



## Your partner in security

Companies often utilize security software with pre-installed default settings, making them susceptible to malware, viruses, data leaks, and hackers. We go above and beyond to ensure that your privacy is always protected.

### HIPAA Security

As a HIPAA-compliant company, we have deployed modern processes and software across the entire company to ensure both technical and physical safeguards for all Electronic Protected Health Information (ePHI). This includes:

- mandatory HIPAA compliance training courses for all team members
- the usage of Perimeter 81, a next-generation, HIPAA-compliant VPN that enables a stronger user-centric security posture based on identity and context
- the option to sign a Business Associate Agreement (BAA) with Edge, thus establishing a legally-binding relationship to ensure complete protection of Protected Information (PHI)



### Systems and Data Security

Through the use of Drata, our security and compliance automation platform, we are able to continuously monitor 100+ security controls, enabling us to confidently prove our security and compliance posture every single day. This also fosters a security-first mindset and culture of compliance throughout the entire company.



Additional security measures include:

- AI-based active end-point security to prevent, detect, and remediate known and unknown threats, helping protect all our systems regardless of location
- employing NIST 800-53, a set of standards and guidelines that the U.S. government uses to help federal agencies and contractors meet the requirements set by the Federal Information Security Management Act (FISMA)
- configuring 700 hardening settings in our operating systems, web browsers, Microsoft Office, Google Suite, and all other software
- compliance with ISO 27001 and SOC 2



## People Security

No matter how many security measures are applied, at its core, security begins with our people. Our entire company is trained on security ethics from the U.S. Defense Information Systems Agency, with refresher courses every 6 months.

Additional measures include:

- the execution of Non-Disclosure Agreement (NDA) by all employees, providing legal protection if proprietary information is improperly disclosed
- 100% computer encryption, ensuring all computer data can only be accessed with an employee's password
- 2-Factor Authentication, as well as additional security settings such as Authenticator apps and FIDO2 YubiKeys.

Ambassador Photos



To learn more about our security compliance:

