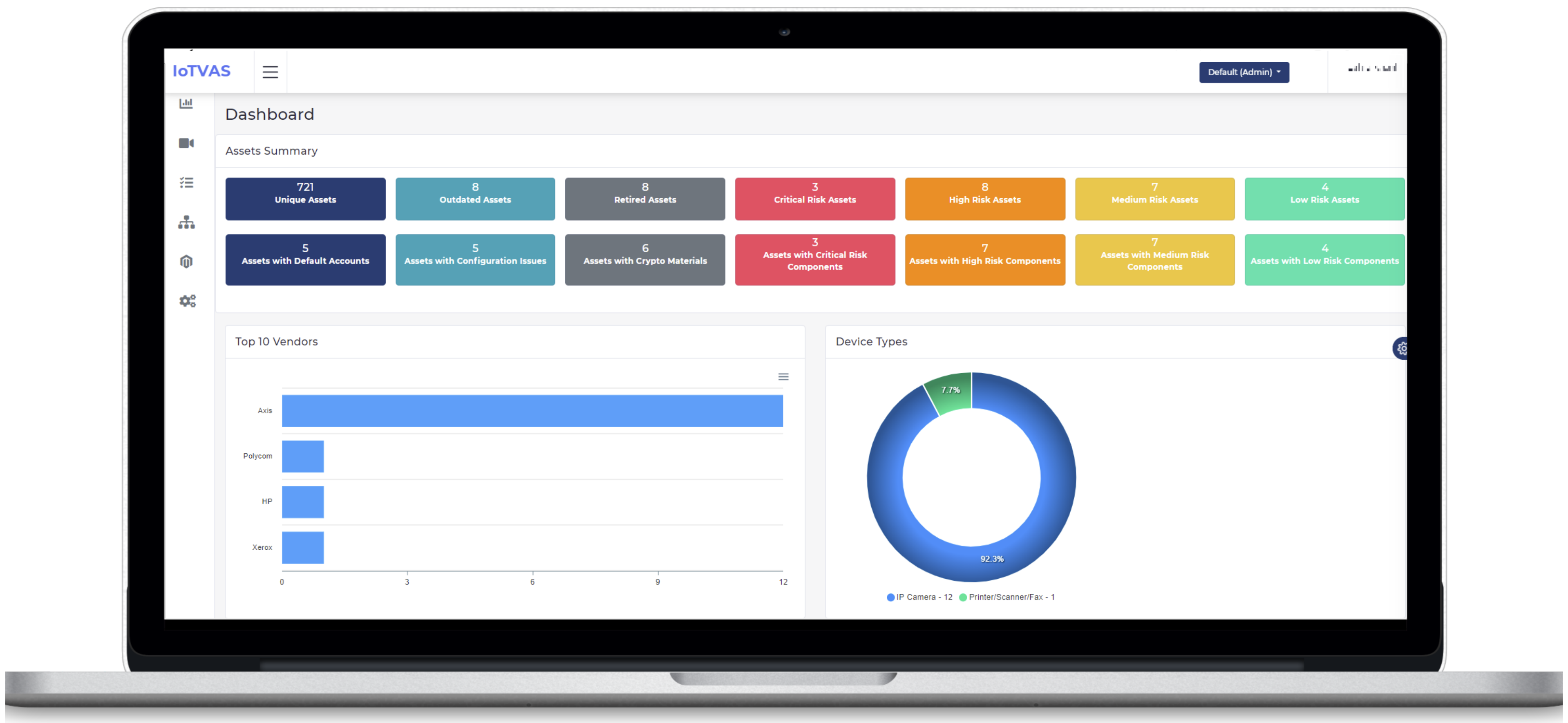
FIRMALYZER

Connected device discovery and vulnerability assessment made ***automated, proactive and effective***



THE PROBLEM

The number of network-connected devices in enterprise networks is growing which unlike workstations, laptops and servers are not properly identified and monitored by IT security teams within organizations. While many consider these devices to be "simple", most of them run flavors of Linux or a real time operating system included with their firmware that are vulnerable in the same way as servers, desktop operating systems and applications. The only difference is that IT administrators cannot install OS monitoring agents or anti-malware software on OT/IoT devices as they do for their fleet of servers and workstations. This makes these devices a prime landing point, attack pivoting and malware persistence in enterprise networks. Therefore, a compromised IoT device may remain undetected for months while being used as a launchpad for attacking internal hosts or exfiltrating sensitive data.

