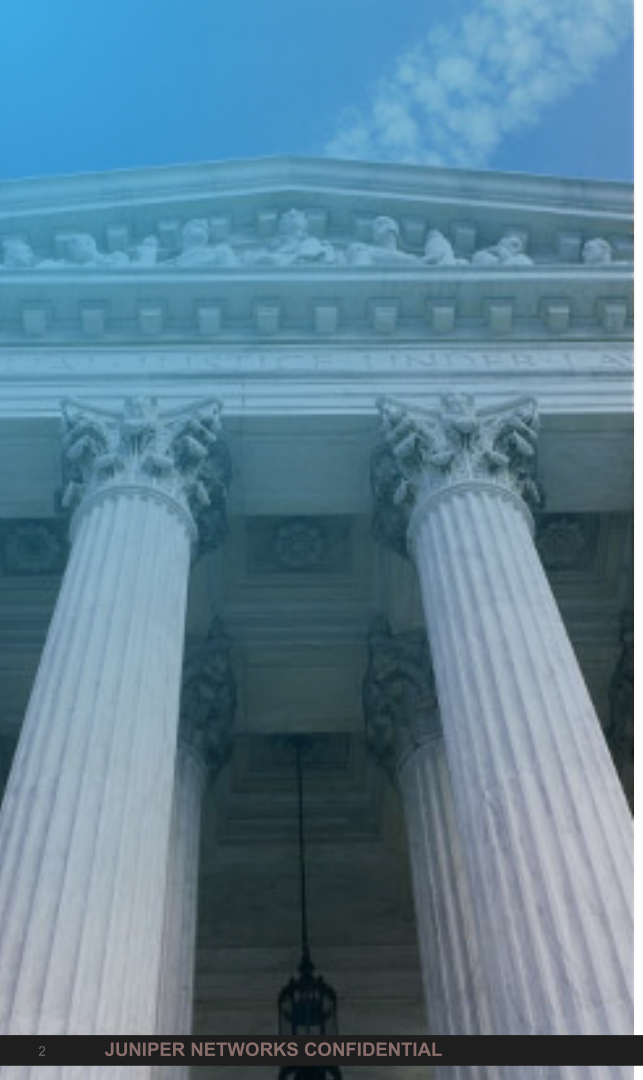
# SDSN for IoT

## Stopping threats to the new IoT network

Ben Baker – benbaker@juniper.net



# Legal Statement Regarding Current Products and Intentions

This statement of product direction sets forth Juniper Networks' current intention and is subject to change at any time without notice. No purchases are contingent upon Juniper Networks delivering any feature or functionality depicted on this statement.

