

# The Bullhorn Platform

Security Architecture and Compliance

**Bullhorn**<sup>®</sup>



## Table of Contents

<b>Executive Summary .....</b>	<b>3</b>
<b>Introduction: Pure SaaS Solutions for Recruiting .....</b>	<b>4</b>
<b>The Bullhorn Platform Layers .....</b>	<b>4</b>
<b>Multi-tenant Architecture .....</b>	<b>5</b>
<b>Scalability: Enabling Growth Without Complexity .....</b>	<b>8</b>
<b>Reliability: Ensuring Bullhorn is Always Available .....</b>	<b>8</b>
<b>Security: Accountability at Every Level.....</b>	<b>11</b>
<b>Ensuring Compliance .....</b>	<b>14</b>
<b>Flexibility: APIs and Ease of Integration .....</b>	<b>15</b>
<b>Conclusion .....</b>	<b>17</b>

## Executive Summary

Bullhorn's relationship management platform is designed to help companies of all sizes grow their business and scale rapidly, create more profitable customer relationships, and improve customer satisfaction.

We are technologists, and we built the Bullhorn platform to be incredibly powerful, reliable, secure, scalable and flexible. Bullhorn has always been on the cutting edge of innovation in areas such as mobile and email functionality, while also prioritizing data security with SSAE 16 Type II audits and other measures of protection. Our goal is to transform traditionally transactional and database-driven staffing software to a strategic and authentic tool that is focused on customer relationships.

Bullhorn is continuously evaluating its auditing program and how it fits in the context of our clients' needs, as well as its effectiveness against new and emerging threats and compliance challenges. As a service provider, our platform must meet the expectations of not only our customers, but also their customers, stakeholders, and partners. This document examines how Bullhorn fulfills mission-critical IT requirements that are essential to recruiting companies such as reliability, flexibility, and scalability. It also looks at how Bullhorn has built its infrastructure in secure datacenters to meet two of the most important requirements for every staffing and recruiting firm: security and compliance.

## Introduction: Pure SaaS Solutions for Recruiting

Introduced in 1999, software as a service (SaaS) enables software vendors to deliver business-critical services to customers when they need them, via the Internet. SaaS vendors host and manage all the applications, systems and hardware that provide these services. As a result, customers don't have to invest significant capital upfront to build an application infrastructure, and they avoid the labor and costs associated with maintaining it.

Many of these vendors' solutions, however, are not pure SaaS implementations. Instead, these solutions still follow the principles of client-server computing, which means customers must download, install, and run special software to use these vendors' systems. Additionally, many software vendors have built their systems without a multitenant architecture. A system without a multitenant architecture is not flexible enough to suit the rapidly changing, always evolving business of staffing and recruiting.

Since 2001, Bullhorn has provided thousands of staffing and recruiting companies with an integrated applicant tracking system (ATS) and customer relationship management (CRM) system based on a multitenant architecture. This white paper explores each layer of the Bullhorn architecture and platform and describes how each layer supports the business and technology requirements of today's staffing and recruiting firms.

## The Bullhorn Platform Layers

Bullhorn is a 100% pure SaaS solution and comprised of the three layers below:

### Software Applications

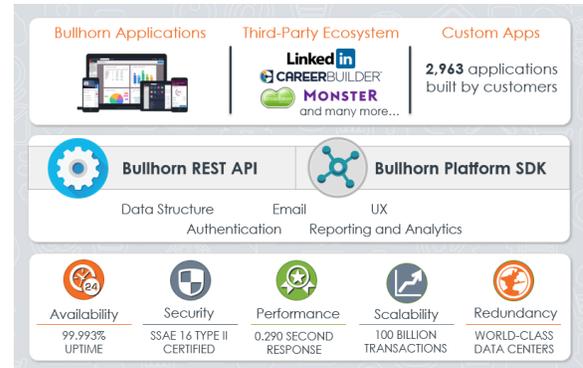
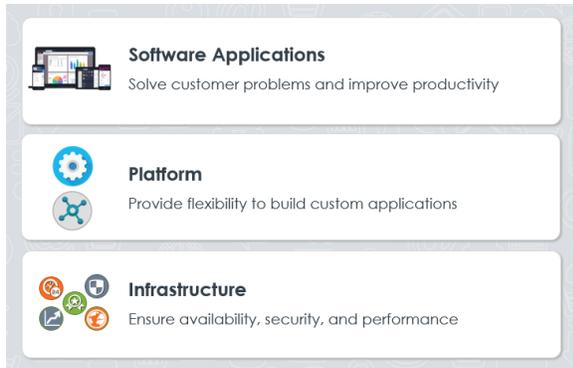
Customers connect to Bullhorn applications, third-party applications, or custom applications built by customers. When users login and interact with Bullhorn, security protocols ensure data access, integrity, and ownership.

