White paper

Security and Infrastructure

velaro

info@velaro.com 1-800-983-5276 velaro.com

Contents

Contents 2
Introduction 3
1. Cloud Hosting and Management 3
2. Application Security 3
2.1.1. Secure URLs 4
2.1.2. Data Encryption 4
2.1.3. Application Firewalls 4
2.1.4. Anti-virus File Checking 5
2.2.1. Agent Security Settings 5
2.2.2. Visitor Security Settings 6
2.2.3. Storage Security Settings 6
2.2.4. Compliance Mode 6
2.2.5. Agent Authentication and Authorization 7
3. Data Privacy 8
3.2.1. Opt-in Cookie Control 9
4. System Architecture 9
5. Infrastructural Security 10
6. Operational Security and Best Practices 11
7. Disclaimer 14

info@velaro.com 1-800-983-5276 velaro.com

Introduction

Velaro's Enterprise Chat Software-as-a-Service (SaaS) application has been providing best-in-class click-to-chat solutions for over two decades. As one of the original SaaS providers, our goal has always been to provide our customers with the best experience possible. This philosophy permeates through every aspect of Velaro because we recognize that it is our software that often provides you with the very first chance to interact with potential customers and leave a powerful impression.

At the core of the Velaro experience are a set of fundamental technologies and infrastructural components that we have put in place to ensure the utmost in data integrity, security, scalability, and system uptime. The components include cloud hosting and management, application security, system architecture, network security, and operational security.

1. Cloud Hosting and Management

1.1. Microsoft Azure Cloud Services

The Velaro platform is hosted on Microsoft Azure Cloud Services. Azure is a cloud computing platform and infrastructure for building, deploying, and managing applications and services through a global network of Microsoft-managed datacenters. It supports both Platforms as a Service (PaaS) and Infrastructure as a service (IaaS) and enables hybrid solutions that integrate cloud services with customers' on-premises resources. Microsoft Azure is SOC 2 compliant.

2. Application Security

2.1. Chat Security

Velaro's enterprise chat system allows organizations to interact with your website visitors in real-time. Velaro conducts these interactions based on standard HTTPS protocols and ports. Since Velaro leverages the built-in capabilities of your web browser, there is never a

need to force your website visitors to download or install any additional plugins, applets, flash, or java apps.

2.1.1. Secure URLs

Accessing Velaro via Transport Layer Security (TLS) technology protects your information using both server authentication and data encryption, thereby ensuring that your data is safe, secure, and available only to registered users in your organization. Velaro's application security model ensures that, after authentication, your user identity accompanies every request to the Velaro server so that segregation of customer data is strictly enforced.

2.1.2. Data Encryption

All chat data from both visitors and agents is encrypted, both in-motion and at-rest. Data in- motion is encrypted using Secure Socket Layer/Transport Security Layer (SSL/TSL) at 256-bit strength using a trusted public certificate authority. Data at-rest is encrypted using Transparent Data Encryption (TDE). See https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview?view=azuresql&tabs=azure-portal for more information about TDE.

2.1.3. Application Firewalls

When visitors launch a chat session on your website, the chat window that is displayed to your visitor communicates directly with the Velaro servers. Your website visitors and your agents who receive incoming chat requests are never connected directly to each other over the Internet. All communications happen through the Velaro servers. As information is processed throughout the chat, Velaro has hardware and software components in place that monitor and filter the information flow. Some of these components include enterprise-grade firewalls, intrusion detection systems, and application content filters.

2.1.4. Anti-virus File Checking

As Velaro allows your agents to upload and share files, the system continuously scans all file transfers using the latest anti-virus software technology.

These systems, in addition to the Velaro application itself, significantly reduce the risk of an external security attack by preventing unauthorized access, or the injection of malicious and potentially harmful content.

2.2. Agent Console Security

Whether your organization uses the Velaro agent desktop or the browser-based agent console, your data is secure. The agent console has been engineered to meet and exceed industry-standard security practices. Like the chat sessions, all agent communication occurs over standard internet protocols. Chat data is encrypted in-motion and at-rest.