**This presentation is subject to NDA stipulations**


IoT Ransomware

# IoT – The Art of Optimization

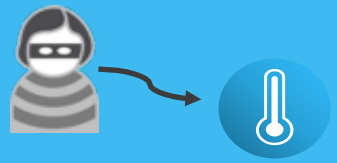

Optimal outcomes

# IoT – Security Threats


Destruction & Chaos

# IoT ransomware – a flow chart…

Malware infiltration



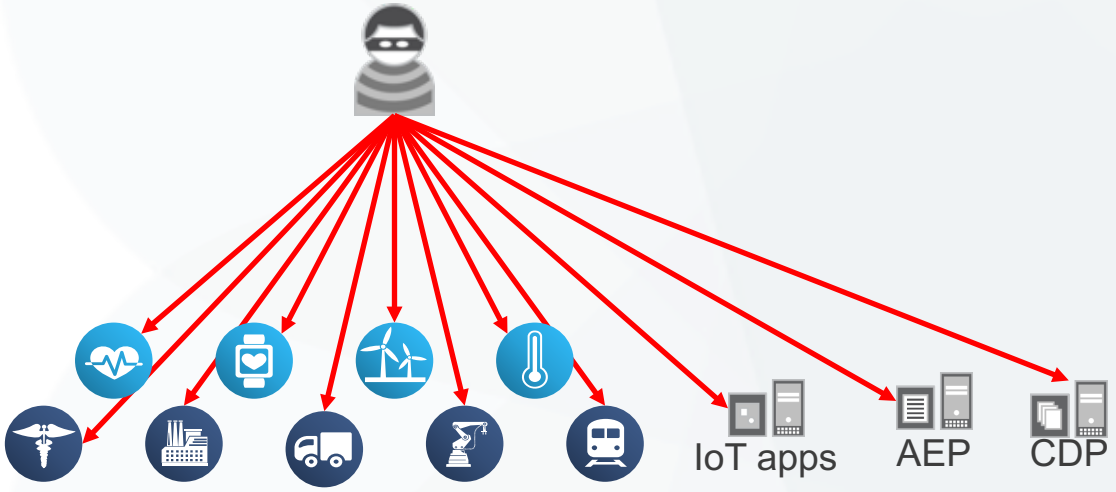
Threatens destruction

# Getting ransomware and malware into IoT networks

DNS spoofing

Default passwords

Phishing attacks




Both IoT devices **and** IoT application servers / supporting servers

# Real world examples of IoT malware / ransomware

## Example 1:

**Thermostat ransonware**

http://motherboard.vice.com/read/internet-of-things-ransomware-smart-thermostat


## Example 2:

**Amazon cameras malware**

http://www.securityweek.com/malware-found-iot-cameras-sold-amazon

## Example 3:

**Jeep remote control**

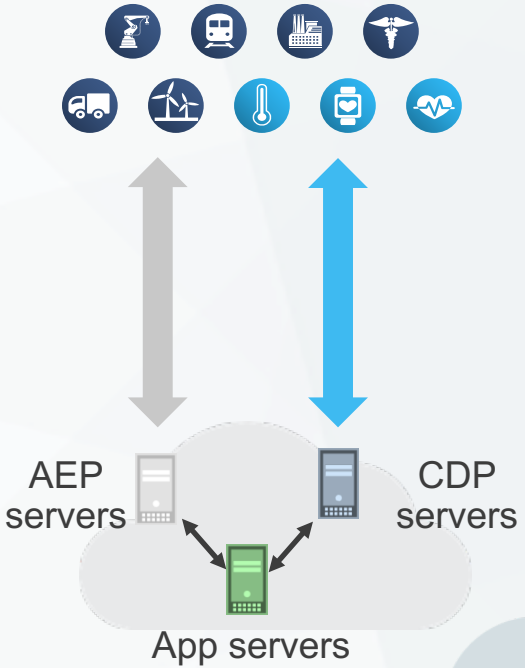
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

# Targets for IoT Ransomware and Malware

IoT devices

## Server side IoT

- IoT application servers
- Application Enablement Platforms
- Connected Device Platforms

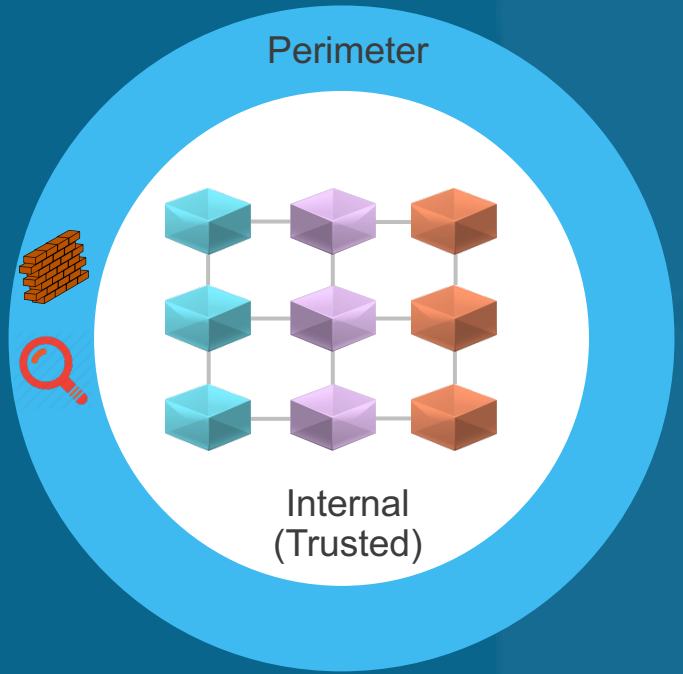


# Potential IoT ransomware

| IoT Ransomware | Impact |
| --- | --- |
| Connected home mayhem | Injury, destruction, death |
| Misdirect connected cars | Injury destruction, death |
| Stop traffic lights | Gridlock, mayhem, injury |
| Medical device remote control | Injury, death |
| Deactivate water quality sensors | Sickness, death |
| Remote control of industrial IoT | Injury, destruction, death |


Software Defined
Secure Networks
(SDSN)