### Platform

At the core of Bullhorn is the Platform. It not only powers the Bullhorn applications, but also allows your own custom application development. This is done via Bullhorn's powerful application programming interfaces (APIs) and Software Development Kit (SDK).

### Infrastructure

The multitenant cloud architecture is comprised of databases, file servers, web servers, and application servers. It is housed in a highly secure hosting facility to ensure availability, security, and performance.



## Multitenant Architecture

Bullhorn has built its ATS and CRM system with a multitenant architecture. Widely used in cloud computing and SaaS, multitenant architecture consolidates a business application and its associated services into one software instance. This single instance can serve multiple customers (or tenants), while keeping each customer's data and unique configuration separate.

**This approach makes it easy for Bullhorn to maintain and update the ATS and CRM for all users.**

Solutions that do not use a multitenant approach have separate instances of their application and data for each customer. Separate instances for each customer make those systems harder to maintain and slower to update. Bullhorn's multitenant architecture provides the following benefits to customers:

- **Cost effectiveness.** With multitenancy, Bullhorn technology manages only one instance of the ATS/CRM. This creates an economy of scale that would not be possible if Bullhorn managed a separate system with dedicated hardware and software for each customer.
- **High availability.** With only one infrastructure to maintain, Bullhorn can precisely control critical system attributes such as availability. Bullhorn's availability is an industry-leading 99.993% uptime, which ensures the recruiters who depend on ATS/CRM services every minute of the day can access the system from anywhere, at any time.
- **Security and compliance.** Because staffing and recruiting companies work with sensitive personal data, they must run secure operations and demonstrate compliance with government and industry regulations. All data management and customer activities are processed with stringent security measures within the Bullhorn infrastructure and platform, and verified with a SSAE16 Type II certification. As an extension of this program, Bullhorn continuously evaluates its program to ensure effectiveness against new and emerging threats and compliance challenges

- **Flexibility.** The dynamic world of staffing and recruiting is marked by constant change. The Bullhorn ATS/CRM was designed from the ground up to be configurable, customizable, and extensible, featuring open APIs and SDKs that enable agile responses to economic and industry changes.

**Multiple instances of the core application across the server farm ensure optimal performance, reliability, and resource allocation.**

In its implementation of multitenancy (figure below), Bullhorn maintains multiple instances of the core application across the server farm to ensure optimal performance for the tens of thousands of recruiters that login and use Bullhorn every day. Every instance of the core application is built with identical source code. This approach not only provides redundancy that boosts service reliability, but also provides the greatest return on investment from the vast resources in the application cluster.

Load-balancing servers direct each user request to the first instance of the core application that can process the request. This round-robin method of routing and processing requests boosts the performance of many application functions and ensures that clustered resources are never idle.

Logic in the core application carefully partitions the configuration and data of each customer, ensuring each customer's sensitive data and transactions remain completely separate from those of every other customer. More detail on this topic is discussed in the application- and database-level protections sections.



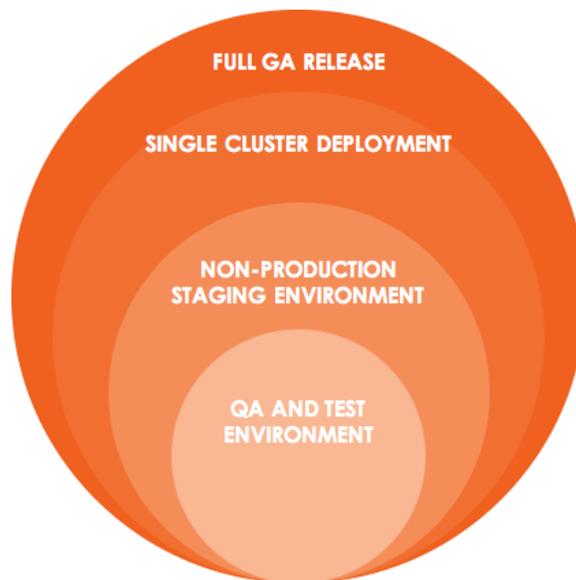
**Streamlined Maintenance for Increased Reliability**

