



COODA
AI-driven cyber risk insights

AI Driven Cyber Risk Insights

Product Overview
November 2020

Showcase actionable risk insights

Footprint offers Actionable Security Insights and correlation with Compliance & Cybersecurity Risks



Fully automated, AI-translated technical vulnerabilities into business risk insights.



Zero-day attack enhancement
Real risk exposure analytics
What-if predictions



Risk prioritization relevant to their business profile and compliance requirements. Progress monitoring & reporting.



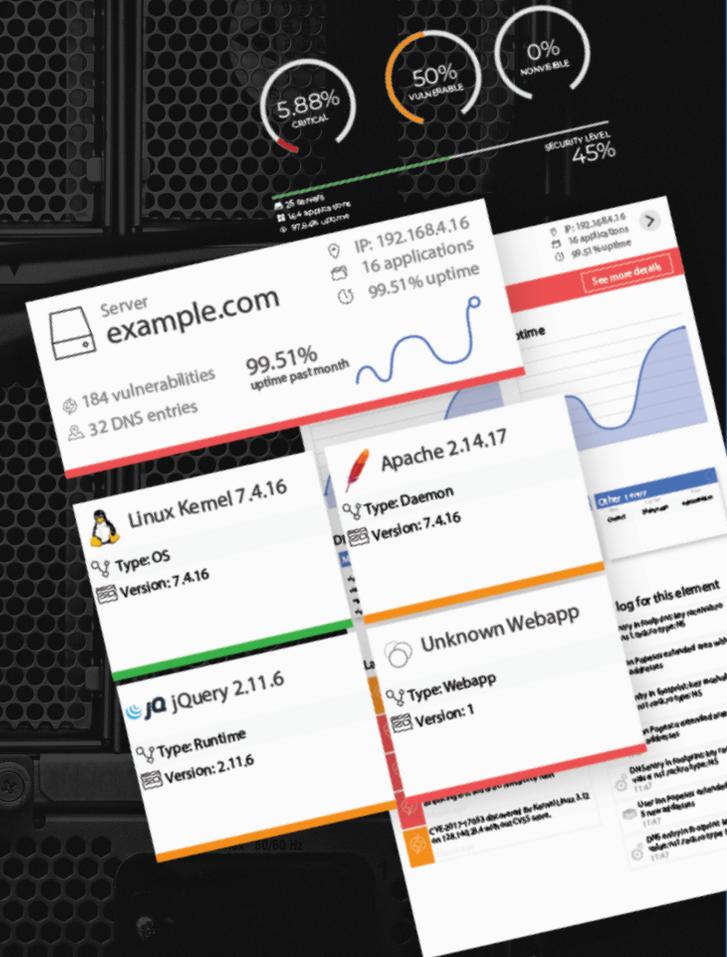
Easy to use, easy to understand. No technical staff required on Customer's side. Customer Executives can understand and act upon our reports.



Customers can receive Footprint as a fully-managed service or in a self-catered manner. They could choose to manage vulnerabilities themselves or have that done by professionals automatically.



24x7 continuous oversight
Realtime Alerts
Compliance Reports
SLA Reports
Live Dashboards



Manage your company's Cyber Footprint

Footprint helps you:



Bridge business expectations with cyber security operations



Consolidate Risk and Compliance Management



Identify known and unknown assets present in the network



Improve operational efficiency through automation and continuous monitoring



Evaluate your threat exposure and current attack surface



Widen your visibility into assets and track their evolution

Manage your company's Cyber Footprint

Footprint helps you:



Bridge business expectations with cyber security operations

Showcase Vulnerability Management benefits to both technical and business audiences

Automated stakeholders' dashboards and reports using Machine Learning

Streamlined decision making based on automatically translated technical vulnerability insights into business risk for upper management

Prioritization of risk based on both business and technical contexts mapped to your organization

Real-time feedback between business and operational teams

Manage your company's Cyber Footprint

Footprint helps you:



Identify known and unknown assets present in the network

Perpetual periodic scanning of configured scan surface (CIDR blocks, DNS, URLs, Hosts)

Automatic discovery of internal and external endpoints and services

Device, OS and Service fingerprinting (using blackbox agentless and whitebox agent-based techniques)

Automatic classification of identified applications and servers

Historical snapshot of identified assets

Identify rogue / shadow IT devices & services

Manage your company's Cyber Footprint

Footprint helps you:



Evaluate your threat exposure and current attack surface

Discover vulnerabilities based on known security databases (NIST, vendor-specific) correlated with threat intelligence information

