IoT Security

Improving the Use of IoT in the Public Sector

Mark Bleecker
Sales Manager, IoT Security
mbleecker@paloaltonetworks.com

June 2021

Massive Vulnerability Found Across 100's of Millions IoT Devices - “Ripple20”

According to a press release, the series of zero-day vulnerabilities in a widely used low-level TCP/IP software library is developed by Treck, Inc. These vulnerabilities, given the name Ripple20, affect hundreds of millions of devices (or more), and include multiple remote code execution vulnerabilities.

https://www.securitymagazine.com/articles/92611-massive-vulnerability-found-across-100s-of-millions-iot-devices

Fish tanks

"Someone used the fish tank to get into the network, and once they were in the fish tank, they scanned and found other vulnerabilities and moved laterally to other places in the network," Justin Fier, director for cyber intelligence and analysis at Darktrace, explained to CNN Tech.

Security cameras

Ring, a home security products provider owned by Amazon, was hit by a class-action lawsuit in the U.S. for reports of multiple hacking incidents on its security cameras that left victims traumatized.

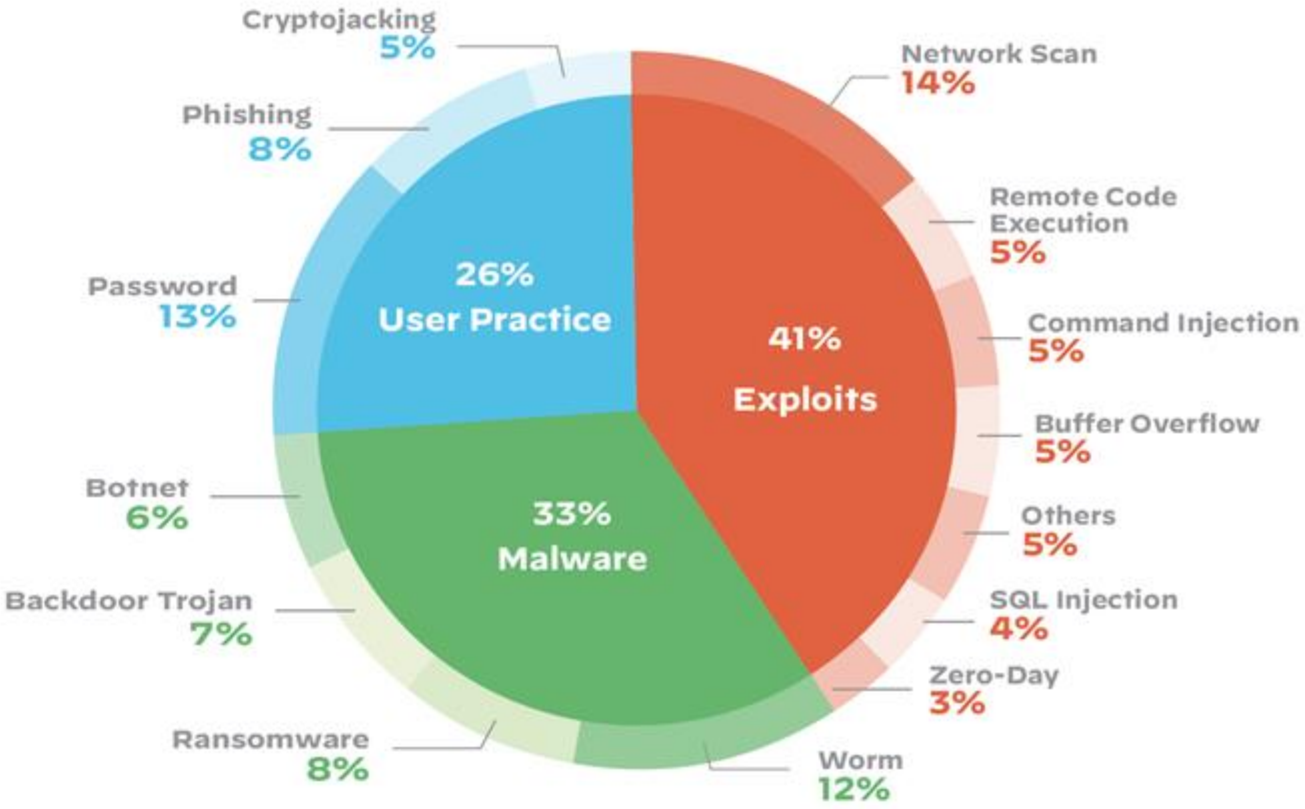
Printers

The report highlighted that 60 percent of businesses in the U.K., U.S., France, and Germany suffered a print-related data breach in 2019, which resulted in a data loss that cost companies an average of more than US$ 400,000.