Bullhorn has refined its multitenant approach by splitting clusters of application servers, web servers, file servers, and databases at the platform and infrastructure layers into several independent “swimlanes.” Swimlanes enable Bullhorn to exercise tighter control over system maintenance.

**Updates and maintenance are reviewed and tested at multiple levels.**

This ensures they are functionally complete, thoroughly documented and tested to ensure customers experience a seamless and secure upgrade experience.

- Each update is initiated and owned by a Product Manager and supported by a Technical Product Manager. Together they offer extensive technical, product, and market experience.
- All development changes to customer-facing production systems are documented in a change request tracking system and include description, severity, status, and owner of change.
- Quality assurance personnel test development changes to the production environment in a non-production environment before they are released to production.
- A separate Release Engineering Group approves all development changes to production.
- Deployment of development changes to production systems is restricted to the Systems Engineering Group.



After multiple rounds of quality assurance, certification, and release to non-production environments, Bullhorn releases updates to one swimlane in the production environment. After verifying the updated swimlane performs as expected for a sustained period of time, Bullhorn Technology Operations applies the update to the remaining swimlanes in production. In the event an update introduces an issue, Bullhorn Technology Operations and the Engineering team can identify and fix the problem quickly, minimizing any impact on the customer base.

## Scalability: Enabling Growth Without Complexity

Another advantage of Bullhorn's implementation of a pure server-side, multitenant architecture is that it enables customers to scale rapidly. Because they work in an environment defined by constant change, recruiting firms must be ready to turn on a dime. They must be able to add staff and business services quickly during market peaks and adapt just as rapidly during downturns.

### **Bullhorn's platform enables customers to seamlessly scale rapidly.**

A flexible, multitenant architecture lets Bullhorn update ATS and CRM systems quickly to introduce new features and bug repairs, keeping pace with rapidly changing business conditions. Since 2001, this approach has enabled numerous organizations that rely on Bullhorn's business services to expand their operations seamlessly, increasing staff levels from the hundreds to the thousands in some cases.

At the platform layer, the Bullhorn applications run on the same source code. Every customer's distinct database is based on the same fundamental schema, or structure, which includes records, fields, tables, relationships, stored procedures, and other database elements.

When the application is updated at the platform layer, this common code base streamlines the process, making it efficient, tightly-controlled, and repeatable. This contrasts starkly with platforms comprised of individual, customized application versions, which would require lengthier and more complex maintenance efforts. Because each customer works with the same core application and basic database schema, Bullhorn must update just once, with exceptional speed and precision.

Another benefit of the common-code base and database schema is the elimination of the "forklift upgrade," the painful migration of an application from one major release to another. Bullhorn is able to completely control upgrades because it develops, builds, and deploys each release of the core application just once.

## Reliability: Ensuring Bullhorn is Always Available

Successful recruiting and staffing businesses depend on up-to-date data and immediate response from ATS/CRM systems to fulfill their clients' needs. The difference between making a key placement and disappointing a client can come down to a fraction of a second. As a result, the ATS/CRM is a mission-critical system; it must be accessible from anywhere and available at all times.

To ensure exceptional reliability for its ATS/CRM, Bullhorn has designed its infrastructure to provide 99.993% uptime. In fact, Bullhorn is so confident in its system availability that it publishes the real-time status of the Bullhorn production environment. View the status of the production environment at any time by visiting <http://status.bullhorn.com>.

## Fault Tolerance: No Single Point of Failure

To deliver business continuity for our customers and ensure that there is no single point of failure, Bullhorn employs a sophisticated redundant architecture. Our swimlane architecture provides completely isolated environments that allow us to fail customers over to a completely separate infrastructure cluster in the event of a hardware failure. In addition, within each swimlane, Bullhorn employs large pools of redundant hardware at each tier of the technology stack.

