

# Describing the Cloud

## *Details of CambridgeSoft's Hosted Computing Environment*

**T**RADITIONAL ENTERPRISE SCIENTIFIC SOFTWARE deployments have been complicated and expensive. They require a data center with office space, power, cooling, bandwidth, networks, servers, and storage. They also rely on a software infrastructure, and a team of experts to install, configure, and run them. In the scientific world this is further complicated by the expertise needed in science, as well as in I.T., in order to effectively manage these solutions. Like other IT solutions, they need development, testing, production, and failover environments.

Cloud-computing from CambridgeSoft offers a way out, so you can focus on your business - presumably discovering new compounds, and not running computer systems.

Businesses are already running all kinds of applications in the cloud - like CRM, HRIS, finance, ERP, and even custom solutions. These applications can be up and running in a few days, which is unheard of with traditional enterprise business software. They cost less, because you don't need to need to pay for the people and infrastructure needed to run them (or at least you are sharing the cost). And in practice they're more scalable, more secure, and more reliable than most in-house deployed solutions.

CambridgeSoft's Hosted applications provide a Cloud Computing solution to your research I.T. needs. In theory, how the "cloud" works is irrelevant - but in practice, customers need to see details to trust that CambridgeSoft's hosted environment is secure and private. This article provides the details.

### *CambridgeSoft's cloud resides in a SaaS Type II Facility*

CambridgeSoft's SaaS applications reside in a SaaS Type II facility, and have completed annual SaaS 70 audits (audit reports are available to qualified customers). Our data center is secure, and ensures continuous power supply and high-bandwidth internet connectivity. The continuous power is guaranteed by battery and generator backup, and live power supply failover. Our internet uptime is guaranteed by a combination of the top six Tier One providers, running in separate trunks. In addition, the entire data center is daily mirrored to a separate physical backup facility for disaster recovery (running in a physical separate facility, on a different power grid, and different Internet providers).

The primary and backup data centers includes 24x7x365 physical security (including biometric access to the hardware), as well as 24x7x365 monitored firewall and data security. Physical

security includes fire detection and control. Data security is described further below.

### **Security**

Security at our state-of-the-art facility, data backup and mirroring, and infrastructure, address the basic concerns around hosted data centers. CambridgeSoft performs a variety of preventative maintenance to ensure a secure and successful SaaS operation. Our applications let customers focus on their science and business needs while the day-to-day physical components are handled for them.

CambridgeSoft provides the following services:

- **Data Center Space:** CambridgeSoft offers single-tenancy and multi-tenancy SaaS configurations (i.e., dedicated or shared instances), storage, and backup.
- **HVAC:** Provided via data center grade HVAC cooling and humidity control, and all required electricity for the customer.
- **Environmental Controls:** The system is powered with redundant cooling tower and air handlers equipment that maintains temperature and humidity to rigid industry standards. Systems are monitored 24x7.
- **Fire Detection and Suppression:** Our facility is equipped with electronic smoke and fire detectors monitored 24x7. Our facility is also equipped with a pre-action dry pipe suppression system.
- **Security and Access:** Physical security and access is provided by a system of access cards, biometric readers, keys and additional controls.

*Cyber-security: By the time you hear about a new cyber-threat, your data will already be protected against that threat.*

CambridgeSoft's SaaS products include the support and preventative maintenance generally required to ensure maximum server uptime.

This includes:

- Proactive software patches and installation for the Operating System and Server Software.
- 24 x 7 automated monitoring of the server and services to ensure the server is up and running properly.
- 24 hour staff familiar with your specific environment.

All specifications subject to change without notice.

