CODA Footprint Security, Privacy and Architecture Reference

Securing and Protecting the Data within the Footprint Ecosystem

Introduction:

At CODA Intelligence, information security is deeply embedded into our DNA, and is therefore present in everything we do. In fact, the company was started by a highly-talented team of Cyber Security Engineers. These engineers, who were working as cyber security consultants, realized the need for a more comprehensive vulnerability identification and remediation solution. Knowing that the solution they were looking for was not readily available, they set out to create the CODA Footprint platform from scratch. The platform that they created, incorporated many of the security techniques and processes that they had developed over their years of consulting. Being that the CODA engineers were well versed in cyber-attack methodologies, tools and techniques, they made certain that security was integrated within CODA Footprint, from the ground up - At CODA, security is integral and not an after-thought! The Company certified its operations as well as its software development processes according to ISO 27001:2013 cert no. I3655/21 & I3656/21 granted by QSCert, valid until 02nd of July 2022.

As a valued partner, we want to make certain you have an understanding of the security measures that are in place on our platform so that you can rest assured that we are following all of the best practices and accepted security principles to ensure that your information, and that information of your customers, is adequately protected and secured. We also want to make sure that the data governance and ownership structure is transparent and thus the roles and responsibilities each party has to ensure data protection with the CODA Footprint environment.

This quick-reference document highlights the many ways that CODA secures their platform and protects any data that is collected, be it data from the MSP portal or data from the customer portal and also the roles and responsibilities of each party: CODA Intelligence, Partners, End-Users.

Securing Access to the Footprint Platform Hosted by CODA

CODA Intelligence has put in place a secure framework and several fundamental security controls in place to protect and secure access to the Footprint platform. Among these measures include controls such as password complexity, account lockout, optional 2-factor authentication, encrypted communications, application layer firewall, network-layer firewall and system hardening. In addition, we run a series of tests, including vulnerability scans and penetration tests, to ensure that the platform is adequately protected from cyber-attacks and to confirm that the security controls we have put in place are operating effectively (see table below).

The information provided below is intended to deliver more insight into the specific controls that are put in place for each of the critical components of the CODA platform, Including the infrastructure, applications, data, user accounts and the Footprint agent technology.

Cloud Infrastructure used by CODA Hosting – Data Centers, Networks and Systems:

The infrastructure is made up of the underlying systems (compute, virtualization, containerization, operating systems and storage), the networks for IP communications and the data centers that physically house these components (facilities, racks, cooling, power, etc.).

The various applications that make up the Footprint ecosystem rely on this infrastructure for proper execution, operations and for security. Therefore, these infrastructure components play a key role in securing and protecting the various Footprint applications and all related data. The following highlights the security controls instituted on these various infrastructure components.

Data Centers

- CODA's platform leverages infrastructure from well now public Cloud providers, who are world leaders in providing sound, secure and redundant data center services, including AWS and Azure. These providers also offer various public Cloud configurations including Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS), both of which we leverage for various subsystems of our CODA platform.
- Regardless of which Cloud provider is actually hosting the platform, or providing Cloud services, all of them offer SOC-2 type 2 audited services.

Networks

- The networks housing the CODA platform are protected by a stateful firewall that blocks all Internet access to the respective systems, allowing only HTTP and HTTPS traffic inbound. The Networks are also protected from Distributed Denial of Service attacks (DDOS), by employing a WAF service available from the public Cloud provider of choice.

Systems

- All systems are built and configured such that they meet the CODA standards for hardening and logging. In addition, these systems are actively monitored by our team of engineers.

Footprint Applications:

There are a variety of individual applications and libraries that together make up the CODA Footprint platform, these applications include:

- Customer web applications which provide the portals for MSP's and their customers
- Web Services APIs
- Database Services (SQL and nosql)
- Scan Engines
- Backend Applications
- Frontend Applications

- Message Queues

In case of CODA Hosting, the Footprint web portal is housed in a public Cloud, meaning that it is exposed to the general Internet and therefore can be directly attacked, therefore we have taken extra measures to ensure that these web applications are secured and tested, which includes:

- Following secure coding principles and practices (OWASP 10).
    - For more information on the OWASP 10, please refer to the following: https://www.owasp.org/index.php/Top_10-2017_Top_10
- Using a Web Application Firewall (WAF) to sit transparently between the web apps & services and the Internet, and monitor all layer-7 HTTPS traffic
- Preforming regular security tests on our own web apps to ensure that they cannot be compromised and that they do indeed institute the OWASP 10 principles and best practices

Footprint Data:

It is all about the data, and as such that sensitive data must be well retained, protected and secured!!