Our complex virtualization and redundant hardware in both our network and application layers ensure that all Bullhorn data is safe, secure, and readily accessible. We have physical and logical redundancy at every layer, leveraging multiple edge routers and load balancers, with dynamic switching protocols to seamlessly failover customers if necessary. Bullhorn also has multiple redundant connections into our data centers from separate providers, giving us the unique ability to sustain ISP failures.

**Bullhorn's redundant architecture, along with the actions we take to constantly test our infrastructure, result in our world-class business continuity plan.**

The fault tolerance measures and the disaster recovery processes for every Bullhorn subsystem are summarized as follows:

- **Firewall:** Should the primary firewall server fail, the backup firewall server takes over as the primary server and handles all traffic. Once the failed server is restored to online status, that server becomes the backup firewall.
- **HTTP and mail load balancing:** Should the primary load-balancing server fail, the backup load balancer becomes the primary server and handles all traffic. Once the failed server is restored to online status, it becomes the backup load balancer.
- **Active Directory and DNS:** The production environment includes three Active Directory Domain Controllers and DNS servers. In this configuration, any two of the three can fail, and the third can assume all traffic. When a Domain Controller/DNS server is brought back online, it re-enters the production pool.
- **Web servers:** In the event of a failure, the load balancers immediately remove the failed server from the pool. Once a failed web server is brought back online, it re-enters the pool.
- **Application servers:** The Bullhorn production environment has a clustered application server pool, and there is no single point of failure.
- **File servers:** All files are stored on a storage area network (SAN) comprised of fiber-based SAN disk arrays. Additionally, the entire array is mirrored to a duplicate set of disks for full redundancy, providing exceptional data availability.
- **Report and ancillary application servers:** These servers operate in a pooled configuration in order to distribute and optimize server load.
- **Database servers:** Should the primary database server fail, the backup database server takes over as the primary and assumes all traffic. Once the failed server is brought back online, it becomes the backup database server.

- **Email:** Email servers are clustered. As in the case of Bullhorn application servers, there is no single point of failure in the configuration.
- **Network and telecommunications equipment:** All network and telecommunications equipment is redundant, and all servers have at least two network interfaces.
- **Internet connectivity:** Bullhorn's primary telecommunication lines are maintained using multiple peering relationships with Tier 1 providers; together these redundant lines load-balance the internet traffic traveling to and from the Bullhorn platform. In the unlikely event any line fails, the others are capable of handling Bullhorn's full workload.
- **Power:** All power to the data center is conditioned, fail-safe, and features an automatic power-transfer bridge system. The data center employs two potent backup diesel generators that guarantee availability even during major power outages. Bullhorn boasts partnerships that ensure ongoing delivery of diesel fuel to power its generators indefinitely.
- **Backups:** Differential backups are taken nightly, transaction-log backups are taken every 30 minutes, and full-tape database backups are taken weekly, encrypted, and stored at a secure offsite facility.

### The Bullhorn Data Centers

Bullhorn uses three geographically separate colocation data centers. CenturyLink facilities are located in Boston (Waltham), Massachusetts and Slough, United Kingdom. The Switch SUPERNAP facility is located in Las Vegas, Nevada. Our data center partners cover the physical security procedures including network provider redundancy, power/electrical redundancy and failover, HVAC, fire suppression, and physical access control. Our facilities have accredited certifications and operate at or above industry standards.

**Bullhorn partners with CenturyLink and Switch, who together provide a network of state-of-the-art data centers in the U.S. and UK that are SSAE16 compliant.**

Bullhorn's primary telecommunication lines are maintained using multiple peering relationships with Tier 1 providers; together these redundant lines load-balance the internet traffic traveling to and from the Bullhorn platform. In the unlikely event any line fails, the others are capable of handling Bullhorn's full workload.

