CODA

AI-driven cyber risk insights

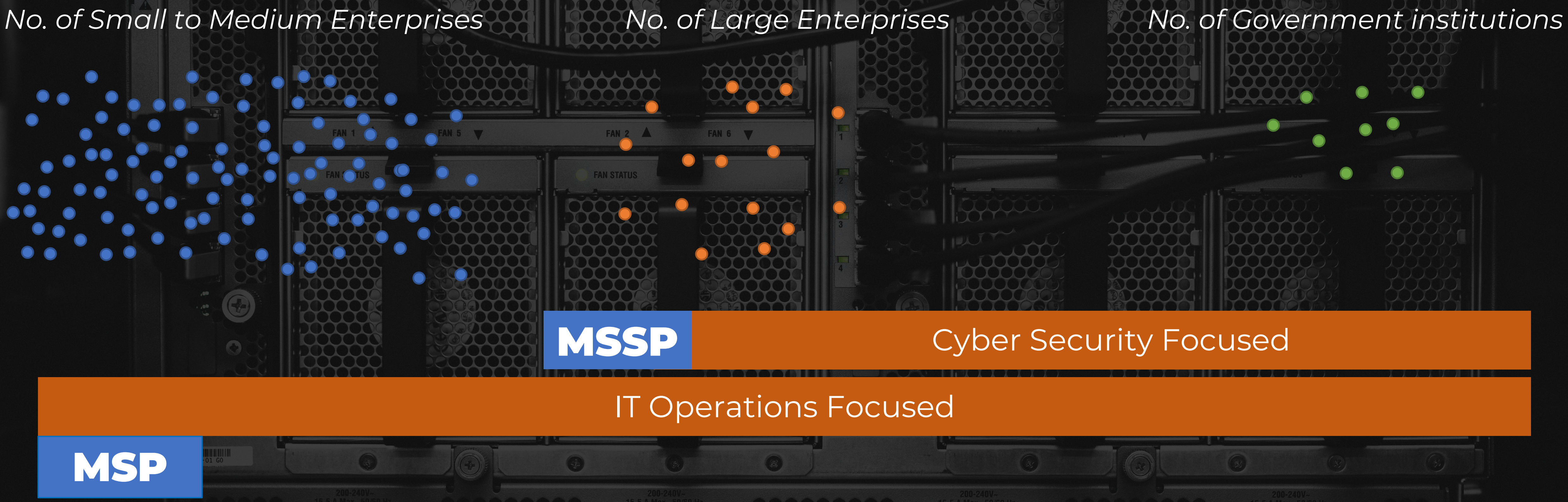
Footprint

AI-Driven Managed Security Services for Managed Service Providers

Product Presentation

October 2020

The world as we know it



No. of Small to Medium Enterprises

No. of Large Enterprises

No. of Government institutions

MSSP

Cyber Security Focused

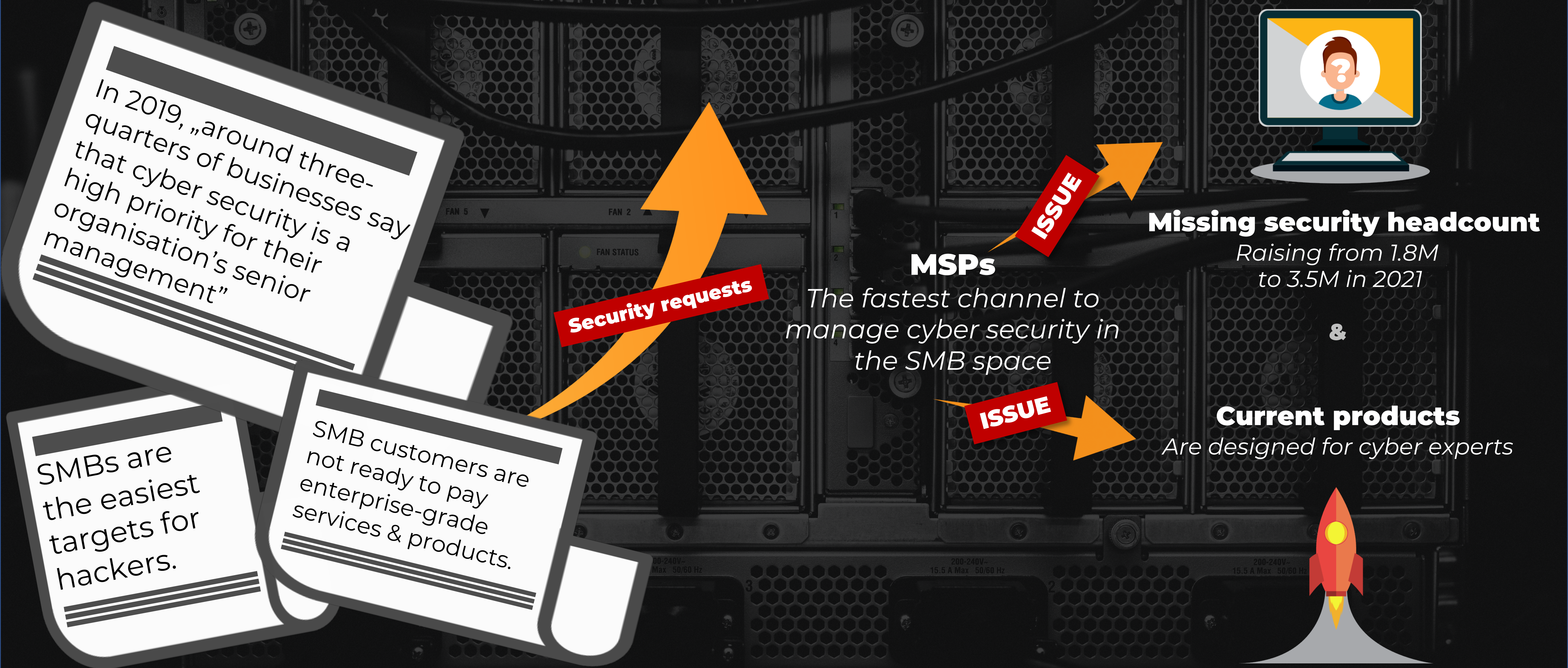
IT Operations Focused

MSP

CODA
AI-driven cyber risk insights

Footprint

The problem



In 2019, „around three-quarters of businesses say that cyber security is a high priority for their organisation's senior management"

SMBs are the easiest targets for hackers.

