aikido

Essential

SaaS CTO Security Checklist

This practical checklist is designed to help SaaS CTOs harden both their app and company security.

Each item is tagged for different company stages: Bootstrap, Startup, and Scaleup. Use the right rules for your company's current stage and customize them depending on your assets and environment.

We believe that security shouldn't feel like a burden. Lighten the load by automating checks and regularly revisiting the list as you grow.

Your company

- [ ] **Enable 2FA for critical services** Bootstrap Startup Scaleup

  Secure Gmail, Slack, AWS, and other vital services with two-factor authentication (2FA). If compromised, these platforms can be used to access other services or launch hard-to-detect social engineering attacks. Turn on 2FA by buying hardware Yubikeys for your employees or by using the Google Authenticator app. Avoid less secure SMS-based 2FA unless you have no other option.

- [ ] **Use DMARC to secure your email** Bootstrap Startup Scaleup

  About 90% of cyber attacks start via email (according to Cisco's Cybersecurity threat trends), so nip this threat in the bud early. DMARC is a widely deployed industry-standard protocol that will help secure your email and domains against phishing.

- [ ] **Run a phishing drill** Startup Scaleup

  It's just good manners to pre-announce this to your co-workers, but we guarantee that some of them will fall for it anyway. Modern phishing emails have realistic-looking designs, working links, and are crafted to create a sense of urgency. A friendly phishing drill is a great training opportunity to help everyone learn how to identify them. Be aware that AI tools will make phishing attacks even more convincing in 2024.

  Good phishing drill tools: • Phished • Riot's Simulation Feature

- [ ] **Check your regulation and compliance requirements** Bootstrap Startup Scaleup

  More and more regulation is being implemented by governments that dictate cybersecurity requirements for many different types of companies, covering everything from data privacy to supply chain security (e.g. GDPR, the EU Cyber Resilience Act, NIS2).

  Contact your country's Centre for Cybersecurity:

  - List of confirmed National Coordination Centres

  Check your NIS2 compliance in Aikido

Set up a bug bounty program Scaleup

Encourage white hat hackers to report vulnerabilities through a bug bounty program. Offer rewards to make it worth their while. We also strongly recommend that you use a bug bounty platform for easy access to skilled ethical hackers.

Recommended platform: • Intigriti

Test your database recovery plan Bootstrap Startup Scaleup

We recommend using a managed database service such as AWS RDS, but it's still a good idea to simulate recovery procedures. This will both familiarize you with the steps you need to take and give you a good idea of how long it will take you to recover.

Use a virtual credit card system with limits Startup Scaleup

Virtual credit card systems allow you to share credit card numbers with your employees, but also restrict them to specific limits and services. No more surprises with credit cards that are suddenly refused!

Great virtual credit card tool: • Spendesk

Your employees

Get everyone accustomed to basic security practices Bootstrap Startup Scaleup

Humans are typically the weakest link in the chain of security. Increase employee awareness by explaining how attackers typically work. This massively minimizes the chance of them falling for tactics that are now more sophisticated than ever. New trend for 2024: educate your employees that they should not share sensitive company data with AI services like ChatGPT!

Great cybersecurity tool: • Riot's Awareness Feature: Albert the slackbot

Encourage personal 2FA for social accounts Bootstrap Startup Scaleup

If an employee's personal social media accounts are compromised, this can make social engineering attacks on others more effective. This could ultimately result in your company's social media pages being taken over. Strongly recommending that your co-workers set up 2FA is a quick win.

Use a VPN for your entire team Bootstrap Startup Scaleup

You can never trust the network you use, so encrypt everything by default. As a bonus, if your VPN offers a static IP address, you can whitelist critical accesses such as production database access for developers.

Enable full-disk encryption on employee devices Bootstrap Startup Scaleup

Encryption is a no-brainer. Someday an employee will lose their phone or laptop, so you need to be prepared. Pro tip: work as much as possible in the cloud and minimize the number of files stored locally on devices.

More tips on device encryption:

- Mac
- Linux
- Microsoft Windows

Use automatic screen lock Bootstrap Startup Scaleup

Get your employees to set up automatic screen lock after only a few minutes of inactivity. Then go even further and get them into the habit of manually locking their devices, especially in public places.

Establish an onboarding/offboarding checklist Bootstrap Startup Scaleup

List all the steps you need to enforce when employees, contractors, interns, or anyone else joins or leaves your company. Make sure that only the right people have access to your company's resources.

GitLab has some great examples:

- GitLab Handbook: Onboarding
- GitLab Handbook: Offboarding

Conduct regular access reviews Startup Scaleup

Even though you've set up an offboarding checklist, some users might still end up with broader access rights than they really need. If one of these users gets hacked, those extra access rights become a risk. Regular access reviews will mitigate these risks.

Enforce single sign-on for all apps Scaleup

An SSO solution such as Google, Microsoft, or Okta, makes it easy to manage user authorizations. It streamlines the process when you need to update a user profile, like when an internship comes to an end, and it's also a great way to define standards in account creation.