Lighting

Multiple reports of security vulnerabilities in smart bulbs. NFL players Twitter accounts compromised.

Unit 42 IoT Threat Report: Top Attack Methods for IoT Devices



Unit 42 IoT Threat Report:
Why are IoT devices the Ideal Entry Point?

- Zero to Minimum Built-In Security
- Browser Interface Vulnerabilities
- Outdated Operating Systems
- Failure to Adhere to Security Best Practices

Unit 42 IoT Threat Report:

The Most High Risk Devices?

Medical Imaging Systems	51%
Patient Monitoring Systems	26%
Security Cameras	33%
Printers	24%
Medical Device Gateways	9%
Consumer Electronics	7%
Energy Management Devices	6%
IP Phones	5%

Why Current Solutions Fail to Protect IoT

Limited Visibility

Cannot identify previously unseen IoT devices, accuracy requires constant effort

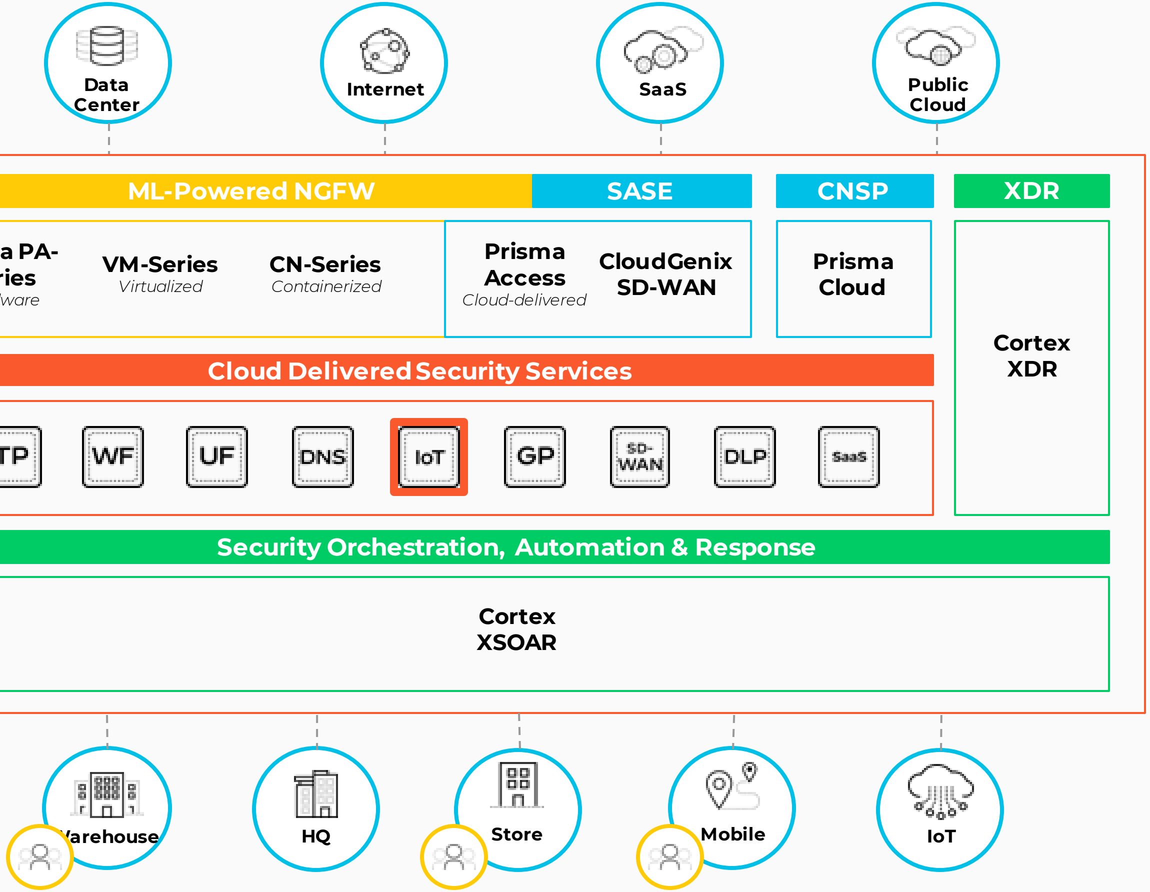
No Protection

Existing visibility-centric solutions do not offer native prevention or enforcement

