



Security and Infrastructure

Technically speaking, **we're really saavy.**

Introduction

Velaro's Enterprise Chat Software-as-a-Service application has been providing best in class click-to-chat solutions for over a decade. 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 times provides you with the very first chance to interact with potential customers, and we all know the power of impressions.

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 application security, system architecture, network security, and operational security.

Application Security

CHAT SECURITY

Velaro's enterprise chat system allows organizations to interact with your web site visitors in real-time. Velaro conducts these interactions based on standard HTTP and HTTPS protocols and ports. These are the same communication protocols used billions of times a day by all standard web browsers. 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 runtimes.

Accessing Velaro via Secure Socket Layer (SSL) 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.

Application Features

- Chat Security
- Agent Console Security
- Authentication and authorization
- Audit Control
- Privacy and Cookies
- Data Storage and encryption

System Architecture

- Multi-tenancy
- Redundancy
- Scalability

Infrastructure Security

- Network Security
- Monitoring
- Physical Security

Operational Security

- Best Practices
- Disaster Recovery
- Data Retention and Backup
- Secure Coding Practices
- Incident Response

When visitors click the chat button or hyper-link text 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 a number of hardware and software components responsible for monitoring and filtering the information flow. Some of these components include enterprise grade firewalls, intrusion detection systems, and application content filters. Additionally, since Velaro allows your agents to upload and share files, the system continuously scans all file transfers using the latest anti-virus software.

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.

AGENT CONSOLE SECURITY

Whether your organization uses the Velaro Agent Desktop or the Web Based Agent Console, rest assured that your data is secure. The agent consoles have been engineered to meet and in many cases exceed industry standard security practices. Like the chat sessions, all agent communication occurs over standard internet protocols. Any agent or organizations may elect to utilize and enforce secure HTTPS (SSL) protocols so that these communications may be encrypted with 256 bit SSL, using a trusted public certificate authority.

As an enterprise-class chat provider Velaro must meet every aspect of your organizations security concerns. Many of those concerns revolve around how your agents interact with the outside world via the Velaro agent consoles. Velaro provides a number of application level security controls which allow administrators to have complete control over their agent's consoles. Most security 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 agents. For example, you may want your support team to have access to remote desktop capabilities but hide these features from your sales team.

A few of these security controls include:

Force agents to use SSL logins

IP-based agent login restrictions

Disable agents and/or visitors from e-mailing transcripts

Disable agents ability to send files during chat

Disable agent to agent chats

Disable agents from copying chat transcripts to the clipboard

Disable agents from pushing web pages during chats

Disable agents from rejecting chats

(via queue alerts)

Disable agents from typing free-formed text, restricting them to just your organization's premade messages

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 this data within Velaro's comprehensive reporting capabilities, 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.

AGENT AUTHENTICATION AND AUTHORIZATION

Velaro provides each user in your organization with a unique user name 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 rules are configurable:

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.

PRIVACY AND COOKIES

Velaro is committed to protecting your privacy and developing technology that gives you the most powerful and safe 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. When personal information (such as a credit card number) is transmitted to other websites, it is protected through the use of encryption, such as the Secure Socket Layer (SSL) protocol.

Velaro occasionally uses cookies to identify visitors and potentially identify them as a return visitor. Velaro does not rely on cookies and can function without them. If cookies are used they are third-party cookies and are marked as coming from the Velaro domain in accordance with industry standards. It is Velaro's policy 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. Velaro cookies can be marked as secure when using an encrypted connection.

DATA STORAGE AND ENCRYPTION

Velaro's data storage system uses enterprise quality RAID 5 storage devices, thereby providing the upmost in storage uptime and availability. Additionally, data storage is only accessible using strongly encrypted communication paths. The Velaro application security model ensures that user identity information accompanies every request to the Velaro server, resulting in complete segregation and privacy of customer data. Customers own their data and Velaro employees cannot access customer encrypted data.

Velaro follows industry standard encryption practices to ensure that your data is always secure. Additionally, Velaro provides an additional layer of encryption that allows our customers to supply their own private encryption key which is only available to that organization. If used, this encryption key pre-encrypts all your chat conversations before being stored permanently on our servers.

System Architecture

Velaro's application is built on using numerous open standards and web based technologies. Some of these include HTTP, HTTPS, XML, SOAP, JavaScript, HTML, Microsoft.NET and ASP.NET, and SQL. Velaro's system architecture is provided by implementing a number of key guiding philosophies, including:

MULTI-TENANCY

For over ten 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 of our customers under a single “virtual” instance of our application and database. This ensures Velaro doesn’t have to provision 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 of Velaro’s customers operating under a single shared set of resources means that we can easily scale our solution and stay ahead of all of our customer’s needs.

Multi-tenancy architectures are significantly different and complex, but something that all customers in the process of choosing any SaaS solution need to consider. It’s hard to believe, but even today many of Velaro’s competitors still rely on a single-tenant architecture, which provide numerous problems of both scalability and reliability. Velaro knows that providing an advanced architecture can sometimes be more difficult, but as pioneers in the SaaS industry, its second nature to us.

Some additional benefits our customer’s derive from Velaro’s multi-tenant architecture include:

The ability for Velaro to see global usage patterns and enhance our solution as needed.