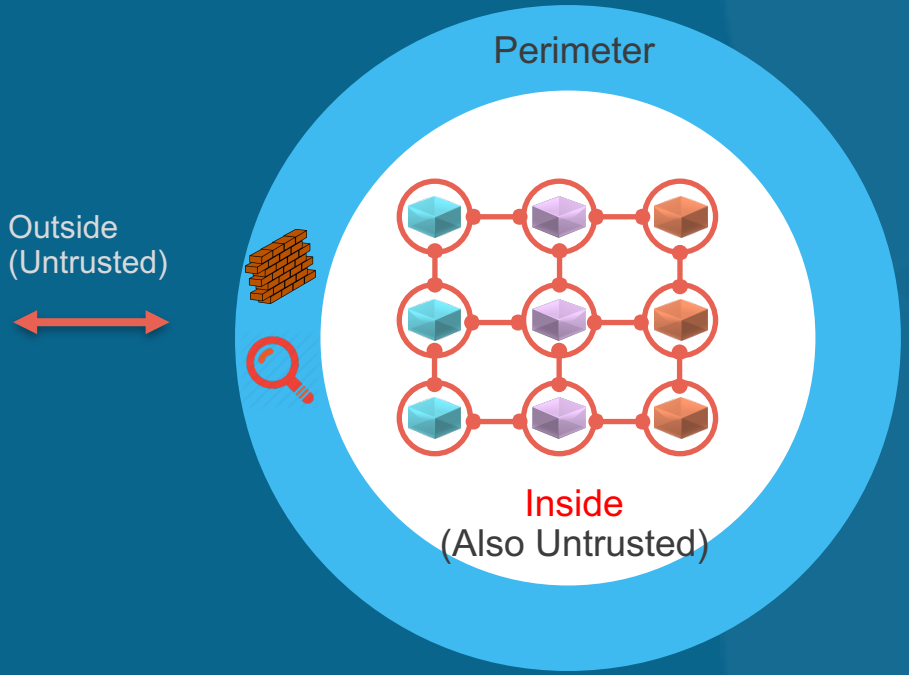
# Perimeter Oriented Security




- Hyper-connected Network Security at Perimeter
- Complex Security Policies
- Lateral Threat Propagation
- Limited Visibility

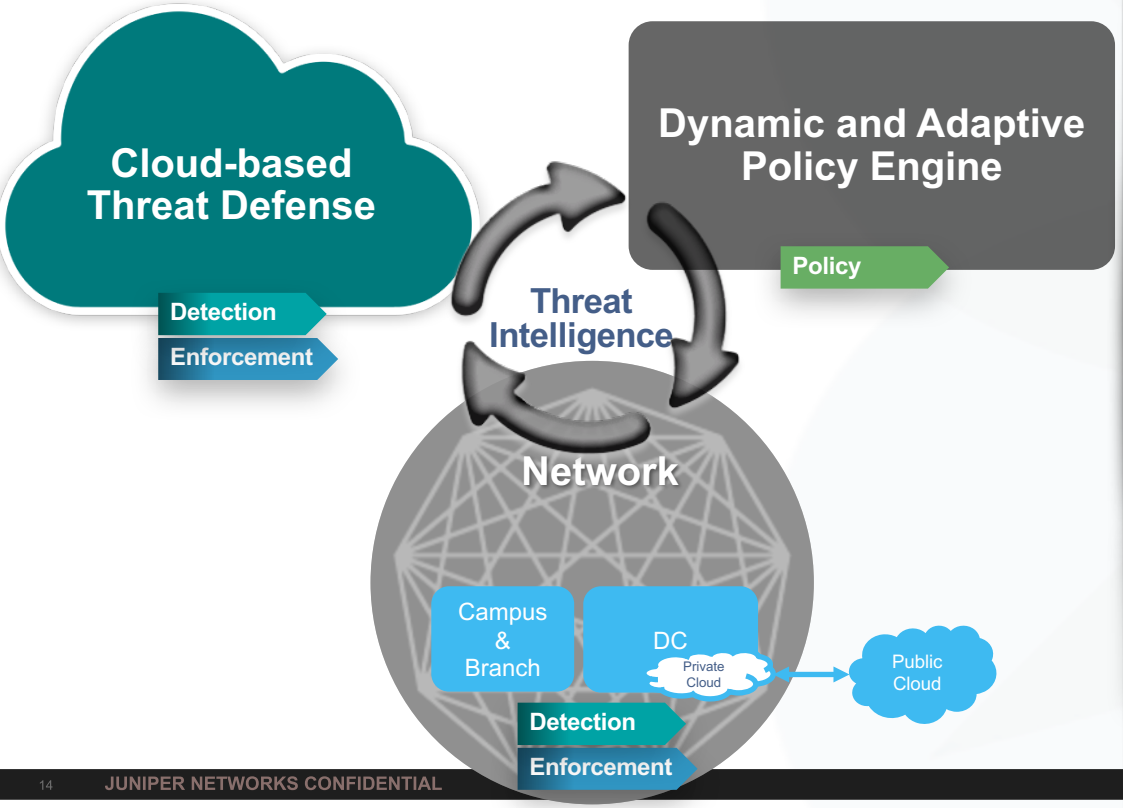
# Software Defined Secure Network

## Delivers Zero Trust Security Model




- Secure Network
- Simplified Security Policy
- Block Lateral Threat Propagation
- Comprehensive Visibility