Hard to Implement

Require changes to network infrastructure, security team workflows and integrations

A Single Platform to Connect and Secure Everything



Data Center

Internet

SaaS

Public Cloud

ML-Powered NGFW

SASE

CNSP

XDR

Strata PA-Series *Hardware*

VM-Series *Virtualized*

CN-Series *Containerized*

Prisma Access *Cloud-delivered*

CloudGenix SD-WAN

Prisma Cloud

Cortex XDR

Cloud Delivered Security Services

TP

WF

UF

DNS

IoT

GP

SD-WAN

DLP

SaaS

Security Orchestration, Automation & Response

Cortex XSOAR

Warehouse

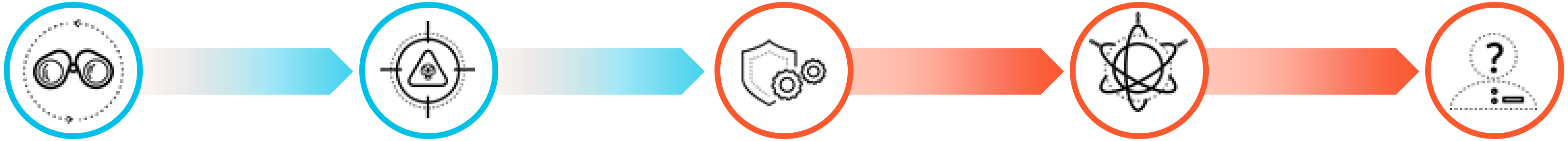
HQ

Store

Mobile

IoT

IoT Security with Palo Alto Networks



1. Understand IoT Assets

- Identify 90+% of devices **within 48 hours**
- ML accurately classifies devices with **50+ attributes**
- Continually detects new and unknown devices

2. Assess IoT Risk

- Passive **discovery of vulnerabilities** and integration with databases
- **Continuous risk assessment** and scoring to prioritize response
- **Vendor advisory** for security patching

3. Apply Risk Reduction Policies

- **Risk-based policy recommendations** to enforce only trusted behaviour of devices and groups
- Reduce attack surface with **context-aware segmentation**
- **Automated enforcement** with Device-ID