Rapidly deploy new solutions and new versions of our product globally to all customers.

SCALABILITY

As part of our growth planning, Velaro always makes it a point to stay ahead of ourselves in regard to the bandwidth, systems and hardware that are required to maintain our service. Velaro spends significant resources in both capacity monitoring and

management. Velaro monitors a number of key performance indicators at all layers of our system. By “staying ahead of ourselves” we have made it a standard practice to not let any of these key metrics fall below specific thresholds in regard to performance and utilization. This means that at no time will any of Velaro’s firewalls, load balancers, network switches, or servers reach any capacity that would cause performance degradation. Velaro always maintains a healthy buffer between our customer’s needs and our application’s capacity.

REDUNDANCY AND FAULT TOLERANCE

Every layer within Velaro’s infrastructure includes the use of multiple shared resources. By providing this redundancy, none of Velaro’s systems allow for a single point of failure. Velaro’s fault tolerance solution includes physical, network, application, and database layer redundancy. This 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. At Velaro, our focus is our customers. We’re here to make sure your needs are met.

Additionally, Velaro’s data center boasts redundant electric utility power feeds from two separate sub-stations. All network devices have battery back-ups by multiple Liebert UPS units. And our 1,000 kilowatt auto-cutover diesel generator – with its 500 gallon fuel tank and disaster fuel delivery contract – ensures complete power redundancy of all network services. In addition, the facility includes multiple Liebert cooling systems, an 18-inch raised floor and advanced fire suppression system. In the aftermath of hurricane Isabelle, when many facilities throughout the region lost power, flooded or overheated, the DataPoint facility remained fully powered, cool, dry and completely operational.

Infrastructural Security

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.

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 Team (NOC) 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 following sample report is generated from one of the three different independent uptime monitoring services that Velaro employs to constantly gauge availability and performance. Please note that these reports are "raw data" reports and by nature include "scheduled maintenance" downtime. Actual uptime and availability is upwards of .03% higher than what these reports present.

PHYSICAL SECURITY

The company hosts their primary servers and network infrastructure at a co-location facility managed by DataPoint, Inc. DataPoint boasts both SAS-70 Type II certification, and PCI DSS compliance.

DataPoint's data centers provide redundant fiber connectivity directly to multiple Tier-1 carriers, including Level 3, XO Communications and Verizon. DataPoint offers a fully redundant Cisco Powered network with 24X7x365 monitoring and redundant power sources.

The primary DataPoint facility is located in the Tide Point complex of Baltimore, MD, where many technology-driven businesses also reside (including Advertising.com (AOL), Under Armour, and Mercy Hospital). The facility is accessible 24x7x365 by approved personnel only. DataPoint's security surveillance system, multi-level card and fingerprint access with 24/7/365 on-site personnel, assure that you have the highest level of monitoring and security. No one accesses the facility without proper authorization and escort.

Operational Security and Best Practices

DISASTER RECOVERY

Disaster recovery and business-continuity-planning are core features that are incorporated into the Velaro system design. Velaro's production system is designed with high availability on every critical system device with automatic fail-over of devices to prevent single points of 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. The Velaro disaster recovery plan incorporates both local and off site backups of all system components and data. In addition Velaro maintains continuous off site replication of critical system data and services to a disaster recovery site to ensure the continuity- of-operations in the event of a disaster.

DATA RETENTION AND BACKUP

Velaro's standard data retention policy means that we keep all your data online and available for real-time access during a period of no less than three year. Every day, Velaro's maintenance procedures are responsible for archiving 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. At a customer's request Velaro is able to 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 can be pushed to your organization's servers in real-time.

Automatic removal of data after a pre-defined period (i.e. after 30, 60, 90 days).

Never archiving data and allowing for longer periods of real-time access.

Velaro's backup policy involves the nightly backup of all critical systems and databases. All backup files are verified, encrypted and then compressed for transfer to an offsite facility. Velaro has partnered with a leading backup software and offsite storage vendor to ensure the most secure and reliable integrity of your data. Velaro's offsite backups are maintained by one of the few organizations that can boast both SOC 1SSAE 16 Type 2 and ISO 27001 certification. A copy of our backup partner's certifications can be produced upon request.

SSAE 16, previously called SAS 70, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). SSAE 16 verifies a service organization has been through an in-depth audit of its control objectives and control activities to ensure processing and hosting customer data is done safely and securely.

ISO-27001 certification is the leading international standard for measuring information security management systems. It sets out requirements and best practices for a systematic approach to managing company and customer information based on periodic risk assessments appropriate to ever-changing threat scenarios.

In addition to regular offsite backups, Velaro maintains a secondary "hot standby" facility where our databases are constantly replicated. In the event of a catastrophic failure of Velaro's primary host facilities, Velaro can rapidly bring all systems back online at our secondary location with little-to-no downtime.

SECURE CODING PRACTICES

Velaro recognizes 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 insure 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

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 uses standard security principles of least required access to perform a function
Always make sure system configurations are in accordance with industry standard best practices, and 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 Network Operations team has the information they need to correct the issue as quickly as possible.

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 pornographic, 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 of 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 de-activated.

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.