Security For Startups

Security Essentials for Startups Taking their First Steps as Cloud Providers

V1.0 February 2017

Acknowledgments

Created by:
Shahar Geiger Maor, Outbrain

Contributors:
Moshe Ferber (@FerberMoshe)
Ofer Smadari, Accezz.IO
Yael Nishri, Vaultive
Ron Peled, LivePerson
Marius Aharonovitz, Click Software
Omer Taran, CybeReady

Table of Contents:

Introduction

Background:

Information security is a complicated subject even for mature enterprises, so it is no wonder that it is a significant challenge for newly founded startup companies. Planning, implementing and maintaining good-practice security can become an important advantage for young startups, one that can be leveraged as a marketing differentiator. On the other hand, poor practices may result in dire consequences.

The most crucial security challenge for young startups is to align security with their business growth so that security controls will match the risks at any point in time (see Appendix 1).

This document was created by the Israeli chapter of the Cloud Security Alliance (CSA). The CSA is a non-profit, community based organization dedicated to defining and raising awareness of Best Practices to help ensure a secure cloud computing environment.

About the Cloud Security Alliance:

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products.

The Israeli chapter of the Cloud Security Alliance was founded by security professionals who are united in a desire to promote responsible cloud adoption in the Israeli market and the startup eco-system.

Visit our Facebook group for more details:

Purpose of the Document:

The main purpose of this document is to help Software-as-a-Service startups (SaaS-SUs) gain and maintain client trust, by building solid security foundations at an early stage of their product development process. In addition, this document should help SaaS-SUs meet some of the most important security and privacy requirements presented by SaaS clients when considering new vendors/products.

Target Audience and General Assumptions

- The document is aimed at cloud-based startups who want to develop their security roadmap
- The target audience are founders, CTOs, Product managers and architects
- The document is a generic guideline. It covers the main pain points only and cannot replace a thorough vendor risk assessment preparation process.
- Adoption of the controls mentioned below and the rate of adoption are dependent on the startup product, business goals, targeted customers and market sectors.

Before You Start

Mapping Your Security Requirements

Security requirements vary between different market sectors and heavily rely on the type of data you collect. When planning the startup roadmap, vendors should estimate at which point in time they'll need to embed which security controls and plan ahead. As a rule of thumb, if startup characteristics match any of the following, prepare for early implementation of security controls:

- Target customers are enterprises - Expect more questions about the shared responsibility model, identity management and security policies.
- The data stored contains high volume of PII or sensitive PII (e.g.: Health info, financial details) or - You might need to comply with more strict regulation and laws (e.g.: HIPAA, GDPR, Privacy Act).
- Target sectors are Health, Government, Financial or Homeland Security - Expect industry specific regulations and more questions about location of services.

Choosing a Cloud Platform

There are many parameters that should be considered when choosing an IaaS/PaaS provider. Most of the parameters are not directly related to security, but some are. Here is a quick list:

- Service location - When targeting enterprises from a specific geographic jurisdiction, it is recommended to keep customers data in the same geographic location. Doing so can relieve compliance efforts and create a competitive advantage.
- Regulations - Clients should strive to work with service providers who align to the same regulation regime.
- Ecosystem - A startup usually strives to consume external software and services for reducing development times. A large ecosystem of knowledge, tools and third party software is an advantage for cloud providers.

Tips

- If targeting enterprises in the US, EU and APAC, consider deploying data storage into all of these regions to relieve compliance efforts.
- IaaS will provide better flexibility and control over PaaS, since you are the owner of your server's configuration. But it also means you have the responsibility to secure those servers.

Application Security

Application security is an important pillar when planning security foundations. Lack of good application development and deployment methods can result in an inability to adhere to regulations and standards and an exposure to application attacks. Neglecting application security practices at the early stages will make it much harder and more expensive to correct at a later stage.

General Recommendations:

- Start with security awareness training for programmers and QA.
- Consider providing clients with recommended guidance on security Best Practices with regard to the offered service. Let your clients know you are taking care of their crown jewels by explaining how they can work with you securely.
- Be transparent. Offering your clients some useful security insights regarding the best ways to integrate your service into the client's environment may position you as a trusted advisor. This proactive approach may help you earn your client's appreciation when evaluating your security risks.