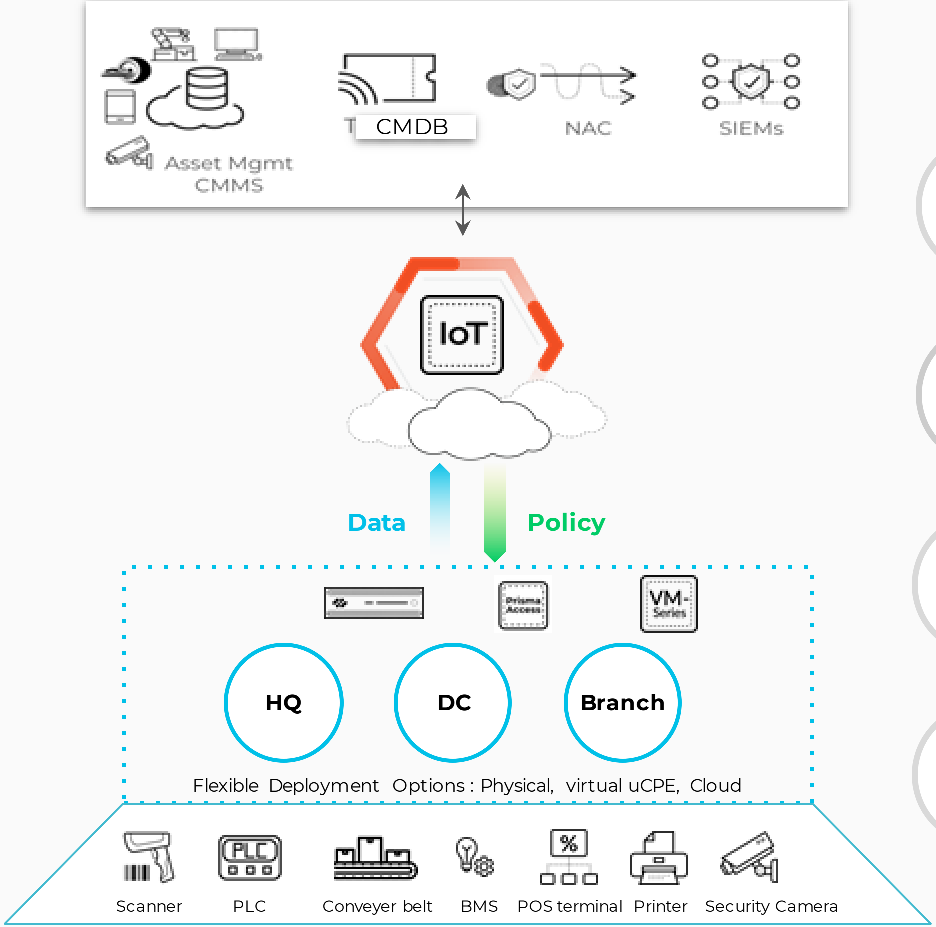
4. Prevent Known Threats

- **Protection from exploits**, C2, spyware and other known threats
- Enhance detail of all alerts with **IOT device context**

5. Detect & Respond to Unknown Threats

- Anomalous activity and **zero-day detection**
- **Stop unknown** file and web-based threats
- Detailed **incident context** for response

Introducing IoT Security - full visibility with in-built security



Complete Asset Visibility & Context - ML Powered

Accurately identify & classify all devices with ML. Agentless. Rich context

In-depth Risk Analysis

Multi-factor risk analysis: threat, vulnerability, device contexts (both static and dynamic behavior)

Built-in Prevention

Reduce risk with automated zero trust FW policies.
Integrated with existing security solutions such as NAC, vuln management

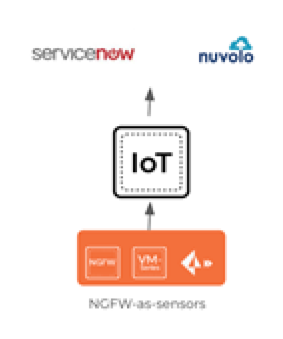
Detect & Respond to Unknown Threats with ML

ML-based device baseline and anomaly detection

Use Cases

Improve security workflows with new IoT visibility and integrations

Improve Asset Mgmt with IoT Visibility



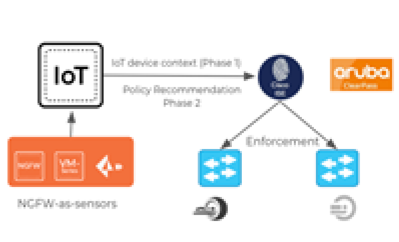
Challenge today

- Increasing risk due to lack of visibility of IoT devices and unmanaged devices.

Use Case:

- Augment existing CMDB with accurate IoT device inventory
- Integrate with existing IT ticket workflow

Reduce threat surface with automated NAC segmentation and risk management

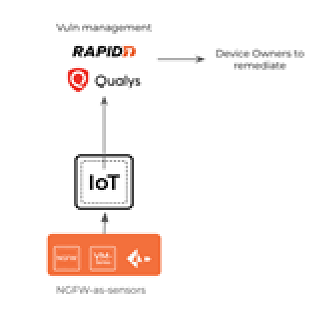


Challenge today

- NAC solutions do not have accurate visibility of IoT devices
- Segmentation manual and complex

Use Case:

- Improve NAC segmentation & policy with IoT visibility & risk context. NAC is a policy control point



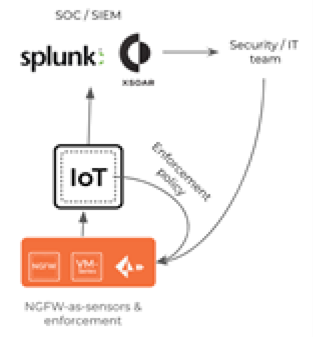
Challenge today

- Today's vulnerability management do not have accurate asset inventory resulting in gaps in vuln assessment

Use Case:

- IoT device CVEs validated with vuln management solutions. Device owners informed to remediate

