IoT Security

Protect Every Device on Your Network

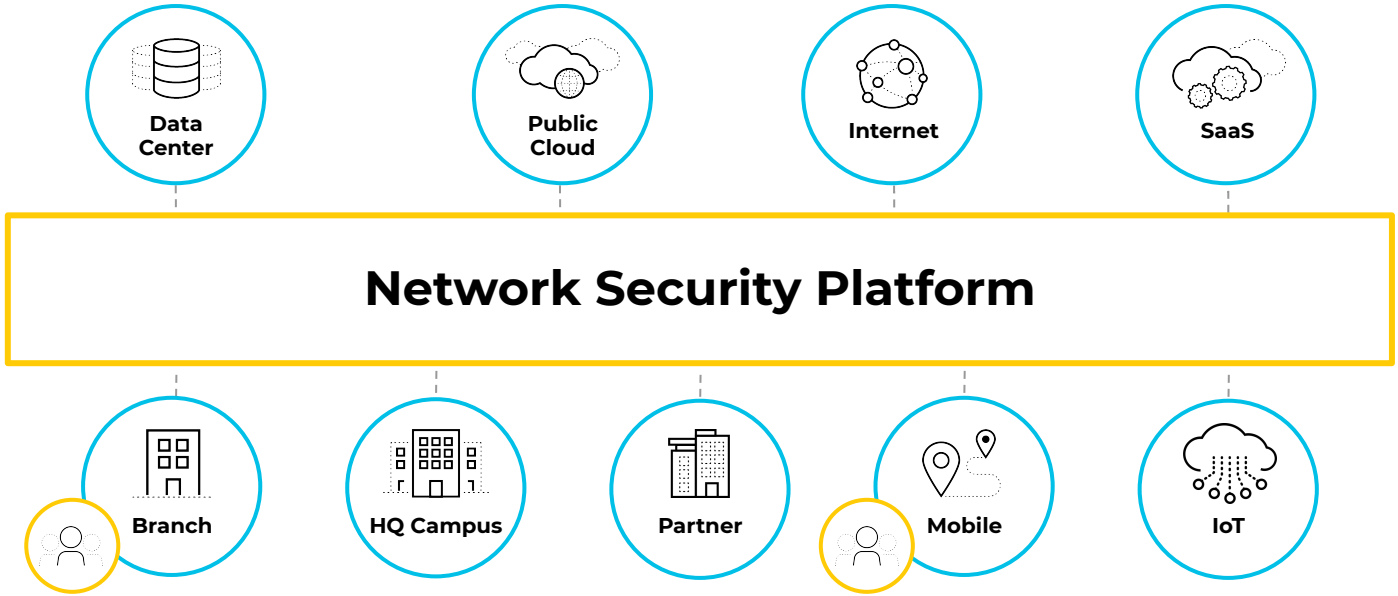
For Healthcare



January 2021

© 2021 Palo Alto Networks, CONFIDENTIAL

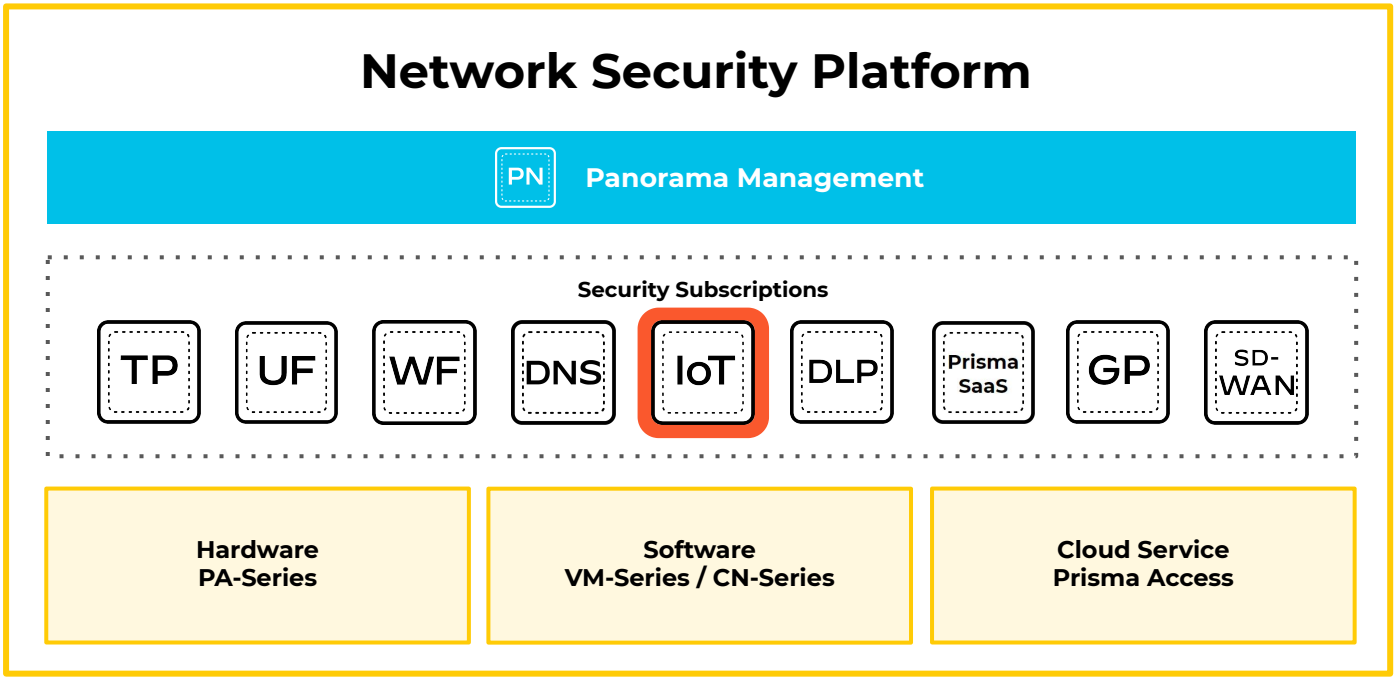
A Single Platform to Connect and Secure Everything



Consistent Integrated Best-in-class

 © 2021 Palo Alto Networks, Inc. All rights reserved.