SMB customers are not ready to pay enterprise-grade services & products.

MSPs
The fastest channel to manage cyber security in the SMB space

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

&

Current products
Are designed for cyber experts

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.

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.

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

Boost presales

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

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.

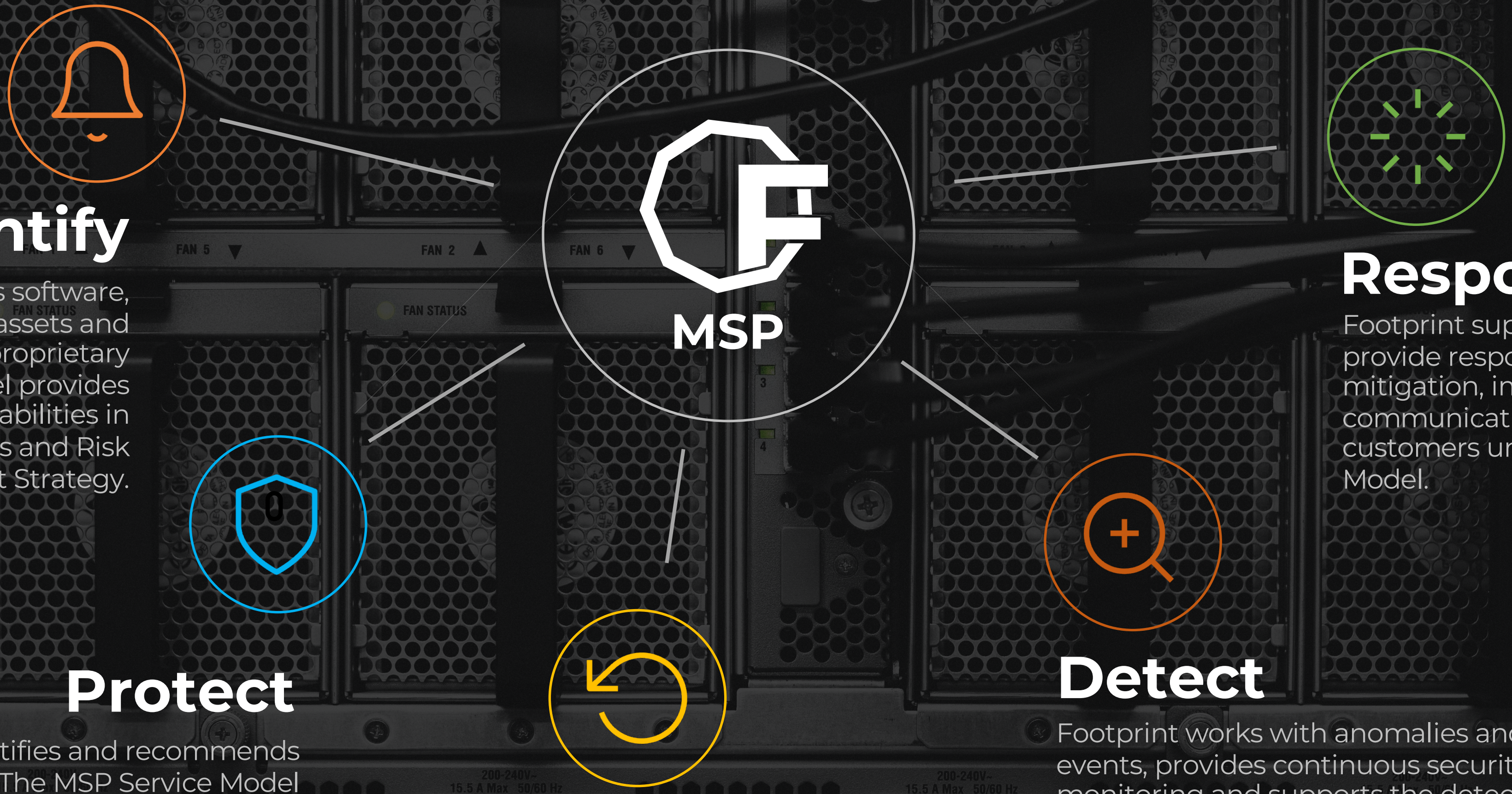
Smoothly upgrade your team's cyber skills with CODA as part of our Partner Enablement Program.

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.