CenturyLink and Switch data centers are secured facilities with 24/7 video surveillance and on-site security personnel, with only authorized personnel permitted on premise. All data center power is conditioned and fail-safe, with automatic power transfer bridge systems. The data centers are world-class hosting facilities with advanced protections that include the following attributes:

- Seismically braced facilities and racks
- Redundant heating, ventilation, and air conditioning
- 100% global power temperature and humidity management

- Very-Early Smoke Detection Alarm (VESDA) and dual-interlock fire suppression systems
- Monitoring 24/7 for HVAC and mission-critical power systems
- Power systems designed to N+1 with room for growth
- Biometric security
- UPS system
- Data center locations are:
  - Close to air transportation
  - Off flight path
  - Close to emergency services
  - Outside of flood zones
  - Earthquake hardened
  - Labeled with minimal signage

For all Bullhorn customers, we take extensive measures to ensure your data will be safe and secure in the event of a non-recoverable hardware failure. Bullhorn performs multiple levels of backups at varying intervals, and can utilize these database backup components to restore customers' data.

## Security: Accountability at Every Level

In a staffing and recruiting firm, the lifeblood of its business and biggest competitive advantage is data. Recruiters take great pains to source and place candidates, and these activities generate mountains of data. All this data is particularly sensitive because it contains personal identity information that could be exploited if it fell into the wrong hands. Additionally, candidate data is the result of weeks or months of a recruiter's efforts; in the case of contact lists, it may represent years of work.

This section will look at the data and privacy protection Bullhorn provides throughout every layer of its platform and architecture, starting at the physical and system levels in the Infrastructure layer, through the application level in the platform layer, across the internet and ultimately, to business users.

### Unmatched Security through External Certification and Internal Audits

Bullhorn undergoes a SOC1 Type 2 audit to verify its controls and process pertaining to security around customer data. The audit covers areas such as internal governance, production operations, change management, data backups, and software development processes. The audits occur in six-month cycles. Bullhorn uses the rolling six-month window to provide our customers and prospects the latest in-year report to align with their audit calendars. The audit ensures that we have the correct controls and processes in place and that they are actively functioning. The SOC audit also provides independent third-party verification and assurance.

Bullhorn has the distinction of being not only one of the first applicant tracking systems to be SOC1 certified, but also one of the first non-Financial industry based software-as-

a-service companies to utilize the SSAE16 framework to provide security assurance for our clients. Bullhorn has successfully provided annual and semi-annual SOC1 reports since 2009, when it was known as SAS70.

Bullhorn's SOC program offers multiple layers of protection and security. The program is designed to cover the key elements of data protection and integrity, while maintaining auditing practices within our business and operational processes. As all customers are concerned with their data and its security, Bullhorn has integrated its SOC controls into standard operating procedures. These procedures cross-functionally span the organization into any team that provides service or support of our clients and platform. The key components of our SOC controls environment include:

- **Corporate Governance:** how we provide oversight of our business and people
- **Change Management:** how we make sure all changes are tracked and properly reviewed
- **Access Control & Management:** who has access to our platform operations and how this access is managed
- **Data Redundancy & Backup:** how data is kept safe and stored in the event of adversity
- **Software Architecture and Development:** oversight of the development effort around our platform

Security and phishing awareness training are required for all employees, contractors, and consultants. In addition to training, Bullhorn also conducts internal phishing simulation tests for all employees. If an employee fails a phishing test, they are provided with immediate feedback and training to help reinforce proper techniques for identification.

### **Accountability at Every Level within Bullhorn**

In this era of cloud computing, many people don't feel they own their data because it's managed remotely. Bullhorn wants to assure customers the data they enter into the system is their property, not Bullhorn's.

### **With Bullhorn, you always own your data.**

Should a customer decide to work with another provider, Bullhorn will encrypt that customer's backup media to prepare it for secure delivery. Customers look to Bullhorn to provide them with unmatched data security.

### **Application and Systems-Level Security**

The physical security at the data centers is exceptionally strong by industry standards; nevertheless, Bullhorn also provides safeguards in the platform and infrastructure layers. Bullhorn has designed its security model with strict application logic that prevents any customer from accessing another's data or configuration.

Only Bullhorn engineers authorized to work with a particular customer can access that customer's data and configuration, and they can do so only to perform necessary systems management, maintenance, monitoring, or backups. Bullhorn performs thorough background checks for every employee and hires only experienced and thoroughly trained IT professionals. Every time a Bullhorn employee accesses a subsystem, the event is recorded in a security log. Additionally, the list of employees authorized to access applications, data, and various subsystems is scrutinized every quarter.

