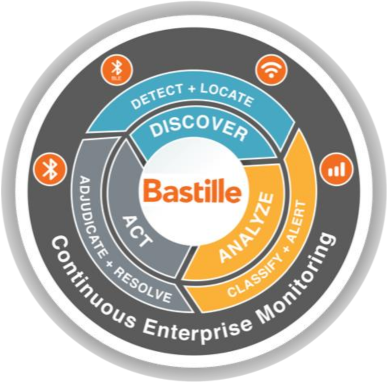
Bastille

How To Detect, Investigate + Resolve RF Devices Entering Your Facilities



DETECT + LOCATE

DISCOVER

ANALYZE

CLASSIFY + ALERT

ACT

ADJUDICATE + RESOLVE

Bastille

Continuous Enterprise Monitoring

Bastille Technical Brief
ISART Conference
August 12, 2020

Presented by:

Dr. Bob Baxley, *CTO*

Problem Definition and Motivation

4.7 BILLION CELLULAR PHONES

Source: Statistica

Bastille

8.4 BILLION BLUETOOTH DEVICES

Source: Statistica

9 BILLION Wi-Fi DEVICES

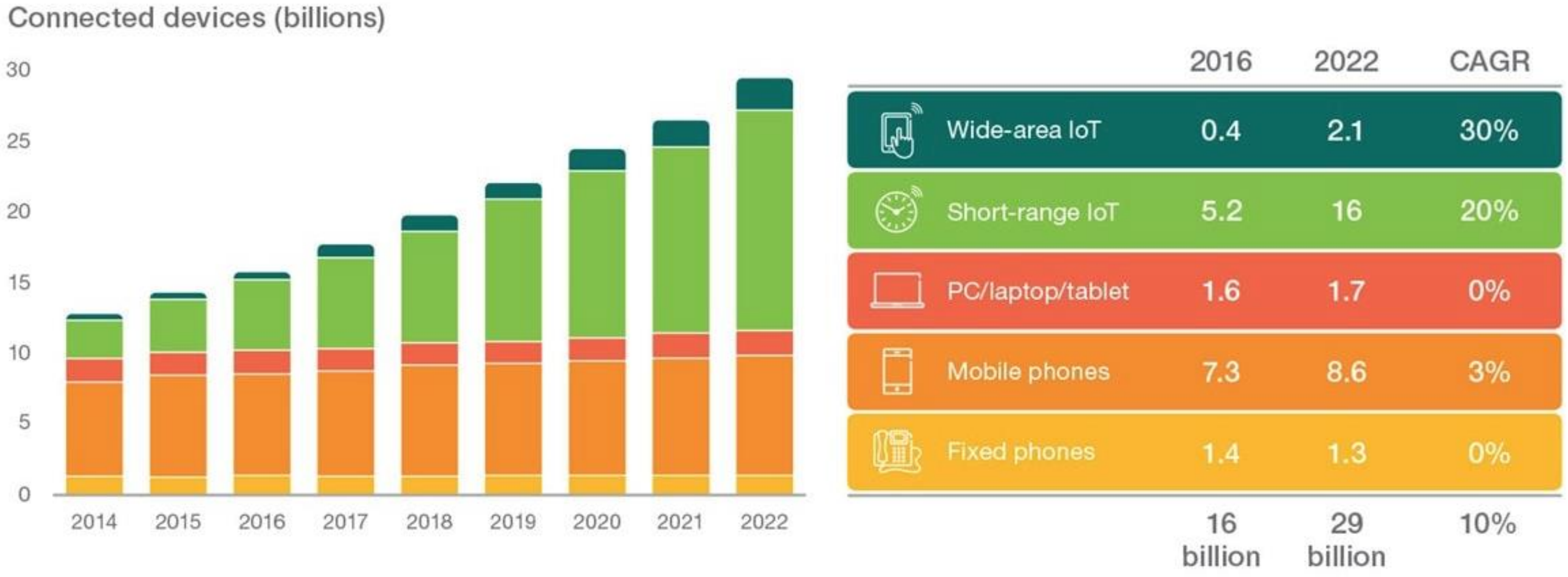
Source: Statistica

Bastille

IoT Devices Growing Fast and 70% Have Radios (Radio = Radio Frequency Communication Interface)

Today there are …

22 billion connected devices, and **15 billion** have radios



	2016	2022	CAGR
Wide-area IoT	0.4	2.1	30%
Short-range IoT	5.2	16	20%
PC/laptop/tablet	1.6	1.7	0%
Mobile phones	7.3	8.6	3%
Fixed phones	1.4	1.3	0%
	16 billion	29 billion	10%