Discover known service or application versions

Discover network visible common configuration errors

Assess vulnerability risk score and exploitability

Analyze exposure from external and internal attack postures

Manage your company's Cyber Footprint

Footprint helps you:



Consolidate Risk and Compliance Management

Automate compliance tracking with different Industry Standards

Assign Custom Business Impact for services and applications

Prioritize Patch Management based on business drivers and exploitability factors

Increase Risk and Compliance process maturity through Automated KPIs

Manage your company's Cyber Footprint

Footprint helps you:

 Improve operational efficiency
Through automation and
continuous monitoring

-  Track remediation and SLAs
-  *Integrate with Help Desk/ PSA
-  *Integrate with Log Management Solutions
-  * Provide SOC alerts and views through integrations with SOAR and SIEM
- Custom assignment of attack surface per Business Verticals
- Automated periodic reporting
-  Proactive and automatic notifications

Manage your company's Cyber Footprint

Footprint helps you:



Widen your visibility into assets and track their evolution

See what attackers can exploit from multiple postures

Analyze vulnerabilities by looking into Threat Feeds and IOCs

Monitor historic snapshots of known assets and services

Discover how configuration changes influence visibility of assets and services

Footprint Delivery Models

Compatible with two service delivery models



Fully Managed

In a fully managed setup, the partner performs all the heavy lifting and the customer only get tracks the results . The Partner is receiving and responding to alerts in order to fix the vulnerabilities according to the agreed Managed Services SLA with the End-User.



Self Service

Under this delivery model the customer manages their cyber risk and decides how to remediate and when to involve the partner by choosing to ask for help directly in the platform.

Footprint-enabled service operating under the NIST CyberSecurity Framework



Identify

Footprint automatically identifies software, hardware and business assets and correlates them using proprietary algorithms. The platform provides end-users with appropriate capabilities in terms of Governance, Risk Analysis and Risk Management Strategy.



Protect

Footprint automatically identifies and recommends missing cyber security controls. Platform covers Awareness & Training, Control Implementation & Maintenance, Processes & Procedures, etc.



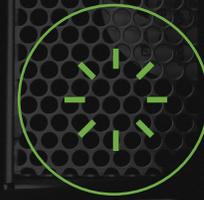
Recover

Recovery planning, Improvements and Communications all fall under the platform build in processes.



Detect

Footprint works with anomalies and events, provides continuous security monitoring and supports the detection process.



Respond

Footprint support its partners to provide response planning, analysis, mitigation, improvements and communication services to its customers.

Footprint-enabled service operating under the NIST CyberSecurity Framework



Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy



Protect

- Identity Management & Access Control
- Awareness & Training
- Data Security
- Information Protection Processes & Procedures
- Maintenance
- Protective Technology