# Software-Defined Secure Network
## Policy, Detection & Enforcement




## Bottoms Up and Top Down Approach –

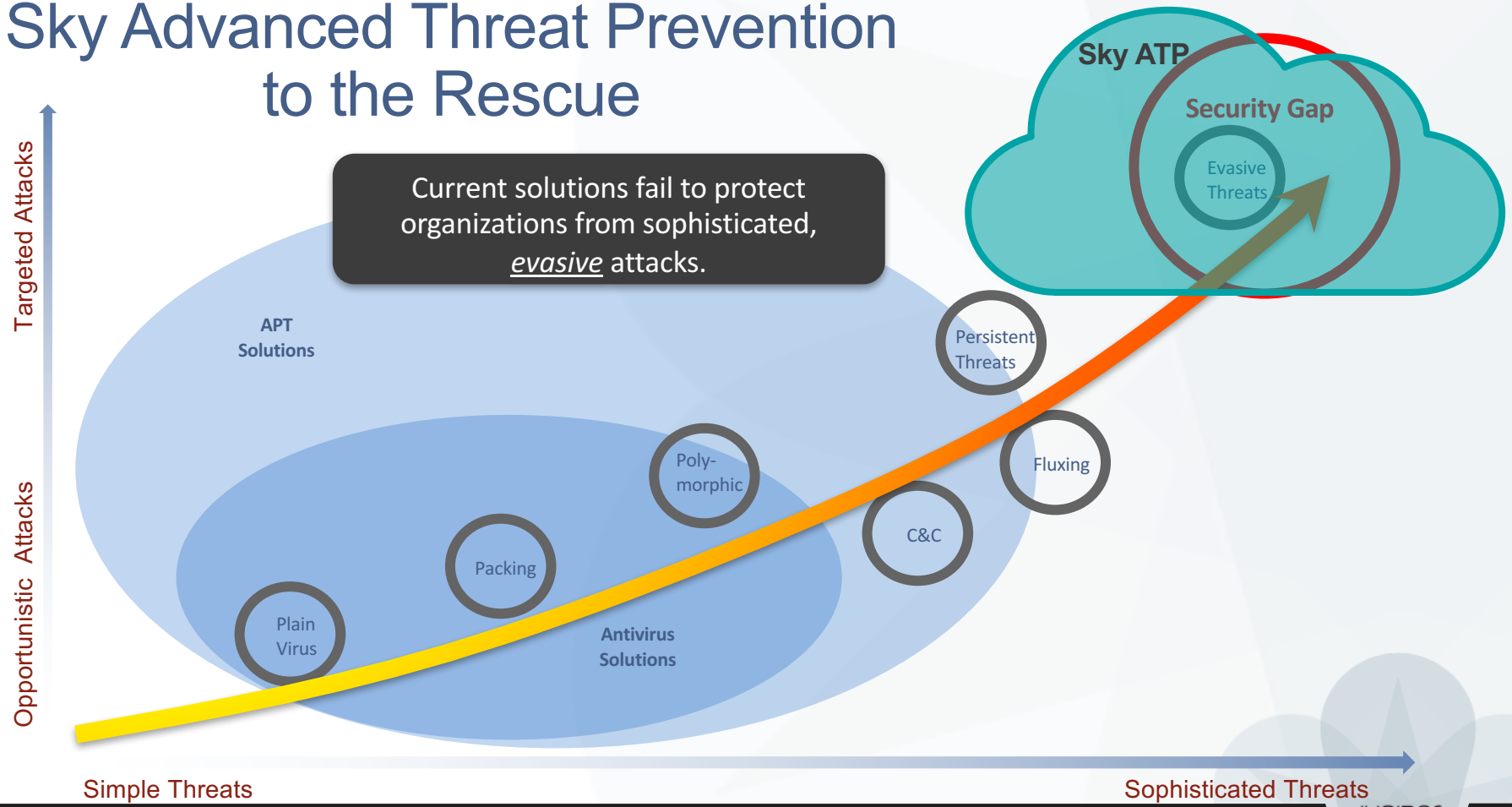
Leverage **entire network and ecosystem** for threat intelligence and detection

