CODA

AI-driven cyber risk insights

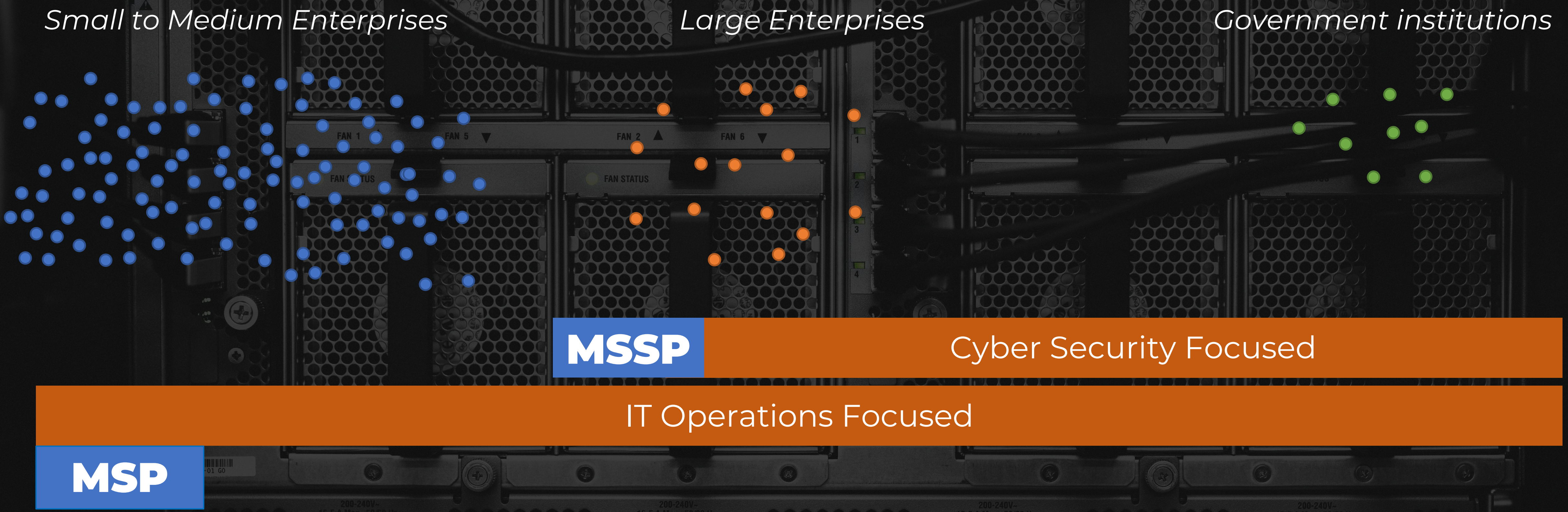
Footprint

AI-Driven Managed Security Services for Managed Service Providers

Product Presentation

October 2020

The world as we know it



Small to Medium Enterprises

Large Enterprises

Government institutions

MSSP Cyber Security Focused

IT Operations Focused

MSP

We’re not protected but we think we are

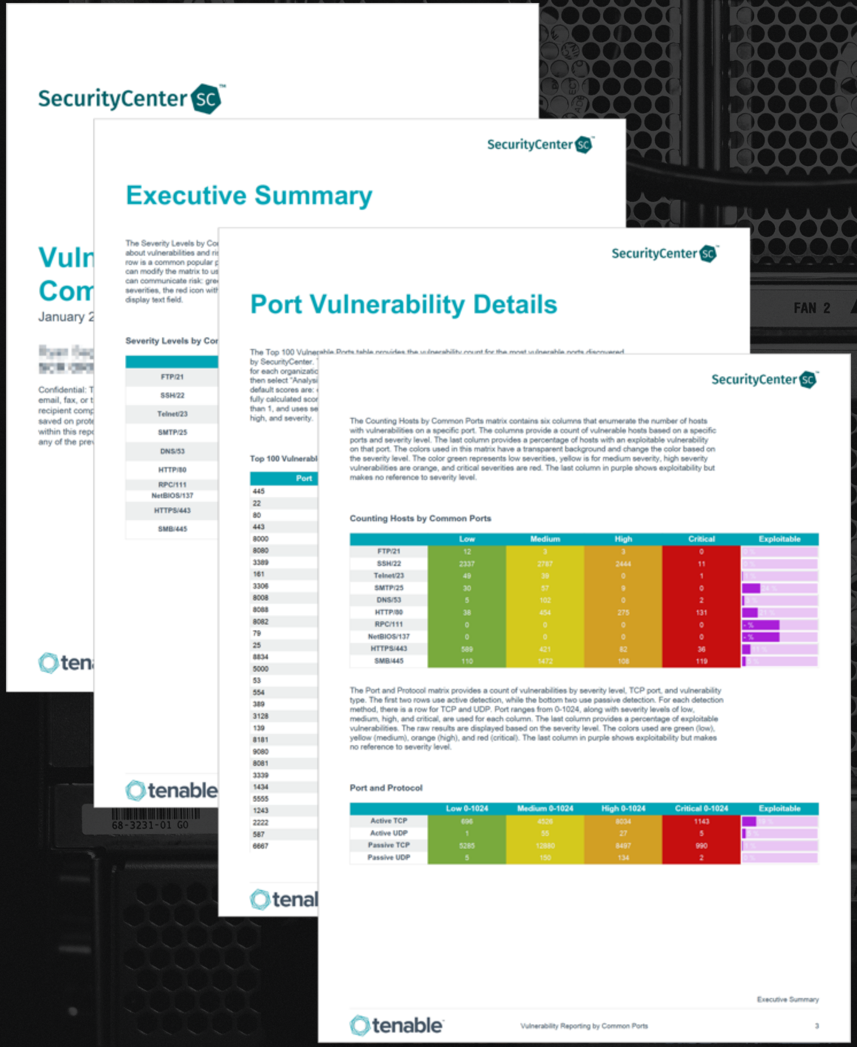
4M USD

Cost/breach

280 days

to isolate

Cybersecurity is a big data problem



SecurityCenter

Executive Summary

Port Vulnerability Details

The Counting Hosts by Common Ports matrix contains six columns that enumerate the number of hosts with vulnerabilities on a specific port. The columns provide a count of vulnerable hosts based on a specific ports and severity level. The last column provides a percentage of hosts with an exploitable vulnerability on that port. The colors used in this matrix have a transparent background and change the color based on the severity level. The color green represents low severities, yellow is for medium severity, high severity vulnerabilities are orange, and critical severities are red. The last column in purple shows exploitability but makes no reference to severity level.

Counting Hosts by Common Ports

	Low	Medium	High	Critical	Exploitable
FTP/21	12	3	3	0	0 %
SSH/22	2337	2787	2444	11	0 %
Telnet/23	49	39	0	1	1 %