Bastille

Source: "Internet of Things forecast," Ericsson

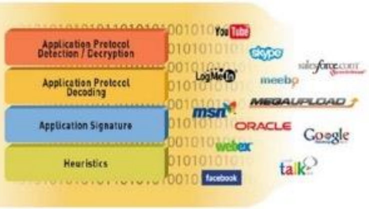
There is Covert Wireless Throughout Today

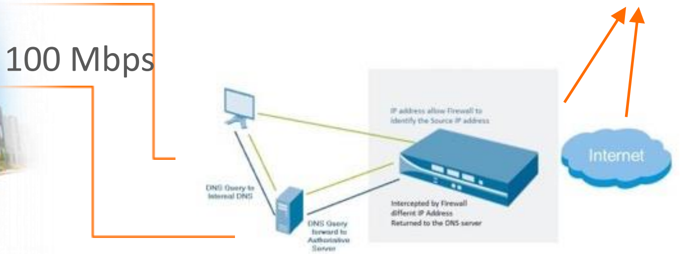
Vulnerable Wireless Devices in the Enterprise Today

On-Net Device Visibility Exists

Huge Dollars Spent to Monitor

100 Mbps Internet Connections





100 Mbps
IP address allow Firewall to identify the Source IP address
DNS Query to Internal DNS
DNS Query forward to Authoritative Server
Intercepted by Firewall different IP Address Returned to the DNS server
Internet

- Intrusion detection
- Exfiltration detection
- APT detection
- Next gen firewalls
- SIEMs

Off-Net RF Devices are Invisible

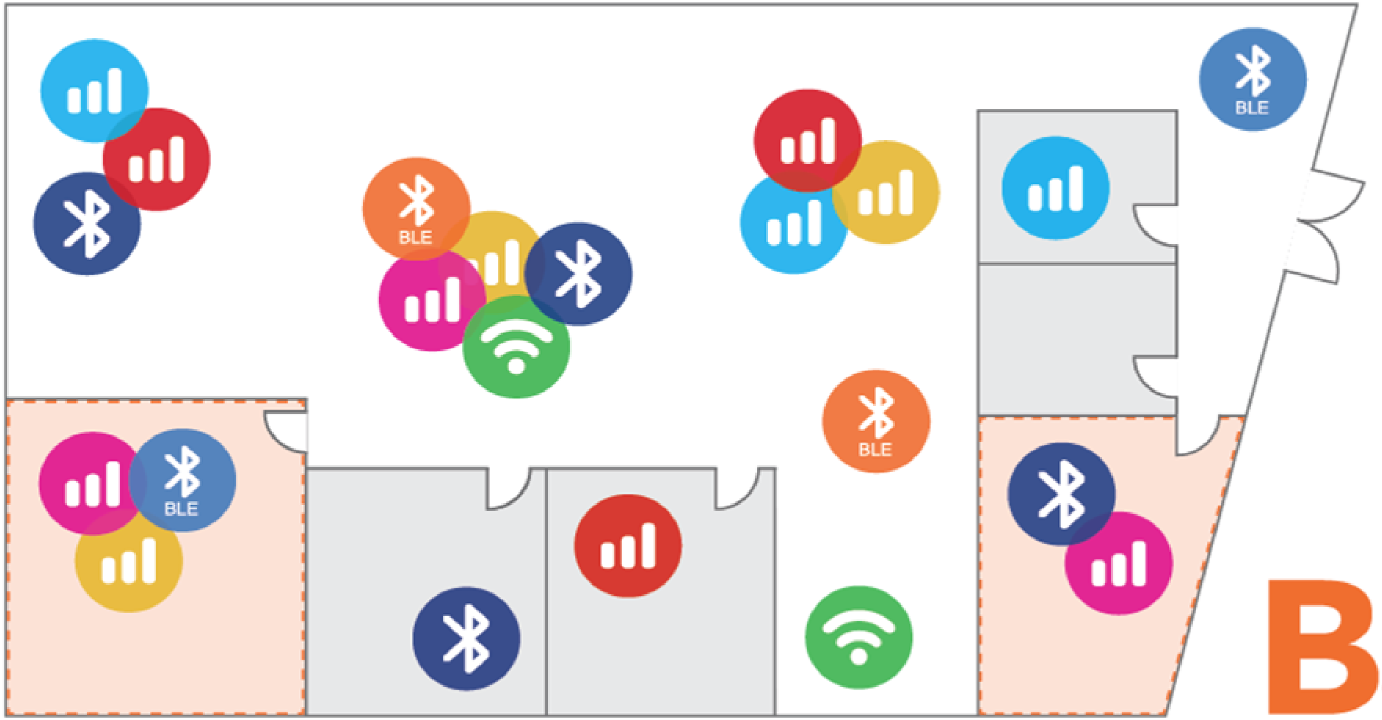
5 Gbps are
Leaving via Radio Signals

NOBODY IS WATCHING!

