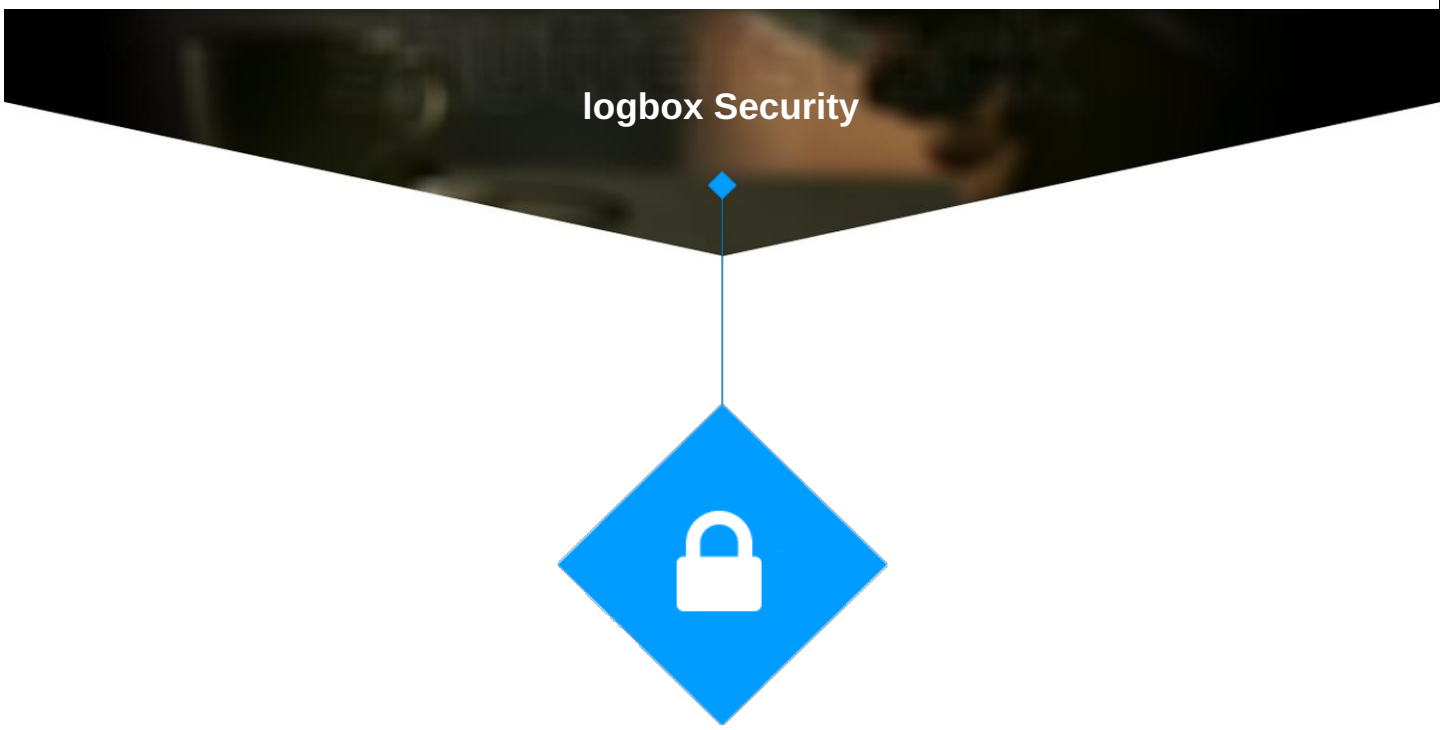
Google Angular 2

Google Angular 2 is a powerful tool for creating and delivering rich Internet applications.

It is an open source HTML5 framework that enables fast and rich business applications and mobile apps. It works on all major OS' plus all major browsers, including Firefox, Google Chrome, Safari and Edge.

We use Google Angular 2 in combination with Microsoft TypeScript for true object oriented development environment.
Learn more: https://angularjs.org/

logbox



When speaking about security, we actually cover more than just one layer. Security is comprised of confidentiality, integrity and availability.

Logbox is developed, hosted and secured at the Microsoft Windows® Azure™ datacenter, a world leading cloud provider, delivering the highest levels of availability, performance and security.

