Let's go

The bridge to possible

Cyber Resilience In Critical Infrastructure

Simon Finn, National Cyber Security Advisor

BRKIOT-1521

Cisco Webex App

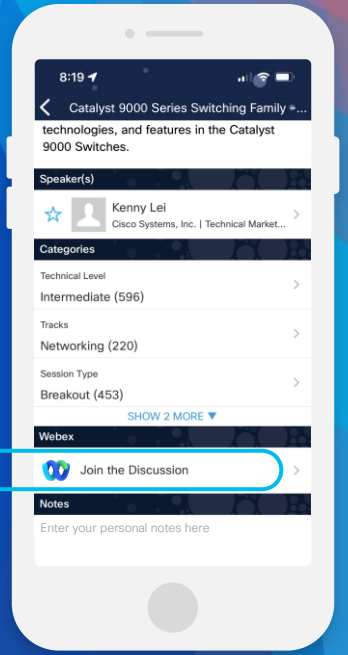
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

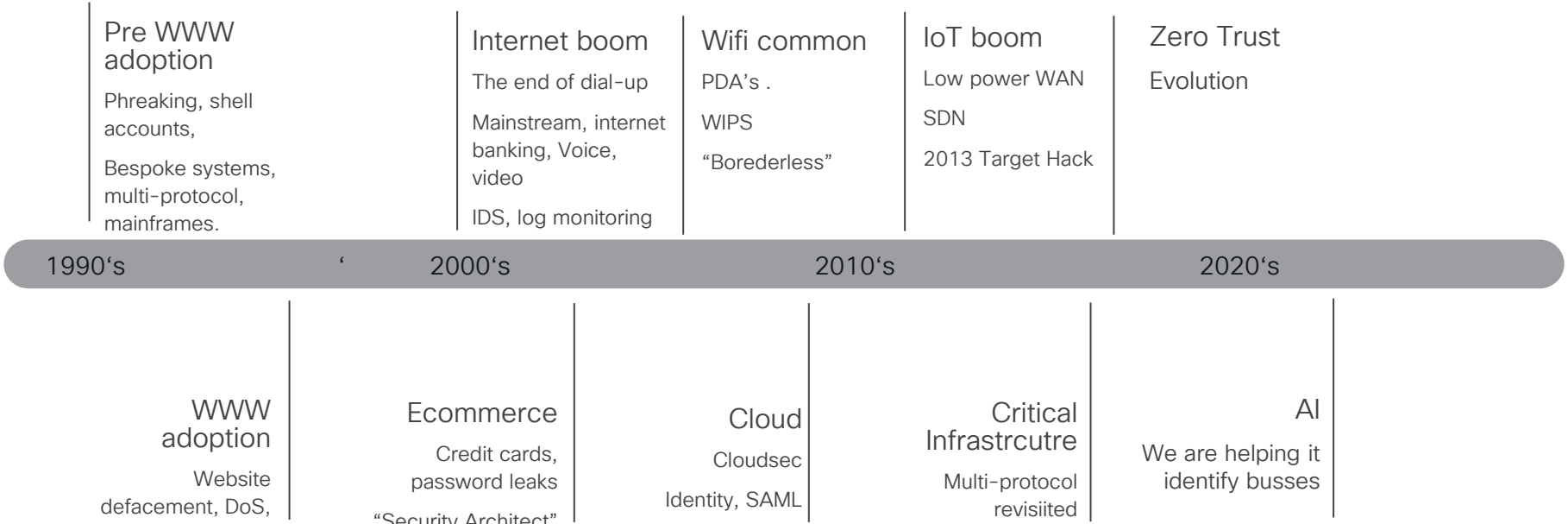
Webex spaces will be moderated by the speaker until December 22, 2023.