As an enterprise-class chat provider, Velaro must meet every aspect of your organization's security concerns. Many of those concerns revolve around how your agents interact with the outside world via the Velaro agent console. Velaro provides application-level security controls that allow administrators to have complete control over their agent console. Features related to agent console security can be enabled and disabled in our web-based administrative control panel. These security features can only be adjusted by the designated administrators you define. Additionally, you can segment your security settings around different roles. Following is a list of the security controls within the Velaro console.

2.2.1. Agent Security Settings

- Allow agents to e-mail transcripts
- Allow agent-to-agent chats within the console
- Allow agents to reject chats that are queued
- Allow agents to copy chat transcripts to the clipboard
- Allow agents to push web pages during chat
- Allow agents to upload files

- Allow agents to block visitors
- Allow agents to delete transcripts

2.2.2. Visitor Security Settings

- Allow visitors to copy chat transcripts to the clipboard
- Mask credit card numbers during chat
- Mask social security number entered during chat
- Mask birth dates entered during chat

2.2.3. Storage Security Settings

- Disable visitor, chat, and survey archival
- Disable storage of visitor e-mail and name
- Mask credit card numbers when archiving chats
- Mask social security numbers when archiving chats
- Mask birth dates when archiving chats
- Enable PGP encryption on transcript offloading integrations

2.2.4. Compliance Mode

With Velaro's Compliance Mode, your account will assume a higher security protocol and Velaro will no longer store your chat transcripts or visitor information. Velaro will maintain a simple record of your chat including start/end times, the agent associated with the chat, and queue wait times. If your organization requires transcripts to be stored off site, then please refer to any of our storage integrations.

In addition, if your company handles protected health information (PHI) data during chat engagements, a HIPAA Business Associate Agreement (BAA) can be executed with Velaro to ensure you remain in HIPAA compliance.

2.2.5. Agent Authentication and Authorization

Velaro provides each user in your organization with a unique username and password that must be entered each time a user logs in. A customer designated Velaro subscription administrator is the only one who has the authority to manage the login accounts under your Velaro subscription.

The password policy is configurable and can be customized to match your organization's corporate password policy. The following password configuration rules are available:

- Password history (prevent use of previous passwords when being changed)
- Password length
- Password expiration
- Password complexity

For security purposes, Velaro locks out users from future login after multiple failed login attempts.

Velaro also provides all customers with granular role-based security options. Every user within your account may be designated as a site administrator, site manager, department manager, or agent. Based on the user's role, they are granted or denied varying levels of account setup and configuration options along with different levels of granularity to your corporate data and reports.

2.3. Secure Form

To allow organizations to maintain PCI Compliance, Velaro features secure forms to capture information from visitors and display it to agents on a one-time basis. This feature is often used in eCommerce implementations, in the case where an agent needs to process a credit card return for a visitor.

Accounts that have secure forms enabled can configure one or more secure forms to capture information. The agent triggers the form to be displayed to the visitor, and when the visitor submits the form, the submitted data is displayed to the Agent in the console. The date is erased after a configurable timeframe.

The Secure form utilizes a separate Azure cloud instance that is distinct from Velaro platform services. The data is captured in memory-based storage, encrypted, and keyed. This key can only be used by the agent requesting the secure form data. Once the form is submitted and the data is displayed, the date is then destroyed and memory overwritten.

2.4. Audit Control

To help organizations maintain compliance with the numerous certifications and standards required by many different industries, Velaro maintains a complete audit trail of all changes to your Velaro account. All changes to your account made within the administrative control panel, and within the agent console are recorded and available for review. Administrators have direct access to the audit report within the Velaro console, which means all audit trail reports can be scheduled and automatically e-mailed to your team in a variety of formats on a daily, weekly, or monthly basis.

3. Data Privacy

3.1. Velaro Privacy Policy

Velaro is committed to protecting your privacy and developing technology that gives you the most powerful and secure online experience. Velaro does not sell, rent, or lease any client information to third parties. Velaro secures your personal information from unauthorized access, use or disclosure. Velaro secures the personally identifiable information you provide on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure.

