

Securing Your Fleet from Cyber Intrusion

Public Transportation & Mobility
September 26, 2018

Why does Conduent care about this problem?

Because Conduent is embedded into the daily operations of thousands of clients.

20 of 20

managed U.S. healthcare plans are clients

Nearly 40%

U.S. hospitals count on our solutions

2 out of 3

touch 2 out of every 3 insured patients in the U.S.

46%

of U.S. electronic toll collection market served

8.9 million

people estimated to travel daily through toll systems we manage

25 million

card holders' experience is modernized with our digital payment solutions

4 of 5

top global phone manufacturers count on our services

#1 provider

of parking solutions in the U.S. with award-winning innovation

43%

of all U.S. child support payments processed annually

3 of 5

top U.S. mobile phone providers rely on us to deliver customer care

Cyber intrusions, without exception, pose a threat in every sector.

Bottom Line Up Front (BLUF)

All of the assets in your environment should be *known, authorized, managed, and monitored.*



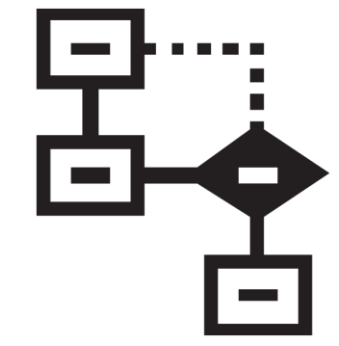
Known

constantly scanning for unknown assets and when found they should be interrogated to determine if they belong



Authorized

only assets that are explicitly authorized should be allowed to remain in the environment



Managed

all authorized assets should be controlled to ensure that they are properly updated and behaving as intended



Monitored

all assets and the network itself should be monitored to maintain situational awareness and provide actionable insight (including quarantining or removing compromised devices)



Cybersecurity incidents in recent news

The Washington Post
Democracy Dies in Darkness

Transportation

Metro cybersecurity audit highlights growing concerns at agencies across the country



New technology, such as that included in Metro's latest series of rail cars, the 7000s, makes the agency more vulnerable to hackers and other cyberattacks. (Bill O'Leary/Washington Post)

by [Martine Powers](#) July 7

Recent News

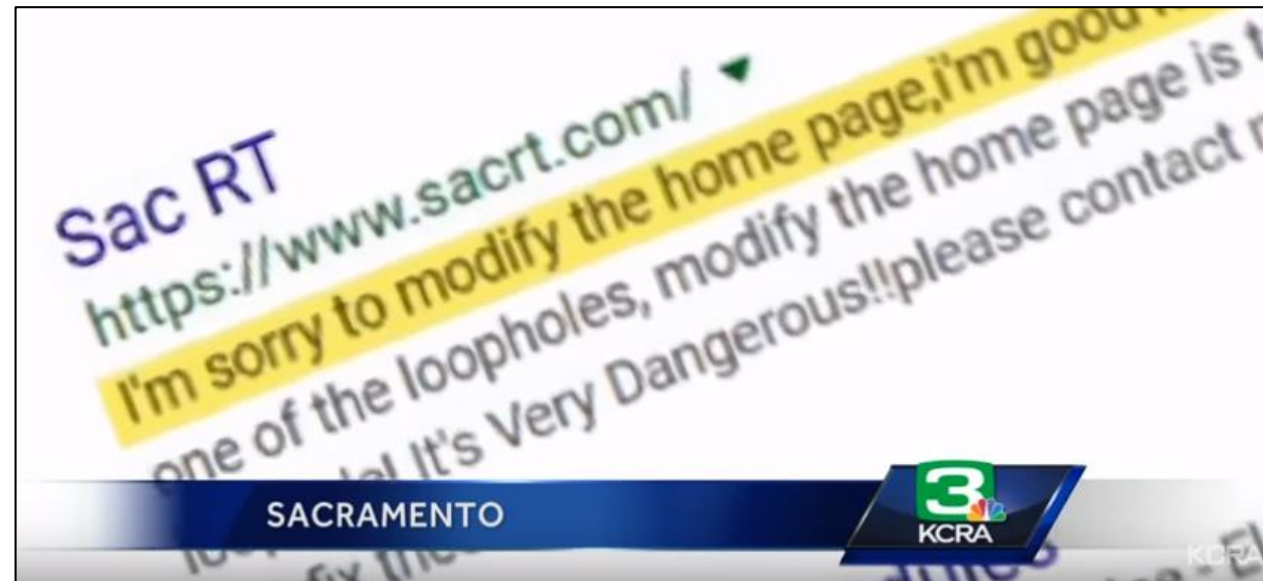
- The Washington Post
July 7, 2018
- [Metro cybersecurity audit highlights growing concerns](#)


Recent News

- Sacramento TV News
November 20, 2017

- [Hackers Attack Sacramento Regional](#)

- [Sacramento Regional Transit Hack](#)




 **KCRA News** ✓
Published on Nov 20, 2017

Sacramento's Regional Transit fell victim to a cyber attack over the weekend. The agency said data was deleted and the hackers even demanded a Bitcoin as ransom.