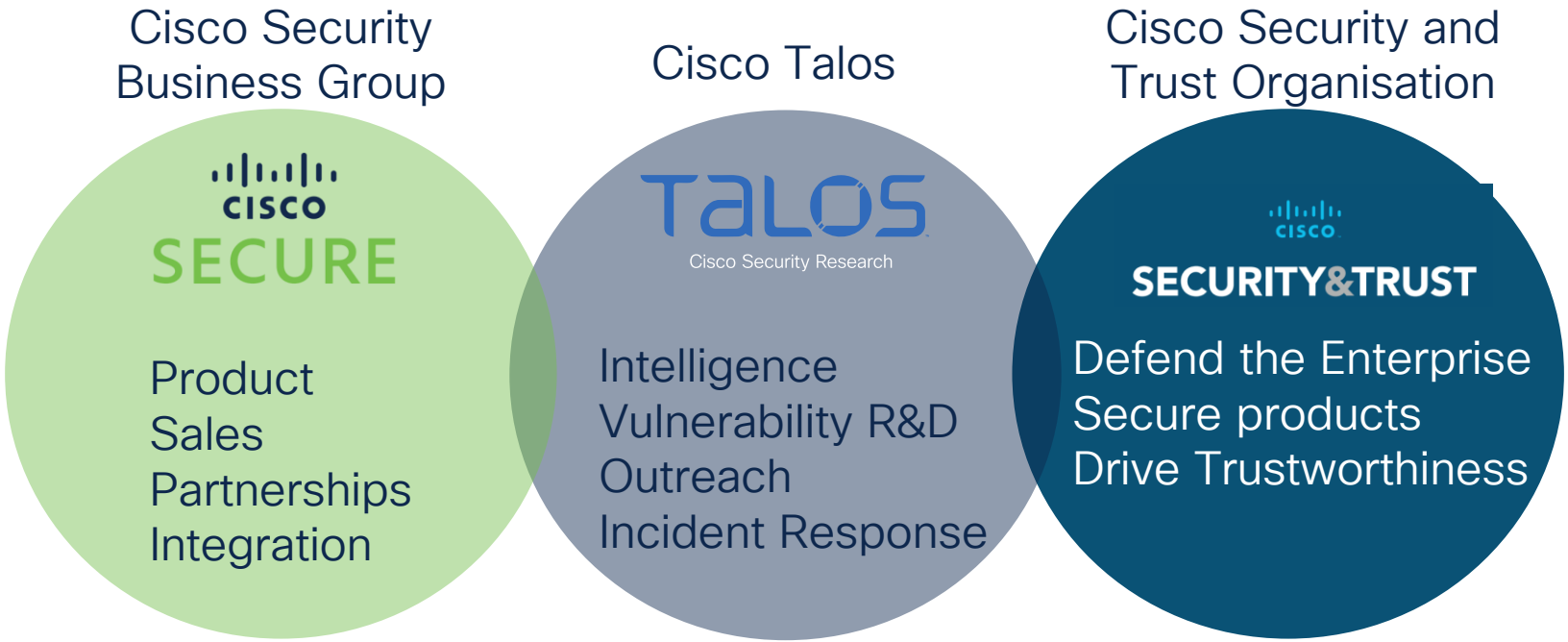
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKIOT-1521

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Vague Career timeline



Disambiguation: Security @ Cisco



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Critical Infrastructure

It’s a wide range of businesses

It’s all parts of a business

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

“Cyber resilience has become one of Australia’s greatest challenges and is critical to the nation’s economic prosperity and security”

Mike Barber, CEO A3C (Australian Cyber Collaboration Center)

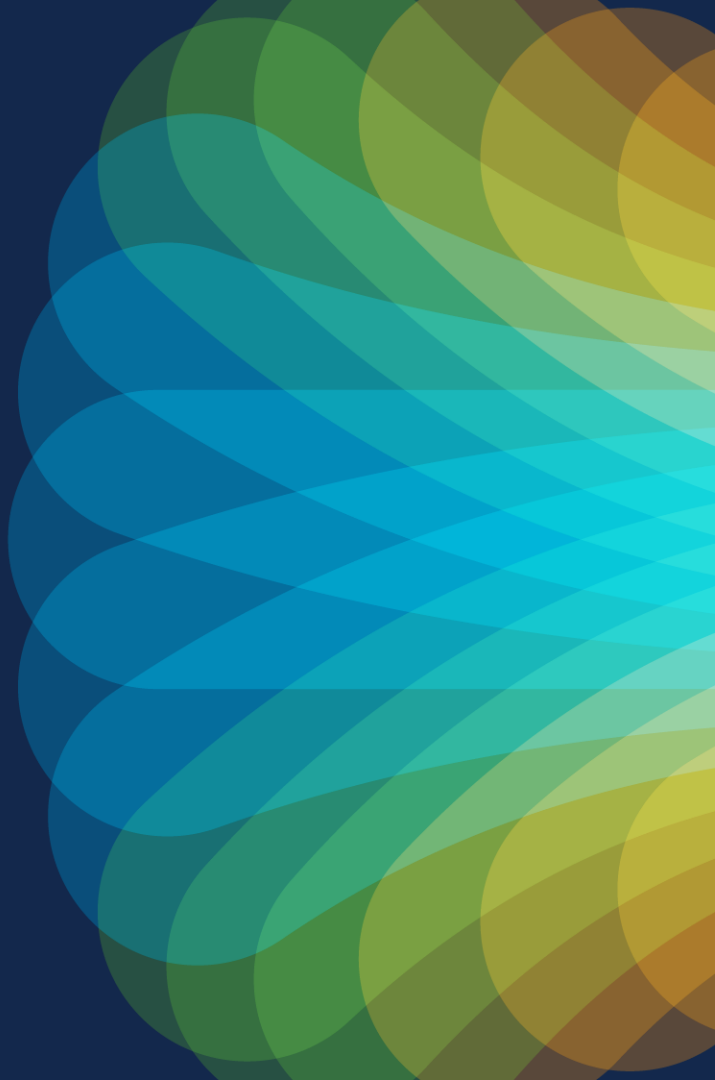
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Threat Insights
- Business Challenges
- Technology Challenges
- Strategic Imperatives
- Strategic Technology Approach
- Conclusion