Network Security Platform Components



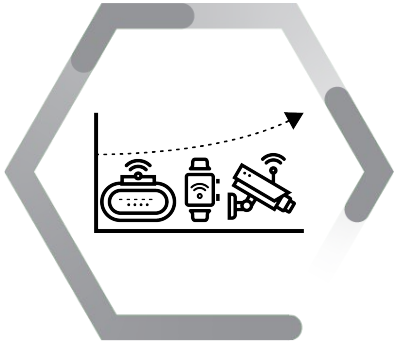
 © 2021 Palo Alto Networks, Inc. All rights reserved.

IoT Security

The Healthcare Industry's Most Comprehensive Solution

paloalto NETWORKS

IoMT & IoT is a Necessity that Introduces Risk



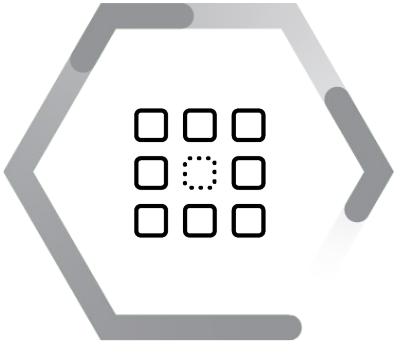
Limited Visibility & Insights

Occupying 50% of all devices, affecting capital planning and patient device allocation



Pose Huge Security & Patient Risk

Vulnerabilities, difficulty patching & unfettered access contribute to breaches; highest breached industry

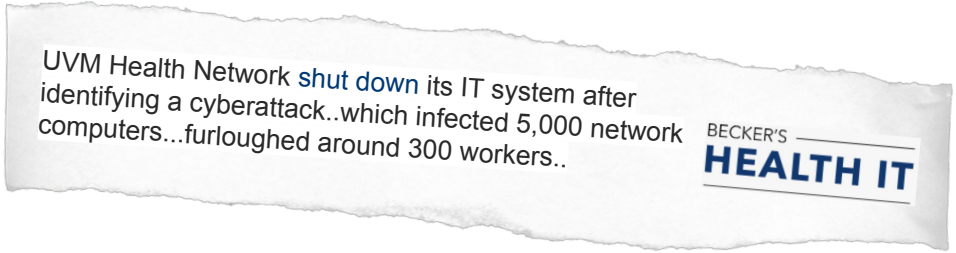


Securing IoT Devices is Hard

Incredibly diverse devices; traditional IT security controls do not work

 © 2021 Palo Alto Networks, Inc. All rights reserved.

One of the Most Targeted Industry for Cybercrime

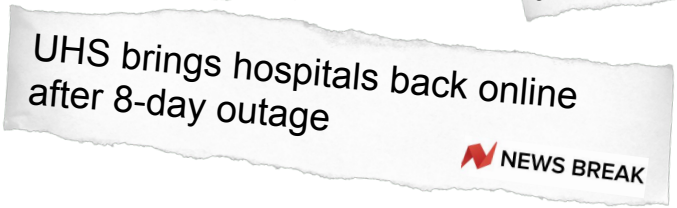










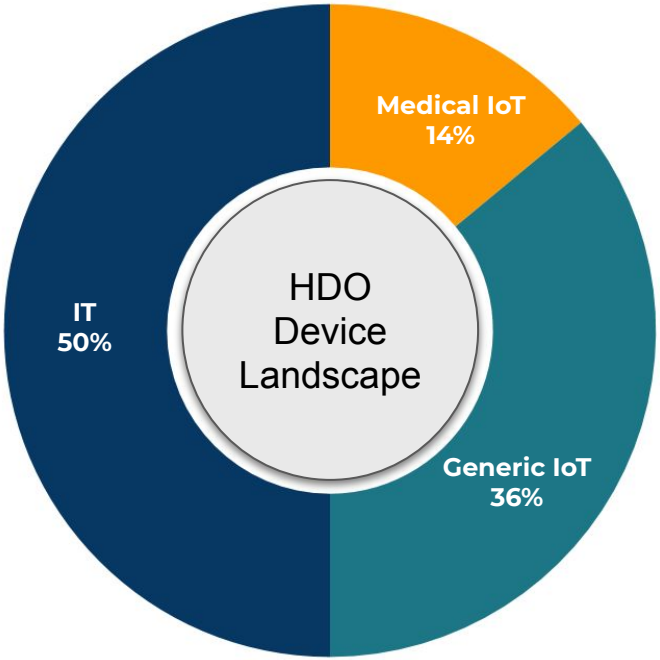






 © 2021 Palo Alto Networks, Inc. All rights reserved.

Healthcare Delivery Organization Device Landscape



50% of devices in Healthcare Delivery Organizations (HDO) are unmanaged

Most deployed Medical IoT devices

- Infusion pump (46%)
- Imaging system (19%)
- Patient monitor (17%)

Medical IoT devices with most security issues

- Imaging system (51%)
- Patient monitor (26%)
- Medical device gateway (9%)

Generic IoT devices with most security issues

- Camera (33%)
- Printer (24%)
- Video gaming devices(10%)

More details in Unit 42 IoT Threat Report

 © 2021 Palo Alto Networks, Inc. All rights reserved.

