

The nature of Internet application delivery requires specific consideration be given to enhanced system security. Users of these application systems want to be assured that the work products created are safe and secure from loss or unauthorized access, particularly in those cases where the nature of the report or imagery is inherently private, such as occurs in Government, Health Care, Financial or Legal arenas. Historically, early Internet architectures and applications exhibited security flaws which were documented in the literature as well as via anecdotal channels. These flaws included basic network and platform considerations as well as application architecture issues which often were carryovers from legacy systems upon which they were derived.

At this point, the “combat lessons learned” from these early real world experiences can be applied in practice when new Internet based systems are designed and built, rendering them much more impervious to attack as well as inadvertent loss of information. Security strategies can be scaled to the problem at hand; more robust security systems can be implemented in those cases where higher levels of security are required. Proper application of the security tool kit which is now available (in conjunction with supporting procedures) allows Internet based service providers to meet and exceed the security levels provided by nearly any other architectural implementation.

The Security Architecture implements a layered approach, with each layer addressing a specific sub-mission of the overall security design. Collectively, these layers result in a robust, safe and secure framework for customer teams to work in without undo productivity burdens.

Security and Availability

Basic Philosophy

The BCS Security Architecture is based on the following considerations:

- Underlying platform and network security layers should be transparent to the user. They should implement the required security functionality for those lower level layers in the architecture without interaction with the user (who is operating in the upper layers of the application architecture).
- The upper layers of the security architecture should be as easy to understand and use as possible, while still providing the basic security functionality required at those layers.
- Access level security for the customer team is defined by specifications made by a security administrator in that team. The customer is able to define who should be able to see which reports or images (and even which parts of a report).
- All data and information is treated at the same, very high, level of security. No distinction is made within the system between documents or work products regarding higher or lower levels of security requirements.
- In the unlikely case that the BCS security architectures are compromised, any information destroyed would be easily recoverable.
- The features and functions as implemented combine to create a feeling of comfort, privacy and safety for the users of the system.
- Security procedures will protect information resources through implementation of sound physical, environmental and administrative controls designed to reduce the risk of physical failure of infrastructure components, damage from natural environmental hazards and use by unauthorized personnel.

Security and Availability

Specifics

Clearly, any detailed description of a security architecture would become a potential risk to that architecture. However, we can easily and safely present the following specifics of the BCS Security Architecture for review:

Layer 1: Physical/Environment

All physical access to BCS Server and network equipment is restricted to authorized personnel only. Only personnel who have a need to access the data center are given access. The BCS hosting location is accessible only via electronic passkeys and code keypads. Personnel must wear their security badges at all times while in the datacenter. There is no 'piggybacking' on access into the datacenter.

The data center environment is protected via fire detection and suppression features, multiple redundant power and air conditioning units as well as multiple redundant backbone network connections. All hardware and software is implemented to achieve High Availability (HA) requirements targeting 100% uptime (not including normal scheduled maintenance windows). Over the last 10 years, the BCS data center has consistently achieved 99%+ sustained uptime and has never incurred a security breach (either physical access or data intrusion or loss).

Layer 2: Network

BCS has implemented robust network security techniques, including at the firewall, router, hub and server levels. These measures are designed to ensure that no unauthorized network access is permitted to the application or data servers. Network devices and firewalls automatically filter out Denial of Service attacks and illegitimate traffic. Automatic monitoring of all network traffic is performed and reviewed for suspicious events.

Security and Availability

Layer 3: Platform

All servers, including Load Balancers, Application Servers and Data Servers are based on the latest Windows Server technology. Full use is made of operating system permission, encryption and access security facilities in order to ensure that only those people who have appropriate authorization to a specific part of the application are allowed to do so (including BCS personnel). All platform software is kept up to date. Automatic monitoring processes are executed from remote server locations to provide automatic notifications to support personnel of outages or component problems, including environmental, power, synthetic transactions, etc. Additional automatics monitoring processes provide alerts for attempted security intrusions. All platforms employ multiple redundant design approaches (including power, network connectivity, server processor, and data storage).

Layer 4: Encryption

SSL encryption is used between server applications and client equipment as well as between BCS servers and back end service providers (such as payment processors) whenever sensitive data is being transmitted. Additionally, any retained sensitive data (such as drivers license numbers) is encrypted in data storage media. Sensitive data such as credit card information is not stored locally and is not available to be viewed by internal staff.

Layer 5: Connectivity

All users of sites are verified at connection time. Only those users who have valid sign-on are permitted onto the site. VPN connectivity is available for remote connection of high authorization users.

Layer 6: Permissions

Users may only view information which they have been explicitly permitted to view by the owner of that information. Permission levels include: None, Read Only, Read/Write and Read/Write/Modify. Each user accessing the application is assigned a 'Role' which in turn defines a collection of specific permissions as described above. User assigned to high security roles is controlled by specific review of executive personnel.

Backup

All application information is fully backed up on a regular basis and can be retrieved if needed, in case of loss. This includes use of offsite backup retention. Full backups as well as incremental and transactional backups are used. Data

Security and Availability

can be recovered up to within 60 seconds of the point of failure in most cases. Full data center disaster recovery can be performed within 48 hours at an alternate physical site (recovery procedures are regularly tested).

Redundancy

All key application components are redundantly implemented in order to minimize the impact of loss of any single one of them. This includes use of multiple redundant power supplies (including multiple redundant backup generators), multiple redundant backbone internet connection paths as well as redundant (and hot fail-over) equipment in the network and server devices.

Customization

Additional security capabilities are employed for specific customer training requirements, including personal encryption keys, ip connection verifications, biometrics verifications and callback connectivity.

Policies

All technical personnel undergo a background check prior to being given access to the servers (logically or physically).

Security policies are audited on a regular basis. Any discovered or suspected security problems are reported immediately to the appropriate management personnel.

Private customer information is not made available for any use other than as defined by customer contract. No use is made of cookies. Customer email addresses, phone numbers or other contact information is not used for any purpose other than to provide support . No personal information is collected about any users other than what is required by mandate or is needed to support the user.