THE CHALLENGE

Traditional endpoint security or vulnerability assessment solutions are impractical for OT/IoT/connected devices vulnerability management for the following reasons:

- *They bring very limited visibility into device internals. There is often no OS/service exception and crash reporting by these solutions.*
- *They often depend on agent installation which is impractical for IoT devices as they have diverse platform architectures.*
- *They perform active network scanning but since OT/IoT devices are often resource constrained, active scanning causes OS crash in most of them.*

IOTVAS SAAS PLATFORM

IoTVAS SaaS discovers IoT/connected devices and their security risks. The platform includes a lightweight software agent that discovers your connected device assets in the local network or on the internet without network traffic capturing or requiring access to device credentials.
It can be integrated with any asset discovery solution that can discover and expose the device manufacturer and model name.
IoTVAS vulnerability detection engine is specifically built for enterprise IoT/connected device security and is based on our global-scale proprietary firmware vulnerability knowledgebase that is constantly growing and evolving automatically as our analysis engine automatically collects and processes new device firmware binaries on behalf of device manufacturers and consumers. Through this knowledgebase, our vulnerability detection engine gains in-depth visibility into the applications running on a target IoT/connected device, their vulnerabilities and associated risks. IoTVAS also keeps tracking the vulnerable devices as they change IP address or move around the network.