Recent News

- KPIX Channel 5
November 26, 2018
- [Muni Hacked](#)





KPIX CBS SF Bay Area
Published on Nov 26, 2016

'You Hacked, ALL Data Encrypted,' was the message at SF Muni stations across the city. Cate Cauguiran reports passengers were getting free rides all day on Saturday.

Recent News


- CBC News Network / CTV News
January 24, 2018
- [Metrolinx Targeted by Cyberattack](#)
- [North Korea cyber attack targets Ontario Agency](#)



Recent News

- **CBSN**
March 29, 2018
- [Atlanta Recovering from Cyberattack](#)




 **CBS News** ✓
Published on Mar 29, 2018

A ransomware attack on the city of Atlanta took down the municipality's online network for five days, leaving residents unable to pay bills, report potholes, use Wi-Fi at the airport, and more. New York Times reporter Alan Blinder is based in Atlanta and spoke with CBSN about why we're likely to see more hacks like this in the future.

Recent News

- **Help Net Security**
August 10, 2018
- [IoT malware found hitting airplanes' SATCOM systems](#)



 **Zeljka Zorz**, Managing Editor
August 10, 2018

Share this article



IoT malware found hitting airplanes' SATCOM systems

Waterfall Security: Trust issues with your firewalls? [Eliminating vulnerabilities that accompany firewalls is a click away.](#)

In 2014, IOActive researchers revealed security vulnerabilities they found in the most widely deployed satellite communications terminals and **presented** potential scenarios attackers could exploit once SATCOM systems have been compromised in the aviation, maritime, and military sectors. In 2018, they demonstrated that some of these theoretical scenarios are, unfortunately, still actually possible.

Ruben Santamarta, principal security consultant with IOActive, presented this latest research at this year's Black Hat conference in Las Vegas, and showed that it's possible for remote attackers to take control of airborne SATCOM equipment on in-flight commercial aircrafts, earth stations on vessels and those used by the US military in conflict zones.

