Date: August 1, 2019

Troops.ai, a Security-First Startup

Troops was started in 2015 with the goal of improving the ways in which customers manage information on their customers, revenue and pipeline in order to help them drive growth and digital transformation. . In order to do that effectively, Troops needed to ingest relevant data from critical business systems including, but not limited to, the CRM ecosystem such as Salesforce, calendar and scheduling systems such as Google Calendar, Gmail and other data sets that are core to a company's operations. From there, Troops applies codified business processes to this data in order to deliver real-time, intelligent, and actionable alerts to help improve things like sales pipeline manage, customer success management, real-time micro coaching, management oversight, and more. .

When we started this journey, we were a tiny team in a room together, excited about the possibility of a better future where human work is not encumbered by endless minutiae of administrative tasks and mindless process. Fast forward to today, Troops powers sales process execution and in-game coaching for public companies like Square, Hubspot, Lyft, Slack and WeWork, fastest growing startups like DoorDash, InVision, Looker, Flexport and many other customers including companies in medical and financial services categories. So how were we able to earn the trust of handling sensitive data for these companies?

Security. From day one, Troops has been overinvesting in security, privacy and encryption in to our application. For us, security is a must-have and is viewed more than ever as a customer-facing feature vs something we must simply check the box on. We recognize the data we work with is the lifeblood of a company and we take it very seriously.

Independent Certification & External Penetration Testing

We knew right away how critical the security of our system and our customers' data will be to the success of our business, so we invested heavily in security from the early days. But we didn't want our customers to just take our word for it. That's why, still as a seed stage company, we enlisted a 3rd party auditor, A-lign, to undergo our fist SOC 2 certification. This decision raised eyebrows with many of our colleagues at seed-stage startups as well as later stage established companies. "Isn't it crazy to commit that much time and resources to SOC certified this early?" they would ask. But we maintained our conviction that security will ultimately be a big reason why our partners trust and rely on Troops every single day. In fact, the team at A-lign said, "Troops is in the top 1% of companies they see in terms of SOC 2 preparedness". In addition to the SOC 2, we enlisted a "white hat" hacking provider with proven reputation to conduct external penetration testing and execute an extensive set of attacks against our entire application surface. The first time around, it was nerve wracking to watch our system get exploited, but we knew that it will only toughen our armour when it's done. We are thrilled to report that we've now completed our SOC 2 Type II audit and penetration testing for 3 years in a row with no exceptions noted on our report. We've also undergone an extensive GDPR gap assessment and ensured that our data privacy and retention policies complies with EU regulations. We're excited to continue investing into data privacy and security as the digital world continues to evolve rapidly. Now let's take a look at some of the ways we secure our systems.

Secrets Management & Encryption

The first step was to ensure that all data is encrypted. SSL Labs scan gives troops.ai an A+ rating because of our certificate length and lack of weak cypher support. We transmit all data using a 2048-bit SSL Certificate with RSA encryption. When the data is stored, it's encrypted at rest with Amazon's Key Management Service (KMS) using the AES-256 cypher, including all backups. In addition, sensitive data in our database is further encrypted at the application layer, using KMS, to prevent unauthorized viewing and access by rogue internal parties. Permission to decrypt the KMS keys is only granted to the servers running the application.

Code Deployment and Preventing Rogue Actors

In today's agile world, continuous releases to production are the lifeblood of any fast-paced technology company. But many of these companies struggle to balance speed to market with ensuring that production code is secure. At Troops, we've invested early in fully automating our continuous integration and deployment pipeline that is fully instrumented inside of Slack. After all, our product today lives primarily in Slack. Since we build this system entirely in-house, by integrating best-in-class SaaS tools with our own code, we were able to build in SOC 2 controls that are validated programmatically. One of these controls is requiring two peer approvals for any code going out to production. We pull these approvals automatically from GitHub, and since our deployment tool is the only entity with permissions to release new code, this control cannot be circumvented (ensuring the 3-person rule). Having our deployment pipeline in Slack also provides push notification for any initiated deployments visible to the security team and a permanent searchable audit trail, discouraging any rogue activity. In addition, all changes are shipped via feature flags furnished by LaunchDarkly that allow us to instantly shut of bad features using an administrative interface without having to wait for a code deployment.

Database Access

Given the amount of sensitive information is stored in our databases, we've made a decision early to partner with StrongDM. Their solution not only allows us to provide centrally managed access with fine-grained permissions to specific database but also ensures every query is audit logged and attributable to a specific individual. In addition, StrongDM provides an ability to enforce strong passwords, session timeout due to inactivity and 2-factor authentication using Duo. Query audit logs and administration is only available to the Troops security team.

IDS, Patch Management & Other Preventative Measures

Besides good best practices, processes, policies and tools, we made a decision to add a layer of monitoring and prevention in case there was an attack. We chose ThreatStack for our intrusion detection and AWS monitoring system. ThereatStack specifically integrates with Kubernetes, our container orchestration framework of choice, audits all AWS access in real time, provides vulnerability notices and file integrity monitoring. The notifications go directly into our Slack where the security team can react in real-time when a threat is detected. To limit the attack surface, we've made a decision to only allow external server access to our infrastructure via Amazon's CloudFront CDN. Given Amazon's reach and proliferation of clients, CloudFront already includes a plethora of security and monitoring features to stop the most common attacks before they get to our servers. For internal access by the security team, Troops uses AES-256 encrypted connection via a VPN with 2-factor authentication and audit logging. We limit production access to the security team and for emergencies or scheduled maintenance. To ensure that attackers can't exploit known vulnerabilities, we've implemented patch management in AWS with unattended upgrades during a daily maintenance window.

Antivirus, Device and Password management

At Troops, we don't store any customer data outside of our data centers, but to secure potential attack vectors, we make sure that all company laptops are secured. We use Jamf device management to enforce disk encryption, strong passwords, password rotation and automatic screen lock after one minute of inactivity. For antivirus and malware detection, we use BitDefender with centralized virus definition management and real time malware detection. Internal secrets for SaaS applications are managed using 1Password business with Duo 2-factor authentication and credentials are granted without an ability to view the underlying password.

Business Continuity & Disaster Recovery

Thanks to today's cloud technologies, including AWS, ensuring business continuity is easier than ever. Still, Troops not only follows all industry best practices, but also does a full disaster simulation test every year. All of our databases replicate to another geographic region. In case of need, we are able to quickly stand up an entire replica of the production environment in another geography automatically with minimal downtime.

Application Level Protection

To further protect Troops application from internal and external threats we've taken a number of measures to secure our application itself. We've added content headers at the edge of our CDN to prevent click-jacking, cross-site scripting and other client-side exploits. Internally, all access to our tools for customer account management are audit logged and most important events are pumped into Slack for additional visibility by the security team.

Policies and Training

Since tools are not fail-proof, Troops has training, processes and policies to encourage good behavior by our employees and contractors. We require background checks, security training, signing of code of conduct and security policy for all new employees as well as annually for all existing employees. We believe that security is everyone's responsibility and talk often about it cross-functionally.

The Work Is Never Done

We hope you found this post helpful to see a sample of things we do at Troops to maintain the highest level of security. But we are not resting on our laurels. Every year we make improvements to our application security, tooling and infrastructure as new threats emerge and industry best practices are updated. We are proud to stand with our partners to help them run their customer facing teams effectively and ultimately make more money and grow faster while ensuring that their data is in good hands with Troops.