Microsoft Windows® Azure™ is operating in a geographically distributed facility. While running 24/7 the facility is taking various measures to protect operations from power failure, physical intrusion and network outage. External access to our servers is controlled by multiple layers of firewalls, intrusion detection and prevention systems, load balancers and routers, which are configured and monitored according to industry best practices. Please read more about Azure's security features and capabilities

SECURITY LEVELS HIGHER THAN DESKTOP SYSTEMS

Logbox Is better secured than your own desktop environment. With Logbox your data isn't stored on your computer - e.g. if your computer crashes, or gets lost, or stolen, all your data remains completely safe and unaffected.
In addition to Microsoft's responsibility for the datacenter, we take our own measures to better secure the data stored in our own databases.

SOME OF THE SECURITY MEASURES WE TAKE:

SSL:

Our servers have SSL certificates so all data transferred between the users and the service is encrypted.

User Access & Permissions:

Only persons invited by you, with user permission levels selected by you, will have access to your organization's data. You can remove any user(s) whenever you want. You also have the option to invite Customer Care for support purposes only, at your total discretion.

Password Protection:

At a minimum, Logbox takes the following measures to protect your password:

Users must choose a strong password

Automatic lockouts are enforced

Data Protection and Backup:

Our service has been designed for high availability, with redundancy built into every level of our hosting infrastructure, including redundant power, network, database and web servers.

All customer data is backed up daily. Every transaction is saved into three different servers so we can immediately recover your data in case of hardware failure. We also run a continuous backup into a secondary facility for further data protection. We also run a continuous background task which backs-up the data into a back-up facility for further real-time data protection.

- when incorrect passwords are repeatedly entered
- Activation of a new password can be done only via access to email account.

  The browser is not allowed to save your login (which eliminates access from a stolen or compromised computer) and, in addition
- Stored passwords are encrypted - even we can't see your password.

ADDITIONAL STEPS YOU CAN TAKE TO REMAIN PROTECTED

We work very hard to keep logbox secure. Here are some additional simple steps you can take in order to keep your password better protected:

1. Create a password nobody can guess, so don't use dictionary words or family names. Be cryptic or use multi-word pass phrases - easy to remember, hard to crack.
2. Don't share your password with anybody.
3. Don't write your password on a sticky note and attach it to your computer.
4. Keep your browser software up to date.
5. Make sure you only login at logbox

שאלות ותשובות:

שאלה: היכן ה- Data Centers של הספק? באיזה ארץ יאוחסן המידע של הלקוח?
תשובה: הולנד , אמסטרדם – Microsoft Azure

שאלה: מהי גישת הארגון להצפנת מידע? האם מצפינים מידע באחסון ו/או מידע בתנועה?
תשובה: מוצפנת בתנועה ובמנוחה

שאלה: כיצד מנוהלים מפתחות ההצפנה?
תשובה: ניהול אוטומטי על ידי מיקרוסופט

שאלה: האם יש לספק מערכת לניהול זהויות המאפשרת להקצות הרשאות לפי תפקידים והצורך לדעת?
תשובה: כן – ROLES

שאלה: האם הספק תומך במנגנוני הזדהות חזקה 2 Factor Authentication? אם כן, באילו מנגנונים?
תשובה: התמיכה קיימת

שאלה: כיצד הספק ממדר ומפריד בין המידע של לקוח מסויים למידע של לקוחות אחרים?
תשובה: שכבה אפלקטיבית לניהול דיירים ב- DB ובנוסף ברמת ה- DB שימוש במנגנון row level security

שאלה: האם וכיצד יבוצע ניטור על הפעילות בחשבון של הלקוח בענן? אילו יכולות ניטור מספקים?
תשובה: כניסות משתמשים, לוג על פעולות במערכת.

שאלה: על איזה אירועי אבטחת מידע ידווח הספק ללקוח? כיצד הספק מגדיר אירוע אבטחת מידע?
תשובה: ניסיון פריצה , פעילות חשודה

שאלה: לכמה זמן (כמה שנים) יישמר המידע של הלקוח בסביבת הענן?
תשובה: לא מוגבל

שאלה: אילו מדדי RTO, RPO מציע הספק?
תשובה: RPO - חצי שעה , RTO - 4 שעות

שאלה: האם הספק הגדיר תכנית המשכיות עסקית והתאוששות מאסון?
תשובה: כן

שאלה: כיצד הספק נפטר ממדיה /אמצעי אחסון שאין לו צורך בהם יותר? האם הספק מקפיד על השמדה "מאובטחת" של המדיה?
תשובה: ניהול על ידי ספק הענן.

שאלה: האם ישנם מגבלות ליכולת הצמיחה בענן (אילוצי scalability)?
תשובה: לא

שאלה: האם ניתן להגדיר גישה למערכת רק מתוך הרשת הארגונית?
תשובה: כן. באמצעות הגבלת ה- IP