3.2. Cookies

Velaro uses cookies to identify visitors and return visitors. However, Velaro does not rely on cookies and can function without them. Velaro does not to store any sensitive information in a cookie, and all cookies except for the “returning visitor” cookie are only saved for the duration of the visitor’s session. Please see the Velaro Privacy Policy for additional details: https://velaro.com/privacy-policy/.

3.2.1. Opt-in Cookie Control

Velaro can interface with the visitor opt-in cookie control on your website to modify how cookies are used based on visitor choice settings.

3.3. Data Storage and Encryption

Velaro leverages Microsoft Azure storage, a highly durable, massively scalable cloud storage platform. Data storage is only accessible using strongly encrypted communication paths. The Velaro application security model ensures that user identity information accompanies every request to Velaro servers, resulting in complete segregation and privacy of customer data. Customers own their data and Velaro employees cannot access customer encrypted data.

4. System Architecture

Velaro's application is built on using numerous open standards and web-based technologies. Some of these include HTTP, HTTPS, XML, JSON, SOAP, JavaScript, HTML, Microsoft.NET and ASP.NET, and SQL. Velaro's system architecture is provided by implementing several key guiding philosophies, including multi-tenancy, scalability, redundancy, and fault tolerance.

4.1. Multi-Tenancy

For almost twenty years, Velaro has been driving innovation in the Software-as-a-Service (SaaS) market. From the very beginning, our applications have been built with the ability to support all our customers under a single "virtual" instance of our application and database. This ensures that Velaro does not have to provide individual servers and resources specifically for each customer. With Velaro you never have to worry about running out of resources or experiencing the performance problems that can result with alternative configurations, allowing you to add hundreds of agents instantly. Having all Velaro's customers operating under a single shared set of resources means that we can easily scale our solution and stay ahead of all our customer's needs.

Some additional benefits our customers derive from Velaro's multi-tenant architecture include:

- The ability for Velaro to see global usage patterns and enhance our solution as needed.
- Rapid deployment of solutions and versions of our product globally to all customers.

4.2 Scalability

The Velaro multi-tenant architecture itself is inherently scalable, and for the underlying system resources, Velaro leverages the Microsoft Azure platform for scalability. Because the extent of the Azure platform worldwide, Velaro can quickly and easily scale to handle high traffic volume spikes, localized access, and large volumes of accounts and users.

4.3. Redundancy and Fault Tolerance

Every layer with Velaro's infrastructure includes the use of multiple shared resources on the Microsoft Azure cloud platform. By leveraging this redundancy, none of Velaro's systems allow for a single point of failure. Additionally, there are several mechanisms built into Microsoft Azure software-controlled infrastructure to ensure services and applications remain available in the case of a failure.

5. Infrastructural Security

5.1. Network Security

Velaro actively monitors all system entry and exit points for malicious traffic. Velaro utilizes industry leading intrusion prevention system, gateway anti-virus and firewall solutions providing state-full packet inspection of all traffic entering and leaving the Velaro system. Additionally, Velaro utilizes industry leading best practices and benchmarks to provide a secure operating environment. Our secure system

configurations are hardened and regularly audited using published system benchmarks from the Center for Internet Security (CIS) and The National Institute of Standards and Technology (NIST).

Additionally, Velaro regularly conducts both internal and external vulnerability assessments of the Velaro System to ensure that we are continuously providing a secure operating environment and that all security and monitoring controls are actively protecting our customers against the latest security threats.

5.2. Monitoring and Uptime

The ability to identify and act upon potential security incidents is mission critical to your chat system. Velaro's Network Operations Center (NOC) team continuously monitors all system components for security, availability, and performance. All issues are automatically reported to the Velaro NOC team, so they can assess and provide immediate response to any issue that

may arise. Velaro's continuous monitoring strategy ensures that Velaro system maintains the highest levels of availability and security.