Utilize **any point** of the network as a **point of enforcement**

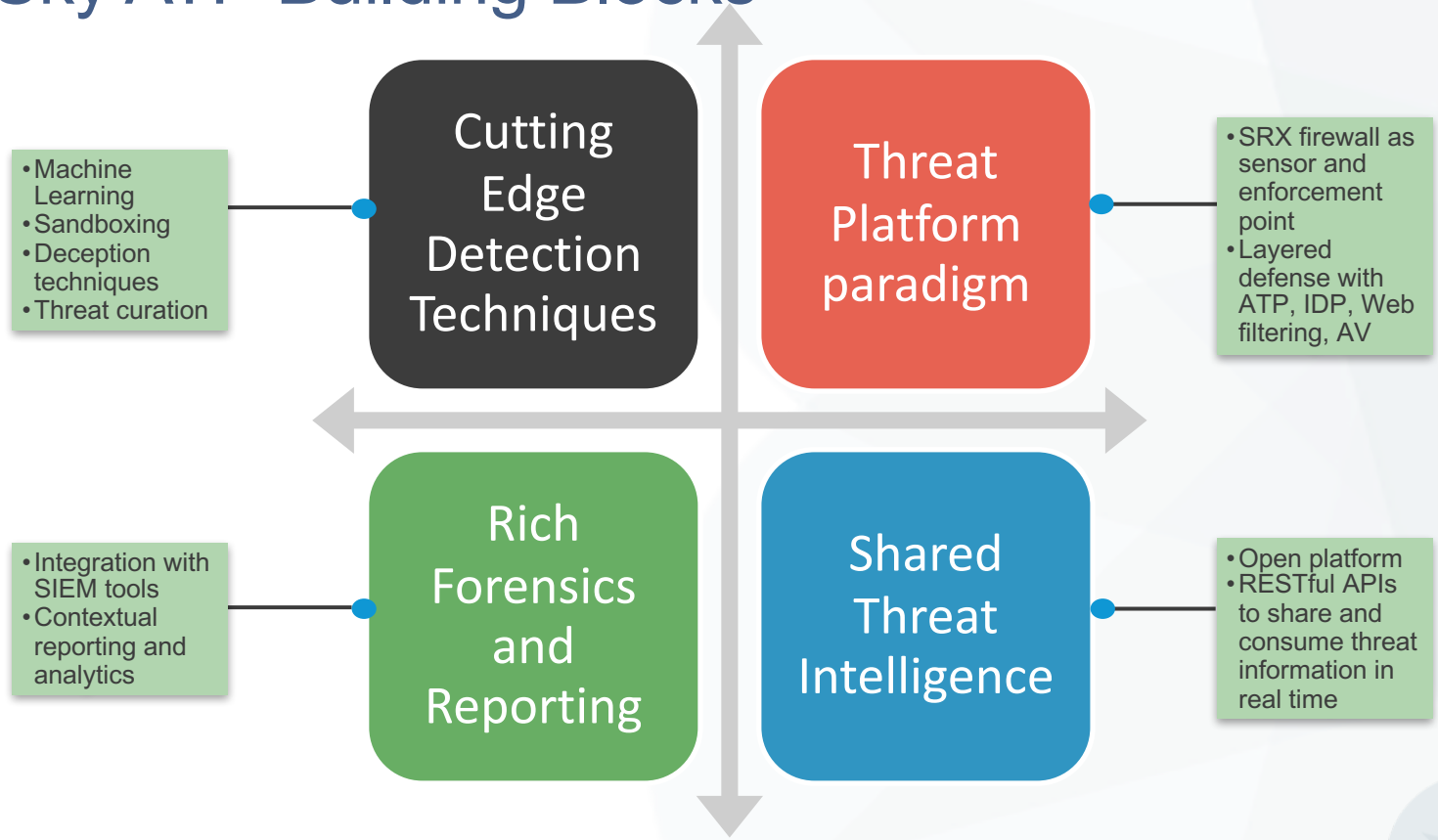
**Dynamically execute policy** across all network elements including third party devices


Detection: Sky ATP

# Sky Advanced Threat Prevention to the Rescue



# Sky ATP Building Blocks



# The ATP Verdict Chain

## Staged Analysis: combining rapid response and deep analysis


Suspect files enter the analysis chain in the cloud

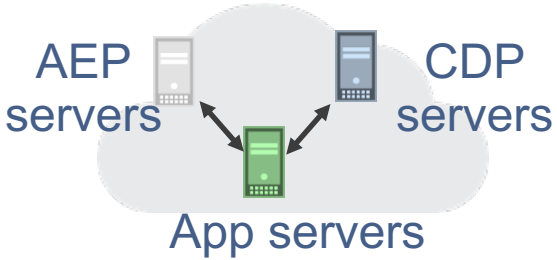
**Cache lookup: (~1 second)**
Files we've seen before are identified and a verdict immediately goes back to SRX

**Anti-virus scanning: (~5 second)**
Multiple AV engines to return a verdict, which is then cached for future reference

**Static analysis 1st stage: (~5 second)**
The static analysis engine does a deeper inspection, with the verdict again cached for future reference

**Dynamic analysis: (~7 minutes)**
Dynamic analysis in a custom sandbox leverages deception and provocation techniques to identify evasive malware. The 2nd stage Static Analysis run in parallel