SMTP/25	30	57	9	0	24 %
DNS/53	5	102	0	2	3 %
HTTP/80	38	454	275	131	21 %
RPC/111	0	0	0	0	- %
NetBIOS/137	0	0	0	0	- %
HTTPS/443	589	421	82	36	11 %
SMB/445	110	1472	108	119	5 %

The Port and Protocol matrix provides a count of vulnerabilities by severity level, TCP port, and vulnerability type. The first two rows use active detection, while the bottom two use passive detection. For each detection method, there is a row for TCP and UDP. Port ranges from 0-1024, along with severity levels of low, medium, high, and critical, are used for each column. The last column provides a percentage of exploitable vulnerabilities. The raw results are displayed based on the severity level. The colors used are green (low), yellow (medium), orange (high), and red (critical). The last column in purple shows exploitability but makes no reference to severity level.

Port and Protocol

	Low 0-1024	Medium 0-1024	High 0-1024	Critical 0-1024	Exploitable
Active TCP	696	4526	8034	1143	19 %
Active UDP	1	55	27	5	5 %
Passive TCP	5285	12880	8497	990	1 %
Passive UDP	5	150	134	2	0 %

Executive Summary

tenable   Vulnerability Reporting by Common Ports   3

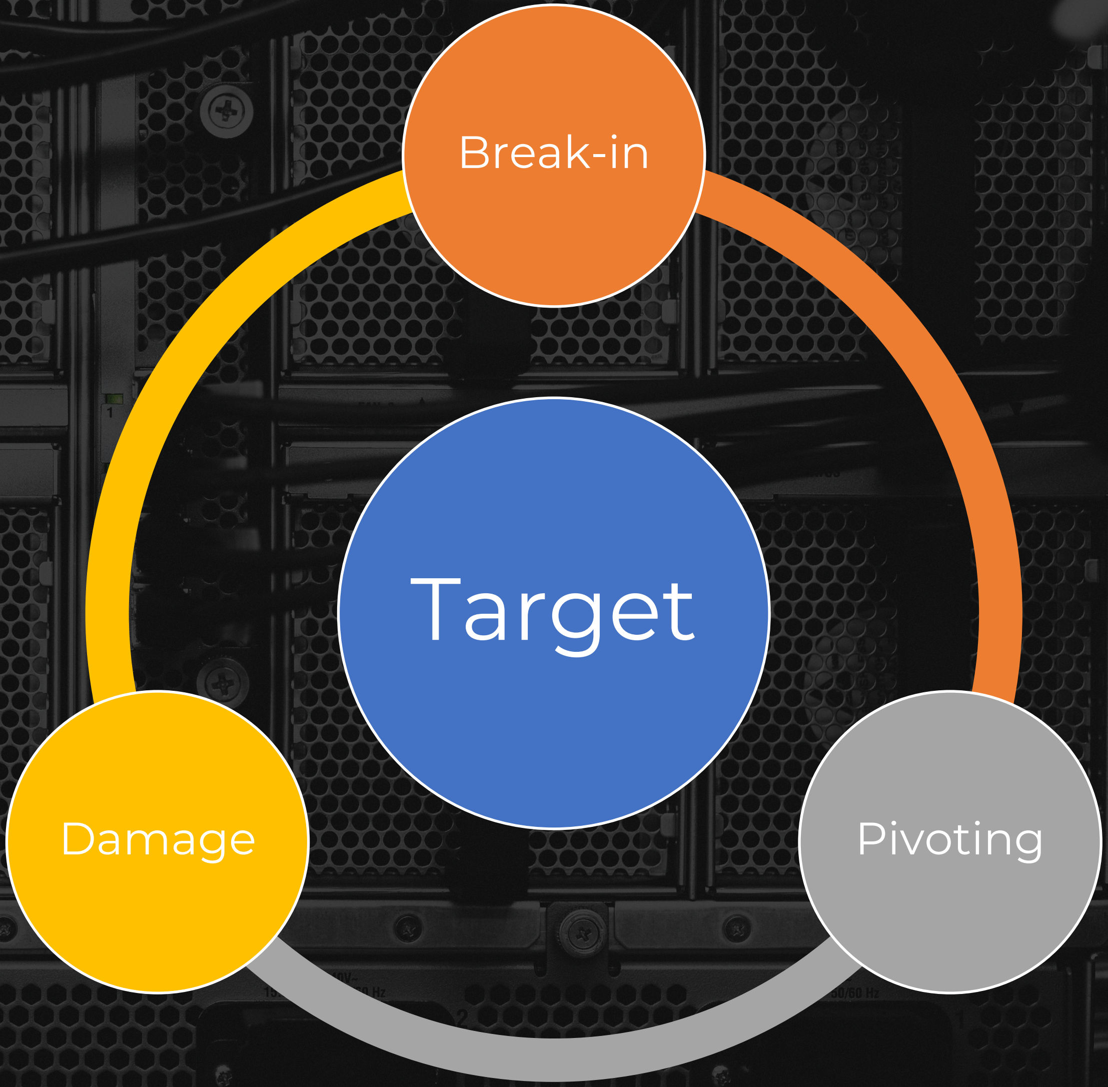
- Avg. 10K vulnerabilities in on 600 assets - where to start?
- Patch management is delayed and ineffective
- Avg. MTTP is between 60 and 150 days
- Large disconnects between functional teams (IT/ cyber/ business/risk)