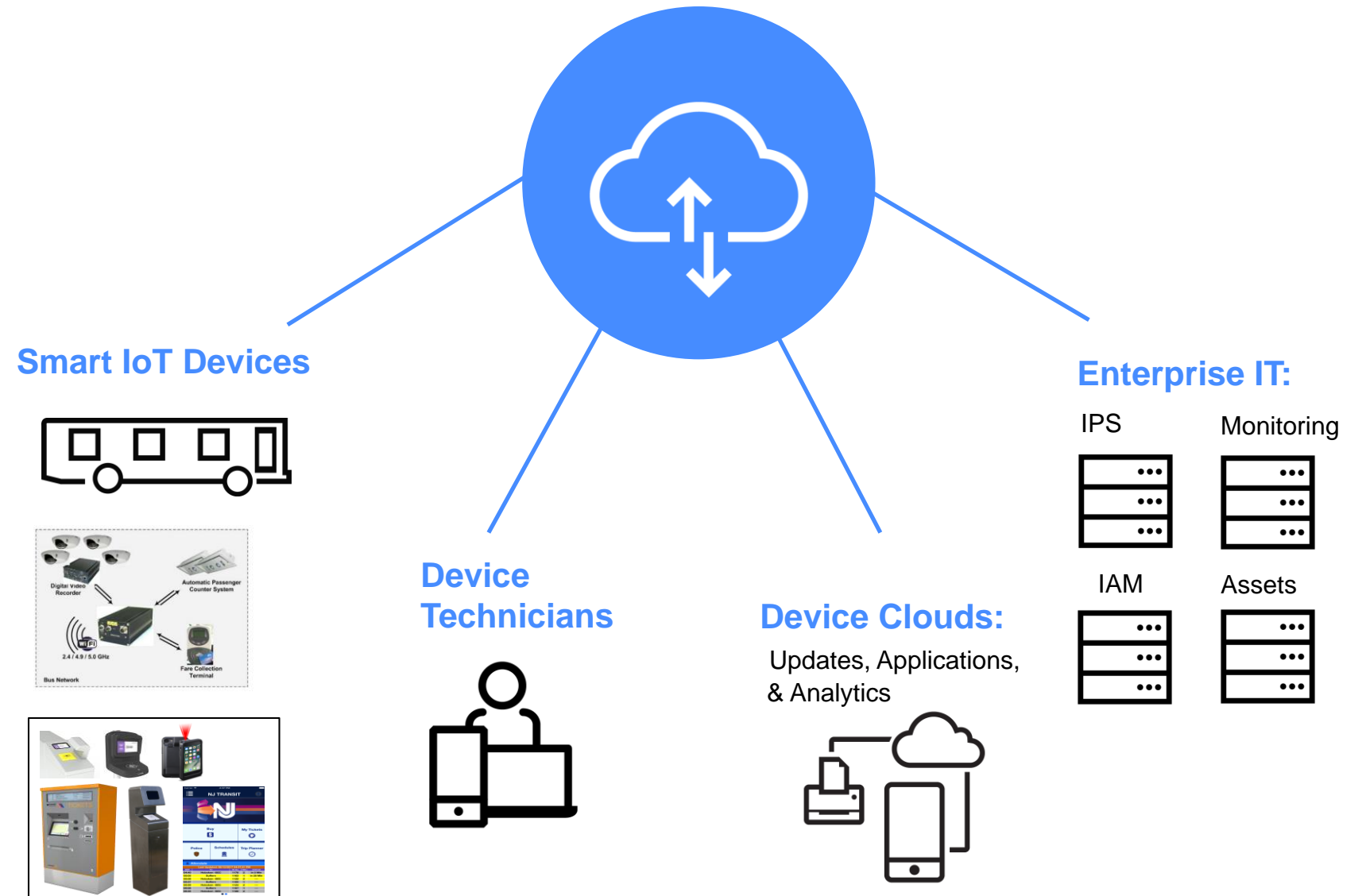


Protecting your agency from intrusion

The Problem

- General purpose and smart computing technology increases the value of IoT devices
- It also introduces vulnerability through entry points for cyber intrusions
- As each new device is added to a system, the risk increases exponentially
- The evolution towards end-to-end systems and MaaS will require comprehensive protection against risks