Back up, then back up again Bootstrap Startup Scaleup

Back up all critical assets and attempt to restore them frequently so you can guarantee that they're working as you expect. Startup phase bonus point: use standard RDS backups, but make sure you enable cross-region backups using AWS Backups to safeguard against full-region failures.

Enable cloud budget alerts Bootstrap Startup Scaleup

One sure-fire way to detect that someone is mining Bitcoin on your cloud account after a takeover is to have budget alerts on all your cloud accounts to monitor expenditure.

Use cloud posture management tools Startup Scaleup

Cloud providers offer so many features that it’s easy to shoot yourself in the foot. Use a cloud security posture management (CSPM) tool to scan your cloud.

CSPM Tools: • Cloudsploit • AWS Inspector

Set it up in seconds with Aikido

Protect your app from DDoS attacks Startup Scaleup

A Distributed Denial-of-Service Attack (DDoS) can have devastating consequences on businesses. Protect yourself by integrating basic DDoS protections with a content delivery network (CDN) like CloudFlare or CloudFront.

Set up surface monitoring (DAST) Startup Scaleup

Deploy DAST tools to simulate attacks and identify vulnerabilities in your web app’s front-end. Hackers will do it, so you need to as well.

Recommended tools: • ZAP

Set it up in seconds with Aikido

Make sure you can redeploy infrastructure from scratch Scaleup

Document your infrastructure using infrastructure-as-code. This acts both as documentation and an easy recovery mechanism.

Install next-gen antivirus software on employee devices Scaleup

Next-gen antivirus software doesn't impact performance as much as old security software used to. They're amazing at reporting and management, so you can act quickly when a user is infected.

Great antivirus software: • CrowdStrike • SentinelOne

Your infrastructure

Use SSL certificates for your website Bootstrap Startup Scaleup

Encrypting communications through SSL certificates ensures privacy, but also keeps your users safe from being tampered with when they visit your site.

Check your SSL compliance with: • Qualys SSL Labs

Check your website's basic security Bootstrap Startup Scaleup

Websites can be exposed to many different classes of vulnerabilities, but you can prevent some of them just by using the appropriate configuration on the server.

Check your website configuration: • ZAP

Set it up in seconds with Aikido

Keep development, staging, and production cloud accounts separate Startup Scaleup

While you could create virtual networks inside your cloud accounts to keep staging and production separate, you'll end up continually managing user access rights for new devs. We recommend keeping development, staging and production infrastructure in completely separate cloud accounts. All cloud providers offer unified billing, so that's one less headache.

Update your OS and docker containers Startup Scaleup

Regularly download all security updates for your operating systems and frequently update your machines. For servers, you can delegate this to a PaaS provider like Heroku or AWS Beanstalk.

Scan your Docker security using: • Syft • Grype • Trivy

Set it up in seconds with Aikido

Check your LLMs for the most common exploits Bootstrap Startup Scaleup

If you're implementing LLMs into your organization, it's a good idea to test them for the most common exploits. This is critical if you're opening them up to your customers!

Check the most common exploits:
- OWASP Top 10 for LLMs

Monitor servers for performance anomalies Startup Scaleup

Takeovers will often be used to steal your data or set up your servers to be used as bouncers. This kind of activity can be detected by watching for unusual patterns in metrics such as network bandwidth, CPU and memory consumption, and disk usage.

Server monitoring tools:
- New Relic
- Sysdig

Monitor subdomain takeover opportunities Startup Scaleup

Subdomain takeovers are a favorite way for hackers to listen in on user cookies. This can happen when a CNAME record points to a service you no longer use (e.g. an old S3 bucket that no longer exists). Use a tool to monitor for this risk every so often.
Tip: Aikido scans your subdomains every 24 hours.

Set it up in seconds with Aikido

Restrict deployment credentials by IP address Startup Scaleup

CI/CD systems get hacked all the time (read about a real-life example). When you give deployment credentials to your CI systems, make sure to lock them to specific IP addresses as an extra layer of defense.

Check if you're well configured with Aikido

Use strict CSP headers disallowing inline JavaScript Bootstrap Startup Scaleup

CSP headers can protect you from common cross-site scripting (XSS) attacks by providing an additional security layer that controls which dynamic resources are allowed to load. That prevents attackers from injecting scripts into your web pages.

Check if you've set them up correctly with Aikido

Your code

Enforce a secure code review checklist Bootstrap Startup Scaleup

Always prioritize security during coding, and that goes for pull requests as well. Adjust the checks you carry out depending on where the code is. Dealing with user entry is one thing, dealing with business structures is another. Use your common sense, but also make yourself familiar with typical security flaws.

Tip: ask potential candidates about security during interviews.

Read more: OWASP Top Ten

Use static code analysis tools Bootstrap Startup Scaleup

Static code analysis tools can quickly overwhelm you with a lot of meaningless false-positives. But they can also help you discover vulnerabilities inside your code and increase security awareness in your team. Reduce friction by integrating these tools into your workflow and use post-commit checks that automatically comment where code reviews are performed.