CODA
AI-driven cyber risk insights

Footprint

The anatomy of an attack

Even a simple ransomware exploits at least 3 vulns.



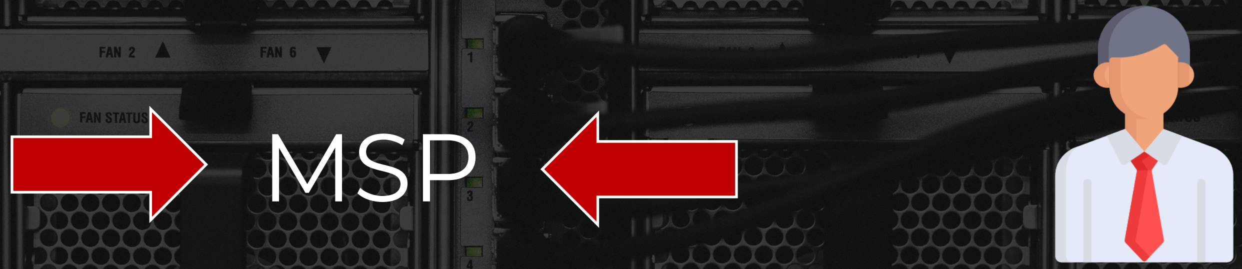
MSPs are called to act on cybersecurity but they don’t have the resources

84%

who do not use an MSP would consider using one if they offered the “right” cyber security solution

93%

would consider moving to a new MSP if they offered the “right” cyber security solution, even if they weren’t planning to change



MSP

Missing security headcount
Raising from 1.8M to 3.5M in 2021

“Underserved and Unprepared: The State of SMB Cyber Security in 2019” By: Vanson Bourne

Due to the cyber skills gap

MSPs cannot deliver cyber security services to the large amount of existing and new customers.

Implementing enterprise cyber technology in the SMB market is not feasible.

Using enterprise technology to deliver managed security services to the SMB market is not financially sustainable.

MSPs require dedicated solutions to win this battle.

What an MSP is expected to provide

1. Complete visibility
2. Business context
3. Technical context
4. Cyber context
5. Actionable risk insights
6. Remediation results

Footprint enables you to deliver all the above with its built-in automation and integrations with zero upfront investment and engineering overhead.

Introducing Footprint

Automating and Scaling Vulnerability Management Services for Managed Services Providers (MSP)

Increase Brand Awareness
Fully white labeled, running under your domain, your logo.
Run your own sales campaigns.

Boost presales
Using Footprint you can access new customers through our Online Funnel (Self-Service Registration). Automated presales and lead generation.
Preliminary Check-up

Our AI Engine leverages current staff into a Cyber Ops Team
Leverage security services using your existing team.
You don't have to hire any ethical hacking experts.
Natively integrated with all your sales and engineering platforms.

Increase Recurring Revenue
New revenue streams: compliance/cyber assurance, managed security services
Boost sales of existing products & services through customer awareness

Increase Customer Retention
Showcase value to customers with Security Posture Monitoring, with recurrent automated reports.
Provide Customers with real-time alerts, dashboards and relevant SLA, Risk Reports and Remediation Plans.

Footprint v6 **is Available Right Now through our Partner Program!**

CODA
AI-driven *cyber risk insights*

Footprint

Introducing Footprint

Automating and Scaling Vulnerability Management Services for Managed Services Providers (MSP)

Fully Multi-Tenant

Manage all Customers using the same UX for your engineers, finance, sales, presales and support teams.