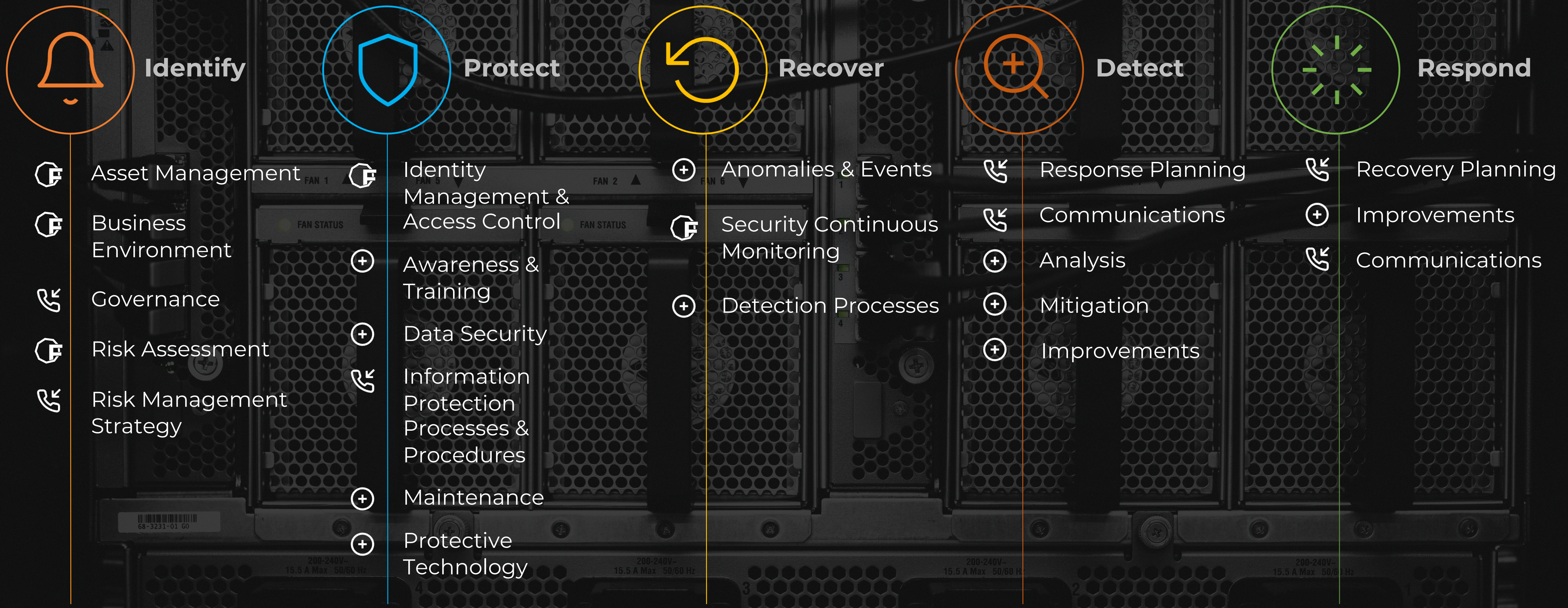
Detect

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

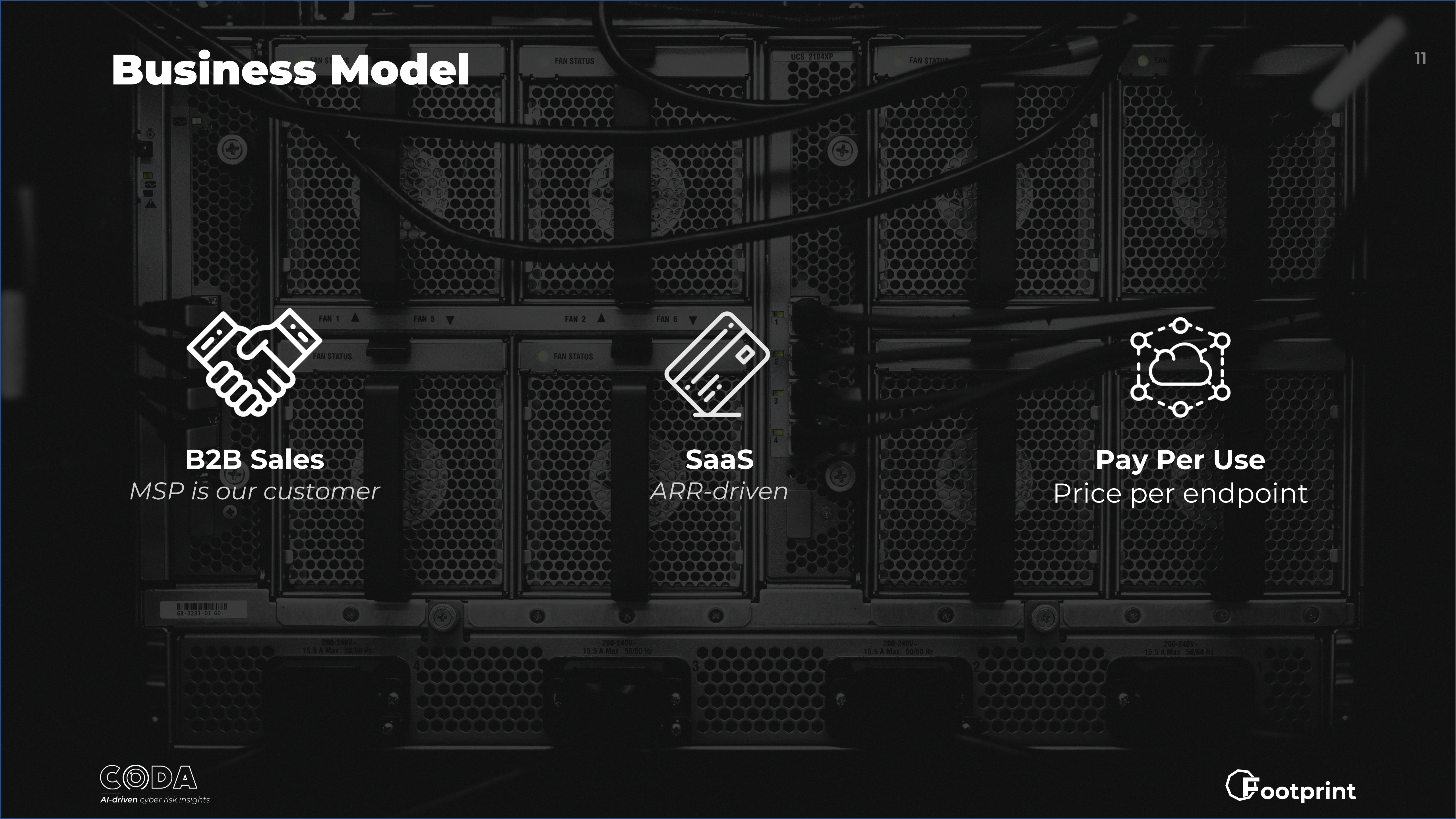
Legend

Ⓕ 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

Competitive environment

Major players in the market target the enterprise segment.