Why Current Solutions Fail to Protect IoMT & IoT



Limited Visibility

Signature-based approaches lack accuracy and cannot identify new unknown devices



No Protection

Existing solutions are alert only, with no prevention or enforcement

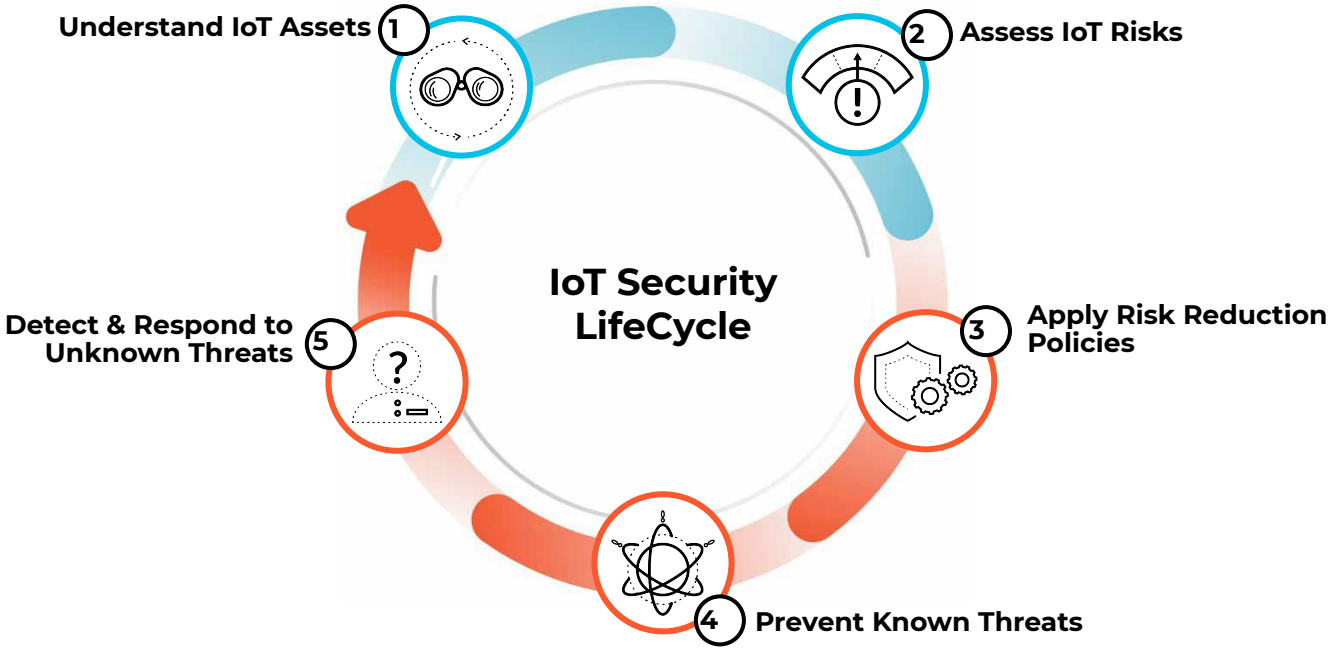


Hard to Implement

New processes, integrations and staff are required to enable basic IoMT security

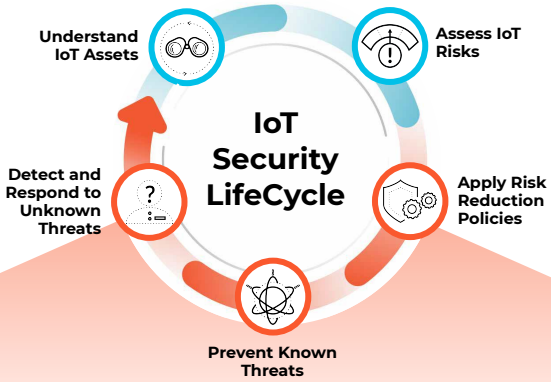
 © 2021 Palo Alto Networks, Inc. All rights reserved.

The Right Methodology to Secure all IoT Devices



 © 2021 Palo Alto Networks, Inc. All rights reserved.

The Right Methodology for Clinical Device Management



Identify

Passive

ML-driven

50+ attributes

Onboard

Automated

Context-aware

NAC/CMMS integrations

Optimize

Resource allocation

Utilization

Vendor information

Retire

Data protection

Compliance

Decommission

 © 2021 Palo Alto Networks, Inc. All rights reserved.

IOT SECURITY - The Healthcare Industry's Most Comprehensive Solution



Quick & Accurate Discovery

Uses ML and crowdsourcing to expand visibility and insights to all devices, even those never seen before



Built-in Prevention

Instead of alert-only, our Security Services keep medical and other devices safe from all threats



Maximum ROI & Patient Experience

Expanded APP-ID provides visibility, focused operational insights, and enhanced security

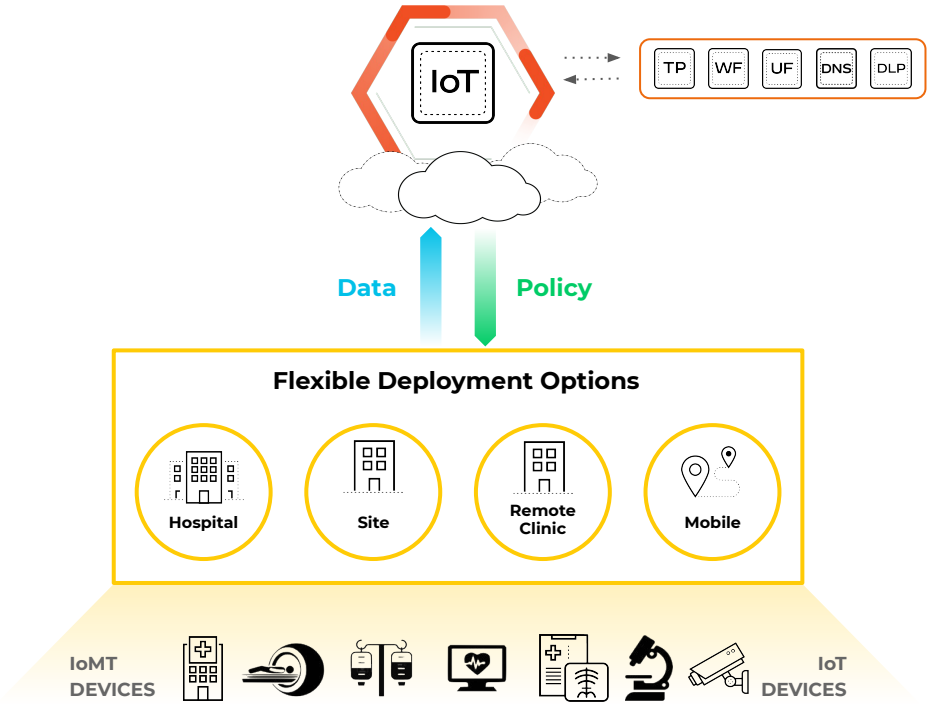


Effortless Deployment

A single platform seamlessly integrated into existing workflows for infrastructure, security, and clinical teams

 © 2021 Palo Alto Networks, Inc. All rights reserved.