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Insights



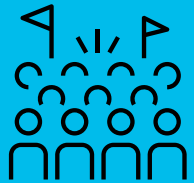
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Trends

Knowledge

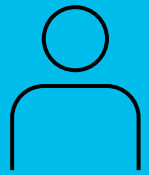
Speed and Scale

Organisation



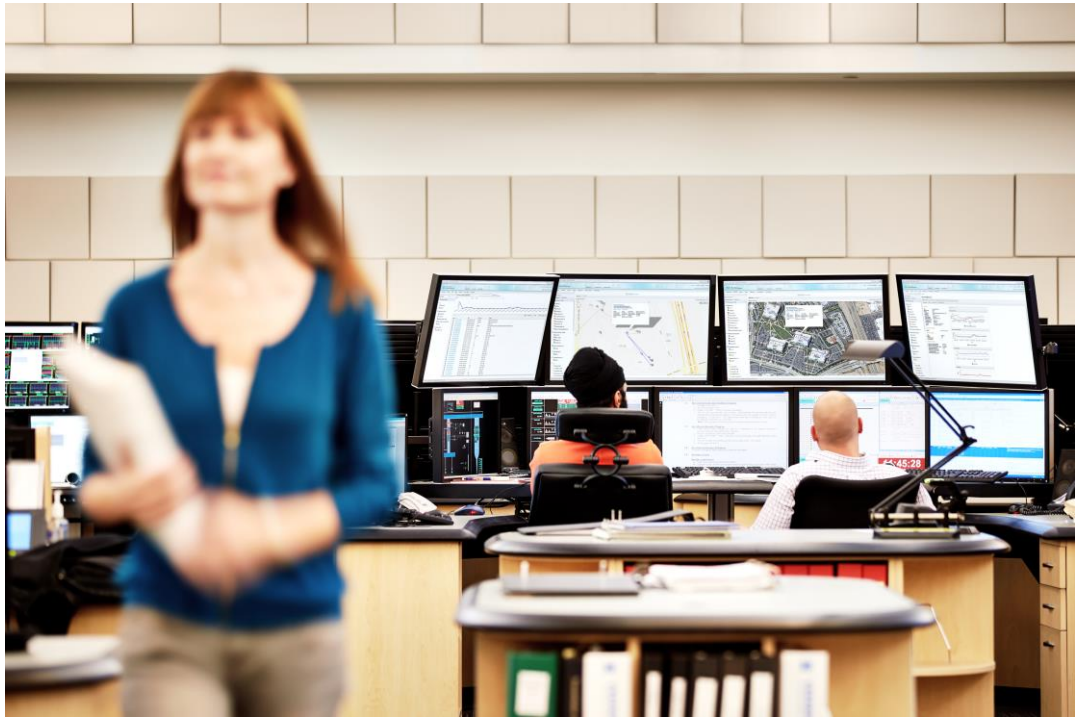
Enhanced TTP

Insider Threat



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Assume you are already compromised



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Business Challenges

Digitalising brings benefits

Safety & Resiliency

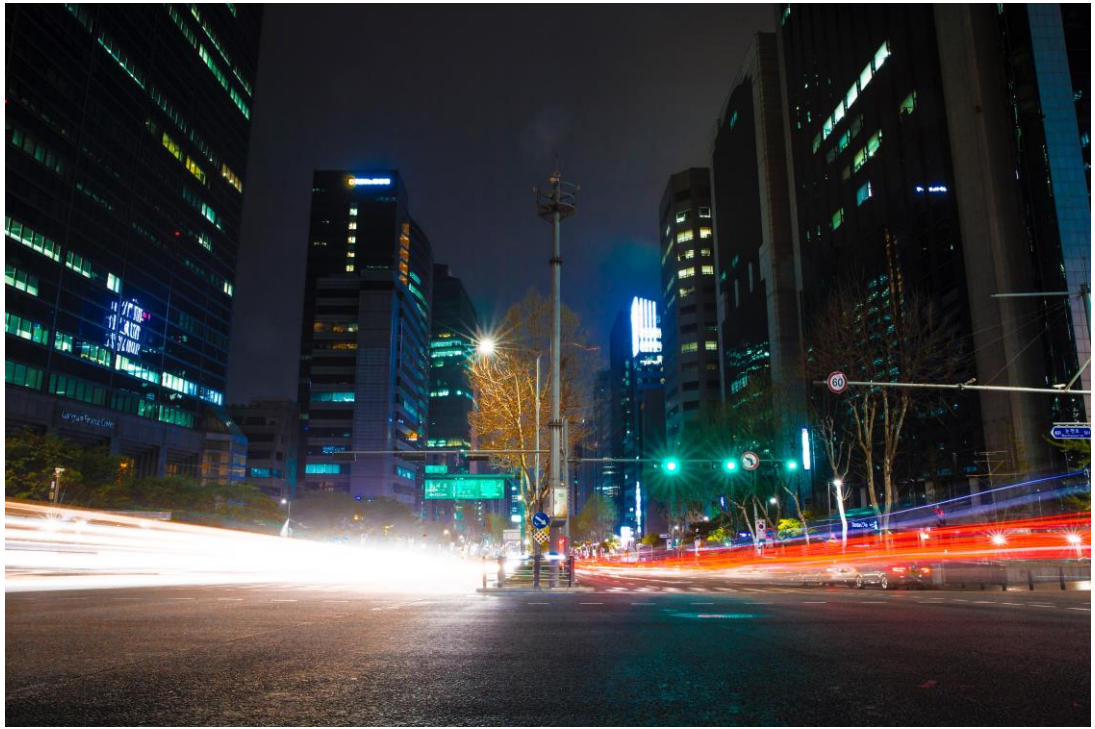
- Smarter protective systems
- Emergency capabilities
- Removing humans from danger