US 1 800 315-7300 INT'L 1 617 588-9300 FAX 1 617 588-9390 EMAIL [info@cambridgesoft.com](mailto:info@cambridgesoft.com)

EU 00 800 875 20000 UK +44 1223 464900 JP 0120 146 700 WWW [www.cambridgesoft.com](http://www.cambridgesoft.com)

MAIL CambridgeSoft Corporation 100 CambridgePark Drive Cambridge, Massachusetts 02140 USA

ChemBioOffice, ChemBioDraw, ChemBio3D, & ChemBioFinder are trademarks of CambridgeSoft Corporation ©2009

**CambridgeSoft**<sup>®</sup>  
[www.cambridgesoft.com](http://www.cambridgesoft.com)

## Describing the Cloud

### *Details of CambridgeSoft's Hosted Computing Environment*

- Comprehensive monitoring of vital system resources including CPU Utilization, memory, and disk capacity to supplement the standard server uptime and service availability monitoring

**Weekly Patch Management:** All software updates are performed during off-hours maintenance windows. By default these windows are between 10:00 p.m. and 4:00 a.m. EST on Saturday and Sunday. Critical software updates and security patches are applied during other times as appropriate.

CambridgeSoft will test certain updates such as Microsoft updates within the secure test lab prior to releasing patches to customers. This provides a first-hand look at the effects of releases, and how they may impact CambridgeSoft applications.

**Emergency Patch Management:** Emergency patch installation is performed without the need for your notifying CambridgeSoft. That means that when you hear about a new cyber-threat, hacker attack, or system vulnerability, CambridgeSoft investigates the threat and takes appropriate action. Typically this occurs behind-the-scenes before you would know about it, since the public news media reports come well after the internal cyber-security information sources that we rely upon. Our Security and Operating System Patch Management protocol includes:

- CambridgeSoft continuously monitor industry-leading vulnerability reporting services providing optimal security assurance.
- Newly disclosed operating system vulnerabilities and security patches are evaluated by our System Administrators to determine the threat level.
- If a disclosed vulnerability is determined to be a threat, we test and install security patches/updates promptly.
- CambridgeSoft reserves the right to schedule emergency maintenance at any time, without customer intervention, to remediate pending high-risk vulnerabilities that could threaten the current security posture.

***Backup security and maintenance: SaaS price includes routine offsite tape backup, and all other routine software maintenance tasks.***

CambridgeSoft provides management of customer hardware year round in various configurations. We operate scheduled maintenance windows each week, although in practice, patches

are typically released and installed on a monthly basis.

**Tape Rotation:** 5 times per week tape rotation. Tapes are initially stored within the data center, and CambridgeSoft removes tapes offsite weekly.

**Backup, Restore, and Disaster Recovery Solutions:** Our disaster recovery protocol is based on restoring tape backup, plus data mirroring from an off-site location for a robust disaster recovery option. Furthermore, CambridgeSoft carries insurance on our equipment for the full replacement value of such equipment, plus replacement costs to reinstate customer data in case of physical loss.

***Physical security: Hosted software means you can focus on Science instead of focusing on Security.***

**Data Center Maintenance:** CambridgeSoft performs weekly testing of its physical Data Center components to ensure maximum operability, and to identify any preventative maintenance needed. Generators are typically tested each week to sufficiently run based on operations guidance. HVAC, Fire Suppression and Temperature Controls are monitored 24x7x365. If any component fails within the operations components, an alert is generated to the internal staff so issues can be immediately acted upon. CambridgeSoft also provides an Intrusion Protection Services (IPS) as part of our standard offering.

**Power Maintenance:** The Data Center is served by a telecommunications-grade power feed from the utility company and is protected from power surges. Electricity is fed into the building through multiple entrances, with redundant A-B power feeds. Our power supply has a 1-megawatt diesel generator supporting the data center in the event of a power failure. Both 48 volt DC and 110 volt AC power are available. Power equipment includes:

- Telecommunications-grade power feed with redundant A-B power feeds through multiple entrances.
- 1 x 120 Volt 30 Amp circuit ("A" Primary)
- 1 x 120 Volt 30 Amp circuit ("B" Secondary)
- Power Strips: Two 30A Twist-lock horizontal mount metered power strips
- Liebert UPS Battery Backup System that is monitored and maintained by Liebert protects the data center power

All specifications subject to change without notice.