The data contained within the CODA platform, be it user account information, vulnerability scan data, customer information, reports, etc. is highly sensitive to the parties that own this data. Therefore, at CODA we have taken many steps to ensure the security, privacy and integrity of this data. Some of the measures we have in place include:

- **Data in-Flight** - Using SSL Encryption for all data being transmitted from the customer site to the CODA Platform. This includes any data being transmitted by the Footprint agent technology and any data being transmitted back-and-forth, between the web browser and our web applications. For the web Applications CODA supports TLS v1.2 and v1.3 and a minimum encryption key size of 128 bits
- **Data At-Rest** - We use Database-level encryption to ensure that the Footprint databases are encrypted at rest, ensuring that databases are protected from prying eyes of people who might have access to the storage, infrastructure or disks.
- **Database Access Controls –** The database that houses all the information and data cannot be directly access except by the Footprint application and our DevOps Team (solely for purposes of DB maintenance, troubleshooting and customer support)
- **Application Access Controls** – Only authenticated authorized users are allowed to access the end-user (tenant) data based on their privileges and credentials. Authentication can be either covered by Footprint (i.e. – local to the Footprint tenant) or via SSO with Microsoft IDP.
- **System Hardening** – We apply secure configuration standards to harden the data base servers, to reduce their attack surface
- **Data Retention** – We backup all data that's hosted within the Footprint platform for 365 days. Whenever a tenant is removed, all their data except for their registration is completely erased from the Instance.

Footprint End-User Accounts:

User accounts are an essential part of the secure authentication to any web portal application, and Footprint is no exception. Therefore, CODA has instituted a few best-practice measures to ensure that the user accounts, and their password information are fully protected

- **Enforced password complexity settings -** Using software called zxcvbn, which is a password strength estimator, allows us to set a password complexity policy which is based on password strength without a strict password complexity policy. Through pattern matching and conservative estimation, it recognizes and weighs 30k common passwords, common names and surnames according to US census data, popular English words from Wikipedia and US television and movies, and other common patterns like dates, character repetition (aaa), character sequences (abcd), keyboard patterns (qwertyuiop), and l33t speak.
- **Enforced account lockout settings** – User defined setting to lockout an account after 10 consecutive failed login attempts
- **2-factor authentication options** – Today this is built on Microsoft IDP with 2 FA enabled but we will also support other SSO providers in the future as per our roadmap.
- **Password Encryption** – All passwords that are created, be it for the MSP or their end-users, are hashed using HMAC functions and salting.
- **Access Controls** – Footprint has a variety of roles that can be assigned to a user and each role has a varying level of access-controls assigned, which limit what activities a user can perform and what data they have access to, within the Footprint platform.

Footprint Agent Technology:

The Footprint agent is a workhorse and a key component of the Footprint ecosystem. This agent is responsible for gathering a lot of valuable information about the host system that it is running on and reporting that data back to the CODA Footprint collector. Since this Agent runs with an admin-level system account it must be properly secured and protected.

To accomplish this, CODA has built-in features within the agent:

- All communications, to the CODA cloud, is always initiated by the Footprint agent. The agent itself does not accept any inbound network connections or requests.
- All communications from the agent to the Footprint platform is encrypted using TLS and a minimum encryption key size of 128 bits.
- Mutual authentication between the Agent and the Footprint console occurs upon each communication.
- All outbound agent communications are authenticated using an application token and use server certificate validation between the agent and the Footprint Cloud platform.

Footprint Security Assurance Testing:

Being that we are a cyber security company at heart and because we have the capability of testing web applications for flaws and vulnerabilities, we use this expertise to test the Footprint web applications.

For this testing, we use various tools and proprietary methodologies as part of our internal web app penetration testing (pen testing) process. We also undertake periodic external independent third-party audits and pen tests. This is done as an added level of assurance that our internet exposed web applications are not vulnerable to common Internet-based attacks such as multiple injections such as SQL, XPATH, code manipulations, Cross-site scripting, Cross-Site Request Forgery, Fuzzing, buffer overflows, error handling.

Any vulnerabilities identified during any testing will immediately be tracked and assigned an engineer for remediation. Once the remediation process has been completed, a follow-up will immediately be run to ensure that the proper steps have been taken and that the vulnerability or flaw is indeed fully remediated.

Since change is inevitable, as the Footprint platform evolves, we also perform this penetration testing whenever a major update is released.

Security Assurance Activity	**Frequency**
Vulnerability Scan	Major Version Release
Penetration Testing	Upon Request
Secure Code Review	Upon Request

Ongoing Monitoring:

Our engineers are continuously monitoring the platform for any performance, capacity, functional and security issues. Besides proactive security assurance, we ensure data privacy and transparency through our DPA which ensures our Security Incident Response Teams have a sound process to responding to operational risk including cyber-attacks as well as operational and security incidents that may lead to potential data breaches.

Our transparency policy covers full disclosure of any incidents in our ecosystem and therefore we allow anybody to access live our Support Portal located here: https://support.codaintelligence.com/

Securing Access to the Footprint Platform Hosted by Partners

When Footprint is hosted by our Partners, CODA is solely responsible to secure the Application's Code and access to Global CODA Services for the Partners.

The responsibility of securing the infrastructure where the Footprint platform is hosted, as well as Customer's data solely lies on the Partner that's hosting Footprint. In this situation, CODA's responsibilities are limited to the application code and binaries only. All responsibility regarding customer data backup and security lies with the Partner. Activities such as activating, managing and operating the Web Application Firewall, Security Operations Center, SSL Inspection, SSL Certificate Renewal, System, Network, Database and Cloud Hardening, Incident Response, Data Backup, Disaster Recovery, Business Continuity, High Availability, Identity and Access Management for the Infrastructure and the Footprint Platform itself, Internet Access Security, DNS Security are to be performed by the Partner.

CODA Footprint Architecture Reference