Tips:

- Start small, but learn from the big players: *https://aws.amazon.com/security/* , *https://azure.microsoft.com/en-us/services/security-center/*
- Each development environment has its own security implementation and best practice docs. Use them.
- Make sure to authenticate all services & validate all input.
- Explore solutions such as AWS Parameter Store, AWS KMS or Azure Key Vault for storing your application secrets (encryption keys, connection string, etc.).

Authentication and Authorization

Authentication (identity validation) to cloud apps is most likely to be the first line of defense. Implementing advanced methods of user authentication and authorization (granting permissions) may help reduce the risk of unauthorized access.

- All customer accounts should be authenticated and authorized.
- Admin and privileged user accounts inside your application should support 2FA mechanisms.
- Do not attempt to recreate the wheel. Follow existing standards and Best Practices (e.g.: OAuth, SAML, OpenID).

Tips:

- Deploying a good directory solution with identity federation support is essential when building identity management policies.
- Deploying Identity Federation solution where your customers act as identity provider (IDP) and you are the solution provider helps gain customers trust.
- Store your customer's password according to Best Practices. Most development frameworks provide libraries for implementing hashing, salting and more.
- Think about password reset flow for your customers.

APIs: The More, the Better

- Provide as many APIs for your clients as possible (support self-serve, reduce overhead and increase client satisfaction). This applies to both the application and infrastructure levels.
- For each API access, make sure to cover: Authentication, Authorization and Audit capabilities.

Tip: Privacy may bring many good examples for the use of self-serve APIs (e.g.: on-line tracking of personal data being collected by the service, self-deletion/update of client data, etc.).

SSDLC (Software Security Development Lifecycle)

According to security best practices, optimal implementation of security should be incorporated in systems by design. Implementing tools and methods for threat modeling, secure code review, static source code analysis, vulnerability testing and continuous training for staff will make your system more secure.

Tips:

- Start with threat modeling and security training as they are the easiest to begin with.
- Incorporate threat modeling first. Dynamic analysis will come later and should be integrated into the build creation process.
- Automate as many activities as possible to avoid becoming a bottleneck for other development efforts.

Platform Security

This document was written with the assumption that the startup is deployed on an IaaS/PaaS platform. While securing the cloud platform falls under the responsibility of the cloud provider, securing the running instances and the management dashboard is the cloud consumer's responsibility.

General Recommendations

- Understand the shared responsibility module between you and your provider. Most mature providers have detailed documentation on that topic.
- Always have a copy of your critical backups outside the cloud environment.
- Consider deploying to more than one region in your cloud provider platform in order to increase reliance from region level failures.

Management (Client) Dashboard

The IaaS/PaaS management dashboard is the most popular attack vector. Failure to protect management dashboard can result in an inability to provide your services for good.

- Follow your service provider's security Best Practices checklist.
- Avoid using the Master/Root account on your dashboard. Create sub-accounts with relevant roles and use those instead.
- Protect your admins with 2FA. Revoke unused API keys.
- Protect your DNS. Domain Name Servers have become popular attack vectors.
- Create procedures for storing API keys and other secrets in a safe location.

.

Tips

- Activate management dashboard logging tools such as AWS Cloud-Trail from day one.
- Create roles for operations admins, and separate account management to different roles.
- Explore cross account permission to limit blast radius in case of an account hijacking.
- Use designated email address for your master cloud account (helps against phishing attempts).

Data Flows and Network Separation:

- Plan for resource separation. Separate between production, test and development environments and between different services and roles.
- Use a Distributed Denial of Service (DDOS) protection as-a-service solution. It is usually cost effective and most DDOS protection services can later be upgraded to a more robust Web Application Firewall (WAF) service.
- Visualize your assets and present a simple and clear diagram chart to help clients gain a better understanding about the system and place their trust in it.
- Always use VPN for connecting to your cloud data center.

> **Tip**: Since you can't control the underlying OS in PaaS, put the emphasis on other compensating controls, such as application security.

Physical Security:

- Since you are most likely a SaaS/PaaS provider, physical security is probably managed by a third party. Collecting your data center's SOC2 reports in advance can be very useful, as you will likely be asked for them by your prospects and customers. Creating an established process for sharing your data center's SOC 2 audit reports with your clients will be viewed as proactive move that builds trust.