Zero-Touch & Instant Provisioning

Easy installation and operation
Platform is provisioned for MSPs in the next business day after signing the partnership agreement.

Comprehensive Scanning Engines

Agentless and Agent-Based Scan Engines.
Decisions based on Machine Learning and Threat Intelligence Correlations.
Flexible deployment models for Customers – internal & external scans.

Cloud Agnostic

Running in the MSPs cloud of choice: AWS, Azure, GCP, Oracle Cloud, your Private Cloud or CODA Cloud. MSPs own all data.

Native Integration

With MSP dedicated tools: PSM, RMM, SIEM, etc.

Footprint v6 **is Available Right Now through our Partner Program!**

MSP Delivery Models

MSPs can deliver services in 2 delivery models towards end users

Fully Managed

In a fully managed setup, the MSP performs all the heavy lifting and your customers only get the results. MSPs are receiving and responding to alerts in order to fix the vulnerabilities according to their Managed Services SLA with the End-Users.

Self Service

Under this delivery model end customers manage their cyber risk and decide how to fix them and when to involve MSPs in remediation by choosing to ask for help directly in the platform. MSPs can then assemble their action plan.

Drive more revenue with CODA Footprint

We enable multiple revenue streams for our MSPs

Generate New Business

Become one of our tiered partners and earn up to 40% margins on product sales.

Add your value-added services on-top of Footprint.

Get more customers online by using our demo and trial features to acquire new clients.

Generate Cloud Consumption

All cloud consumption will be reported under your name.

Be it AWS, Azure, GCP, Oracle Cloud or any other public or private cloud of your choice.

Run it in CODA's Cloud if you prefer a fully managed instance.

Deliver More Services

Footprint creates the business case for new .

Leverage Footprint to deliver fully managed VRM services to your Customers.

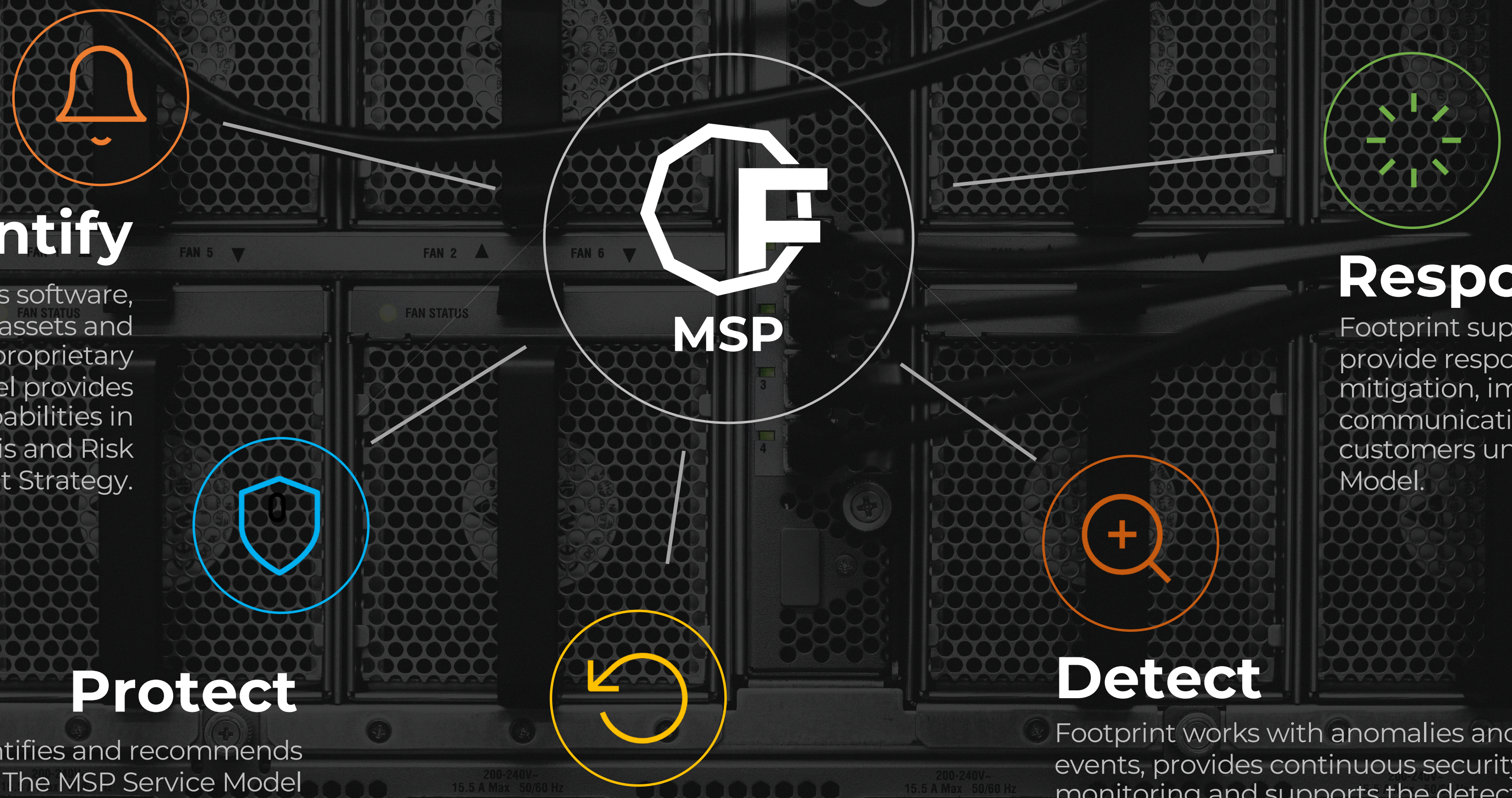
Smoothly upgrade your team's cyber skills with CODA as part of our Partner Enablement Program.

