SalesScreen – Security Overview

Introduction

The security and confidentiality of our customers' data in SalesScreen is of the utmost importance to us. We constantly strive to provide an application whose every security aspect has been thoroughly taken into consideration and addressed. Our Information Security Management System (ISMS) is ISO 27001 certified and is constantly evolving with updated guidelines and new industry best practices.

This document contains a description of the most important measures and procedures we use to ensure the confidentiality, availability and integrity of our customers data. The contents of this document are updated on a regular basis as we introduce new security measures or introduce major changes in our architecture.

Access Control

PROVISIONING

To minimize the risk of data exposure, SalesScreen adheres to the principles of least privilege and role-based permissions when provisioning access. Employees are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. All production access is reviewed at least quarterly.

AUTHENTICATION

To further reduce the risk of unauthorized access to data, SalesScreen employs multi-factor authentication for all access to systems with highly classified data, including our production environment, which houses our customer data.

PASSWORD MANAGEMENT

SalesScreen requires employees to use an approved password manager. Password managers generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password-related risks.

Device Management

All workstations issued to SalesScreen personnel are configured by SalesScreen to comply with our standards for security. SalesScreen's default configuration sets up workstations to encrypt the harddrive, have strong passwords, and lock when idle. Mobile devices that are used to engage in

Dogu SalesScreen AS
Karl Johans gate 13, 0154, Oslo, Norway

company business are required to be enrolled in the appropriate mobile device management system, to ensure they meet SalesScreen's security standards.

Cloud Service Provider

We use Microsoft Azure as our exclusive cloud provider. All our services and data are hosted in Microsoft Azure facilities in Europe. Microsoft Azure uses industry-leading security measures and privacy policies to protect their infrastructure. For more information on these security measures, please visit https://azure.microsoft.com/en-us/overview/trusted-cloud.

Storage

WHAT WE STORE

We store basic information about each user in our database. This information includes, at a minimum, the name and email of the user. The phone number of each number can also be stored within SalesScreen, but this is an optional feature. In addition to the personal data that is stored for each user, we store data on sales activities that is registered with our service.

WHERE WE STORE IT

For persistent storage we use Azure SQL Databases located in Microsoft's North Europe data-center (Ireland). Our service consists of multiple database instances, with customers spread across these instances. For our Enterprise customers we offer the opportunity to reserve a dedicated database that will only be used by that single customer. Back-ups for each database are stored in Microsoft's West Europe data-center (Netherlands).

ACCESS CONTROL

All our databases are configured with a firewall, that limits the set of IP addresses that can connect with them. The firewall is configured using a white-list of approved IP addresses. This list is reviewed monthly. Access to our production databases are reserved to senior members of our staff. The databases are configured to only accept secure connections, ensuring that credentials are never transmitted over an insecure line.

BACK-UPS

All our databases are configured with a feature called Point in Time Restore. This feature allows us to back-up our databases to any point in time within the retention period. We currently operate with a 35 days retention period which is the maximum allowed by Azure.

In addition, we have configured a feature called Standard Geo Replication for all our databases. This feature adds a read-only database in a separate Azure region, we currently use the West

Dogu SalesScreen AS
Karl Johans gate 13, 0154, Oslo, Norway

Europe region. In the event of a region-wide Azure outage, this read-only database can be restored within 5 minutes.

All our databases are encrypted using Azure Transparent Data Encryption, ensuring that the databases, backups and logs are encrypted at rest.

DATA RETENTION

Customer data is removed immediately upon deletion by the end user. SalesScreen hard deletes all information from currently running production systems and backups are destroyed within 35 days. SalesScreen's hosting provider, Microsoft Azure, is responsible for ensuring removal of data from disks is performed in a responsible manner before they are re-purposed.

SCALING

All our databases are hosted within an Elastic Database Pool, which mean that they share resources among them. As the resource consumption of each database vary over time, pooling them together allows us to make sure the collection of databases has enough resources combined. The Elastic Pool can be scaled at any time, to handle increased traffic loads.

THREAT DETECTION

We have auditing configured for all our production databases, and we store the audit logs for each database for 180 days. All these logs are stored within our Azure account, and access is only given to system administrators. We use a feature called Azure Threat Detection, that notifies system administrator of suspicious activity, such as failed login attempts, in real-time.

Dogu SalesScreen AS
Karl Johans gate 13, 0154, Oslo, Norway

Servers

Our application runs on a collection of Azure App Services. These are virtual machines running IIS that are configured by Microsoft according to best practices. These virtual machines are easily scalable and can be replicated to different regions ensuring that our customers from all corners of the world receive the best possible performance.