Best-in-Class Healthcare IoT Security



- Available on Hardware, Software and Cloud-delivered
- Scale linearly with multi-tenant cloud infrastructure
- Leverage leading prevention from other Security Services
- Automate workflows with playbook driven integrations

 © 2021 Palo Alto Networks, Inc. All rights reserved.

IoT Security Features & Capabilities for Healthcare



1. Understand IoT Assets

- Identify 90+% of devices **within 48 hours**
- ML accurately classifies devices with **50+ attributes**
- **Continual detection** of new and never before seen devices
- **Maximise ROI** with utilization & remote maintenance insights

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
- Visibility into **FDA Recalls** & Manufacturer MDS2 Specifications

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 & Expanded App-IDs

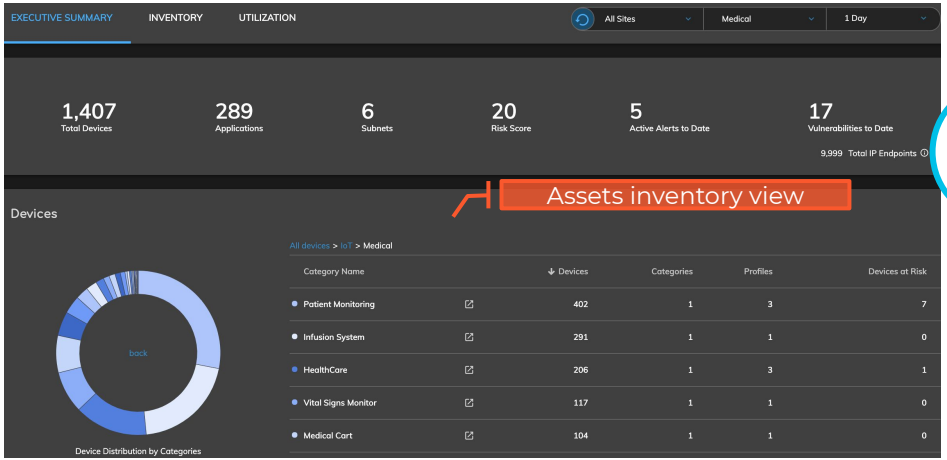
4. Prevent Known Threats

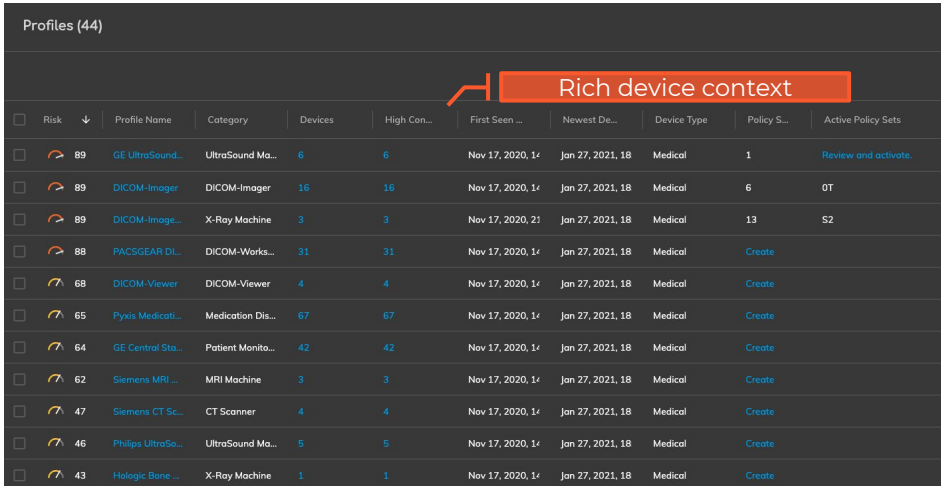
- **Protection from exploits**, C2, spyware and other known threats
- Enhance detail of all alerts with **IOT device context**

5. Detect & Respond to Unknown Threats

- Anomalous activity and **zero-day detection**
- **Stop unknown** file and web-based threats
- Detailed **incident context** for response
- Alert **MDS2 manufacturer** specification vs behavior anomalies

 © 2021 Palo Alto Networks, Inc. All rights reserved.