The subsystems at the platform and infrastructure layers include the Bullhorn core application server, web servers, servers running operating systems such as Windows and Linux, database servers, and file servers. Security measures for these subsystems are summarized as follows:

- **Internet Protocol (IP) systems security:** Internal IP systems, such as web servers, are protected by network address translation, port redirection, and non-routable IP addressing schemes.
- **Operating System security:** Bullhorn enforces tight operating-system-level security by providing a limited number of access points to all production servers. Administrators apply operating system patches and security updates regularly, and they harden every server by disabling and/or removing unnecessary users, protocols, and processes.
- **Database Security:** Database access is controlled at the database-connection level. Access to production databases is limited to just a few distinct points.

### **Database-Level Security**

Only a few Bullhorn employees are authorized to access customer data, and they only can do so through a limited access point bridging the platform and infrastructure layers. Additionally, Bullhorn encapsulates and manages each customer's data as a separate, distinct database. Implementations by many other providers don't manage each customer's data in a distinct database, which could expose customers to risk below the application level, in the infrastructure layer at the database level.

### **Internet Security**

Bullhorn provides exceptional levels of protection against hackers, beginning with firewalls that prevent unauthorized outside access. To protect customer data and communications traveling across the internet, Bullhorn leverages the strongest encryption products available today, including 128-bit Geotrust Transport Security Layer (TSL) Certification and 1024-Bit RSA public keys. Should hackers intercept a transmission, they would be unable to parse and understand the data exchanged between the Bullhorn application and its end users.

To access Bullhorn, users must have a valid username and password combination. During transmission, username and password combinations are encrypted with TSL protocols, and an encrypted session ID cookie is used to uniquely identify each user.

## Managing Security Inside the Recruiting Firm

Bullhorn provides all the tools, processes, and access control level (ACL) capabilities needed to allow, restrict, and deny employee access to specific data and functions. Enterprise systems administrators can assign ACLs based on fine-grained criteria such as roles, employment status, and other business rules detailed in the company's security policies. Administrators also are responsible for enforcing strict security measures within their organizations, such as requiring users to regularly update their login credentials with strong passwords.

## Ensuring Compliance

Compliance is critical to the daily operations of every staffing and recruiting organization. Various sectors, such as healthcare, air travel, and state, local, and national government agencies, follow strict hiring requirements. Regulations can involve a wide range of candidate attributes, such as diversity, country of origin, education, professional certification and criminal background, to name a few. Additionally, many countries have strict regulations about protecting personal data to ensure privacy and to combat identity theft.

**Bullhorn follows strict industry and government standards for compliance, beginning with a complete audit trail of every transaction in its data center.**

Much of this compliance is covered under the SSAE 16 audit, discussed in depth in the "Security" section of this document. SSAE 16 provides guidance to independent auditors who perform Type I audits. The Type I audit ensures all data center processes and procedures are strong and fully documented. Additionally, SSAE 16 describes the even-more stringent Type II audit, which Bullhorn undergoes.

The Bullhorn data center also complies with multiple governmental standards for personal identity compliance, including Massachusetts General Law Chapter 93H and its regulations 201 CMR 17.00, one of the strictest sets of personal identity regulations in the United States.

These regulations protect against identity theft, and requirements include:

- Written procedures for protecting personal identity data.
- Strict limits on the personal information that can be collected.
- A qualified security officer on staff to monitor and manage personal identity protection.
- Encryption for any data transported from the datacenter to another location.

## Privacy Shield

Bullhorn was one of the first companies to be certified by the European Union and U.S. Department of Commerce under the EU-U.S. Privacy Shield Framework for the collection, use, and retention of personal information transferred from the EU to the U.S. supporting transatlantic business.

To join the voluntary Privacy Shield Framework, Bullhorn self-certified to the U.S. Department of Commerce and publicly committed to comply with the framework's requirements. Bullhorn completed a rigorous process to align numerous privacy policies with the new regulations before receiving its certification.

The new arrangement includes stronger data protection obligations for companies receiving personal data from the EU, safeguards on U.S. government access to data, effective protection and redress for individuals, and annual joint review to monitor the implementation.