Upsell / Cross-Sell Security Products

Increase Customer awareness allows you to deliver more Professional and/or Managed services towards them.

Ability to drive online sales through our Funnel uniquely positions you towards new potential Customers on your entire service portfolio.

Footprint enables 360° MSP AI-Driven SOC



Identify

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

Respond

Footprint support its partners to provide response planning, analysis, mitigation, improvements and communication services to its customers under the MSP Service Model.

Protect

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

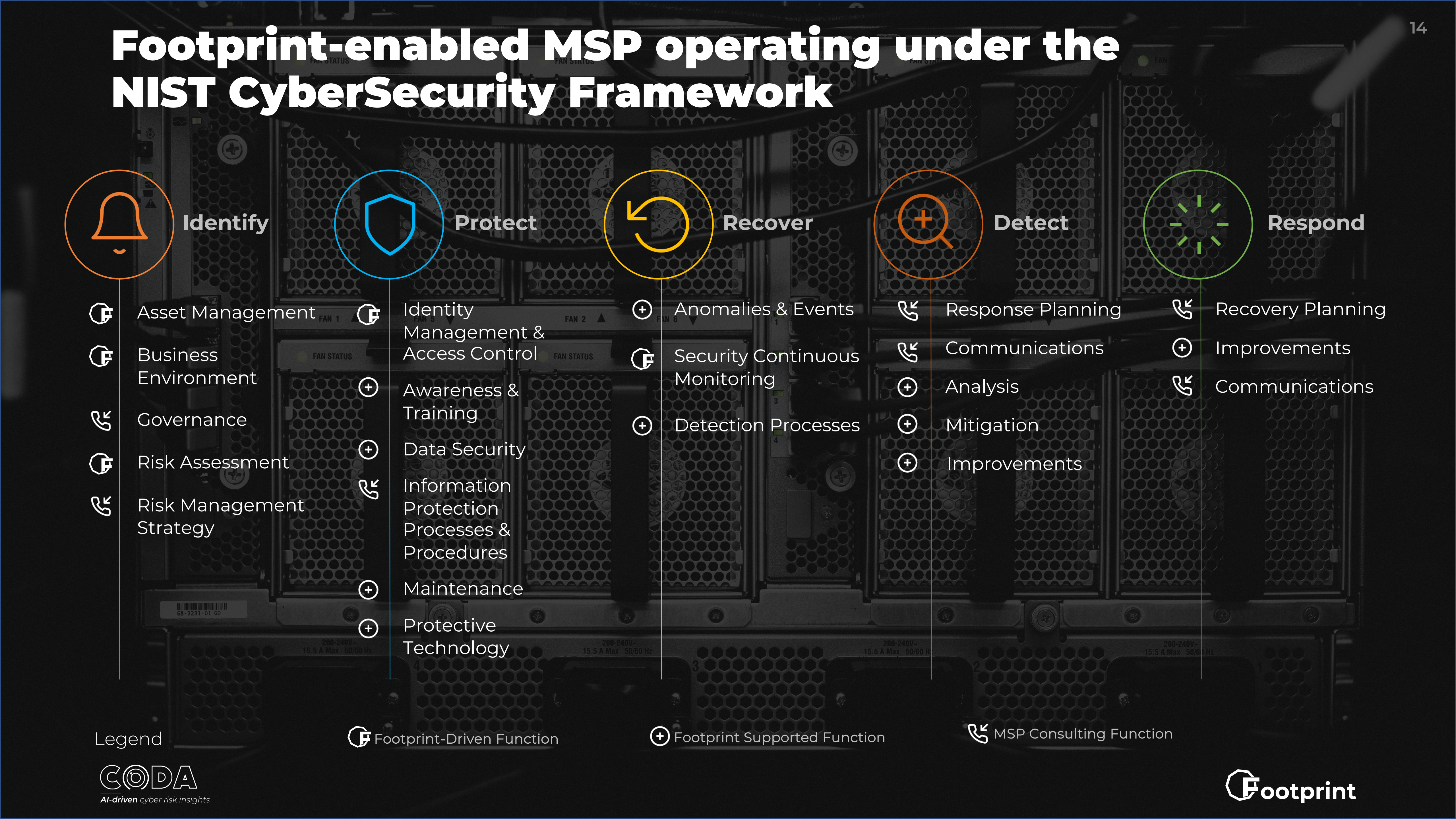
Detect

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

Recover

Recovery planning, Improvements and Communications all fall under the MSP Service Model.