Sustainability & Efficiency

- Net Zero
- Data Driven Decisions
- Improved Quality of Life

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Your business is digital



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

IT/OT Inter-dependency has already happened

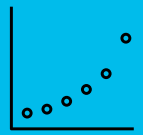
Two worlds **converged**

IT and OT need to come together to secure the business

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

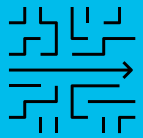
Business Challenges

Scale of Data



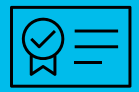
Attack Surface

Complexity



Cyber Skills Shortage

Compliance



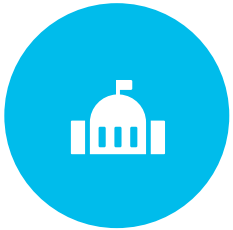
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cybersecurity is a board level concern

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Governance

Cyber Regulatory Complexity

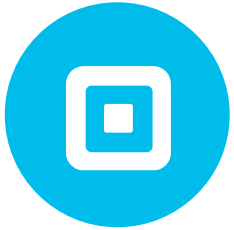


Multi-Agency (e.g. FIRB, DoHA)

Regulations span multiple government agencies, leading to fragmented oversight.

Multi-Level (fed/state/local)

Cybersecurity regulations exist at the federal, state, and local levels, creating complexity.



Low commonality (standards and priorities)

Different agencies have misaligned standards and priorities for cybersecurity.

The complex and fragmented nature of cybersecurity regulations across multiple government agencies, levels and regulators creates challenges for organizations.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Sample of Incident Reporting Requirements

Country	Scope	Timeframe	Sev. definition
Australia	Defined CI assets	12 Hours- Severe (call) 72 Hours- Other	”Significant or relevant impact”
Australia	IRAP certified services	Undefined	Defined in ISM as types of incidents
Australia	Privacy Data	Undefined	Any system with privacy data
Australia	Ransomware (proposed)	Undefined (WIP)	Ransomware incident
China	”Network operators”	“relevant provisions”	Undefined
EU	”Essential Entities”	<24hrs	Undefined
EU	Privacy (GDPR)	72 hours	Personal data breach
Korea	Information/DC providers	“Immediately”	Event resulting from an attack
India	SP/DC/Cloud	“Reasonable timeframe” 6 Hrs	Defined examples (includes targeted scanning)
Singapore	Critical Infra	2hrs/14 days	”Prescribed Cybersecurity incident”
Thailand	Critical Information Infra	Undefined	Any illegal action
UK	Telco services	Undefined (WIP)	Undefined

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Australian Government Cyber Shields

Strong Business and Citizens

Safe Technology

Threat Sharing and Blocking

Protected Critical Infrastructure

Sovereign Cyber Capacity and Skills

Resilient Region and Global leadership

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

To summarise....