> **Tip:** Make sure to proactively set a process for sharing the data center's SOC 2 audit reports with your clients.

Protecting Your Machines

- When developing on IaaS, it is the cloud consumer's responsibility to make sure virtual machines are fully patched, hardened and scanned periodically. Due to the dynamic nature of cloud services, automation is highly recommended here.

> **Tip:** Adopting a Red/Black software deployment methodology can reduce patching and hardening efforts.

Encryption and Key Management

Encryption of data at rest is mandatory for complying with certain regulations and standards. There are various types of encryption levels and proper analysis should be made in order to choose the best solution for your requirements.

- Use standard encryption protocols and algorithms (IPSEC, TLS) for all data in transit, including APIs and remote access connections.
- Use cloud provider tools to encrypt data at rest. Most of them will support encrypting volumes and DBs with provider-owned keys. These solutions are simple and relatively inexpensive.
- Once matured, consider moving your keys to a Hardware Security Module (HSM) or key management service.

> **Tip:** Most cloud providers support storing encryption keys in a designated HSM. This is an expensive, yet very efficient solution.

Security Management

Transparency

Transparency is an important cornerstone when attempting to win customers' trust. Without true transparency into the vendor's operations, it will be very hard to demonstrate maturity and gain customers' trust. To be more transparent, you should document relevant security policies and share them with your customers.

- The vendor should have a documented set of security policies and procedures.
- The vendor should have documented Disaster Recovery and Business Continuity procedures to apply when services goes down.
- The vendor should consider an open status page for its services (e.g.: G Suite Status Dashboard).

Tip: Policies should be very clear and friendly so that all employees can understand and follow them. Long, tedious policies may look appealing for IT auditors but they are not necessarily as effective. There is no need to create dozens of different policies. Try to focus on what you think is most important to address your highest security risks.

Tip: Getting examples from other companies, providers and templates is good, but try to avoid "copy-paste" solutions. Additionally, consulting with others can be beneficial. Try to find a "security mentor" from the tech community for guidance.

Industry Standards:

Alignment with industry standards makes it easier for the client's audit/compliance department to attest that they have properly vetted the vendor. Vendor should strive to comply at least with one of the major IT Security and Management standards (e.g: ISO-27001, ISO-22307, CoBIT and SSAE 16 SOC2/ISAE3402).

Tips:

- Identify the most effective standard to comply with, according to your industry and prospective clients. Don't over-qualify yourself with an unnecessary array of expensive accreditations.
- If your customers are enterprises, expect to have a mandatory request to comply with either SSAE16 SOC 2 or IS27001 certifications.
- If you are hosting protected health information (PHI) of US citizens, you must comply with the HIPAA security and privacy rules.
- If you are hosting Personally Identifiable Information (PII) in the EU or on EU citizens, you will need to comply with EU GDPR laws.
- Consider getting accredited with advanced standards (ISO 27018 /ISO27017 / CSA STAR) if you want to differentiate your services as highly secure.

Vulnerability Assessments:

All vendors should undergo periodic vulnerability assessment and penetration tests on their environment. The goal is to provide unbiased evidence of the security of your service's infrastructure/system.

Tip: It is highly recommended to provide your clients with a summary of findings and mitigation plan of the latest vulnerability assessment. Some clients will settle for a formal attestation letter by a professional third party auditor.

Incident Response:

Clients will expect the vendor to be able to contain and notify of any security event that might impact them with full transparency. Remember, Incident Response is not about creating an end-to-end methodology to tackle every potential use case, but rather devising a basic procedure to identify the case and demonstrate some proven level of due-care while handling security incidents.

Tips:

- Try to index logs and events in a way that will make it easier for you to isolate logs per client.
- Automate log collection, correlation and alerting. Focus on actionable alerts.
- Consider cyber insurance, it is turning to be a mandatory requirement.
- Do note that if you are hosting PII, you may be required by law to perform breach notification procedures in an event in which customer data has been breached. Be prepared for that event and encrypt the PII to lower your risk exposure.

Log Management:

Collecting, indexing and analyzing logs and audit trails are mandatory to comply with regulations.

- Plan ahead. Think of how you can easily index, search, access, aggregate and filter logs.

Tips:

- Provider's tools, such as AWS Cloudtrail/ Cloudwatch-logs and GCE StackDriver logging, are very efficient tools to start your log collection process.
- When your startup is still small, only collect and store logs. Once it begins to grow, add more real-time detection and analysis capabilities.