Their products are complex, hard to implement and maintain and require advanced cyber skills to work with.

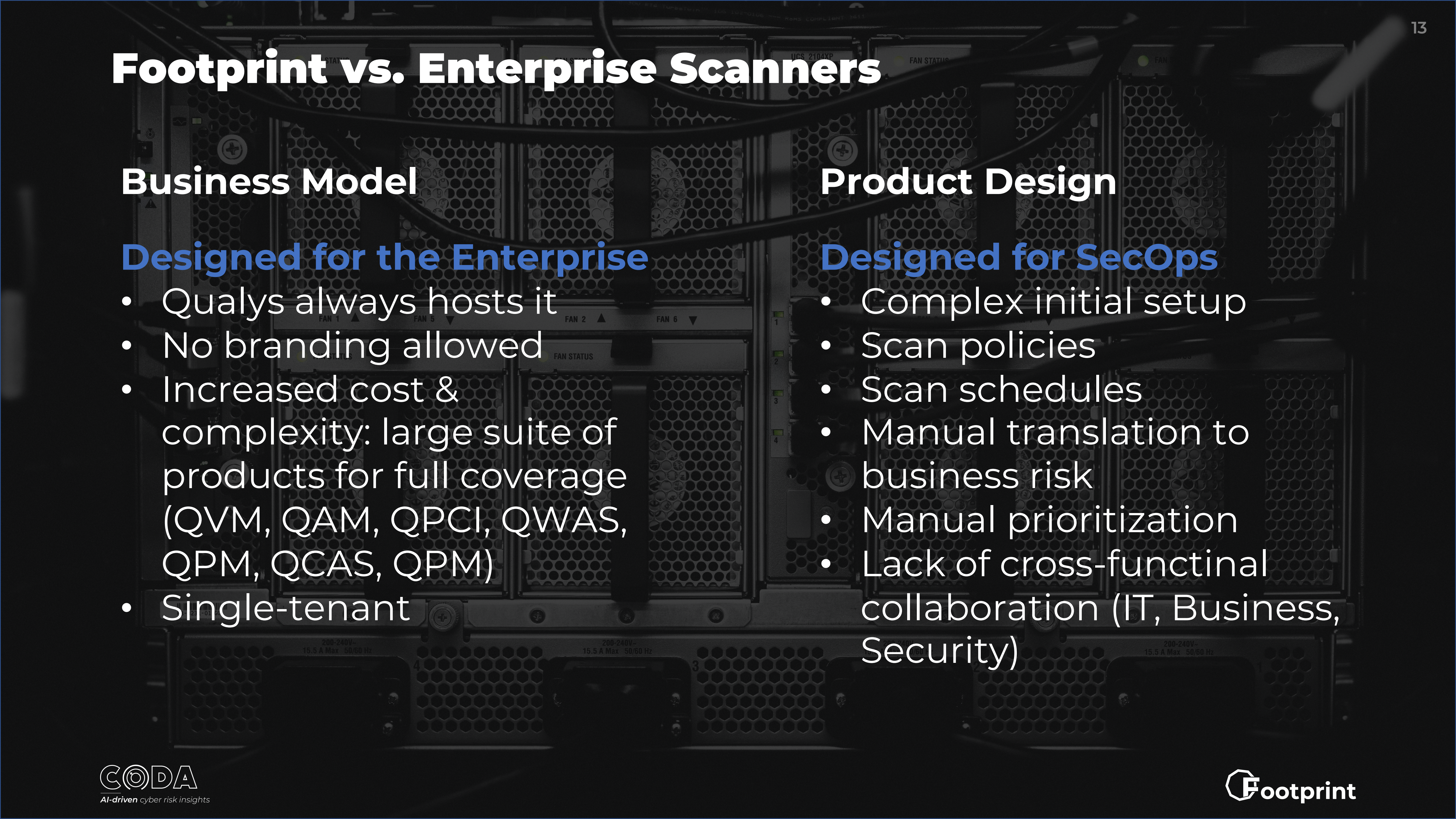
Reports must be created by dedicated analysts.
Alerts must be filtered and manually curated.

Their business model is not friendly for MSPs (single tenant, hosted by the vendor, lack of branding capabilities, etc.)