US 1 800 315-7300 INT'L 1 617 588-9300 FAX 1 617 588-9390 EMAIL [info@cambridgesoft.com](mailto:info@cambridgesoft.com)

EU 00 800 875 20000 UK +44 1223 464900 JP 0120 146 700 WWW [www.cambridgesoft.com](http://www.cambridgesoft.com)

MAIL CambridgeSoft Corporation 100 CambridgePark Drive Cambridge, Massachusetts 02140 USA

ChemBioOffice, ChemBioDraw, ChemBio3D, & ChemBioFinder are trademarks of CambridgeSoft Corporation ©2009

# Describing the Cloud

## *Details of CambridgeSoft's Hosted Computing Environment*

- 1-megawatt diesel generator in the event of a power failure

**Environmental Controls:** Our data center building has a fully redundant HVAC system – maintaining temperature and humidity to rigid standards. Systems are monitored by staff both on-site and off-site, 24x7.

**Fire Detection and Suppression:** Our data center facility is equipped with enterprise-grade electronic smoke and fire detectors monitored that are monitored 24x7. Our facility is also equipped with a pre-action dry sprinkler system along with fire extinguishers placed throughout the building.

**Security and Access:** Physical access is secured through a host of automated and physical controls including video surveillance, proximity access cards and biometric security controls.

**Firewall:** Cisco Adaptive Security Appliance (ASA) 5520 with failover. This firewall appliance, deployed as a redundant pair, supports up to four 10/100/1000 interfaces and one 10/100 interface. The firewall device is capable of processing 450 Mbps of firewalled traffic (225 Mbps IPSEC), and up to 280,000 connections (9,000 connections per second). Includes SSL/Ipsec VPN for remote access.

### Integration

Integration with CambridgeSoft's Software-as-a-Service is identical to integration with the same Software-as-a-Purchase, and at Enterprise level (highest level of automated integration)

CambridgeSoft acknowledges that SaaS adopters have are concerned about integration issues, and we have designed our SaaS software to address those concerns. The following concepts have guided our SaaS development:

- SaaS products are the same software as our Enterprise-level products, which provide a maximum of automated integration.
- SaaS software is locally installed with a remote database, so all other software on your desktop computer will integrate with SaaS software in a seamless manner.
- All CambridgeSoft products can exchange information seamlessly with cut-and-paste, or by importing appropriate data formats.
- No VPN setup; no remote desktop; no VMware barrier—the SaaS integration is transparent to you, with SaaS programs running just like other programs

### Performance

Application performance and speed are state-of-the-art, and uptime is guaranteed

***Bandwidth: top speed availability, including in Europe and Asia***

CambridgeSoft operates a robust regional backbone that includes connections to multiple Tier 1 providers. Bandwidth is part of a shared 100 Mbps Internet feed, with 10 Mbps of dedicated bandwidth. Bandwidth is delivered on redundant burstable 100 Mbps connections.

In addition, there are redundant circuits carrying to our facilities, and this is monitored 24x7. Customers can access bandwidth utilization and QoS information via a password-protected customer management console. Fiber within the Facility is provided redundantly by these Tier 1 providers: Verizon, Verizon Business, Qwest, Verocity, AboveNet, and DSCI.

CambridgeSoft currently runs several SaaS applications in Europe and Asia from our US-based server, with good speed results. Japanese, Chinese, and other 2-byte character sets can be used in our multi-tenancy setup with no special modifications, and can be used in our single-tenancy setup with some modifications. All menus and messages are in English, but our articles and literature listed in Section 8 are also available in French, German, and Japanese.

***Ensure Internet uptime with 24x7x365 Continuous Monitoring and Trending Analysis***

CambridgeSoft's 24x7x365 monitoring includes a combination of real-time and trending data measurements for the most common system and performance data points. CambridgeSoft System Administrators continuously monitor key performance statistics to maintain the highest availability and performance. Real-time and historical trending of these statistics allow for targeted and on-going performance tuning.

**Real time alert generation:** Alert generation defined by predetermined thresholds:

- 60 Second poll times
- Connectivity Link Status (ICMP)
- Server CPU Utilization
- Server Memory Utilization
- Logical Drive Space (up to 3 logical drives or volumes)

All specifications subject to change without notice.