Rapid Threat Response and Enforcement



Challenge today

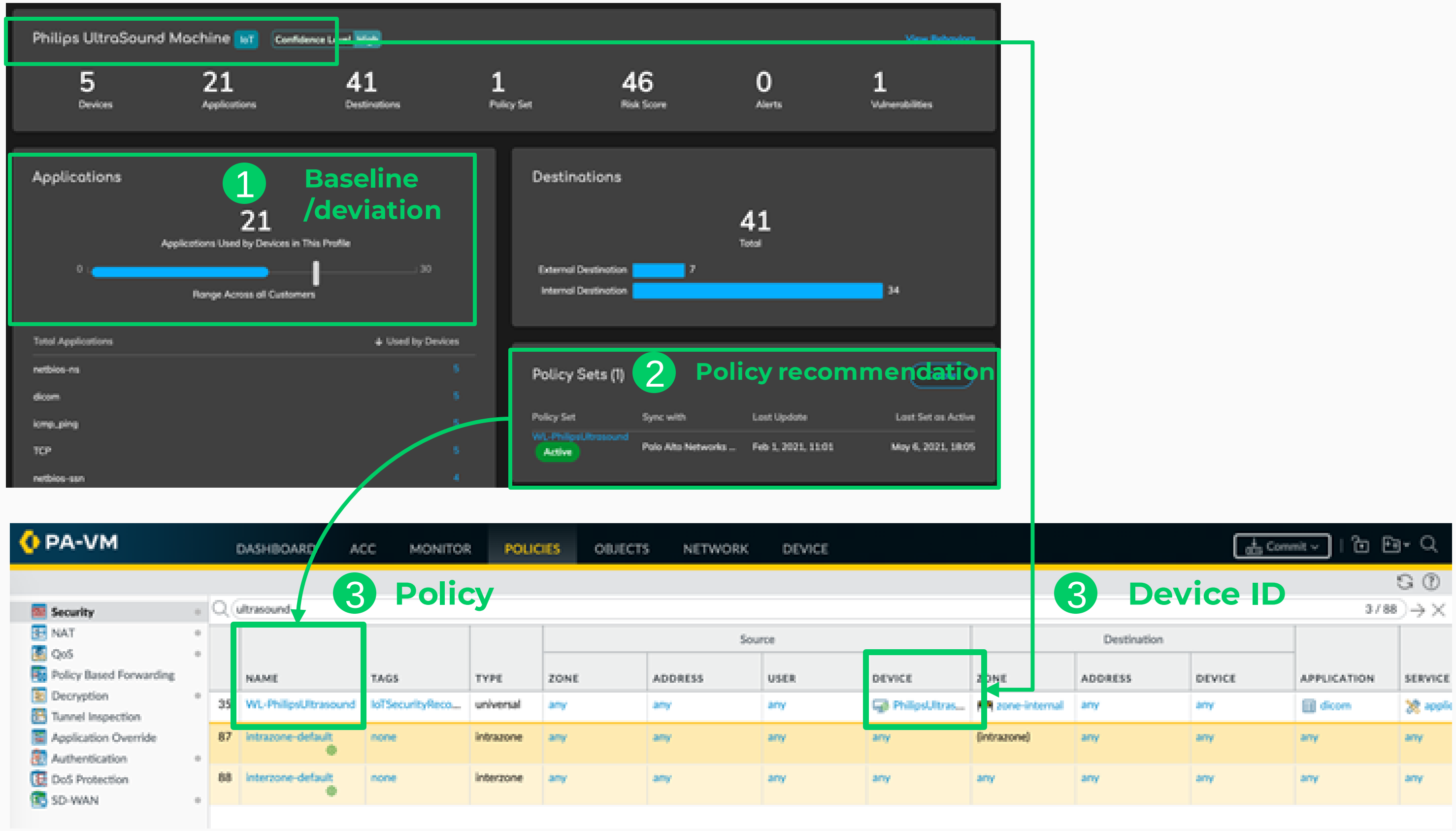
- SOC team lacks coverage for IoT & unmanaged devices. EDR agent approach not applicable to IoT

Use Case:

- IoT threat alerts to SIEMs / SOC
- SOC threat incident investigation → sec team for enforcement action

Built-in zero-trust policy enforcement and threat prevention

IoT
Data
NGFW



Philips UltraSound Machine IoT Confidence Level High

View Behaviors

5	21	41	1	46	0	1
Devices	Applications	Destinations	Policy Set	Risk Score	Alerts	Vulnerabilities