RAPID7

Qualys®

tenable™



Footprint vs. Enterprise Scanners

Business Model

Designed for the Enterprise

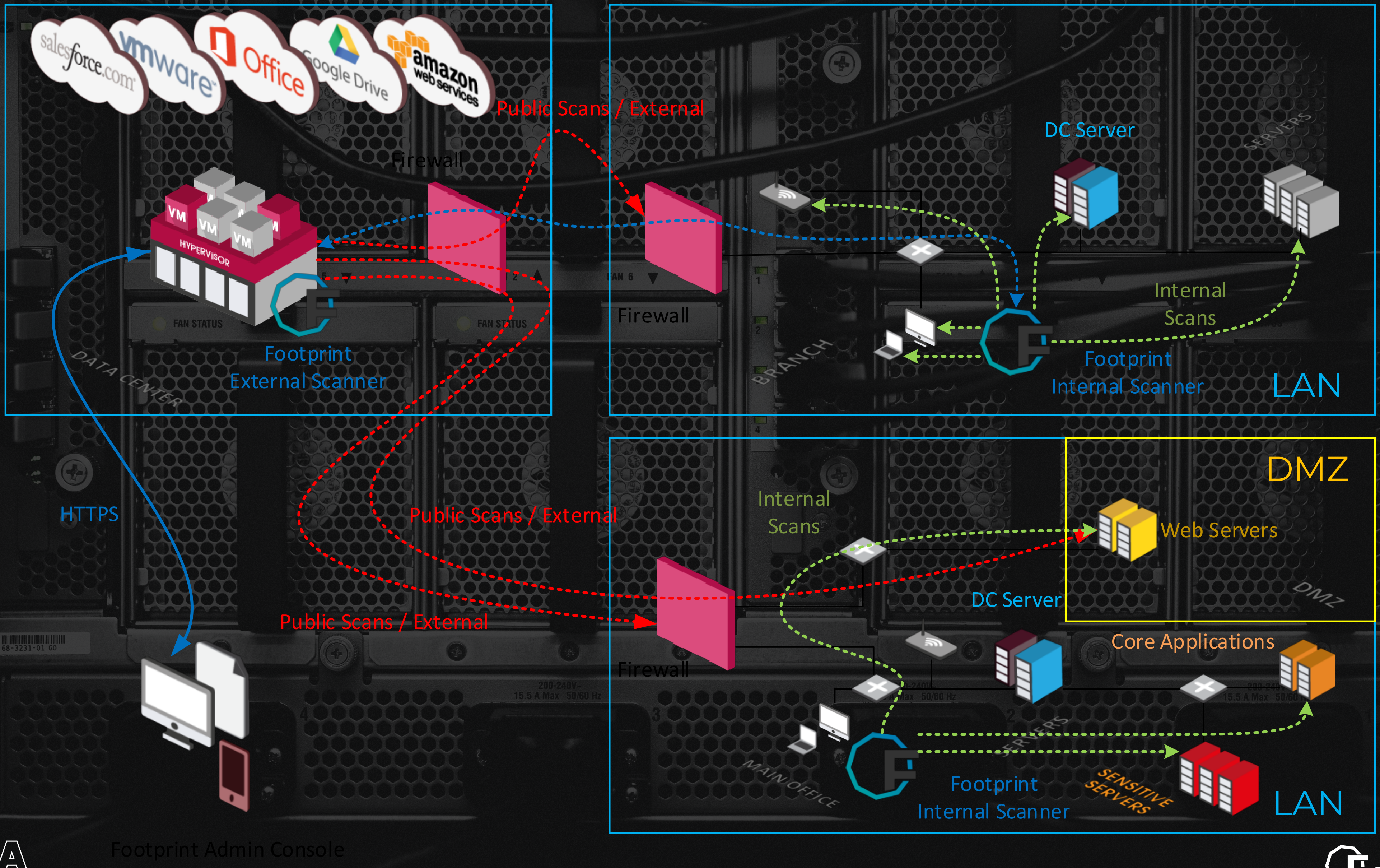
- Qualys always hosts it
- No branding allowed
- Increased cost & complexity: large suite of products for full coverage (QVM, QAM, QPCI, QWAS, QPM, QCAS, QPM)
- Single-tenant

Product Design

Designed for SecOps

- Complex initial setup
- Scan policies
- Scan schedules
- Manual translation to business risk
- Manual prioritization
- Lack of cross-functinal collaboration (IT, Business, Security)

Footprint High Level Design



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

- ↗ Live Dashboards
- ↗ E-mail alerts
- ↗ Availability SLA Monitor
- ↗ History Dashboard
- ⊛ Fixes / Recommendations
- 🔍 Multi-tenant
- 🔍 Whitelabeling
- ⊘🖥 Windows Agent

- ⇥ 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

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

Legend ⊘🖥 Vulnerability Enumeration & Asset Management ⊛ Patch Prioritization ↗ Reporting Capabilities 🔍 SOC Integration ⇥ Solution Usage