THE FIRMALYZER DIFFERENCE

PRIVACY PRESERVING

Does not collect sensitive data

SAFE ON DEVICES

Vulnerability detection does not affect devices

AGENTLESS

No need to touch devices

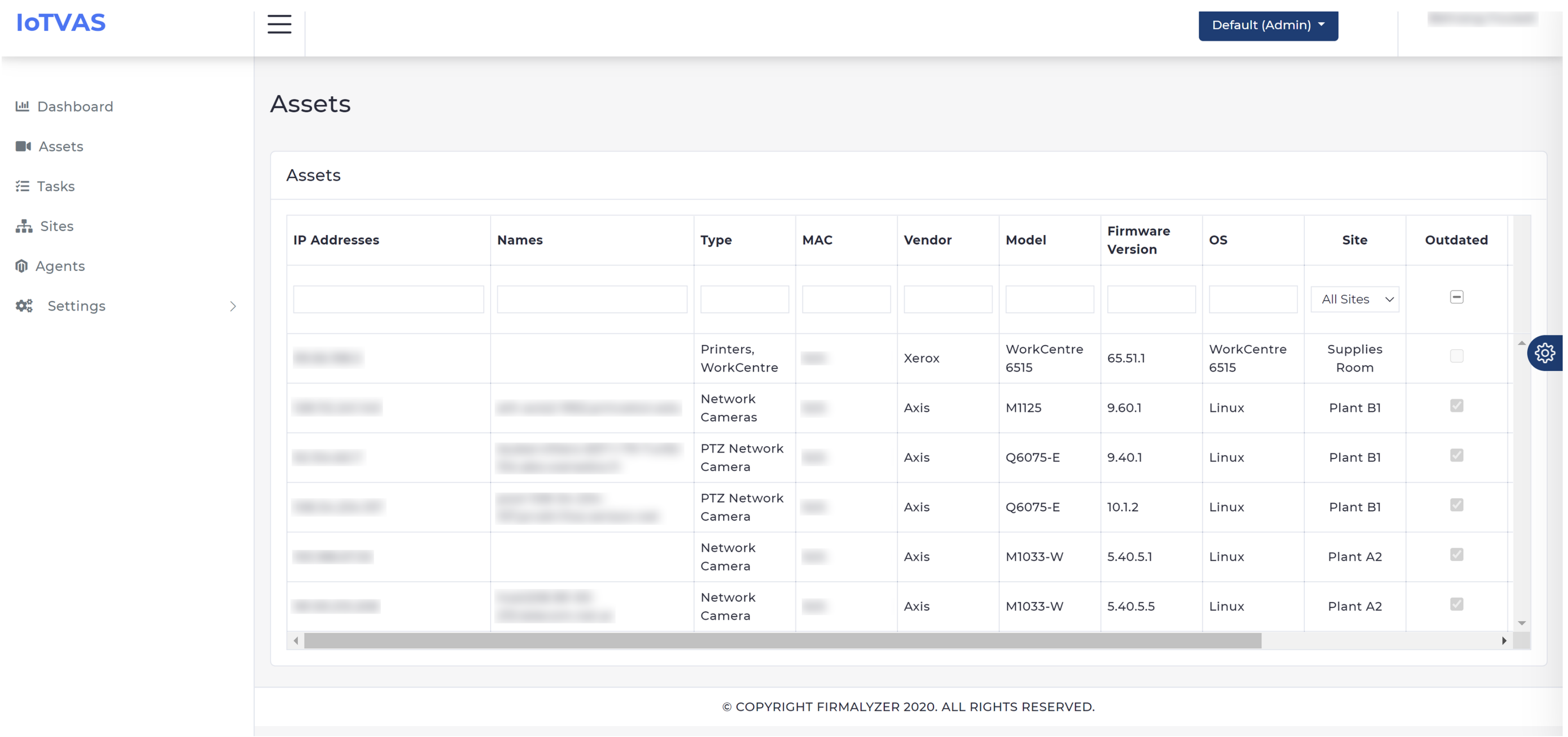
PROACTIVE

Detects vulnerabilities before they are exploited

RELIABLE

No false-positives

IoTVAS automatically identifies connected devices and associated risks. No firmware file upload, access to the devices or network scanning is required.



IoTVAS

Default (Admin) ▾ [redacted]

Assets

Assets

IP Addresses	Names	Type	MAC	Vendor	Model	Firmware Version	OS	Site	Outdated
								All Sites	⊟