We are defending against organized adversaries

.. with ever evolving, new, fast and stealthy attacks

.. That can come from anywhere, at scale

.. Across a larger attack surface

.. With more heterogeneity

.. And expensive/scarce resources

.. And more compliance obligations

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Technology Challenges

Future Technology Challenges

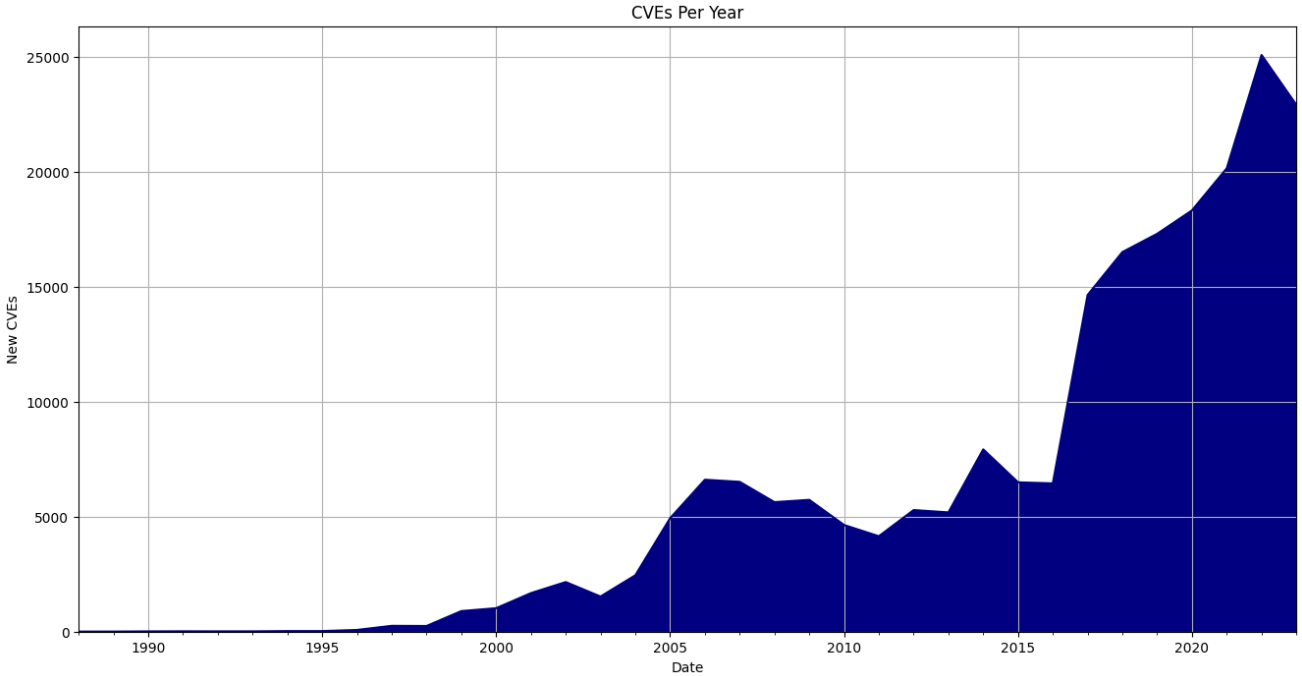
Legacy Systems

AI

Quantum

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Vulnerabilities increase trend expected to continue



Https://cve.icu CVE Data

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

CISA Directive

As of 26th Oct 2023, the CISA directive covers 1021 vulnerabilities, up from 857 in October last year

These are known exploited vulnerabilities

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Australian Cyber Threats – Vulnerabilities

Figure 1: Percentage of vulnerabilities by time to exploit

- 1 in 5 vulnerabilities was exploited within 48 hours of a patch or mitigation advice being released
- half of the vulnerabilities were exploited within 2 weeks of a patch or mitigation advice being released
- 2 in 5 vulnerabilities were exploited more than one month after a patch or mitigation advice was released

Source https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

And it’s getting a lot of focus

FINANCIAL REVIEW Oct 30, 2023

‘Fix software bugs now’: urgent appeal to business

Home Affairs and Cyber Security Minister Clare O’Neil is calling on businesses to immediately patch three major vulnerabilities that Australia’s top cyber spies have warned about for as long as four months and are leaving them open to cyberattacks.

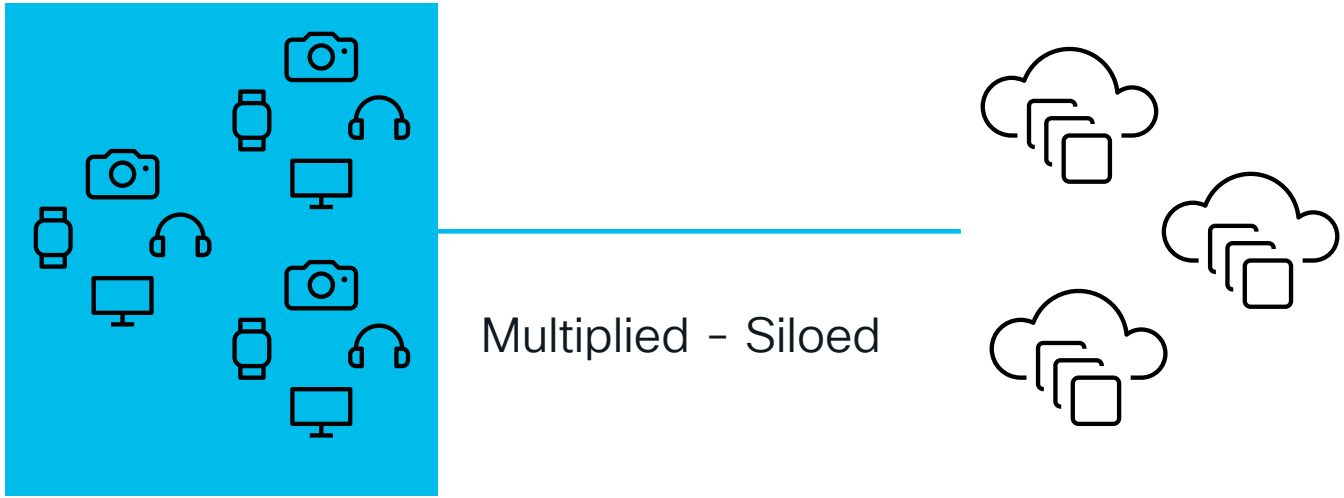
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