CODA
AI-driven *cyber risk insights*

Footprint

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

Q&A

Why are we disrupting the VRM

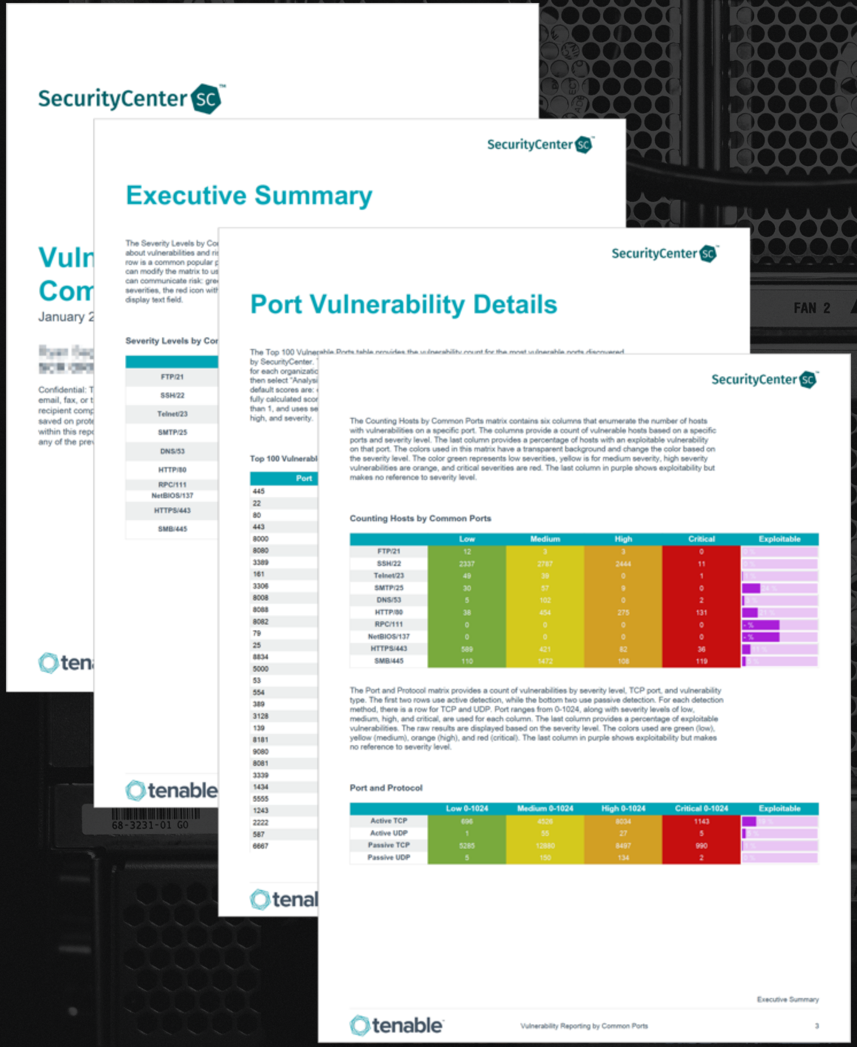
What do companies do in terms of VRM?

Why?

There is a difference between a VA and a meaningful VA.

Just like anybody can pretend to be an ethical hacker these days because they’re using a scanner

It’s also 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 %

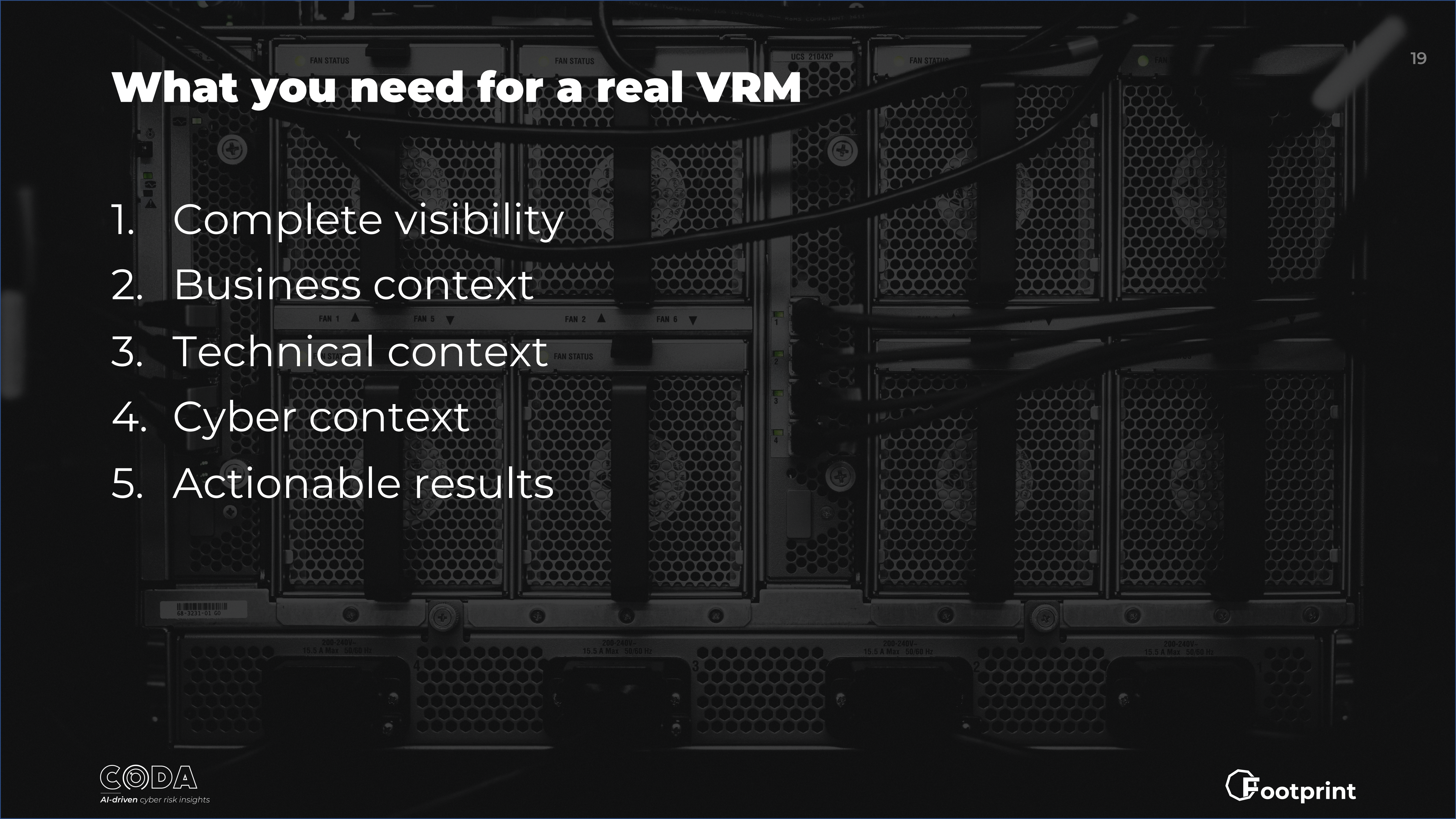
Executive Summary

tenable Vulnerability Reporting by Common Ports 3

- 10K vulns on 600 assets
- Patch management is failing
- Average MTTP is between 60 and 150 days.
- Large disconnect between teams