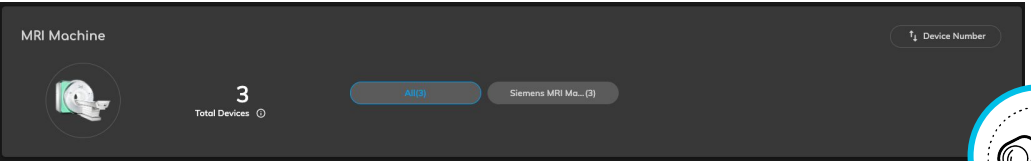


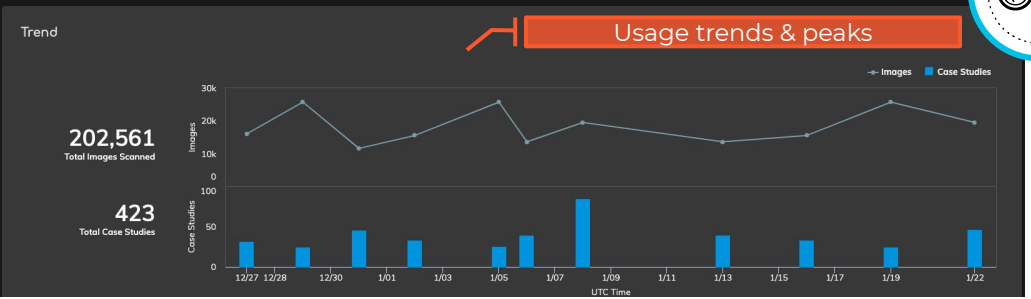
1. Understand all IoT Assets

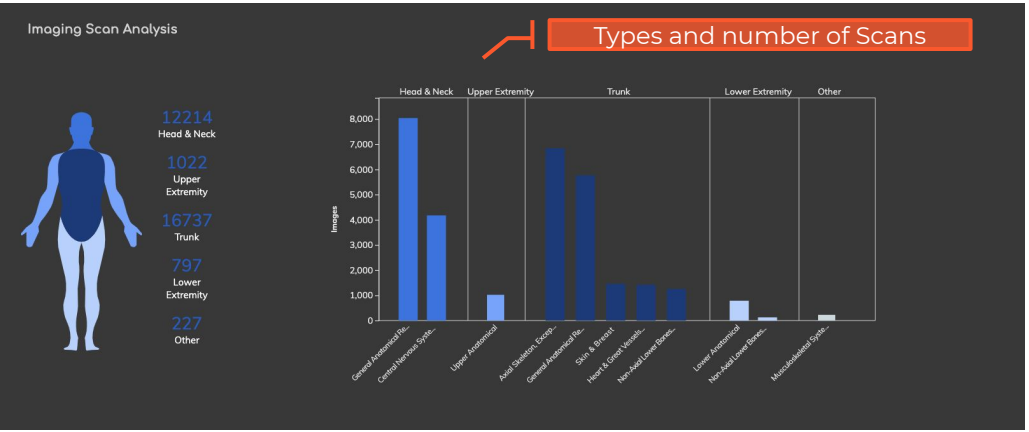
Identify devices quickly and accurately using the unique combination of machine learning and App-ID technology

- Discover any IoMT, IoT or IT device on your network with 90+% found within first 48 hours
- Identifies new, never-seen-before devices and gain deep insights from 50+ attributes
- Continuously monitor and enforce onboarding procedure

 © 2021 Palo Alto Networks, Inc. All rights reserved.





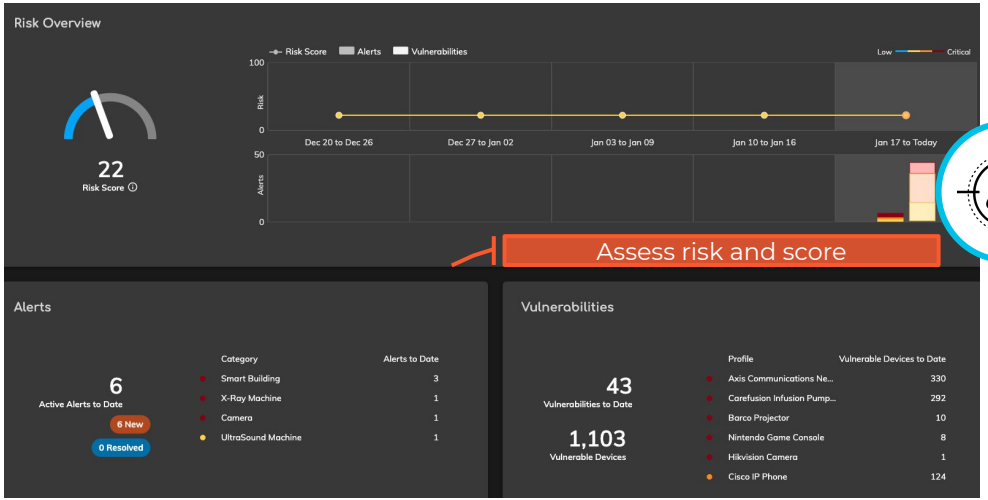


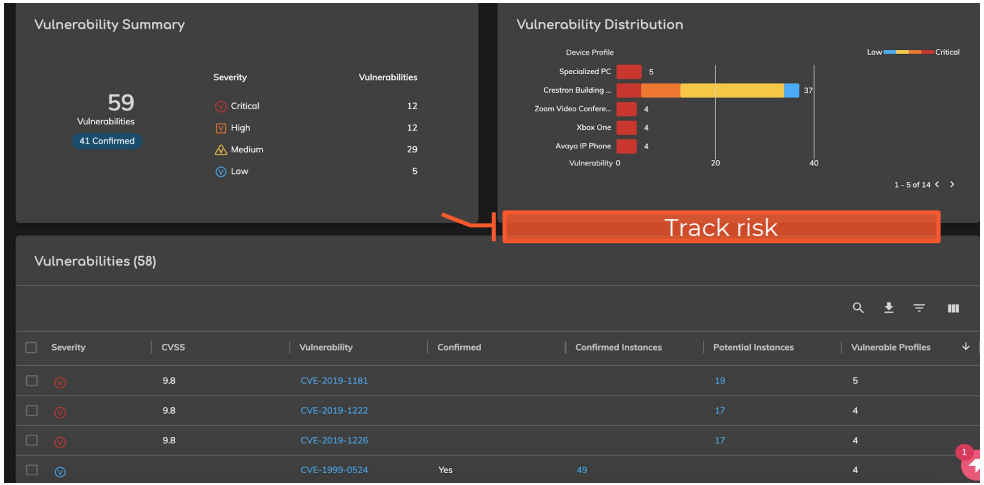
1. Understand all IoT Assets

IoMT device utilization to optimize patient care and capital planning

- Get rich operational insights
- Plan preventive maintenance
- Visualize and generate reports

 © 2021 Palo Alto Networks, Inc. All rights reserved.