IoT is getting complex

‘Basic’ IoT – 2 Layers

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

IoT is getting complex



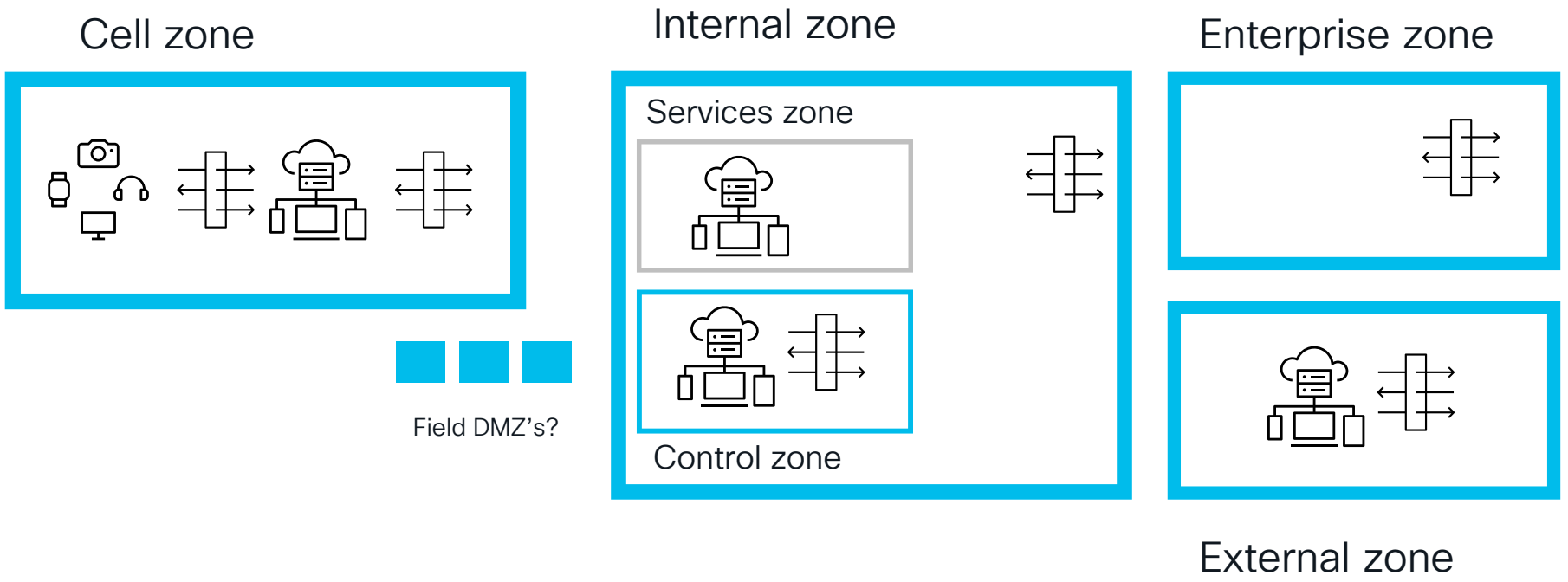
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

IoT is getting complex

Edge compute + Sensor data reuse

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Complex IoT – IEC 62443 Compliance



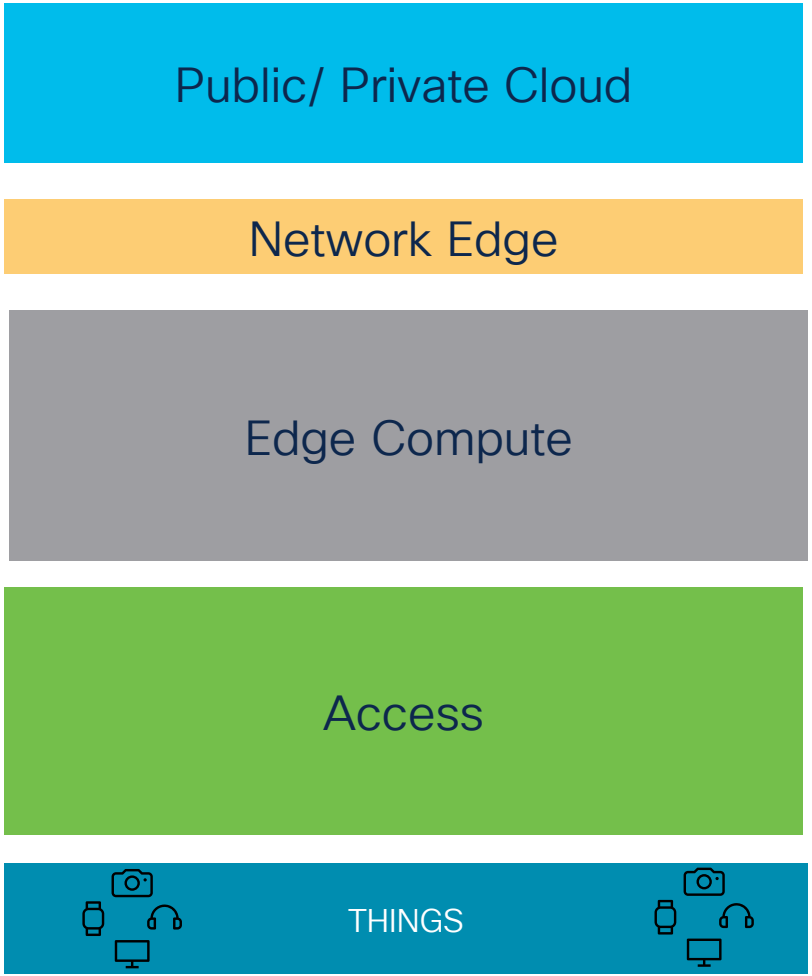
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Strategic Imperatives