CODA
AI-driven cyber risk insights

Footprint



What you need for a real VRM

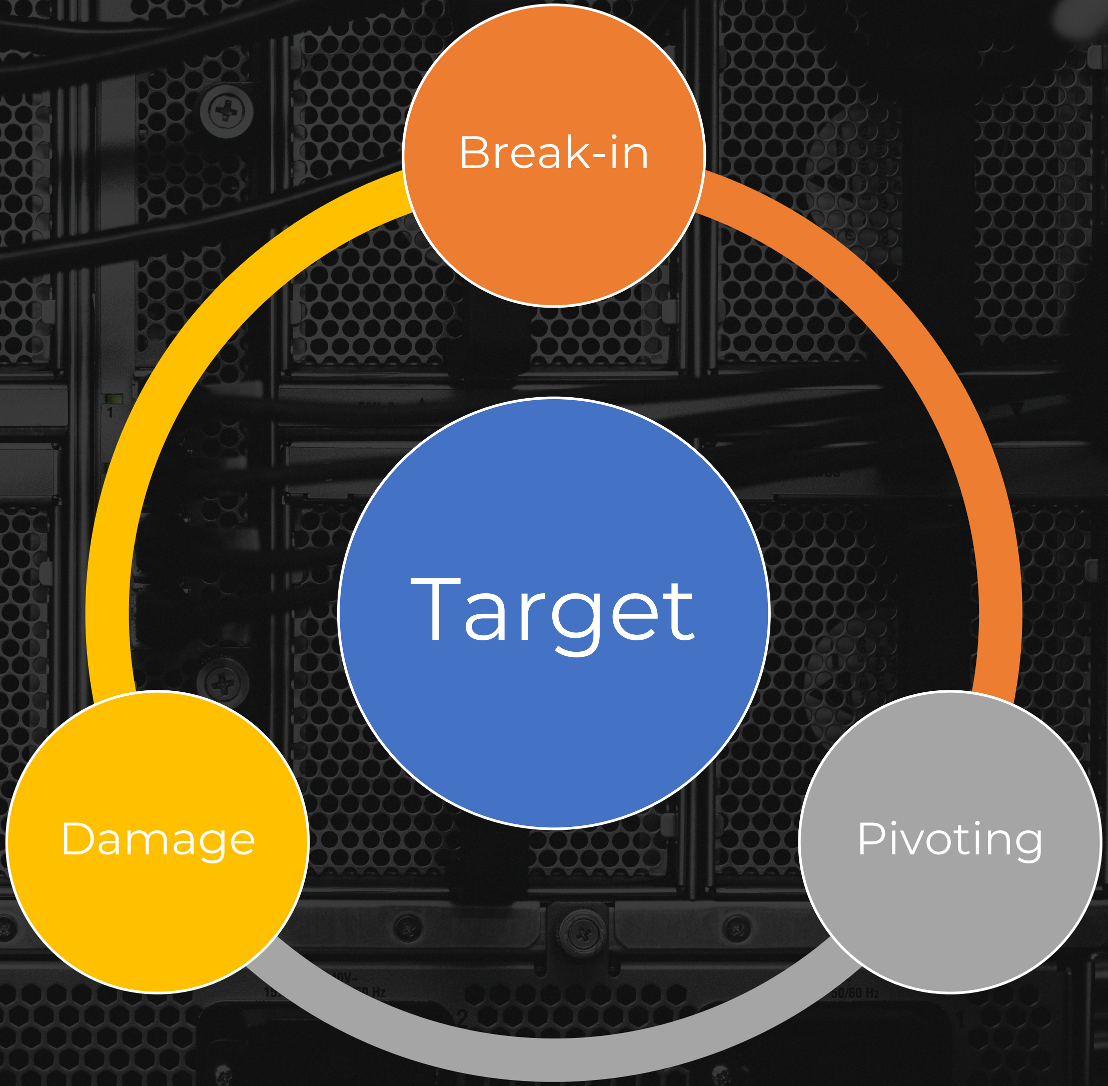
1. Complete visibility
2. Business context
3. Technical context
4. Cyber context
5. Actionable results