PHYSICAL LOCATION

All our App Services are currently located in the North-Europe (Primary) and West-Europe (secondary) Azure regions. These are located in Ireland and the Netherlands respectively.

CONFIGURATION / MALWARE PROTECTION

Running on Azure App Services (PaaS) means we don't directly manage the configuration of the virtual machines. These machines are configured and maintained according to security best-practices by Microsoft at all times.

SCALING

App Services can be scaled within minutes to handle peak loads. When detecting increased load over a period of time, the servers are automatically scaled without the need for human intervention.

BACK-UP

All hardware failure is automatically handled by Azure. We also have a separate back-up App Service configured in the West Europe Azure region. We use Azure Front Door to share the traffic between these two instances. Under normal operations the back-up instance does not receive any production traffic. If a failure is detected on our main server, the Traffic Manager will automatically transfer traffic to our back-up instance.

Logging

We have different logging tools in place to provide an audit trail over both our hosting infrastructure in Azure and the SalesScreen application.

Azure automatically logs all access to our subscription and all changes made to our infrastructure, logging the type of action, the time it occurred and the account that initiated the action. It is not possible for anyone to turn this feature off.

Within the SalesScreen application itself we log key events to provide an audit trail in the event of security incidents. All logs generated by the application are stored separately from the application

Dogu SalesScreen AS
Karl Johans gate 13, 0154, Oslo, Norway

itself. The logs are stored within our Azure account and is backed up to multiple regions. The logs are kept for 365 days.

WHAT WE LOG

We track all the important actions taken by users within our application, storing the exact time it happened and the account that initiated it. Where possible, we also store the IP address and the user agent of the current session.

Important actions include:

- Creation and removal of user accounts
- User session start and end
- Failed password attempts
- Changes in access levels for existing accounts
- Updates to user profiles
- Updates to API keys

SCREENS

Screens are protected by API keys, meaning no valid session is needed to open them. We log all access to these screens with IP address and time of access. It is not possible to circumvent this.

API

All requests that are sent to our API are logged. This includes both failed and successful requests. For each request we store the API key used, the exact time of the request and the IP address from which it originated.

ADMIN ACCOUNTS

To provide support to our customers, we have reserved a number of admin users for a subset of our employees. These admin users are allowed to enter our customers' accounts to help them with any type of problem they are having.

All admin access to customers' accounts is logged. All actions taken by admin accounts are logged on the same level as normal user accounts. There is no way for admins to turn this feature off or circumvent it.

Dogu SalesScreen AS
Karl Johans gate 13, 0154, Oslo, Norway

Encryption

All communication with the SalesScreen application is encrypted in transit. Our APIs and application endpoints are SSL/TLS only. We score an “A” rating on SSL Labs´ tests, and are continuously monitoring these scores to uncover any potential weaknesses.

Business Continuity

We have written Disaster Recovery plans for all critical components in SalesScreen. These plans are tested on a regular basis.

Responding to Security Incidents

We have a documented Incident Response Plan, and we continuously educate relevant personnel on security procedures and policies.

Monitoring

Every aspect of the SalesScreen overall platform is monitored 24/7 to ensure that we always remain informed of status changes.

These aspects include:

- External connectivity: we have multiple uptime monitoring agents located across the globe which periodically (down to the minute) probe the external connectivity of SalesScreen’s key end-points. These key end-points allow a monitoring of the overall health of the service and they include all our APIs and application end-points.
- Server vital metrics: CPU, RAM, Bandwidth, Disk load, etc.
- Database vital metrics: DTU, CPU, Deadlocks, etc.
- Code-level exceptions

Testing

We have configured a development environment in Azure that mirrors the production environment. All software testing is performed in the dev environment, we never do tests using production resources or customer data. The development and production environments are totally separated and does not share any common components.

Dogu SalesScreen AS
Karl Johans gate 13, 0154, Oslo, Norway

All changes are reviewed and tested in the development environment before being introduced to production systems.

Penetration Testing

SalesScreen engages independent entities to conduct application-level and infrastructure-level penetration tests at least annually. Results of these tests are shared with senior management and are prioritized and remediated in a timely manner. Customers may receive executive summaries of these activities by requesting them from their account executive.

Vendor Management

To run efficiently, SalesScreen relies on external organizations to serve as sub-processors. Where those sub-processors organizations may impact the security or privacy of SalesScreen's production environment, we take appropriate steps to ensure our security posture is maintained by establishing agreements that require service organizations to adhere to confidentiality commitments we have made to our customers. SalesScreen monitors the effective operation of the organization's safeguards by conducting reviews of all service organizations' controls before use and at least annually.