# IoT specific Advanced Threat Detection




## IoT servers

Based on Windows or Linux

Juniper Policy Enforcer can stop East-West propagation

## IoT devices

Many are Linux based

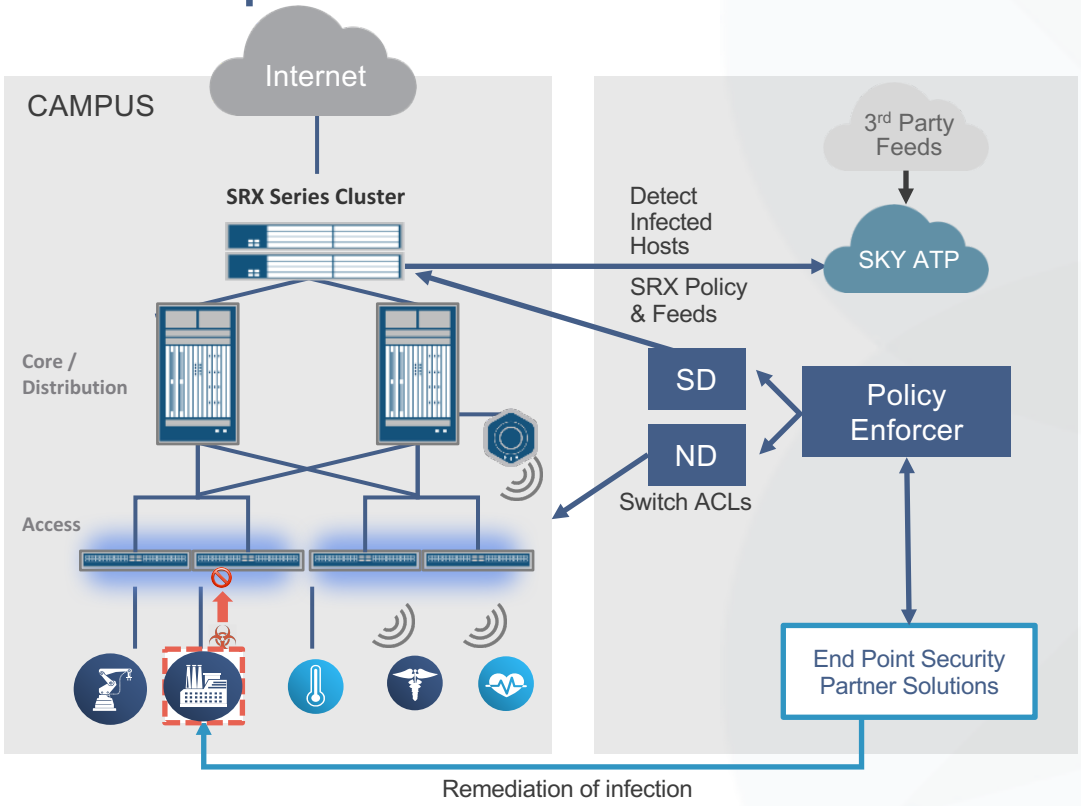
Sky ATP: static & dynamic analysis for IoT malware

Will be tailored for specific devices & applications

**SkyATP supports 3rd party detection integration**


SDSN Solutions to IoT Threats

# Enterprise IoT infection – SDSN solution



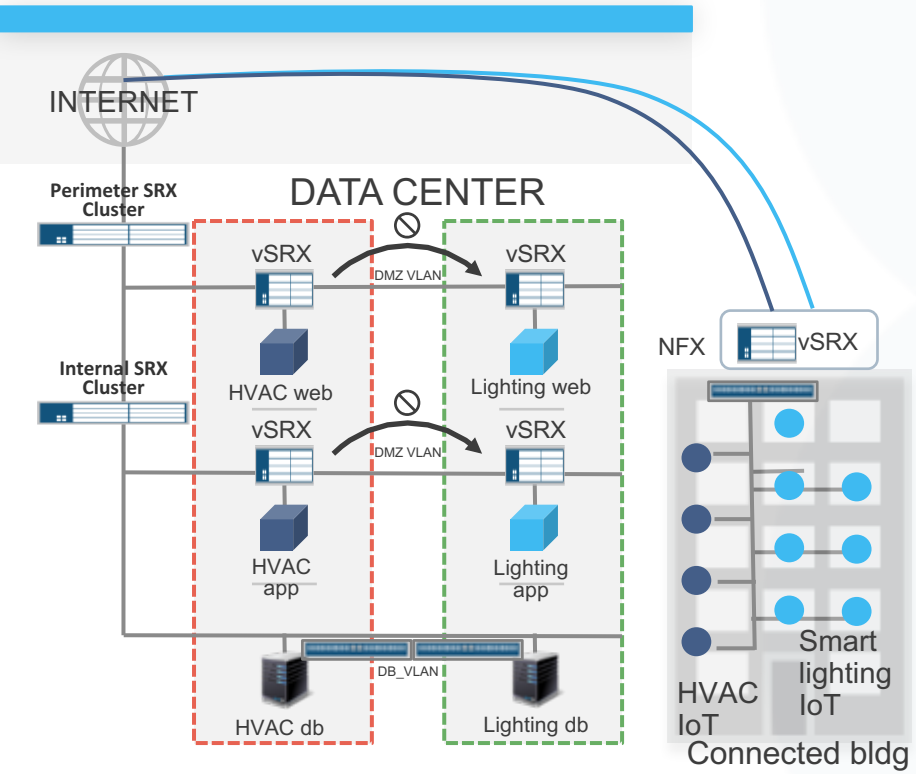

## THREATS

- Lateral threat propagation
- IoT botnet army recruitment

## SOLUTION BEHAVIORS

- SkyATP detection of infected IoT UEs
- C&C feeds
- Policy per IoT device type
- Enforce @ JNPR routers, switches, firewalls using infected host feed
- 3rd party remediation of infection