- Corporate phones
- Personal phones
- Hotspots
- Wearables
- Thermostats
- Sensors
- IoT

What Does Bastille Do?

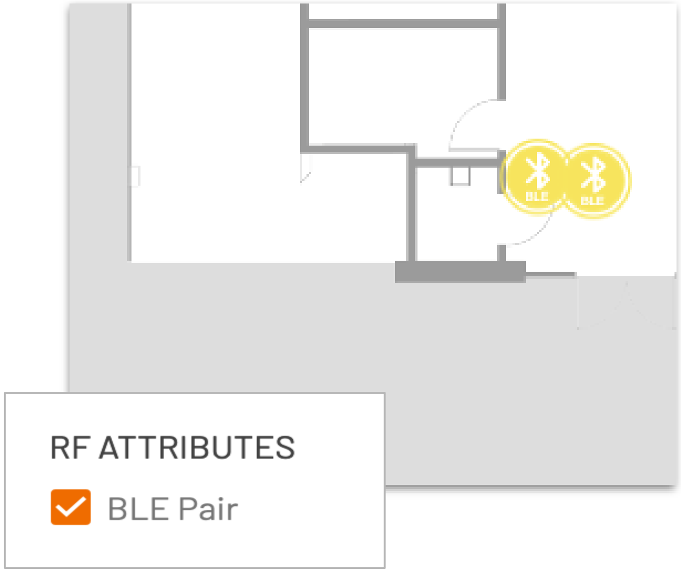
Sense & Locate Cellular, Wi-Fi, Bluetooth, BLE and other RF devices/networks through Software Defined Radio (SDR)



Bastille

Bluetooth Pairing Policy Enforcement

- Nuanced policies for wearables in restricted spaced
- Differentiation between paired and unpaired devices
- Alerting on pairing violation



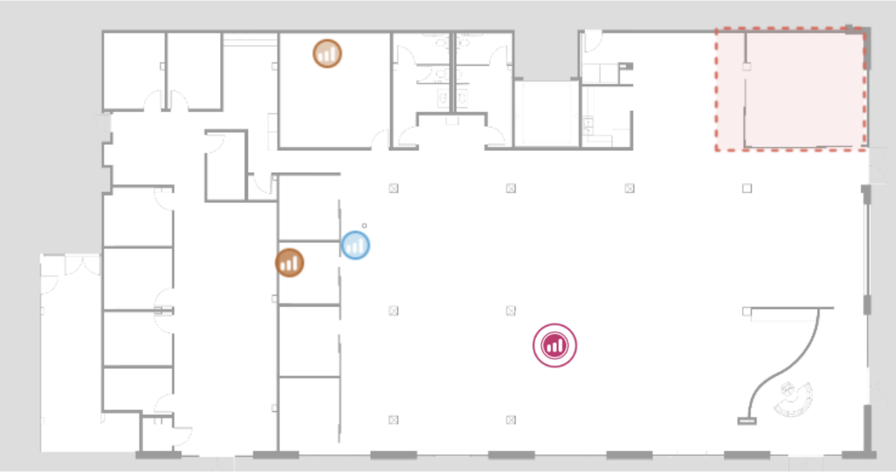
RF ATTRIBUTES

☑ BLE Pair

Cell Phone Location

Bastille Persistently & Accurately Locates Individual Devices in Real Time

- Bastille accurately locates individual phones and other devices and puts real time dots on a map
- Digital demodulation means that we can localize co-located phones



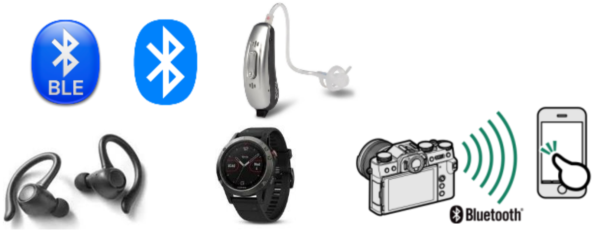
Bastille stores location/device history for after-event analysis and forensics