US 1 800 315-7300 INT'L 1 617 588-9300 FAX 1 617 588-9390 EMAIL [info@cambridgesoft.com](mailto:info@cambridgesoft.com)

EU 00 800 875 20000 UK +44 1223 464900 JP 0120 146 700 WWW [www.cambridgesoft.com](http://www.cambridgesoft.com)

MAIL CambridgeSoft Corporation 100 CambridgePark Drive Cambridge, Massachusetts 02140 USA

ChemBioOffice, ChemBioDraw, ChemBio3D, & ChemBioFinder are trademarks of CambridgeSoft Corporation ©2009

**CambridgeSoft®**  
[www.cambridgesoft.com](http://www.cambridgesoft.com)

## Describing the Cloud

### *Details of CambridgeSoft's Hosted Computing Environment*

- URL/TCP/UDP Port or Content Monitoring (Three Ports/URLs per server)
- Hardware Health and Availability as limited by hardware and Operating System platform
- Windows Event Viewer Entries (1 Specific events per server)
- Windows Service Status (1 Service per server)
- Server SNMP Availability

**Trend Analysis Measurements:** Instantaneous data graphs showing graphical measurements. Values are updated in 5 minute intervals, with historical averages for the previous 12 months.

- Bandwidth Utilization (up to 2 Physical Interfaces)
- Server CPU Utilization
- Server Memory Utilization
- Logical Drive Space (up to 3 logical drives or volumes)

#### ***Ensure software uptime with Fault/Event Management and Remediation***

When an alert is triggered, the Support Center is notified by email, pager, and visual status monitors. System Administrators respond to the alert by invoking notification and escalation procedures established by an Operations Run-Book (ORB) that is developed and updated as appropriate.

**Fault/Event Verification and Isolation:** Internet latency and many other conditions can cause false alarms that can generate unnecessary responses to automated notifications. We perform specific troubleshooting tasks to verify that a fault/alert condition is legitimate. Once the fault condition is confirmed and verified, we initiate the procedures defined in the ORB to remediate the fault, or escalate as quickly as possible.

**System Fault/Event Remediation:** CambridgeSoft strives to identify and resolve issues before they occur; however, once a fault is identified and verified, we begin troubleshooting the issue. This troubleshooting procedure involves in-depth system diagnostics and custom tasks as defined in the ORB. Once a critical fault is corrected, we begin the process to identify the root cause, and a full incident report is available within 2 business days.

#### **Severity Level 1: Emergency**

System failure, failure of a critical system function, or event-driven changes with absolute impact on system availability, security, or the customer's critical business operations, including

but not limited to:

- Covered Systems unavailable to customer or visitors
- Performance degradation significant enough to render covered systems effectively unavailable
- Emergency configuration changes
- CambridgeSoft will assign sufficient resources, apply continuous effort, and escalate as appropriate until service is restored to contracted service levels or until CambridgeSoft determines that the root cause of the issue is beyond CambridgeSoft's control.

#### **Severity Level 2: High**

- Failure of a non-critical system, system function, or event-driven change with significant impact on system availability, security, or the customer's critical business operations, including but not limited to:
  - Intermittent loss of availability
  - Sustained system latency
  - Urgent configuration changes
  - Moderate performance degradation
  - Recurring or unresolved previous events
- CambridgeSoft will assign sufficient resources, apply appropriate effort, and escalate as appropriate until service is restored to contracted service levels or until CambridgeSoft determines that the root cause of the issue is beyond CambridgeSoft's control.

#### **Severity Level 3: Routine**

- Minor failure of a non-critical system, system function, or routine change with no significant, immediate impact on system availability, security, or the customer's critical business operations.
- Routine Support Tickets are completed during Standard Business Hours.

#### ***Ensure hardware uptime with hardware monitoring, maintenance, and redundancy***

##### **Hardware Repairs and Maintenance**

- Should a component of customer's server need to be replaced, CambridgeSoft will coordinate the replacement with the appropriate hardware or maintenance support vendor.
- System and system software updates will be applied as appropriate or deemed necessary.
- Space is unlimited on a per-user basis, and is limited

All specifications subject to change without notice.