Footprint-enabled MSP 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

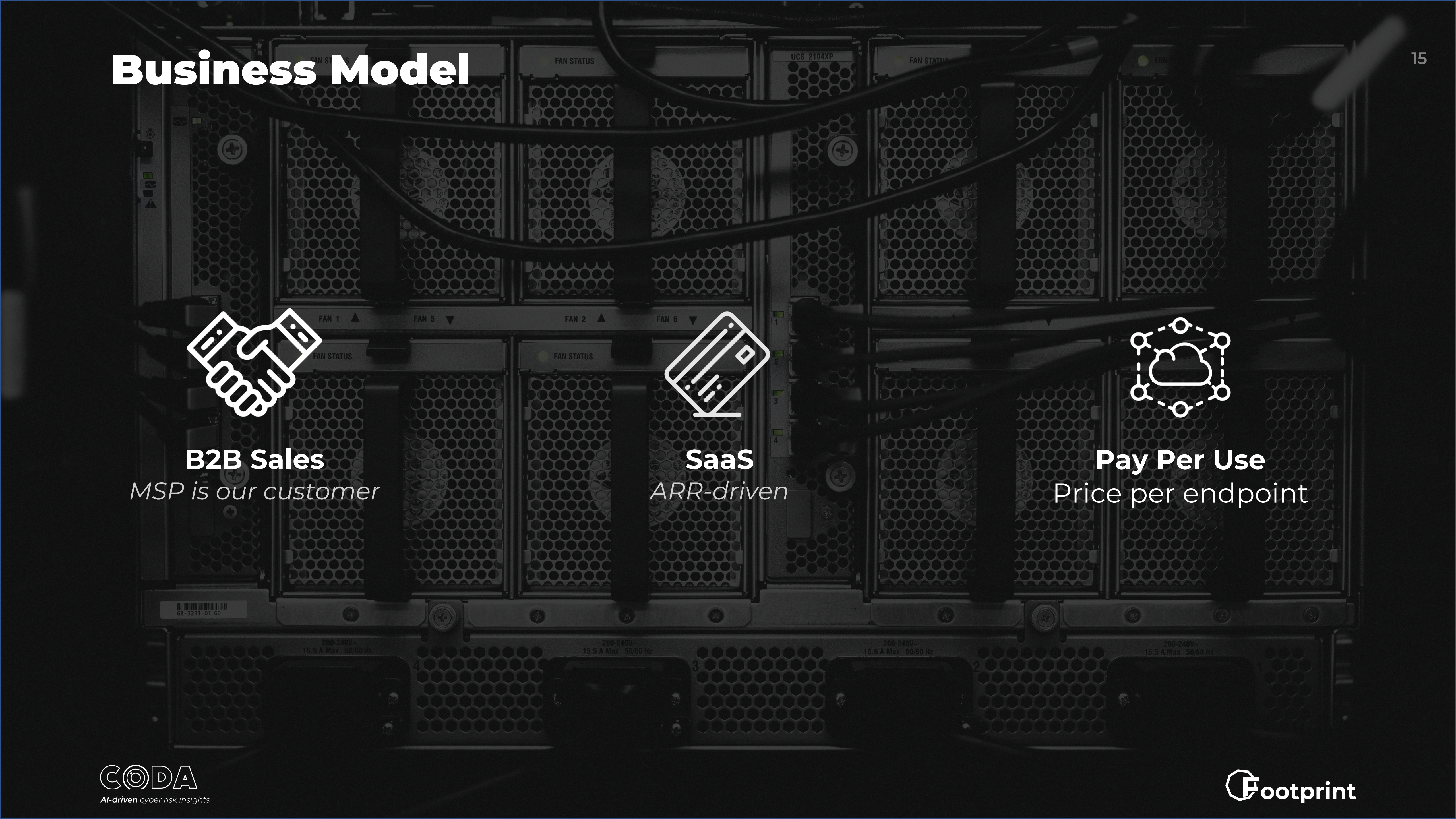
☎ MSP Consulting Function

CODA

AI-driven cyber risk insights

Footprint

Business Model



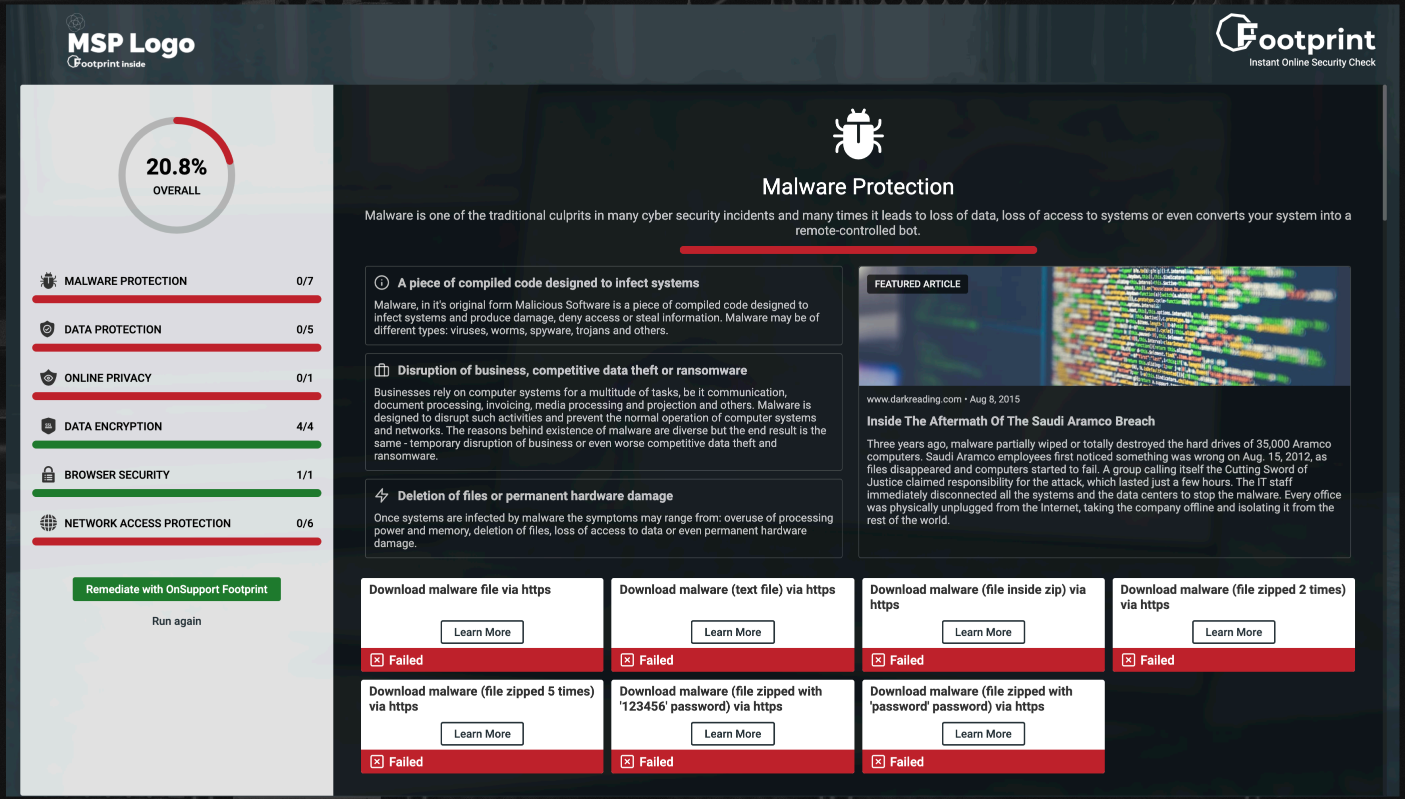
B2B Sales
MSP is our customer

SaaS
ARR-driven

Pay Per Use
Price per endpoint

Fingerprint Network Edge Report

- Just point your customers to https://yourinstance/checkup
- It takes 15 seconds, it’s fully automated and it’s free
- Showcase the vulnerabilities their current Internet connection has (malware, data exfiltration, encryption, browser security, network access protection)
- Make them understand the risks



MSP Logo
Footprint inside

Footprint
Instant Online Security Check

20.8%
OVERALL

MALWARE PROTECTION	0/7
DATA PROTECTION	0/5
ONLINE PRIVACY	0/1
DATA ENCRYPTION	4/4
BROWSER SECURITY	1/1
NETWORK ACCESS PROTECTION	0/6

Remediate with OnSupport Footprint

Run again

Malware Protection

Malware is one of the traditional culprits in many cyber security incidents and many times it leads to loss of data, loss of access to systems or even converts your system into a remote-controlled bot.

A piece of compiled code designed to infect systems

Malware, in it's original form Malicious Software is a piece of compiled code designed to infect systems and produce damage, deny access or steal information. Malware may be of different types: viruses, worms, spyware, trojans and others.

Disruption of business, competitive data theft or ransomware

Businesses rely on computer systems for a multitude of tasks, be it communication, document processing, invoicing, media processing and projection and others. Malware is designed to disrupt such activities and prevent the normal operation of computer systems and networks. The reasons behind existence of malware are diverse but the end result is the same - temporary disruption of business or even worse competitive data theft and ransomware.

Deletion of files or permanent hardware damage

Once systems are infected by malware the symptoms may range from: overuse of processing power and memory, deletion of files, loss of access to data or even permanent hardware damage.

FEATURED ARTICLE

www.darkreading.com • Aug 8, 2015

Inside The Aftermath Of The Saudi Aramco Breach

Three years ago, malware partially wiped or totally destroyed the hard drives of 35,000 Aramco computers. Saudi Aramco employees first noticed something was wrong on Aug. 15, 2012, as files disappeared and computers started to fail. A group calling itself the Cutting Sword of Justice claimed responsibility for the attack, which lasted just a few hours. The IT staff immediately disconnected all the systems and the data centers to stop the malware. Every office was physically unplugged from the Internet, taking the company offline and isolating it from the rest of the world.