Security must be built in, at every layer

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

“Layers”



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

So how do we...

- Have assurance at every layer?
  - Hardware
  - Software
  - Configuration
- Have visibility at every every layer?
  - Logging/Telemetry
  - Security toolsets
  - The right capabilities are in place

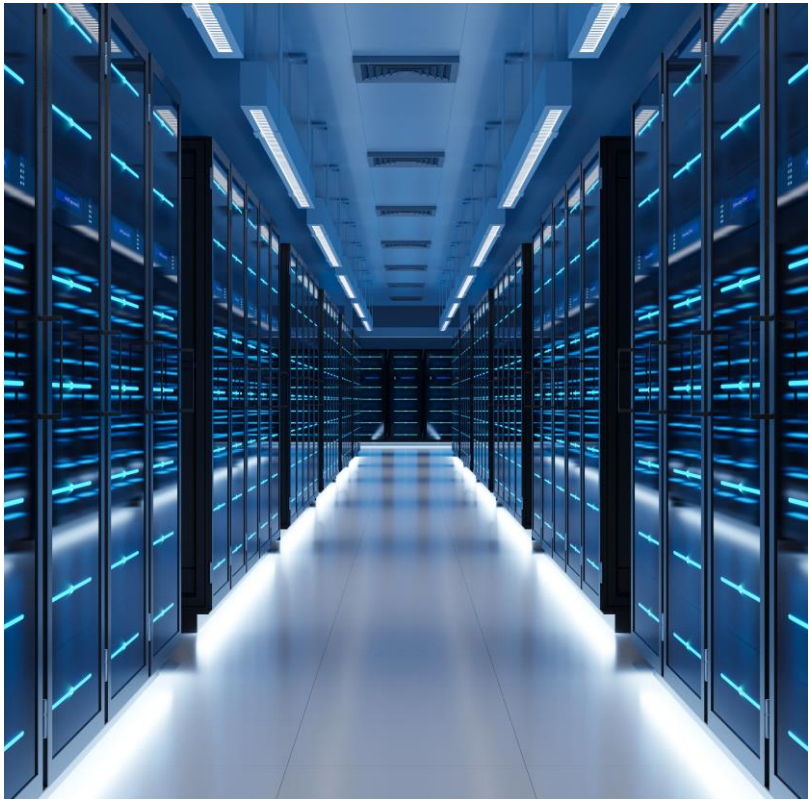
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continuous

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security isn't static

- CI/CD pipelines
- Continuously changing landscape
- Manual processes are expensive
- Point in time compliance
- Are point in time checks making us more secure?
- How to better inform business leaders to make more informed decisions



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Speed and efficiency

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Or... start with efficiency focus to increase speed

- Can we automate?
- Where do you want to spend your time?
- What can we stop doing?
- How to leverage new tools to get better or faster results

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Strategic Technology Approach

A strategic approach

Visibility

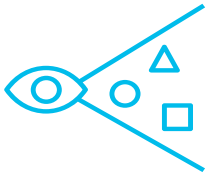
Protection

Integration and Automation

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

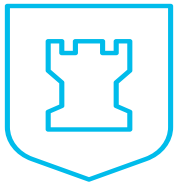
Addressing Business Challenges

Visibility



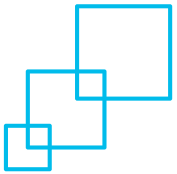
- Know Your Assets
- Know Your Communications/ Dependencies
- Know Your Vulnerabilities

Protection and Mitigation



- Pervasive Controls
- Defend the critical asset that cannot defend itself

Integration and Automation



- Enhance and Simplify
- Speed and Efficacy
- Resource efficiency

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Network is in the Ideal Position

Business Applications: Safety, Efficiency, Mobility

Safety and compliance
Passenger experience
Data Operations
Operational Efficiency