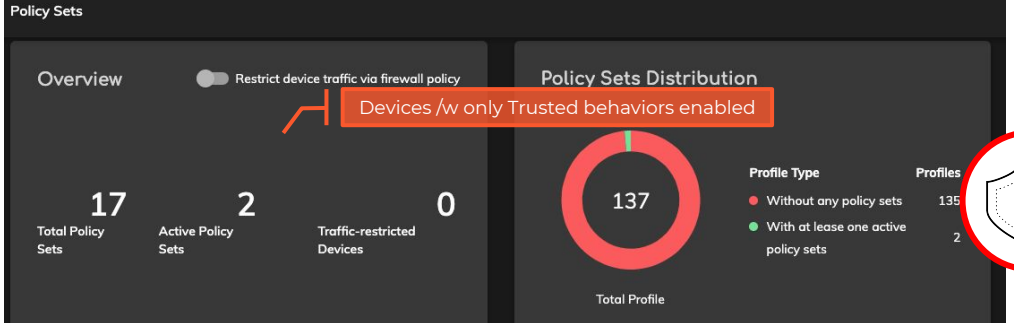


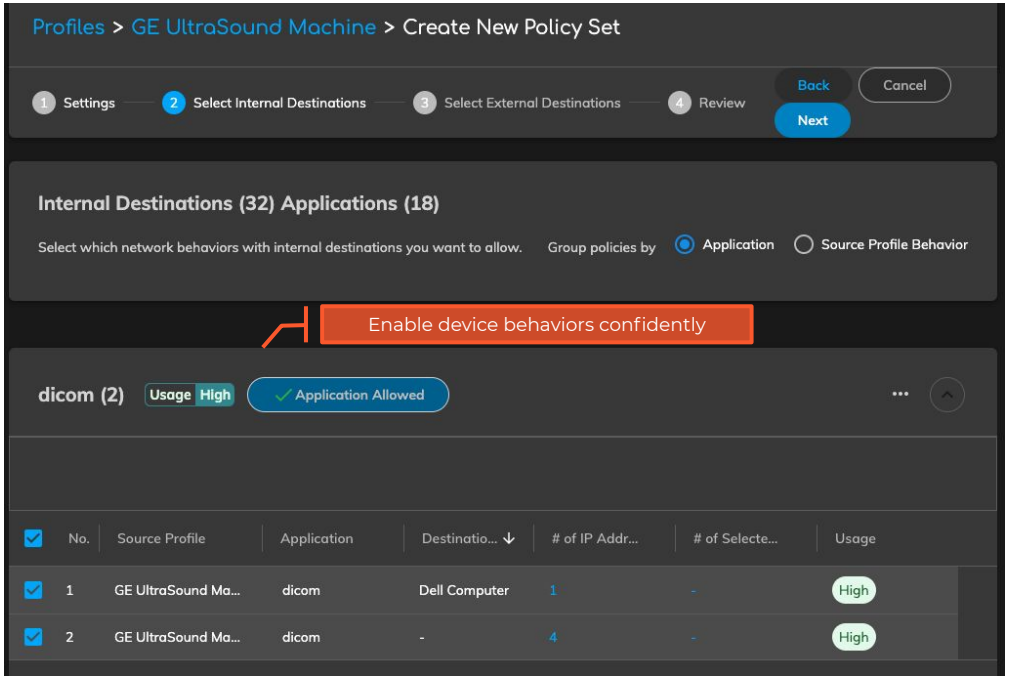
2. Assess IoT Risk

Real-time monitoring and risk scoring allows security teams to prioritize efforts based on individual or groups of devices

- Automatically assess risk based on vendor advisories, MDS2 details, FDA recalls, vulnerability information, anomalous device behavior, Unit 42 and other intel
- Scores and tracks risk changes over time for compliance and retrospective analysis
- Customize risk levels to match existing risk frameworks

 © 2021 Palo Alto Networks, Inc. All rights reserved.



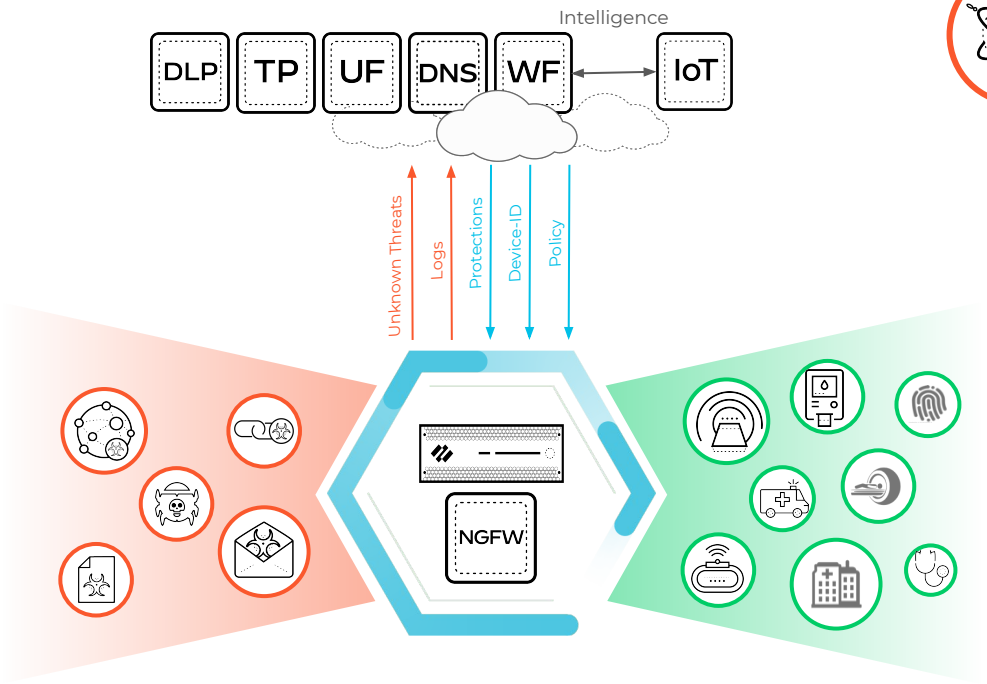


3. Apply Risk Reduction Policies

Consistent profiling of device activity is accurately converted into risk-based policy recommendations, allowing security teams to confidently allow only trusted behavior

- Gain context for segmenting IoMT, IoT and IT devices to reduce your attack surface
- Eliminate pain-staking policy creation for Zero-trust with recommended policies
- Enforce policies natively or via an integration in just a few clicks
- Monitors behavior and applies updates automatically with the new Device-ID construct

 © 2021 Palo Alto Networks, Inc. All rights reserved.