[redacted]		Printers, WorkCentre	[redacted]	Xerox	WorkCentre 6515	65.51.1	WorkCentre 6515	Supplies Room	☐
[redacted]	[redacted]	Network Cameras	[redacted]	Axis	M1125	9.60.1	Linux	Plant B1	☑
[redacted]	[redacted]	PTZ Network Camera	[redacted]	Axis	Q6075-E	9.40.1	Linux	Plant B1	☑
[redacted]	[redacted]	PTZ Network Camera	[redacted]	Axis	Q6075-E	10.1.2	Linux	Plant B1	☑
[redacted]		Network Camera	[redacted]	Axis	M1033-W	5.40.5.1	Linux	Plant A2	☑
[redacted]	[redacted]	Network Camera	[redacted]	Axis	M1033-W	5.40.5.5	Linux	Plant A2	☑

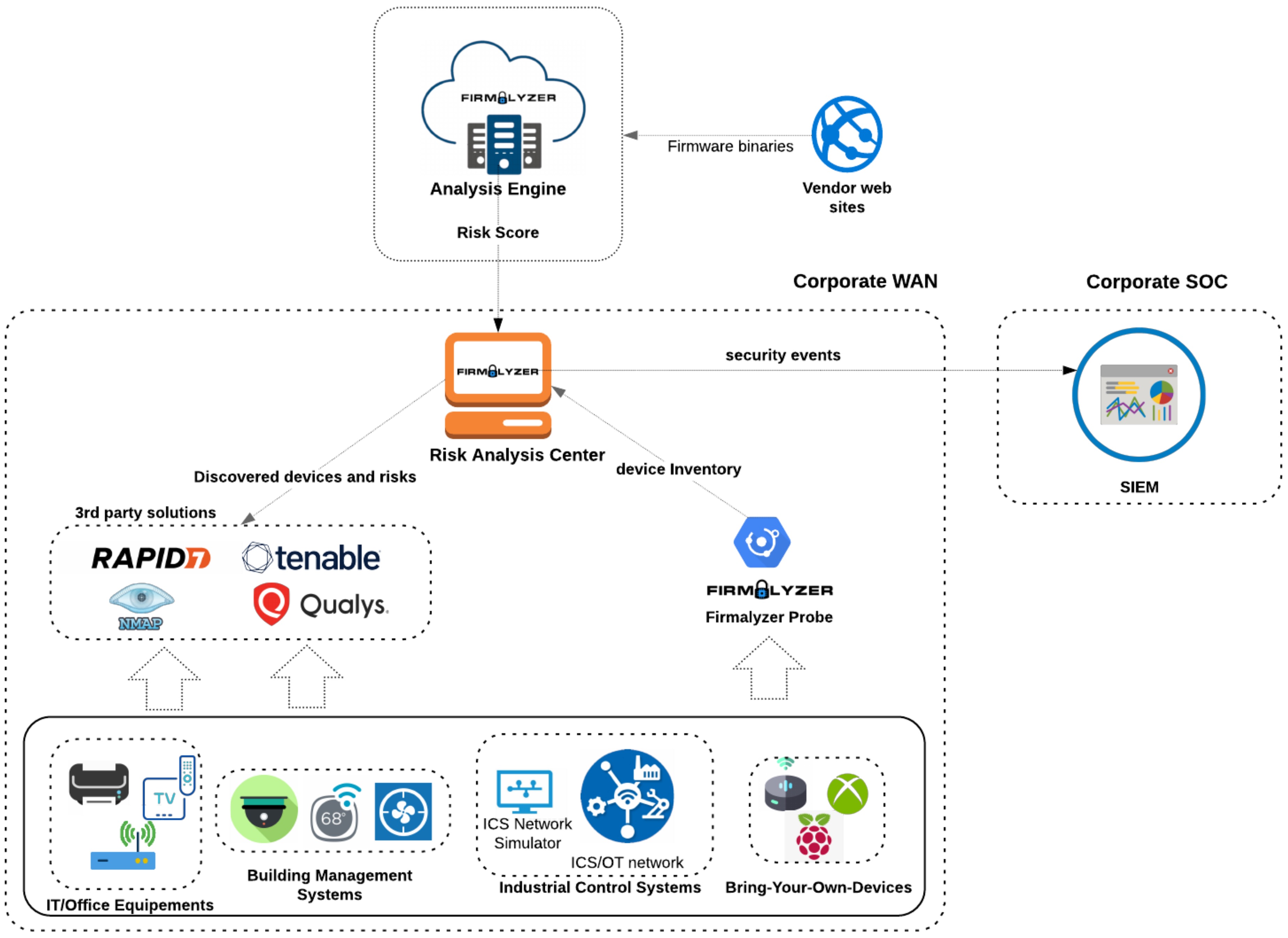
© COPYRIGHT FIRMALYZER 2020. ALL RIGHTS RESERVED.