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

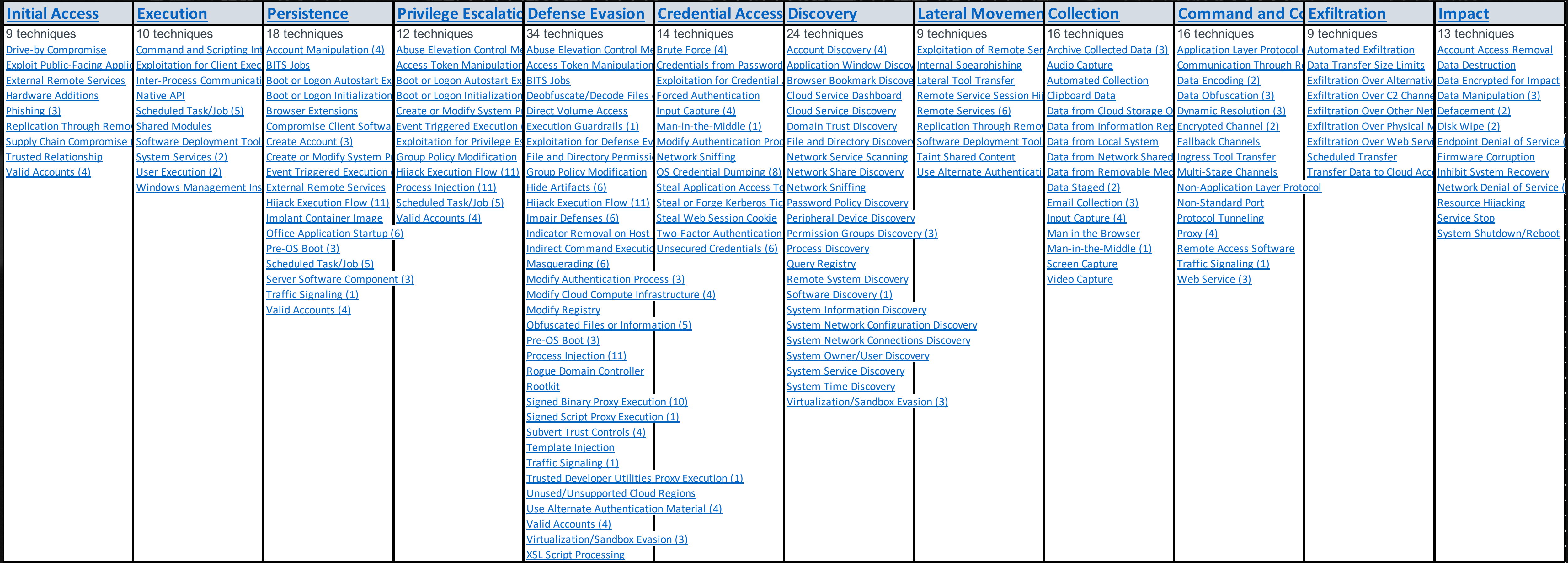
Demo time

The anatomy of an attack

Even a simple ransomware exploits at least 3 vulns.



The anatomy of an attack (detailed)



Initial Access	Execution	Persistence	Privilege Escalatio	Defense Evasion	Credential Access	Discovery	Lateral Movemen	Collection	Command and Co	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	24 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Drive-by Compromise	Command and Scripting Int	Account Manipulation (4)	Abuse Elevation Control Me	Abuse Elevation Control Me	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Ser	Archive Collected Data (3)	Application Layer Protocol (	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Applic	Exploitation for Client Exec	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password	Application Window Discov	Internal Spearphishing	Audio Capture	Communication Through R	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communicati	Boot or Logon Autostart Ex	Boot or Logon Autostart Ex	BITS Jobs	Exploitation for Credential	Browser Bookmark Discove	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternativ	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization	Boot or Logon Initialization	Deobfuscate/Decode Files (	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hi	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channe	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System P	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage O	Dynamic Resolution (3)	Exfiltration Over Other Net	Defacement (2)
Replication Through Remov	Shared Modules	Compromise Client Softwa	Event Triggered Execution (	Execution Guardrails (1)	Man-in-the-Middle (1)	Domain Trust Discovery	Replication Through Remov	Data from Information Rep	Encrypted Channel (2)	Exfiltration Over Physical M	Disk Wipe (2)
Supply Chain Compromise (	Software Deployment Tool	Create Account (3)	Exploitation for Privilege Es	Exploitation for Defense Ev	Modify Authentication Proc	File and Directory Discovery	Software Deployment Tool	Data from Local System	Fallback Channels	Exfiltration Over Web Servi	Endpoint Denial of Service (
Trusted Relationship	System Services (2)	Create or Modify System P	Group Policy Modification	File and Directory Permissi	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authenticati	Data from Removable Med	Multi-Stage Channels	Transfer Data to Cloud Acc	Inhibit System Recovery
	Windows Management Ins	External Remote Services	Process Injection (11)	Hide Artifacts (6)	Steal Application Access To	Network Sniffing		Data Staged (2)	Non-Application Layer Protocol		Network Denial of Service (
		Hijack Execution Flow (11)	Scheduled Task/Job (5)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tic	Password Policy Discovery		Email Collection (3)	Non-Standard Port		Resource Hijacking
		Implant Container Image	Valid Accounts (4)	Impair Defenses (6)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Protocol Tunneling		Service Stop
		Office Application Startup (6)		Indicator Removal on Host	Two-Factor Authentication	Permission Groups Discovery (3)		Man in the Browser	Proxy (4)		System Shutdown/Reboot
		Pre-OS Boot (3)		Indirect Command Executio	Unsecured Credentials (6)	Process Discovery		Man-in-the-Middle (1)	Remote Access Software		
		Scheduled Task/Job (5)		Masquerading (6)		Query Registry		Screen Capture	Traffic Signaling (1)		
		Server Software Component (3)		Modify Authentication Process (3)		Remote System Discovery		Video Capture	Web Service (3)		
		Traffic Signaling (1)		Modify Cloud Compute Infrastructure (4)		Software Discovery (1)					
		Valid Accounts (4)		Modify Registry		System Information Discovery					
				Obfuscated Files or Information (5)		System Network Configuration Discovery					
				Pre-OS Boot (3)		System Network Connections Discovery					
				Process Injection (11)		System Owner/User Discovery					
				Rogue Domain Controller		System Service Discovery					
				Rootkit		System Time Discovery					
				Signed Binary Proxy Execution (10)		Virtualization/Sandbox Evasion (3)					
				Signed Script Proxy Execution (1)							
				Subvert Trust Controls (4)							
				Template Injection							
				Traffic Signaling (1)							
				Trusted Developer Utilities Proxy Execution (1)							
				Unused/Unsupported Cloud Regions							
				Use Alternate Authentication Material (4)							
				Valid Accounts (4)							
				Virtualization/Sandbox Evasion (3)							
				XSL Script Processing							