

## Security, Auditing and General Resources

The below references are intended to be very high-level resources and general recommendations that the Clarity team will gladly review in detail with the Client team if/when it makes sense. Please let us know if you'd like to discuss or collaborate on any of the below items.

### Hardening Within Windows

Please see [Server Hardening guide](#).

### Hardening Resources (external auditing tools)

The below tools are penetration testing, vulnerability assessment and similar tools that Clarity has used in the past to help validate “basic” / standard settings necessary to meet industry security best practices. Ultimately a reasonable combination of the below resources is strongly encouraged to ensure the Client team has external audits of the application with reporting of passing logs that help show a clear adherence to industry best practices for security auditing and compliance.

Detectify - <https://detectify.com/what-is-detectify> - general 3rd party vulnerability and security scanner.

Acunetix – <https://www.acunetix.com/websitesecurity/hipaa-rules/> - 3<sup>rd</sup> party vulnerability scanner and HIPAA configurable audit/reporting tool.

AlienVault - <https://www.alienvault.com/solutions/azure-hipaa-compliance> - 3rd party group that provides HIPAA Compliance auditing and validation / reporting.

SecurityMetrics / Trustwave – [www.securitymetrics.com](http://www.securitymetrics.com) / [www.trustwavecompliance.com](http://www.trustwavecompliance.com) – These groups will enable auditing and to some extent “white hat hacking” attempts that will help provide reporting and validation on a periodic time frame that documents the steps taken to reasonably ensure the application and underlying data meet HIPAA requirements.

### CDN, Security and Performance

Enabling a 3<sup>rd</sup> party CDN that offers built in security and performance tuning generally makes sense for a relatively reasonably priced plan. In addition to providing basic performance tuning and automated file compression, etc. these services typically help provide a “first line of defense” before even allowing traffic to hit the cloud environment. In particular these can help isolate to regional areas that are approved and prevent known hacker organizations and standard, preventable attack patterns.

Cloudflare – [www.cloudflare.com](http://www.cloudflare.com)

Incapsula – [www.incapsula.com](http://www.incapsula.com)