US 1 800 315-7300 INT'L 1 617 588-9300 FAX 1 617 588-9390 EMAIL [info@cambridgesoft.com](mailto:info@cambridgesoft.com)

EU 00 800 875 20000 UK +44 1223 464900 JP 0120 146 700 WWW [www.cambridgesoft.com](http://www.cambridgesoft.com)

MAIL CambridgeSoft Corporation 100 CambridgePark Drive Cambridge, Massachusetts 02140 USA

ChemBioOffice, ChemBioDraw, ChemBio3D, & ChemBioFinder are trademarks of CambridgeSoft Corporation ©2009

# Describing the Cloud

## *Details of CambridgeSoft's Hosted Computing Environment*

- to 50 Gb (very large) overall per application.
- If your application requires more than 50 Gb, which would be very highly data-intensive materials such as videos, extra space is available for \$5/Gb/month.

### Infrastructure and System Maintenance

- CambridgeSoft continually improves infrastructure within the Secure Data Center to serve its customers environment.
- During the course of these improvements, necessary patches, upgrades, and other maintenance activities may result in intermittent outages or system slowness. The customer is always notified in advance of maintenance activities.
- Emergency maintenance can occur at any time to address critical system stability or security issues, and these activities will occur at the discretion of CambridgeSoft. We will make every effort to coordinate emergency maintenance with customers prior to initiation of maintenance activities in an effort to minimize the effects of these activities on customer systems and availability.

### *Ensure firewall security with monitoring and redundancy*

**Standalone Firewall and Firewall Failover:** Our Standalone Firewall provides continuous monitoring of the Firewall and provides notification, incident response, and break fix support in the event of an alert condition. Additionally, System Administrators reduce risks further by verifying critical patches are applied to the firewall in a timely manner, ensuring the ongoing integrity of your security posture.

The Failover Firewall Service is designed to deliver firewall high-availability by providing a dedicated hot-standby. In the event that the primary firewall fails, the secondary firewall detects the failure and begins operation. Typically the failover time is <1 minute.

**Firewall Monitoring:** We provide a combination of real-time and trending data measurements for the most common critical security and performance data points

- Real time alert generation
- 60 Second poll times
- Connectivity Link Status (ICMP)
- Firewall CPU Utilization

- Firewall Physical Memory Utilization
- Firewall Session Allocation
- SNMP Availability

**Trend Analysis Measurements:** Instantaneous data graphs showing graphical measurements. Values are updated in 5 minute intervals and historical averages are available for the previous 12 months.

- Bandwidth Utilization per physical firewall port
- Firewall CPU Utilization
- Firewall Physical Memory Utilization
- Firewall Session Allocation

**Rule Change Management:** CambridgeSoft's data center adheres to strict change management practices that require security policy and rule base changes to be validated for optimal security and availability.

- Routine rule changes make up the majority of security policy changes. These changes do not impact the availability of current production systems and are typically granting access to new users or applications.
- Routine rule changes are completed during standard business hours.
- Routine rule changes are guaranteed completed by Next Business Day
- Emergency Rule changes can be requested 24x7x365.
- Security Engineers will execute Emergency Rule changes within 60 minutes during standard business hours.
- Emergency Rule changes requested outside of business hours are executed within 2 hours.
- We reserve the right to apply Emergency Rule Changes based discovered vulnerabilities to the device or the environment.

**Vulnerability Management:** The data center security team monitors vendor device vulnerability disclosures, new patch update announcements, security advisory boards and CERT Advisories to discover and determine the impact of the latest vulnerabilities to supported systems.

- Continuously monitor for new firewall vulnerability disclosures
- Determine the threat to the Firewall System
- Test and implement patches as needed

All specifications subject to change without notice.

US 1 800 315-7300 INT'L 1 617 588-9300 FAX 1 617 588-9390 EMAIL [info@cambridgesoft.com](mailto:info@cambridgesoft.com)

EU 00 800 875 20000 UK +44 1223 464900 JP 0120 146 700 WWW [www.cambridgesoft.com](http://www.cambridgesoft.com)

MAIL CambridgeSoft Corporation 100 CambridgePark Drive Cambridge, Massachusetts 02140 USA

ChemBioOffice, ChemBioDraw, ChemBio3D, & ChemBioFinder are trademarks of CambridgeSoft Corporation ©2009