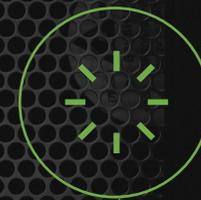
Recover

- Anomalies & Events
- Security Continuous Monitoring
- Detection Processes



Detect

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements



Respond

- Recovery Planning
- Improvements
- Communications

Legend

Footprint-Driven Function

Footprint Supported Function

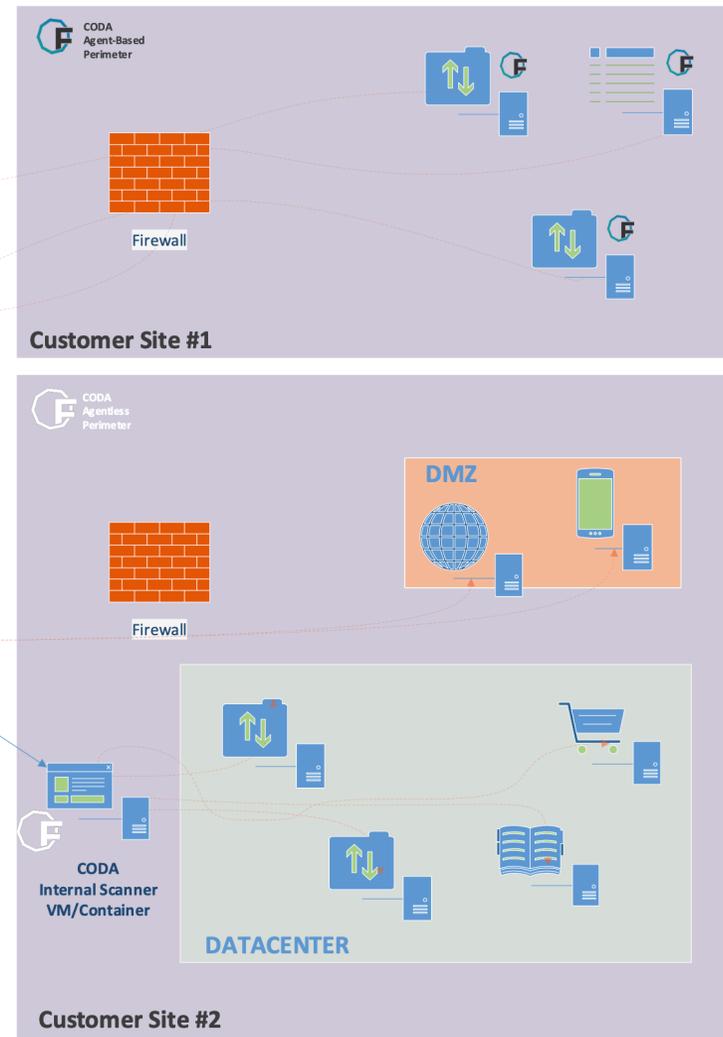
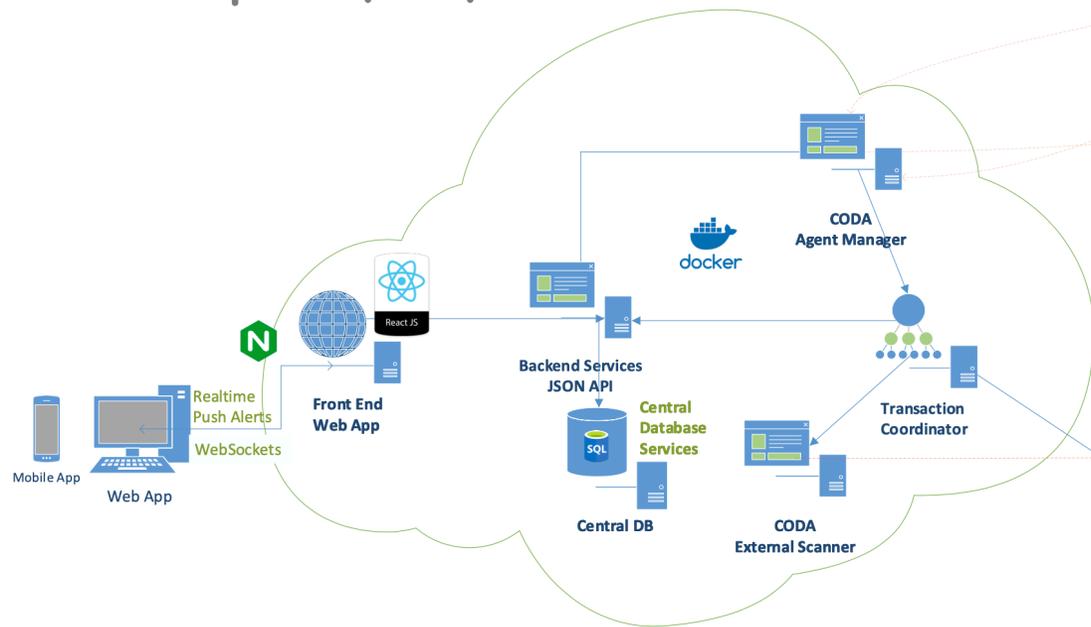
Manual Function

How does it work?



Footprint MSP Instance

OnPrem/Cloud/Hybrid



Agentless

Agent-Based

PROS

- Can be run from the outside or the inside of the organization
- Immediate results from the Cloud with zero effort to deploy
- No changes required to the existing landscape
- Multiple scanning perspectives

- Full device visibility as the agent runs in RING0 (SYSTEM/root privileges)
- Collects local metrics directly (processes, network connections, users, groups, services, scheduled tasks, etc.)
- Ability to scan other local devices

CONS

- TCP/IP connectivity is required
- Limited visibility into internal/DMZ assets (can be increased by deploying internal sensors)
- Limited vulnerability identification due to uncredentialed access

- Must be deployed on each endpoint (can be deployed on a single machine if an AD-integrated setup is chosen)
- Sometimes can't be deployed on locked systems (e.g. ICS/OT)
- Multiple agents on one machine (low overhead, AD-integrated alternative)

How does it work?

1. Build Your Initial Customer Footprint

2. Vulnerability Analysis

3. Reporting

4. Continuous Monitoring



Build Your Initial Customer Footprint

Start with any initial entry points such as IP address ranges (CIDR format), public exposed URLs or FQDNs, domain names, email addresses, or any other DNS entries.