Bullhorn currently partners with TRUSTe for third-party verification of our privacy practices in regards to Privacy Shield, data collection, and processing. We are TRUSTe certified along with Privacy Shield. This allows independent review of our program and practices as related to the EU privacy and data transfer. Previously, Bullhorn was Safe Harbor certified for years, demonstrating our early commitment to our client and their customer's needs and compliance requirements.

To read Bullhorn's privacy policy, click [here](#). To view Bullhorn's EU-U.S. Privacy Shield Framework certification, click [here](#). For more information about the EU-U.S. Privacy Shield Framework, visit [www.privacyshield.gov](http://www.privacyshield.gov).

## Flexibility: APIs and Ease of Integration

For staffing and recruiting companies, ATS/ CRM systems must be flexible to adapt to new trends and developments in their field. Most of the SaaS-based ATS/CRM systems offered by vendors today, however, are functionally rigid. Their platforms aren't flexible enough to let recruiting firms add new business services and increase staffing levels to respond to dramatic changes and new developments. Without an agile ATS/CRM platform, a recruiting firm risks losing its competitive advantage.

**Bullhorn is fully extensible and we encourage customers to take advantage of our open APIs to build custom applications on top of our platform.**

The Bullhorn API provides a programming interface that developers can use to integrate the Bullhorn relationship management platform with custom and third-party applications and data. The API also provides mechanisms that enable developers to customize the Bullhorn user interface with custom components and validations. The API was designed for use by either customers or partners who wish to integrate their products and services with Bullhorn.

For more information, please view these [articles and samples](#).

### Pre-integrated Solutions with Bullhorn Marketplace Partners

The Bullhorn Marketplace is an ecosystem of partner companies that use Bullhorn APIs to develop applications that integrate with Bullhorn. Marketplace partners extend the core Bullhorn application with their own services and applications that fulfill distinct business needs. These services, like the Bullhorn ATS/CRM, are provided over the internet via the SaaS delivery model and let customers quickly integrate business services exactly when they need them. Each partner application is designed to pre-integrate with Bullhorn, and Bullhorn tests and approves all partner offerings before making them available on the Bullhorn Marketplace.

**With Bullhorn's Marketplace, customers can leverage credible solutions that integrate seamlessly with the Bullhorn platform.**

The Bullhorn Marketplace is the one destination for business applications that are pre-integrated to work seamlessly with Bullhorn and enhance the platform's capabilities. Each partner has developed a turnkey solution to fulfill a critical business need, allowing you to focus on your business instead of spending your time and money on one-off integrations. Whether you need to enhance your sales and marketing processes, improve back office efficiency, or save time with robust recruiting operations, all these integrated solutions and more can be found in the [Bullhorn Marketplace](#).



## Extending, Configuring and Customizing Bullhorn for Your Business

Beyond the services available in the Bullhorn Marketplace, the Bullhorn ATS/CRM is completely configurable and customizable to suit each organization's particular requirements. For example, recruiting firms easily can add and change field names and properties, and customize screen layouts and workflows.

Using templates designed for various functional areas of the business, organizations can set up unique screens and workflows for each area. This capability allows employees at a company who work in one department (e.g., Accounting) to see a particular view of Bullhorn; colleagues in another department (e.g., IT staffing) have access to their own view and workflow.

For companies wanting greater customization, [Bullhorn's APIs](#) let companies extend the ATS/ CRM to handle tasks such as custom job posting to websites, integration with proprietary systems, and automation that reduces the time it takes to source and place a candidate.

Customization projects can be handled by an organization's web developers or developers from the Bullhorn Professional Services team.

## Conclusion

SaaS-based solutions are a perfect fit for the staffing and recruiting industry, which is defined by constant change and dramatic new developments in how candidates are hired and placed. Bullhorn first developed its ATM and CRM solution more than 15 years ago, in the early days of SaaS. The company has remained true to the fundamental principles of SaaS delivery by ensuring its application is truly browser-based and built with a multitenant architecture.

By embracing this approach, Bullhorn not only provides customers with cost-effective ATS/CRM solution, but it also ensures customers reap the full benefits of multitenant architecture, including flexibility, reliability, scalability, and exceptional security and compliance with the most stringent regulations available.