# Smart city connected buildings – SDSN solutions



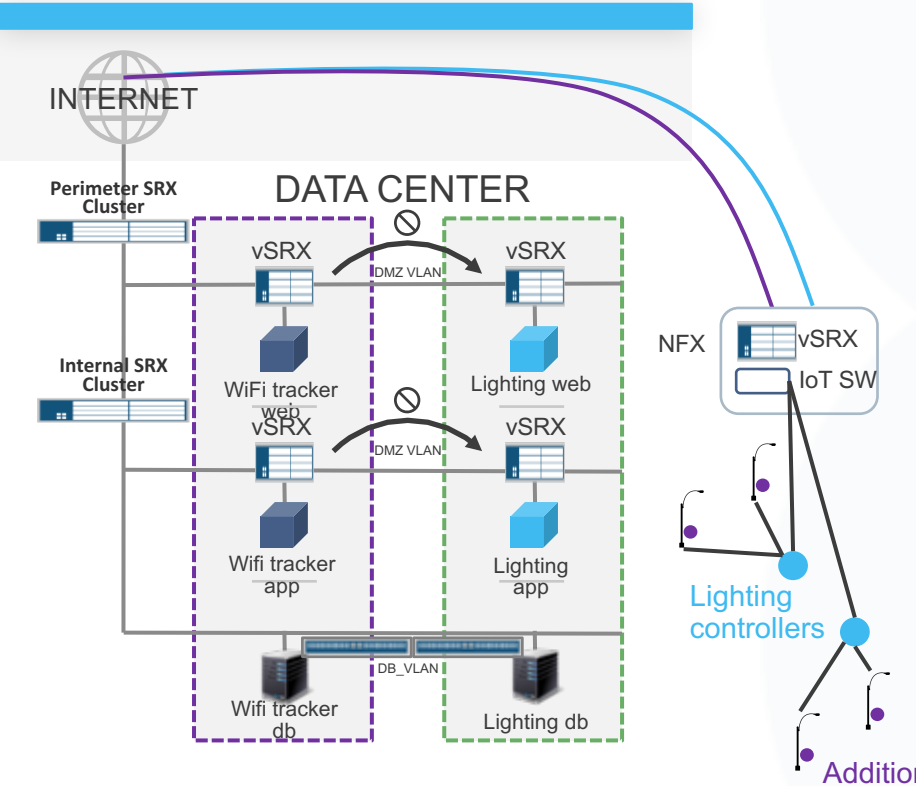

## THREATS

- Malware / ransomware targeted at IoT devices
- IoT device traffic “wandering”
- IoT devices attacking IoT servers

## SOLUTION BEHAVIORS

- SDN w/NFX & Contrail to service chain vSRX
- vSRX / NFX limits lateral threat propagation & quarantines infected servers & IoT devices
- SkyATP detection of infections
  - @ Connected building: infected IoT
  - @ DC: infected app/web/db servers
- vSRX protocol conformance / enforcement
- Traffic policies enforced w/ v/SRX & switches

# Smart city lighting – SDSN solution



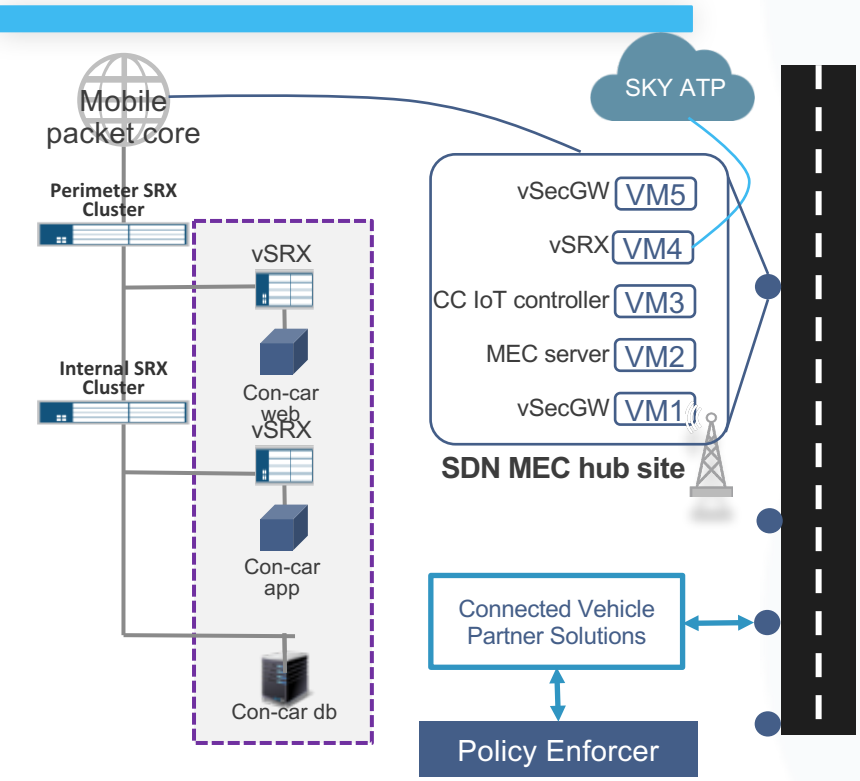

## THREATS

- Malware / ransomware targeted at IoT devices
- IoT device traffic “wandering”
- IoT devices attacking IoT servers