Download malware file via https
Learn More
☒ Failed

Download malware (text file) via https
Learn More
☒ Failed

Download malware (file inside zip) via https
Learn More
☒ Failed

Download malware (file zipped 2 times) via https
Learn More
☒ Failed

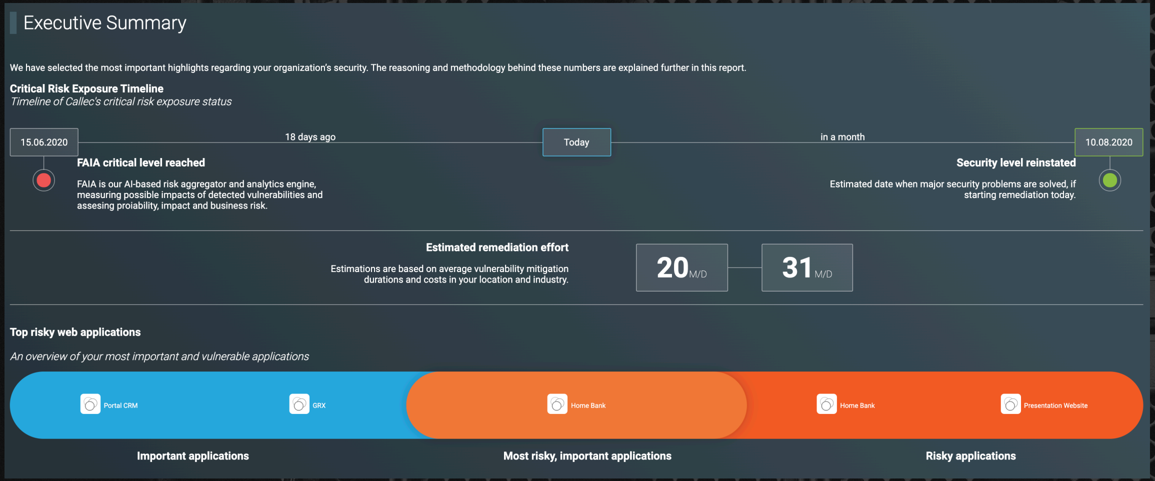
Download malware (file zipped 5 times) via https
Learn More
☒ Failed

Download malware (file zipped with '123456' password) via https
Learn More
☒ Failed

Download malware (file zipped with 'password' password) via https
Learn More
☒ Failed

- Propose the proper remediation solutions and products (NGFW, IPS, DLP, SSL Inspection, Sandboxing, etc)

Footprint Customer Vulnerability Report



Executive Summary

We have selected the most important highlights regarding your organization's security. The reasoning and methodology behind these numbers are explained further in this report.

Critical Risk Exposure Timeline

Timeline of Callec's critical risk exposure status

15.06.2020 — 18 days ago — Today — in a month — 10.08.2020

FAIA critical level reached

FAIA is our AI-based risk aggregator and analytics engine, measuring possible impacts of detected vulnerabilities and assesing proiability, impact and business risk.

Security level reinstated

Estimated date when major security problems are solved, if starting remediation today.

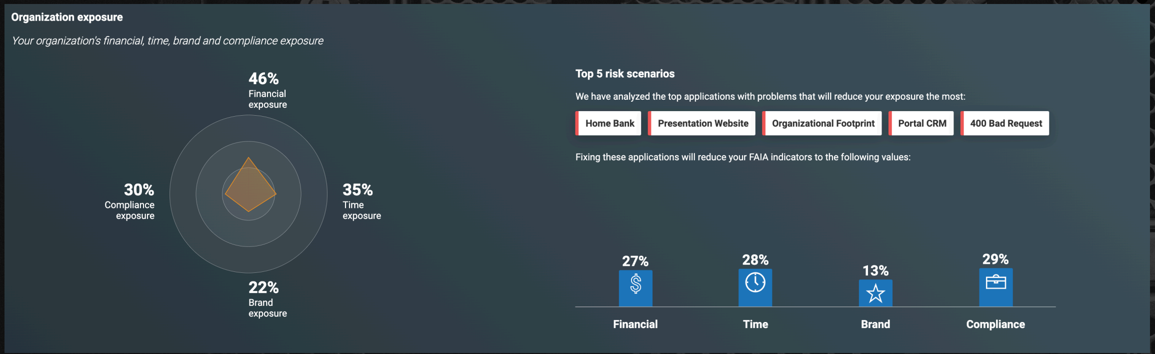
Estimated remediation effort

Estimations are based on average vulnerability mitigation durations and costs in your location and industry.

20 M/D — 31 M/D

Top risky web applications

An overview of your most important and vulnerable applications



Organization exposure

Your organization's financial, time, brand and compliance exposure

Top 5 risk scenarios

We have analyzed the top applications with problems that will reduce your exposure the most:

Home Bank | Presentation Website | Organizational Footprint | Portal CRM | 400 Bad Request

Fixing these applications will reduce your FAIA indicators to the following values:

Deep, comprehensive vulnerability report

Agentless, agent-based or hybrid

Showcase the vulnerabilities in their current IT landscape (cloud, or on-prem: workstations, servers, mobile devices, etc.)

Correlated with personalized business impact and real-world threat intelligence

Make them understand the risks

Propose the proper remediation solutions and products (managed patching, HW/SW upgrades, migrations, etc.)

Showcase and measure compliance and progress in time

Executive Summary translated for non-technical

FAN STATUS
FAN STATUS
UCS 2104XP
FAN STATUS
FAN 1
FAN 5
FAN 2
FAN 6
FAN STATUS
FAN STATUS
68-3231-01 G0
200-240V~ 15.5 A Max 50/60 Hz
200-240V~ 15.5 A Max 50/60 Hz
200-240V~ 15.5 A Max 50/60 Hz
200-240V~ 15.5 A Max 50/60 Hz

www.codaintelligence.com

CODA

***AI-driven** cyber risk insights*

Footprint