KEY FEATURES

- *Rapid deployment that does not require installation of "network taps" or "port mirroring"*
- *Integration with existing IT vulnerability management and network asset discovery solutions*
- *Identification of devices that run outdated firmware versions*
- *Detection of devices that are discontinued/retired by their vendors*
- *Discovery of known vulnerabilities affecting connected devices*
- *Discovery of vulnerable 3rd party components and software libraries in connected device firmware*
- *Safe device probing that does not interfere with device operation*

PLATFORM ARCHITECTURE

Firmalyzer can automatically pull device data (vendor, model and firmware version) from existing 3rd party solutions. The following figure demonstrates the deployment scenario:.

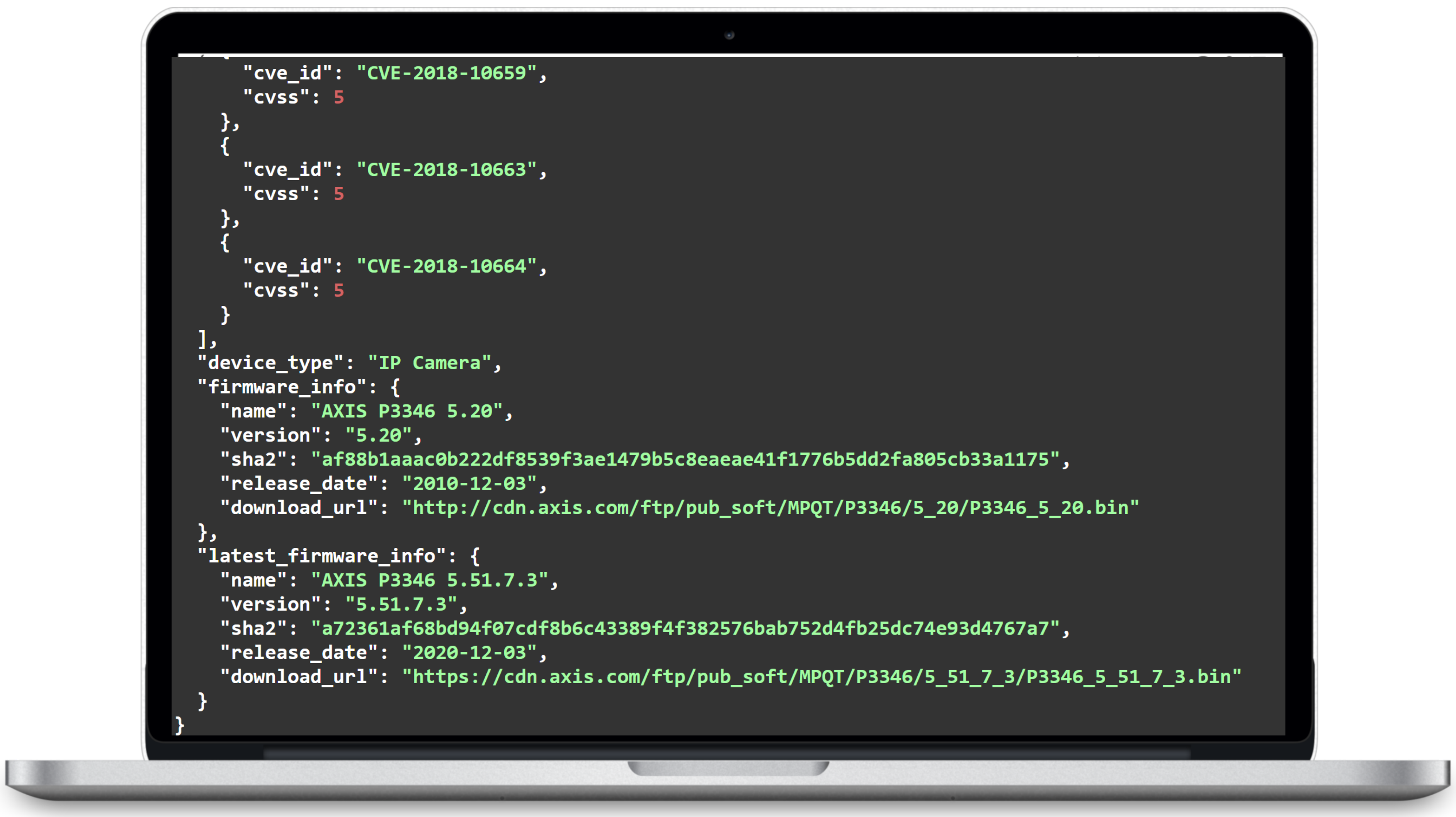


IoTVAS extends the reach of your vulnerability management program to the IoT/connected devices. It can integrate with your existing IT asset management and vulnerability assessment solution, providing accurate device discovery and real-time vulnerability assessment at the firmware code level without requiring network traffic collection or installation of software agents on devices. This allows you to get the most of your existing security tools and proactively find high risk connected devices.

IOTVAS API

IoTVAS API is an IoT/connected device identification and vulnerability assessment solution that can be easily integrated with asset discovery, network port scanners and IT vulnerability scanning tools and enable them to perform:

- *Accurate identification of device manufacturer, model name, device type, device end of life status, firmware version and firmware release date*
- *Safe and in-depth vulnerability assessment of identified device including publicly known vulnerabilities (CVE) and unknown vulnerabilities in device firmware code including vulnerable 3rd party components, default credentials, crypto keys, certificates and default configuration issues.*



```
      "cve_id": "CVE-2018-10659",
      "cvss": 5
    },
    {
      "cve_id": "CVE-2018-10663",
      "cvss": 5
    },
    {
      "cve_id": "CVE-2018-10664",
      "cvss": 5
    }
  ],
  "device_type": "IP Camera",
  "firmware_info": {
    "name": "AXIS P3346 5.20",
    "version": "5.20",
    "sha2": "af88b1aaac0b222df8539f3ae1479b5c8eaeae41f1776b5dd2fa805cb33a1175",
    "release_date": "2010-12-03",
    "download_url": "http://cdn.axis.com/ftp/pub_soft/MPQT/P3346/5_20/P3346_5_20.bin"
  },
  "latest_firmware_info": {
    "name": "AXIS P3346 5.51.7.3",
    "version": "5.51.7.3",
    "sha2": "a72361af68bd94f07cdf8b6c43389f4f382576bab752d4fb25dc74e93d4767a7",
    "release_date": "2020-12-03",
    "download_url": "https://cdn.axis.com/ftp/pub_soft/MPQT/P3346/5_51_7_3/P3346_5_51_7_3.bin"
  }
}
```

KEY ADVANTAGES

- *Uses device fingerprints based on the network service banners of the device, hence there is no need for collection of the device network traffic*
- *Identifies devices in the absence of their MAC addresses, hence it can detect remote devices in segmented networks and over the internet*
- *Provides in-depth real-time device firmware risk analysis of the identified device without requiring the user to upload firmware file*
- *Easy integration with industry standard security tools such as Nmap and OpenVAS*

COMPANY PROFILE

Firmalyzer is specialized in providing security solutions for OT, IoT and connected devices. The company is the provider of the first automated firmware security analysis solution in the market. Firmalyzer's founding team members expertise in security assessment and vulnerability research on OT/IoT devices and communication protocols lays the foundation of our solution and services. We provide tailored solutions to solve challenges faced by IoT device manufacturers and their customers in managing OT/IoT devices risk.

CONTACT DETAILS

Web:
https://firmalyzer.com/
Email:
contact@firmalyzer.com
Phone:
+32 2 8923951
Address:
Place Marcel Broodthaers 8
box 5, 1060 Brussels, Belgium