Device Policy & Automation

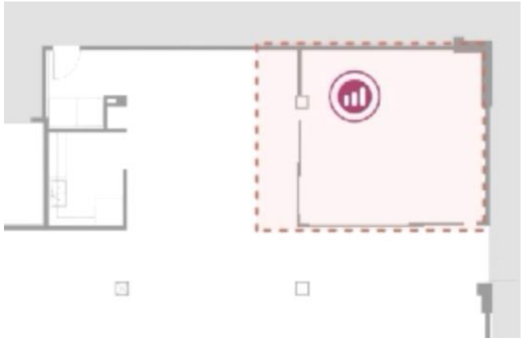
Policy Types

Whitelist

Network Connection



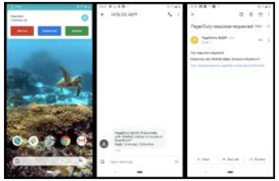
Geofence



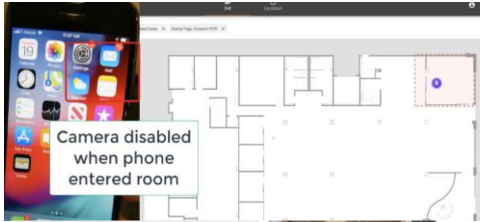
Automated Actions

Incident Response

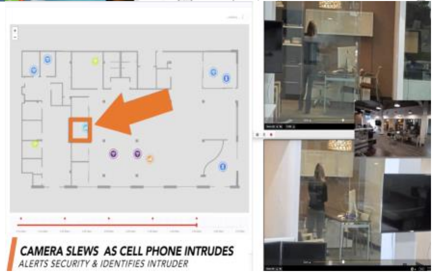
Phone, Email, SMS



MDM / UEM


Camera disabled when phone entered room

Physical Security Tools

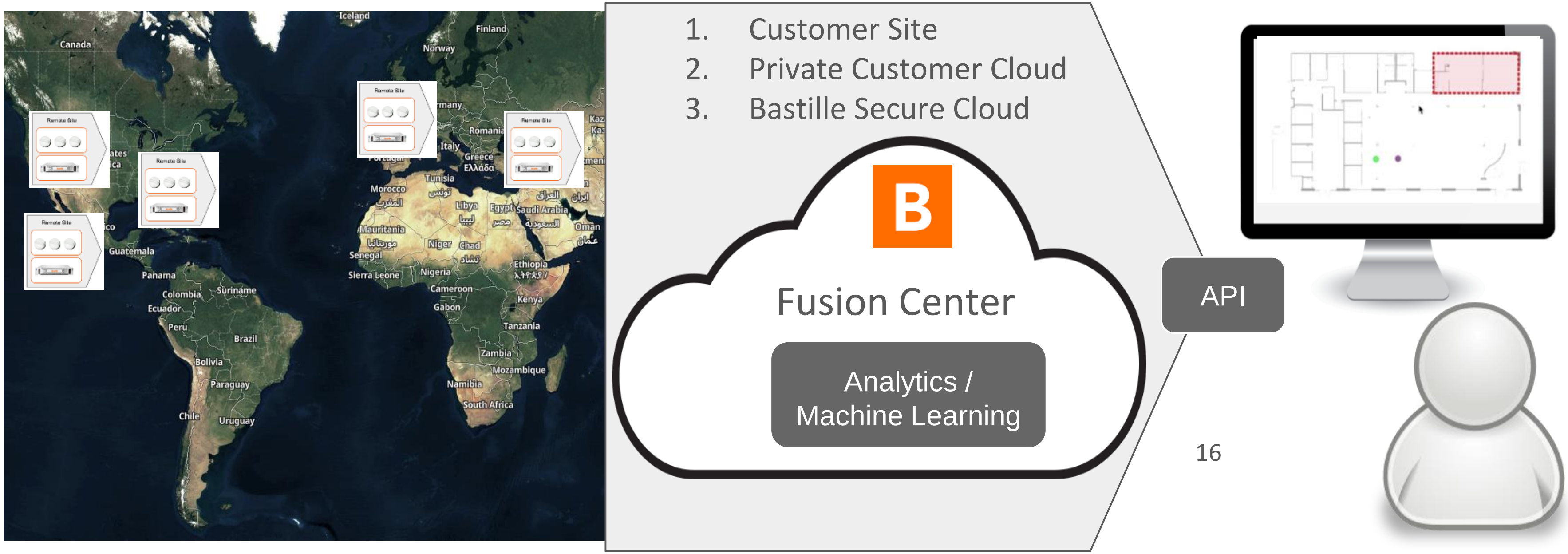

CAMERA SLEWS AS CELL PHONE INTRUDES
ALERTS SECURITY & IDENTIFIES INTRUDER

How does Bastille do that?

Bastille Sensor Arrays

- 25 MHz - 6 GHz visibility
- FPGA on-board for pre-processing
- UL Certified to work in the Plenum space above ceiling tiles
- FCC Certified as 100% passive
- **No Moving Parts**
  - Absolutely no fans. Fan failure can lead to sensor overheating and failure.
  - Advanced sensor power management can use POE+ or wall power barrel connector
- Real-Time Sensor Health Monitoring and Fail Safe
  - Automatic alerting if an individual sensor fails
  - Identification of which sensor has failed
  - System operation continues if a single sensor fails

Bastille Distributed Enterprise Architecture



1. Customer Site
2. Private Customer Cloud
3. Bastille Secure Cloud

Fusion Center

Analytics / Machine Learning

API