Code analysis tools: • Bandit • Brakeman • Gosec • Semgrep

Set it up in seconds with Aikido

Use lockfiles to protect your supply-chain Bootstrap Startup Scaleup

If you don’t use lockfiles, any time you build your application you’ll pull in the latest versions of all open-source packages. Lockfiles limit the number of packages pulled in during the build process, making your app more secure against supply-chain attacks on your open-source dependencies.

Never do your own cryptography Bootstrap Startup Scaleup

Always rely on established mechanisms, libraries, and tools. Cryptography is an expertise. Building your own implementations, or using flags and options you don't fully understand, will expose you to major risks. Libraries such as na.cl expose few options and restrict you to good choices.

Check your packages for their End Of Life (EOL) Startup Scaleup

As packages get older and stop being supported, the risk of exploits increases. You should make sure to upgrade packages that are soon reaching their end of life.

Or set it up in seconds with Aikido's container scanning feature

Keep secrets separate from code Bootstrap Startup Scaleup

Don't commit secrets directly into your codebase. Handle sensitive information separately to prevent accidental sharing or exposure. This allows for clear separation between your environments (e.g. development, staging, and production).

Check your code for secrets with Aikido

Implement a secure development life cycle Scaleup

Adopt a secure development life cycle to help you tackle security issues at the beginning of a project. With the right customization, it provides good insights at all stages of the project, from specification to release, and will allow you to enforce good practices at every stage of the project life cycle.

Read more: Wikipedia article on systems development life cycle

Check your code for malware Startup Scaleup

The number of software supply chain attacks has been on the rise for years. Malicious packages are exceptionally dangerous, as attackers typically act fast after they've succeeded at getting malware into your code. So you also need to react quickly. Note that CVE databases are too slow and won't keep you safe from these kinds of attacks.

Tools: • Socket • Phylum

Set it up in seconds with Aikido

Enforce a secure code review checklist Bootstrap Startup Scaleup

Always prioritize security during coding, and that goes for pull requests as well. Adjust the checks you carry out depending on where the code is. Dealing with user entry is one thing, dealing with business structures is another. Use your common sense, but also make yourself familiar with typical security flaws. Note that LLM-generated code can be prone to hard-to-spot exploits, so be extra careful with this code. Tip: ask potential candidates about security during interviews.

Read more: OWASP Top Ten

- [ ] **Check your JSON Web Token verification algorithms** Bootstrap Startup Scaleup

  JWT can replace session cookies in many places, but are prone to specific attacks such as the none algorithm attack, algorithm confusion attacks, and null byte injection attacks.

  Tools:
  - ZAP (authenticated version)

  Set it up in seconds with Aikido

- [ ] **Run a thought exercise: what would you do if one of your third-party providers gets compromised?** Scaleup

  Think about how to mitigate the damage if they get compromised. For example, Okta was hacked in 2023, but one of its customers, Cloudflare, was not impacted. Why? Because they were prepared.

  Read more: How Cloudflare mitigated yet another Okta compromise

Your application

- [ ] **Run Docker containers with restricted privileges** Bootstrap Startup Scaleup

  Limited privileges makes it hard for successful attackers to take over the host or bounce to other services. Avoid running containers with privileged user roles, such as root on Unix systems, or Administrator or System on Windows systems.

- [ ] **Block cross-account data leakage for multi-tenant SaaS** Bootstrap Startup Scaleup

  You have plenty of options here: use measures such as logically separating databases, multiple physical databases, or code-level separation.
  Tip: for logical separation in code, make sure your ORM layer ensures separation.

- [ ] **Monitor your dependencies** Bootstrap Startup Scaleup

  Applications are built using dozens of third-party libraries. A single flaw in any of these libraries could put your entire application at risk. Reduce this risk by using the right tools to monitor your dependencies for known vulnerabilities.

  Recommended tools:
  - Trivy

  Set it up in seconds with Aikido

Use a web application firewall (WAF) Scaleup

Deploy a WAF to protect web-facing servers against unknown zero-day threats, including unknown SQL injection or XSS threats.

Best tool for this: • AWS WAF

Hire an external penetration testing team Scaleup

Penetration testers take an external and naive point of view of your infrastructure and products. Pentesters will take nothing for granted and will check the most basic assumptions, as well as all of your infrastructure. You can even ask them to start with a full, blind discovery of your infrastructure, which can help you remember old assets.

Read more: 10 things you need to know before hiring penetration testers

Your product users

Enforce a password policy Bootstrap Startup Scaleup

Your user accounts will be much harder to steal if you require them to use complex passwords that include a mix of uppercase and lowercase characters, special characters, and minimum lengths.

Offer a public API with OAuth 2.0 and refresh tokens Startup Scaleup

When providing a public API, make sure you follow standards for access management such as offering a clear OAuth 2.0 authorization screen with clearly defined scopes. Offer short-lived access tokens with fine-grained refresh tokens for an extra layer of security.

Offer single sign-on or 2FA in your own app Startup Scaleup

As you attract higher profile customers, you will be required to implement stronger security practices. This includes offering them 2FA and role-based account management.

Great tools: • Auth0 • Quasr