Device access and communications



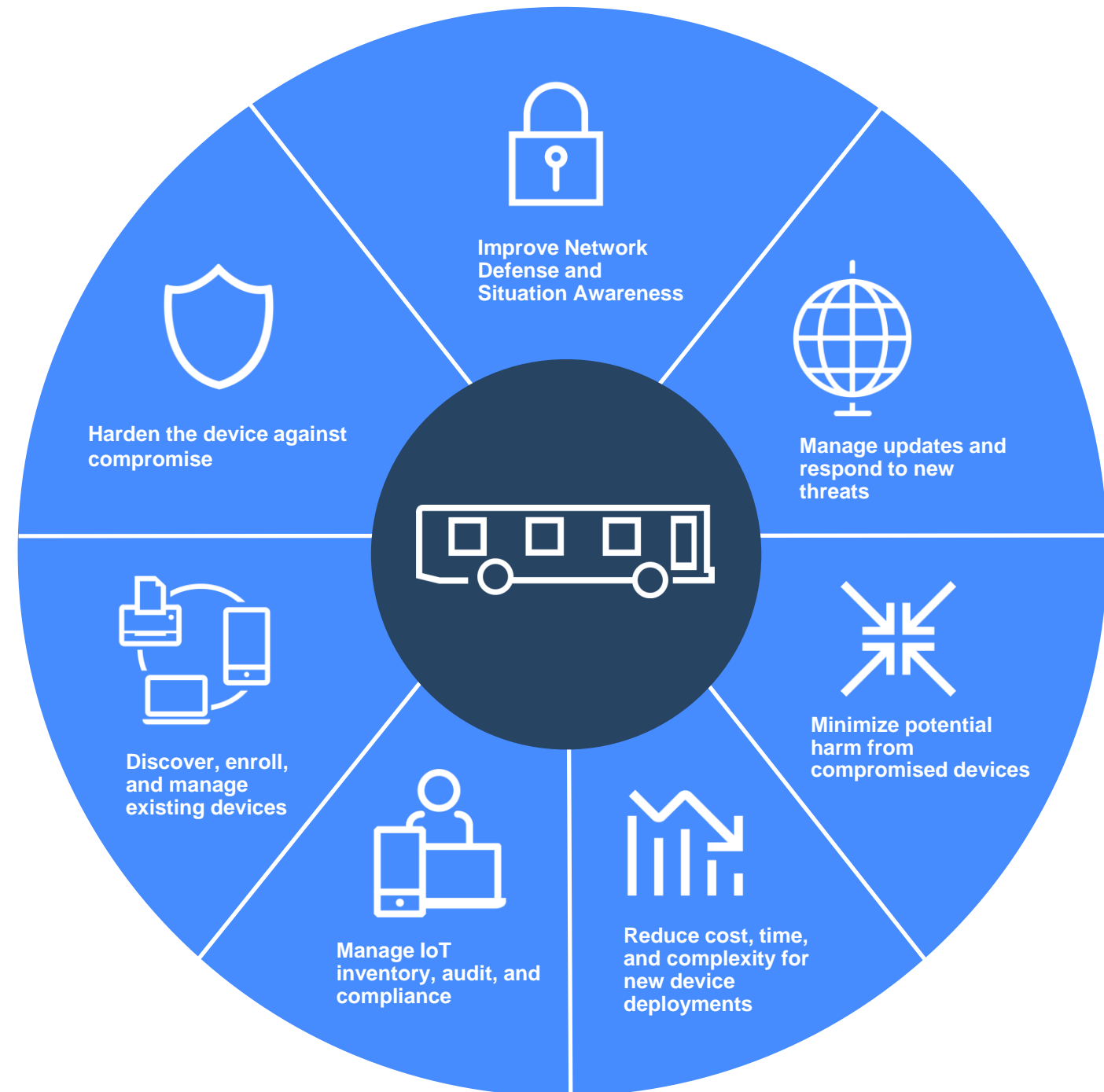
The Need

Defense in-depth approach that:

- Discovers, enrolls, and manages existing devices
- Hardens devices against compromise
- Improves network defense and situation awareness
- Manages updates remotely

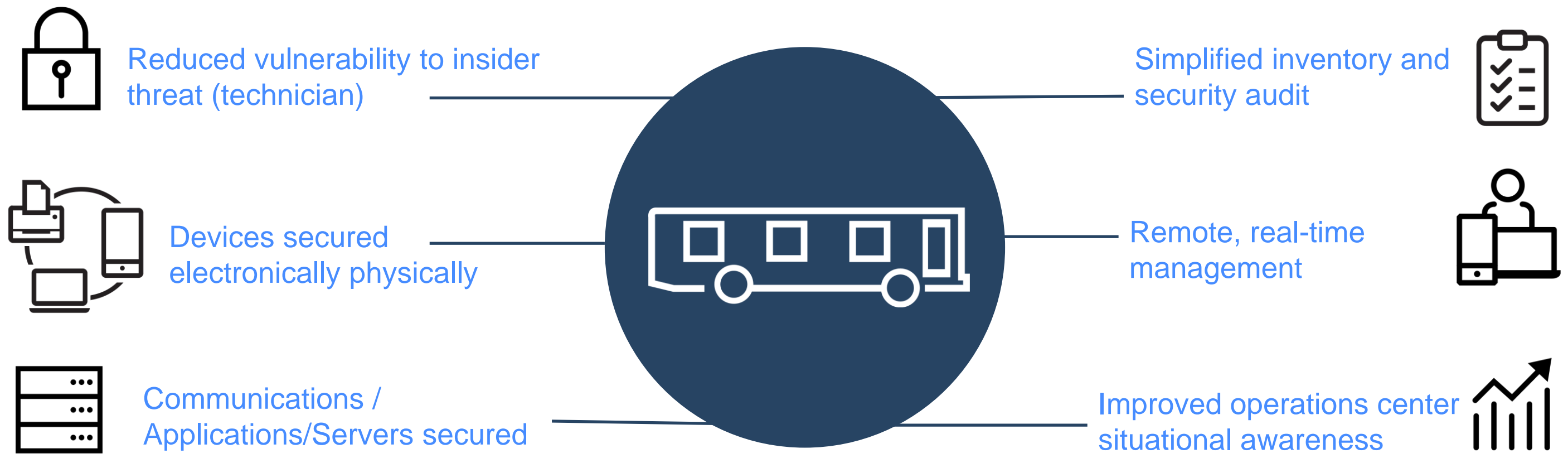
Benefits:

- Minimizes harm from attacks and compromises
- Reduces cost, time, and complexity of new device deployments
- Supports Audit and Compliance



Desired Outcome

Provide modern PKI-enabled IoT cybersecurity on legacy back-office and fleet management systems



Elements of a Cyber Plan

- Follows NIST Cyber Security Framework
- Emphasizes “PROTECT” as the premium concern
- Devices secured electronically and physically
- Simplified inventory and security audit
- Incorporates monitoring as key security element

IoT security features and methodology

Identify	Protect	Detect	Respond	Recover
<p>Device Discovery</p>	<p>Device Hardening</p>	<p>Attack Signature</p>	<p>Incident Analysis</p>	
<p>Device Profiling</p> <ul style="list-style-type: none"> • Manual • Automatic • Built-in 	<p>Profile Based Behavior whitelist</p>	<p>Alert on Profile Behavior Violation/Anomaly</p>	<p>Incident Mitigation</p>	
	<p>Network Hardening</p>			
	<p>Application Hardening</p>			
			<p>Proactively make security improvements (to defend other devices)</p>	



Discussion

CONDUENT

