

**“** *Sanebox is one of those cloud services that I really cannot do without. As a crusader for information security the last 15 years I'm very impressed with their approach to security and privacy.*

Amar Singh,  
Globally recognised Information Security & GRC expert,  
Former CISO, Current Chair of the UK's Security Advisory Group, ISACA.

Zero vulnerabilities per  **WhiteHat**  
SECURITY

## Data Security

### Your data is completely private

SaneBox never looks at the body of your emails. Its algorithms analyze the patterns in your email behavior (which emails you open, respond to, how quickly, etc) to determine what's important to you.

### HIPAA compliant

As a pass-through entity, SaneBox complies with (and exceeds) the requirements of HIPAA.

### Your emails never leave your server

SaneBox never takes possession of the emails, and only analyzes email headers to determine importance. It then asks the server to move some of the emails to a separate folder.

### Active Directory integration

IT administrators can authenticate user accounts without ever exposing credentials via Active Directory.

## Network Security

Our mail processing servers never accept connections from the public Internet. All network access is provided through encrypted VPN tunnels via a bastion server. From there, our servers are accessed by our authenticated engineers via SSH, and all access is logged and audited. There are no exceptions.

## Physical Security

The data centers are housed in nondescript facilities away from major cities, and have extensive setbacks with military grade perimeter control. Authorized staff must pass through two-factor authentication systems, and are under video surveillance at all time.

## Personnel Security

Each of our personnel is hand picked, fully vetted with internal methods. Only select senior engineering personnel are allowed to access our production servers, and access logs are kept at all times.