The multi-layered approach to fault tolerance allows Velaro to maintain industry leading uptime of 99.98%. By guaranteeing this uptime through your negotiated Service Level Agreement, Velaro allows you to provide superior service without compromising reliability, security, or quality.

6. Operational Security and Best Practices

6.1. Disaster Recovery

Velaro performs a full backup of system components and data every 6 hours, with a snapshot every 15 minutes. The enables the restoration of the Velaro system on another Azure data center in the event of a regional catastrophic failure. Velaro actively maintains a disaster recovery plan in conjunction with regular recovery exercises and training to ensure the continual availability of the Velaro system.

6.2. Data Retention and Backup

Velaro's standard data retention policy means that we keep all your data online and available for real-time access for two years. Velaro's maintenance procedures archive any transcripts that are over three years old. Unless requested by a customer, archived transcripts are never deleted; they are simply removed from our online storage media to maintain optimal performance. Any transcripts that have been moved offline can still be made accessible within 48 hours of a customer's request.

Additionally, Velaro offers flexible options for data retention and its enterprise customers. Velaro can accommodate a change in data retention including:

- The ability to by-pass permanent storage within Velaro's archive. Chats may be configured to simply disappear once the conversation is complete.
- Immediate storage on an organization's private server. Chat transcripts and personal information can be pushed to your organization's servers in real-time and is not housed on Velaro servers. This is a critical component of HIPAA compliance mode.
- Automatic removal of data after a pre-defined period (i.e., after 30, 60, 90 days). This automatic deletion process enables Velaro's compliance with GDPR.
- Never archiving data and allowing for longer periods of real-time access.

All backup files are verified, encrypted, and then compressed for transfer to Azure storage.

6.3. Secure Coding Practices

Velaro recognizes the Open Web Application Security Project (OWASP) organization as the authority on web application security and has implemented coding practices around the OWASP standards. Velaro's development team is constantly aware of OWASP (Open Web Application Security Project) exploits. The team always practices secure coding standards to ensure any unknown data received by a Velaro application is validated and Sanitized.

This practice is constantly tested through code reviews and vulnerability testing. A few secure coding practices used by Velaro:

- Input Validation
- Data Sanitizing
- Source code Audits
- Penetration Testing

6.4. Incident Response

Velaro believes the first step in incident response is putting guidelines in place to ensure that incidents do not occur, including:

- Guidelines to ensure that we always use standard security principles of least required access to perform a function
- Always make sure system configurations are in accordance with industry standard best practices
- Services and applications that are not used must be disabled where practical.

Velaro ensures that all security-related events on critical or sensitive systems are logged and an audit trail is maintained. This is important, so if an incident occurs our Operations team has the information, they need to correct the issue as quickly as possible.

6.5. Acceptable Usage Policies

Velaro does not engage customers, or allow the use of our product, on websites that are involved in illegal or harmful activities. These sites include pornography, sites intended to advocate or advance computer hacking or cracking, drug paraphernalia, hate, violence, or racial and ethnic intolerance. While Velaro does not actively scan all our customer's websites for the display or dissemination of these content types, we do take the necessary steps to warn customers of unacceptable use after we learn that it exists. If the content is not removed within a specified grace period, their Velaro account is deactivated.

7. Disclaimer

Velaro, Inc provides this document “as is” without warranty of any kind, either express or implied to, the implied warranties of non-infringement, merchantability, or fitness for a particular purpose.

The statements made in this document have not been audited or certified by any independent auditors. This document is for informational purposes only. While Velaro strives to ensure that all information is accurate, this document could include technical inaccuracies or typographical errors. Velaro Inc. cannot be held liable for any variations or for any future changes to our business that may invalidate certain information within this document.

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 (electronic, mechanical, photocopying, recording, or otherwise), without the prior written consent of Velaro, Inc., except as otherwise permitted by law.

Revision History
July 1, 2022 - N. Derrick Harris
Nov 2, 2020 - N. Derrick Harris
Jan 30, 2018 – N. Derrick Harris
Feb 10, 2014 - Ronald Hill

info@velaro.com 1-800-983-5276 velaro.com