Applications

1 Baseline /deviation

21

Applications Used by Devices in This Profile

0 30

Range Across all Customers

Total Applications	+ Used by Devices
netbios-ns	5
dicom	5
icmp_ping	5
TCP	5
netbios-ssn	4

Destinations

41

Total

External Destination 7

Internal Destination 34

Policy Sets (1)

2 Policy recommendation

Policy Set	Sync with	Last Update	Last Set as Active
WL-PhilipsUltrasound Active	Palo Alto Networks ...	Feb 1, 2021, 11:01	May 6, 2021, 18:05

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Commit

3 Policy

3 Device ID

Security
NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection
Application Override
Authentication
DoS Protection
SD-WAN

ultrasound

3 / 88

				Source				Destination				
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
35	WL-PhilipsUltrasound	IoTSecurityReco...	universal	any	any	any	PhilipsUltras...	zone-internal	any	any	dicom	applic
87	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any
88	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any

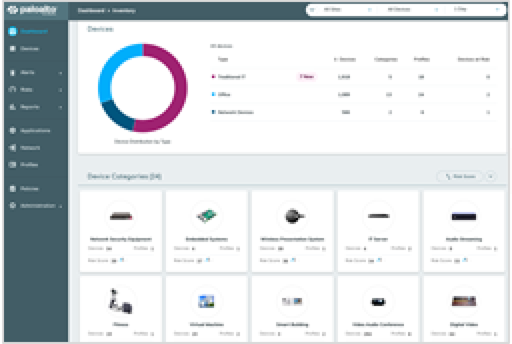
NIST Cybersecurity Framework Alignment

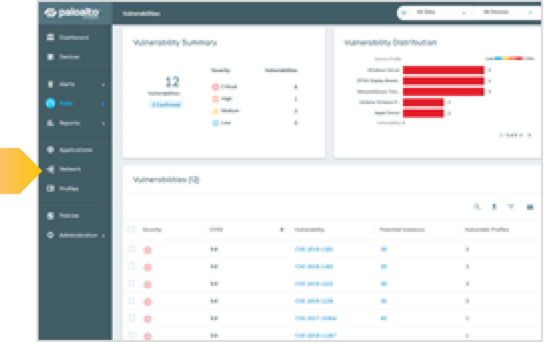
IoT Security delivers information that can be mapped into the NIST Cybersecurity Framework:

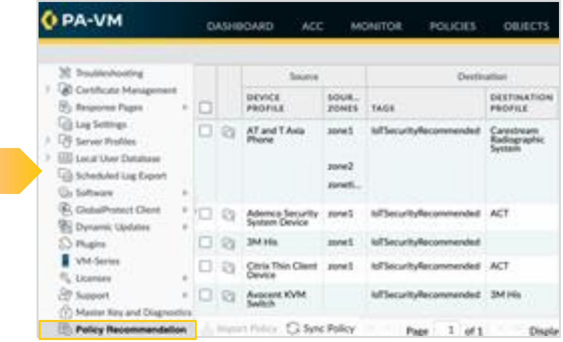
RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

Identify	Protect	Detect	Respond	Recover
• IoT asset discovery & inventory • IoT risk exposure and security posture assessment	• Context-aware network segmentation to reduce attack surface • Zero-trust Policy for IoT • ACLs to only permit trusted behaviors	• Behavioral baselining and anomaly detection for IoT • IoT Vulnerabilities	• Real-time IoT enforcement using network security controls • Quarantine deviant IoT asset • Integration with XSOAR, NAC and ticketing systems	• Recommendations on available patches for CVEs, OS/Firmware

Introducing IoT Security







		Source		Destination	
□		DEVICE PROFILE	SOUR... ZONES	TAGS	DESTINATION PROFILE
□		AT and T Axia Phone	zone1 zone2 zoneN...	IoTSecurityRecommended	Carestream Radiographic System
□		Ademco Security System Device	zone1	IoTSecurityRecommended	ACT
□		3M His	zone1	IoTSecurityRecommended	
□		Citrix Thin Client Device	zone1	IoTSecurityRecommended	ACT
□		Avocent KVM Switch		IoTSecurityRecommended	3M His

Complete Visibility

Accurately identify and classify all devices with ML, including those never seen before

In-depth Risk Analysis

Quickly understand anomalies, vulnerabilities and severity to make confident decisions

Built-in Enforcement

Safely automate enforcement and prevent all threats with your Next-Generation Firewall

Visibility, Prevention & Enforcement all in one platform