We will discover any related assets using reconnaissance algorithms such as DNS probing, WHOIS queries, web crawling and port scanning. Newly discovered assets will be suggested to be added to your Customer Footprint. We will only scan assets in your Footprint.

How does it work?

1. Build Your Initial Customer Footprint
2. Vulnerability Analysis
3. Reporting
4. Continuous Monitoring



Vulnerability Analysis

Immediately after adding an asset to your Customer Footprint we will start scanning it using multiple techniques and scan engines. After port scanning open ports will be scanned for running apps and then specific exploit payloads will be ran against the specific service. This includes OS detection, Service Detection, SSL checks, authentication checks, CVE exploitation, CCE discovery, etc. Once new apps are identified they will be added to your CF. Internal Scanners (VM/Docker Appliance) or Dedicated Software Agents (Installed on the machine or inside an AD) can be deployed to gain more visibility into internal assets.

How does it work?

1. Build Your Initial Customer Footprint

2. Vulnerability Analysis

3. Reporting

4. Continuous Monitoring



Reporting

Technical and Business Contexts are generated automatically by grouping applications based on their purpose in the Customer's Organization. Manual contexts can also be created by Administrators. Custom Business Impacts can be influenced based on customer's BIA in order to influence risk impact. Risk impact is also influenced by Threat Intelligence information such as public exploits in the wild targeting an identified vulnerability. CVR (Customer Vulnerability Reports) cover both Business and Technical relevant information.

How does it work?

1. Build Your Initial Customer Footprint

2. Vulnerability Analysis

3. Reporting

4. Continuous Monitoring



Continuous Monitoring

Scanning jobs will run automatically according to the predefined schedule. Administrators can customize how default scans are being run (which ports are affected and how often a scan is run). Customer Vulnerability Reports (CVRs) are automatically updated once a change is detected in the Customer's Footprint. Users can subscribe to notifications for new vulnerabilities or periodic updates with a specific frequency.

A footprint update can be generated by an update in the global threat feed (such as a new CVE on the existing Footprint) or an update inside the Customer's Footprint itself: such as a new open port inside the firewall, an application update fixing an already-identified vulnerability or generating a new one.

Product Roadmap

Footprint v5 RELEASED

- 📄 Agent-based & Agentless scan engine
- 📄 Uncredentialed Remote Scanning
- 📄 Webapp Scan
- ➔ Online Trial Available
- 📄 Threat Intelligence
- 📄 Business Impact
- 📄 Business View
- 📄 Technical Context

Footprint v6 Q4 2020

- 📄 SSL Checks
- 📄 Integration with 3rd Party Vulnerability Scanners
- ➔ MSP Partner Portal
- ➔ M365 SSO
- 📄 Instant Provisioning for MSPs

Footprint v7 Q1 2021

- ➔ Credentialed Remote Scanning
- 📄 Advanced Webapp Scanning
- 📄 Linux Agent
- 📄 Attack Replay
- 📄 Online Identity Profiling

Footprint v8 Q2 2021

- 📄 Integrations with Service Desk
- 📄 Integrations with Log Management
- 📄 Integrations with CMDB
- 📄 Active Directory Checks
- ➔ VRM Report for Compliance and 3rd parties
- 📄 macOS Agent
- 📄 Vulnerability Evolution

Footprint v9 Q3 2021

- 📄 Native Cloud Integrations
- 📄 Native Virtualization Check
- 📄 Assess Containers
- 📄 What-If Scenarios
- 📄 Most painful/probable attack
- 📄 Assess Apps under development
- ➔ Open API
- ➔ Footprint Mobile App
- 📄 Browser Checks
- 📄 IPv6 Coverage
- 📄 Spear Phishing

We're also working on

- 📄 Network Config assessment
- 📄 Zero-day Risk Analyzer
- ➔ Vulnerability Predictions
- 📄 Integrations with NAC
- 📄 Virtual Patching
- 📄 Community Checks
- ➔ SSO
- ➔ Data Scanning

- ➔ Continuous Monitoring
- ➔ Easy deployment
- ➔ Fully on-prem and on-cloud available
- ➔ Cloud scan
- ➔ User Management
- 📄 MSP Administration Page
- ➔ Customer Vulnerability Report
- 📄 AI-Engine for Contextual Risk Scoring

Legend 📄 Vulnerability Enumeration & Asset Management 📄 Patch Prioritization ➔ Reporting Capabilities 📄 SOC Integration ➔ Solution Usage

Q&A