Data Processing Limitations:

Local privacy laws may require strict personal data processing limitations from cloud service providers.

- Ensure that your platform can support data-processing regional-based limitations, as well as prompt deletion of data, in cases of contract termination.

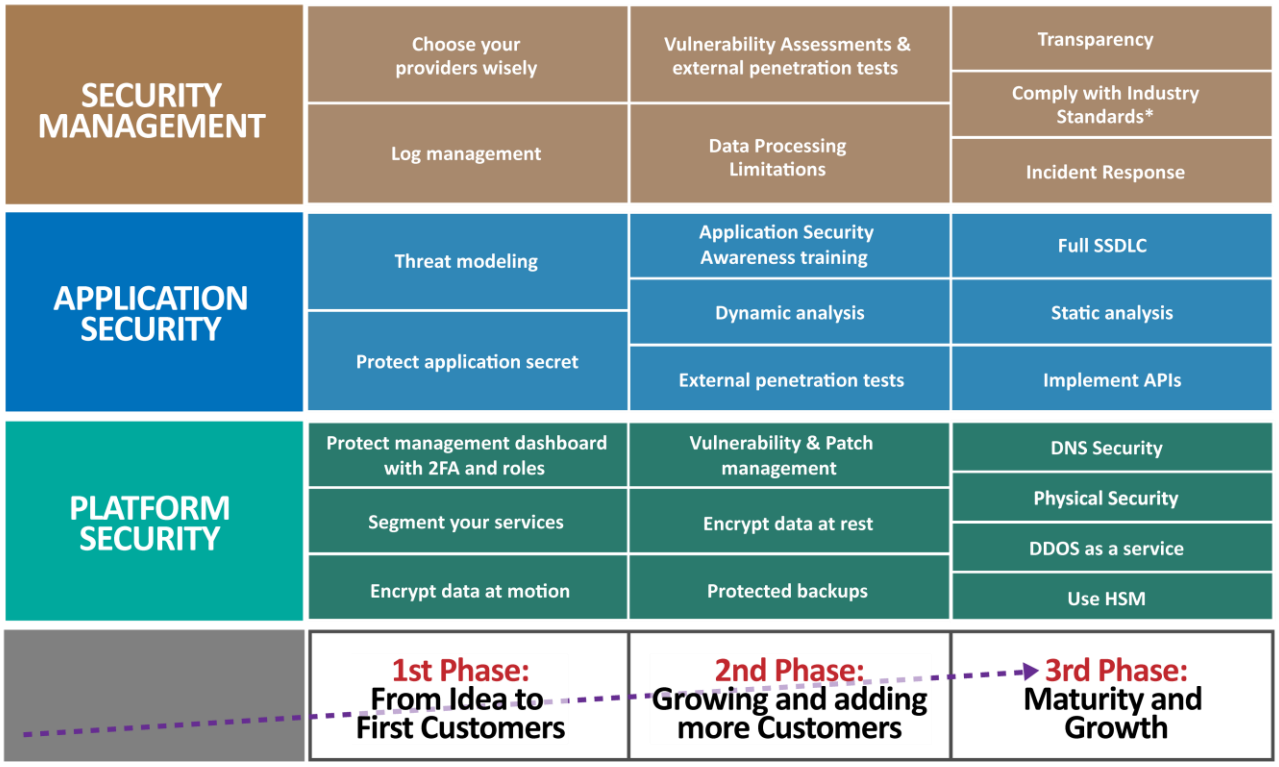
Tips:

- Familiarize yourself with the EU GDPR (European Union General Data Protection Regulation) and other applicable privacy laws and regulations.
- Consult with privacy law professionals. If you host EU PII in the US, consider becoming certified with Privacy Shield. For a more generic option, use the Standard Model Clauses.
- Implement customer data purging and data portability solutions, preferably via self-service.
- Use the Privacy Level Agreement to help you map and document what PII you collect, how you handle it and how you comply with privacy laws and regulations.

Appendix 1

Security Essentials Maturity Model (Applying security controls as you grow)

This advisory diagram was made in order to demonstrate when on the startup lifecycle you need to implement each control.



*Some industries may require compliance with standards as a prerequisite.