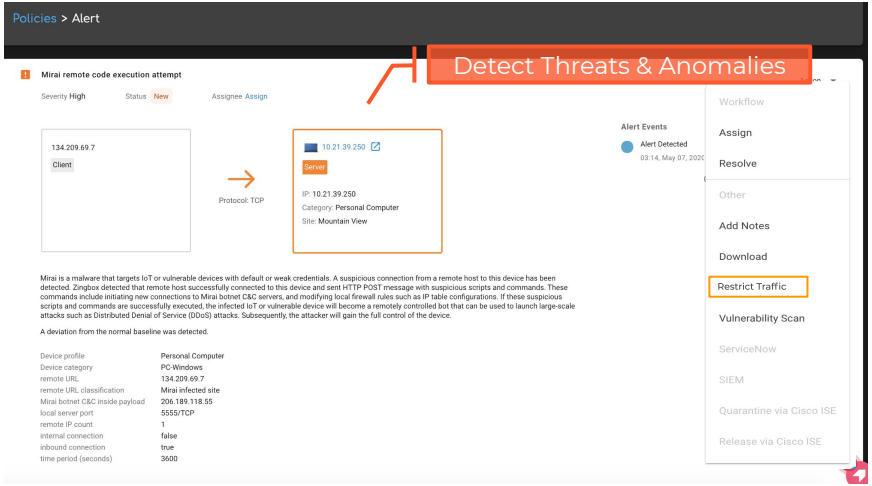


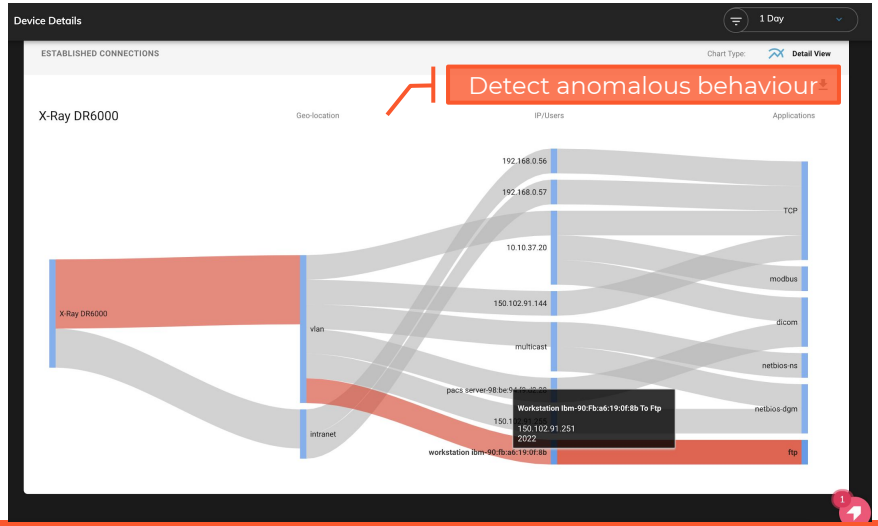
4. Prevent Known Threats

Our leading Security Services stop all threats targeting IoMT, IoT and IT devices.

- Block known targeted IoT malware, spyware and exploits
- Provide safe web access for IoT device and stop bad URLs or malicious websites
- Prevent the use of DNS for C2
- Stop the loss of confidential and patient data
- Eliminate the burden of detection alerts that can be prevented

 © 2021 Palo Alto Networks, Inc. All rights reserved.







5. Detect & Respond to Unknown Threats

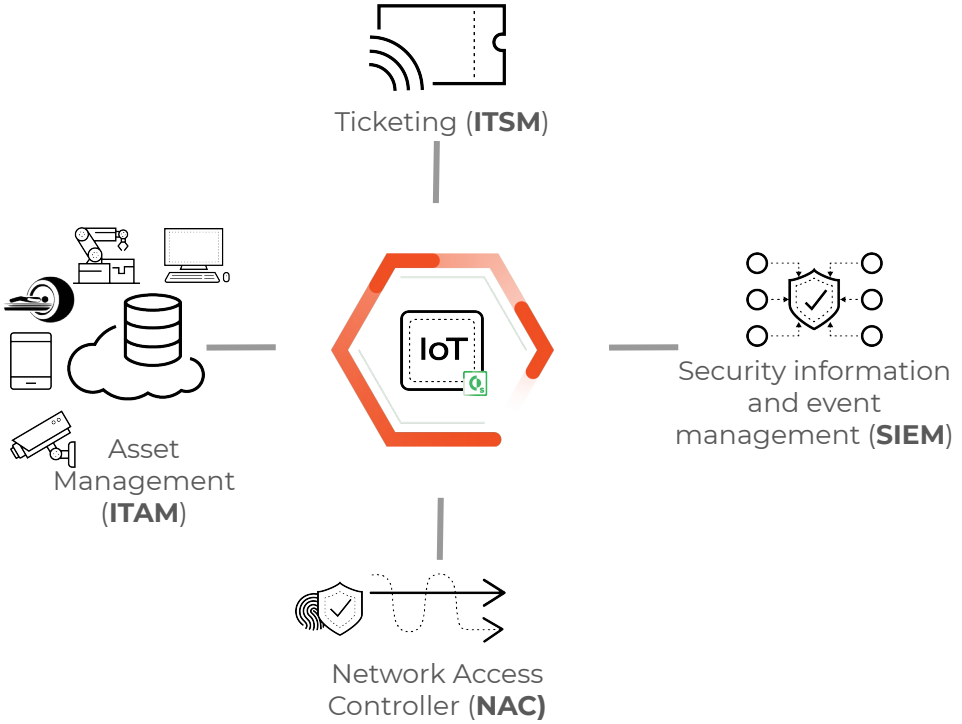
Use existing processes to respond to risks and threats unique to your environment.

- Block unknown file and web-based threats
- Detect and analyze anomalous activity, factoring in MDS2 and other data
- Use detailed device context to help analysis of any alert
- Use customizable playbooks to orchestrate response

 | © 2021 Palo Alto Networks, Inc. All rights reserved.

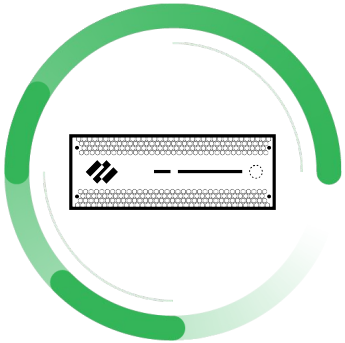
3rd Party Integrations

- Seamlessly integrate into existing security and clinical workflows
- Avoid resource intensive programming with customizable playbooks
- Upgrade to Cortex XSOAR to enable use cases for over 550+ integrations



 © 2021 Palo Alto Networks, Inc. All rights reserved.

Protect Every Device On Your Network



Use Existing Infrastructure

15x Time Saving

Deploy within minutes, no siloed sensors or enforcement products required



Leverage Existing Talent

18x Faster Policy Creation

Maintain current operations and empower your existing Network Security team to protect IoT



Get Complete IoT Security

37x Security Efficiency

Discover, secure and prevent threats on every IoT device in your network with one solution

 © 2021 Palo Alto Networks, Inc. All rights reserved.