## SOLUTION BEHAVIORS

- SDN w/NSX & Contrail to service chain vSRX
- vSRX / NSX limits lateral threat propagation & quarantines infected servers & IoT devices
- SkyATP detection of infections
  - Lighting controllers & Additional sensors
  - @ DC: infected app/web/db servers
- vSRX protocol conformance / enforcement
- Traffic policies enforced w/ v/SRX & switches

# Connected vehicles – SDSN solution



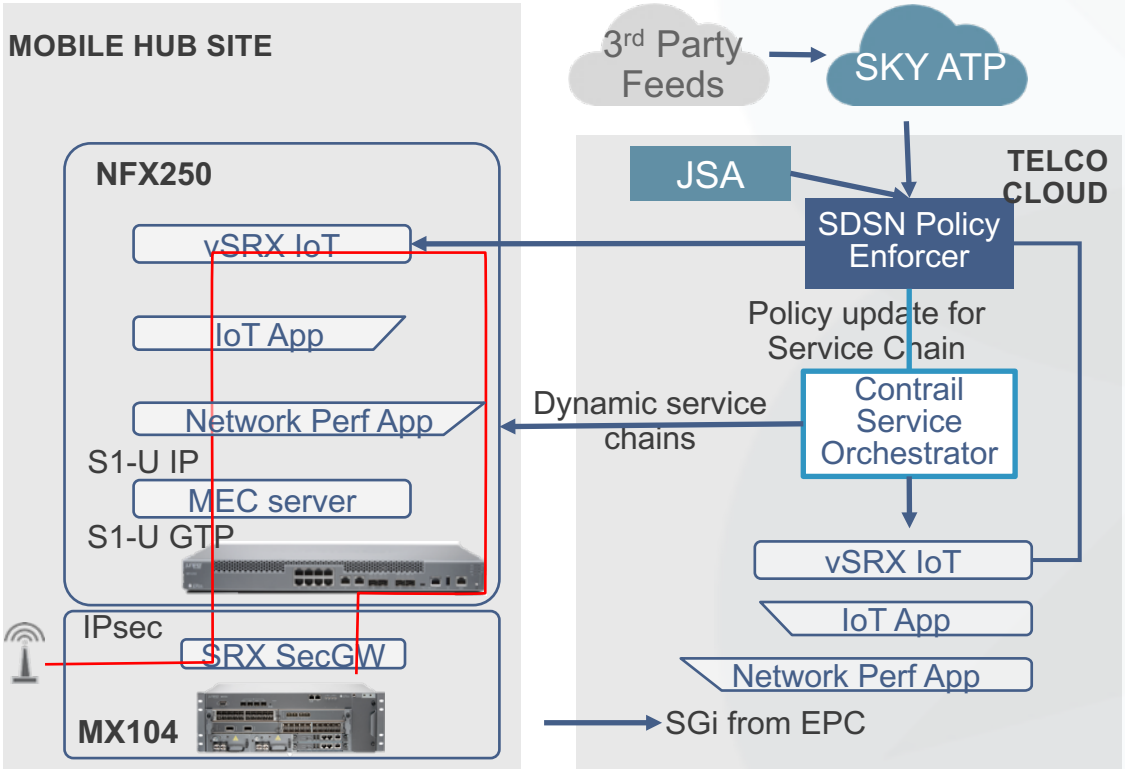

## THREATS

- Disable connected vehicles
- Weaponize connected vehicles
- Vehicle hijacking
- Theft of connected vehicle metadata

## SOLUTION BEHAVIORS

- Enforce network traffic flow policies
- vSRX enforcing protocol conformance
- Sky ATP detects connected vehicle and server side app malware / ransomware
- Quarantine infected vehicles /server side apps
- 3rd party
- MEC for high performance / low latency

# IoT Infected Host Workflow – MEC and mobile




## THREATS

- IoT botnet army recruitment

## SOLUTION BEHAVIORS

- SkyATP detection of infected IoT UEs
- C&C feeds
- Policy per IoT device type
- Enforce @ MEC with vSRX firewalls using infected host feed

# Recap

| SDSN | SDSN FOR IOT | IOT RANSOMWARE & MALWARE | RANSOMWARE & MALWARE |
| --- | --- | --- | --- |
| Detect, policy, enforce | Specific detection for IoT devices | Creating destruction from optimization | Coming to an IoT solution near you |

*BE SAFE: PRACTICE SDSN*

# Thank you