**The SaaS CTO Security Checklist**

This is a basic checklist that all SaaS CTOs (and anyone else) can use to harden their security. Security shouldn’t feel like a chore. Select your startup stage and use these rules to improve your security. This list is far from exhaustive, incomplete by nature since the security you need depends on your assets.

**COMPANY STAGE**

**YOUR COMPANY**

* Ensure your domain names are secured
* Be honest and transparent about any data you collect
* Make sure all your critical services are secured
* Do not share Wifi
* Take special care of your non tech employees
* Have a public security policy
* Have an internal security policy
* Set up a bug bounty program
* Make an inventory of your company’s assets
* Have a security incident response plan

**YOUR EMPLOYEES**

* Accustom everyone to security practices
* Require 2FA in your services
* Encrypt all employee laptops & phones
* Accustom your team to locking their machines while away
* Use a password manager to ensure you only use strong passwords
* Follow an onboarding / offboarding checklist
* Do not share accounts
* Use centralized account management

**YOUR INFRASTRUCTURE**

* Use SSL certificates to secure people using your website
* Check your website's basic security
* Isolate assets at the network level
* Keep your OS up to date
* Backup
* Restrict internal services by IP addresses (your company’s ISP, VPNs, etc…)
* Centralize and archive your logs and make them meaningful
* Protect your application from DDoS attacks
* Keep a list of your servers
* Watch for unusual patterns in your metrics
* Know how to redeploy infrastructure from scratch

**YOUR CODE**

* Enforce a secure code review checklist
* Use a Static Security Code Analysis tools
* Maintain a backlog of security concerns in your issue tracking tool
* Never do cryptography yourself
* Keep secrets away from code
* Perform security oriented test sessions
* Use a secure development life cycle

**YOUR APPLICATION**

* Run it unprivileged
* Monitor your dependencies
* Use a real-time protection service
* Hire an external penetration testing team

**YOUR PRODUCT USERS**

* Enforce a password policy
* Encourage your users to use 2FA
* Monitor your user’s suspicious activities