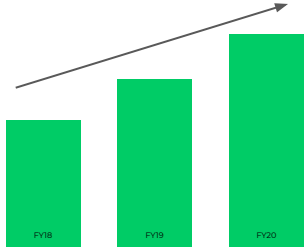
The World's Leading Cybersecurity Company

95
of Fortune 100
Rely on Palo Alto Networks



71% of the Global 2K
Are Palo Alto Networks Customers

#1
in Enterprise Security
Revenue trend 22% CAGR
FY18 – FY20



18% Year-Over-Year
Revenue Growth

77,000
Customers
In 150+ Countries

6 YEARS IN A ROW

J.D. POWER 2020 CERTIFIED ASSISTED TECHNICAL SUPPORT

2020 tsia RATED OUTSTANDING
PALO ALTO NETWORKS | GLOBAL ASSISTED AND SELF-SERVICE SUPPORT

2015 • 2016 • 2017 • 2018 • 2019 • 2020

9/10
Average CSAT Score

Gartner, Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q19, 20 March 2020

Thank You

UNIT 42 & IOT THREAT REPORT 2020

paloalto NETWORKS

DON'T FORGET A TOWEL

UNIT 42

The ultimate question of life, the universe and everything



GLOBAL THREAT INTELLIGENCE TEAM



COLLABORATION



DON'T PANIC

 © 2021 Palo Alto Networks, Inc. All rights reserved.

Unit 42 IoT Threat Report: Highly Vulnerable Medical Devices



of all IoT device traffic is unencrypted



of all IoT devices are vulnerable to medium or high severity attacks

“83% of Imaging Systems Powered by End-of-Life OS”



of all attacks are exploits, making IPS a requirement



of HDOs have a mix of IT and IoMT devices in the same VLANs

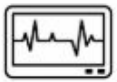
 © 2021 Palo Alto Networks, Inc. All rights reserved.

Unit 42 IoT Threat Report: Most High Risk Devices?



Medical Imaging Systems

51%



Patient Monitoring Systems

26%



Security Cameras

33%



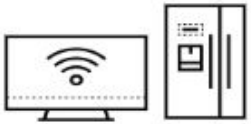
Printers

24%



Medical Device Gateways

9%



Consumer Electronics

7%



Energy Management Devices

6%

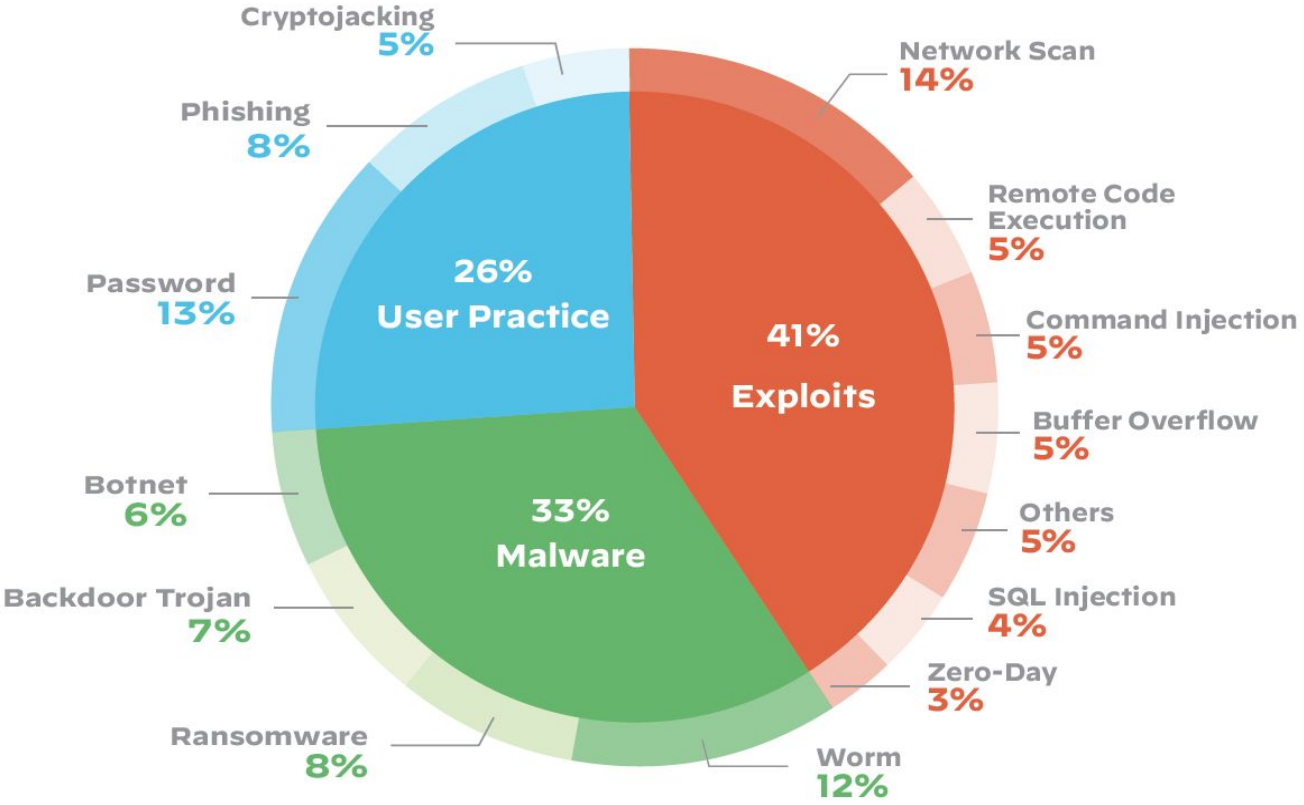


IP Phones

5%

 © 2021 Palo Alto Networks, Inc. All rights reserved.

Unit 42 IoT Threat Report: Top Threats for IoT Devices



 © 2021 Palo Alto Networks, Inc. All rights reserved.

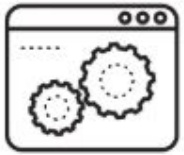
Unit 42 IoT Threat Report: Why are IoT The Ideal Entry Point?



Zero to Minimum Built-In Security



Browser Interface Vulnerabilities



Outdated Operating Systems



Failure to Adhere to Security Best Practices

 © 2021 Palo Alto Networks, Inc. All rights reserved.

Thank you

Trust Every Device On Your Network

