White Paper

Infrastructure and Security

Boardvantage is protected by full-strength encryption and multi-factor authentication, and is hosted in a highly secure site. We maintain a strong perimeter defense using multiple layers of security and constant monitoring. Boardvantage devotes significant resources to continuously improving security with the latest technologies.

Physical security

All computer and network communication systems are housed in a secure, hardened hosting facility with 24x7x365 guard patrols, full surveillance, and biometric access control systems.

System redundancy

Maintained by our own security-screened staff, the Boardvantage system has built-in redundancy at every point, including web, application, file, database, and storage servers.

Network monitoring

Our entire infrastructure is protected by a broad shield of network equipment and software tools. The network is continuously monitored by our staff for any attempted network attacks.

Data security

We encrypt all data using strong ciphers, both during network transport and while resident on computing platforms, so that it cannot be compromised. Each customer's content is segregated into an individual repository and encrypted with a unique key. Only authorized users can access protected data (even Boardvantage systems administrators are barred from access).

Network security

Boardvantage requires customers to use Transport Layer Security (TLS) encryption technology when accessing the Boardvantage application with an Internet browser or iPad® Digital certificates ensure the authenticity of each session. This minimizes the risk of data stream interception between the user's browser and the Boardvantage service.

Mobile security

Our iPad app has a built-in, device-resident Briefcase — a repository for secure offline document storage. All content is encrypted, and can be purged remotely, if the device is lost or stolen. To further prevent discoverability, documents (including notes) can be deleted locally, remotely or automatically based on defined retention dates.

Virus protection

Our vigorous virus control methods prevent the distribution of malicious code that could disrupt service, destroy data, or undermine productivity.

Data backup

We automatically back up all customer data nightly and store it at a secure, off-site facility. All backups are encrypted and any unused, obsolete, or end-of-life media is destroyed to prevent third-party data retrieval.

Operating system security

Boardvantage application servers are hardened at the operating system level. Administrative access is restricted to authorized personnel. Login is possible only through encrypted access with individually authorized and enabled encryption keys. We also regularly review security patches according to vendor specifications.

Internal processes

Boardvantage is SOC2 and ISO27001 certified. Our documented internal processes have been independently audited to ensure that we have the proper controls in place for provisioning, change control, and procedural changes. We not only enforce the separation of roles and responsibilities, and closely supervise employees, we also conduct criminal background checks on each staff member at both the federal and local levels.

External validation

Our security has been hardened by a decade of third-party testing and validation. Between our secured state-of-the-art hosting facilities and our security management program, our "secure from the ground-up" architecture, expertise and execution ensure that our customers receive the highest data protection commercially available.