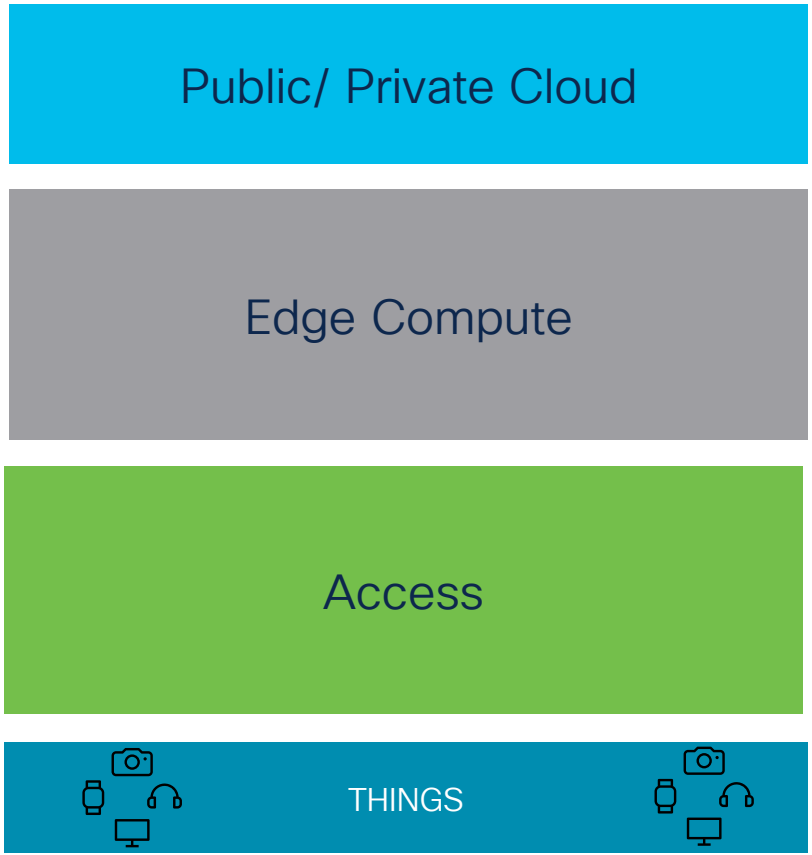
Passenger services
Demand management
Predictive Maintenance
Capacity management

Vehicle-as-a-sensor
Weather Detection
Vulnerable road user detection

Traffic signal phase timing, prioritisation, preemption
Roadway Safety
Vehicle automation

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

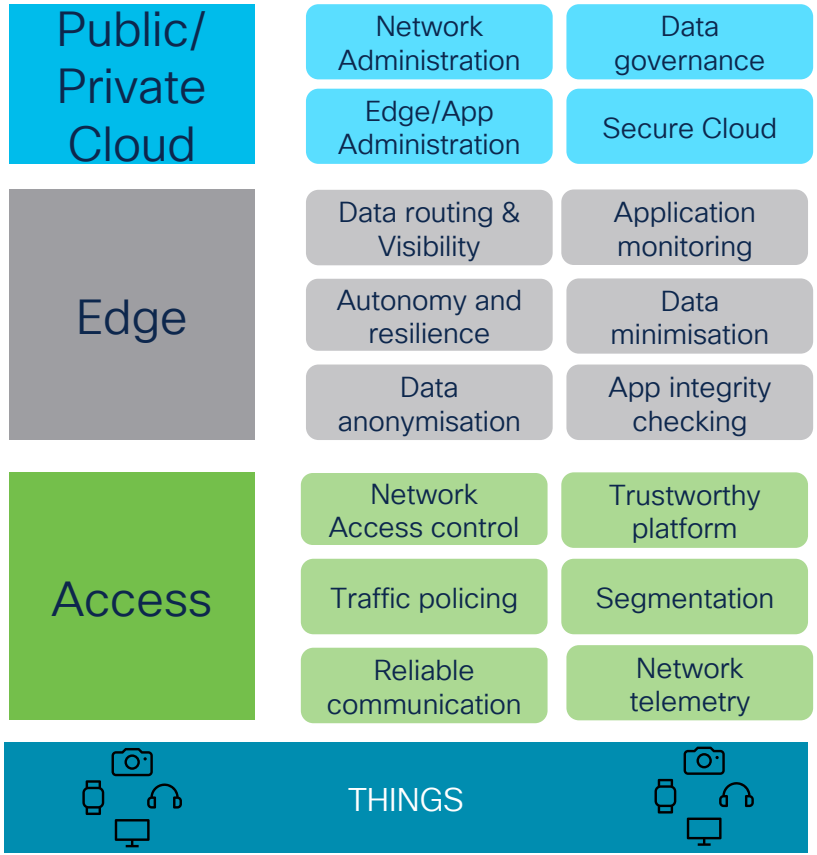
IoT data security – layers



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

IoT data security architecture

Each layer has multiple visibility& protection capabilities needed



Integration and automation is key to deliver

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Visibility

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Know your attack surface

Rapid cloud adoption with multi and hybrid cloud approach

By 2021, over 75% of midsize and large organizations will have adopted a multi-cloud and/or hybrid IT strategy[1]

Expansion of the attack surface that needs to be monitored

50% increase in the number of applications supported by an organization over next two years[2],and sharp increase in distributed workforce

Fragmented and siloed view across cyber footprint

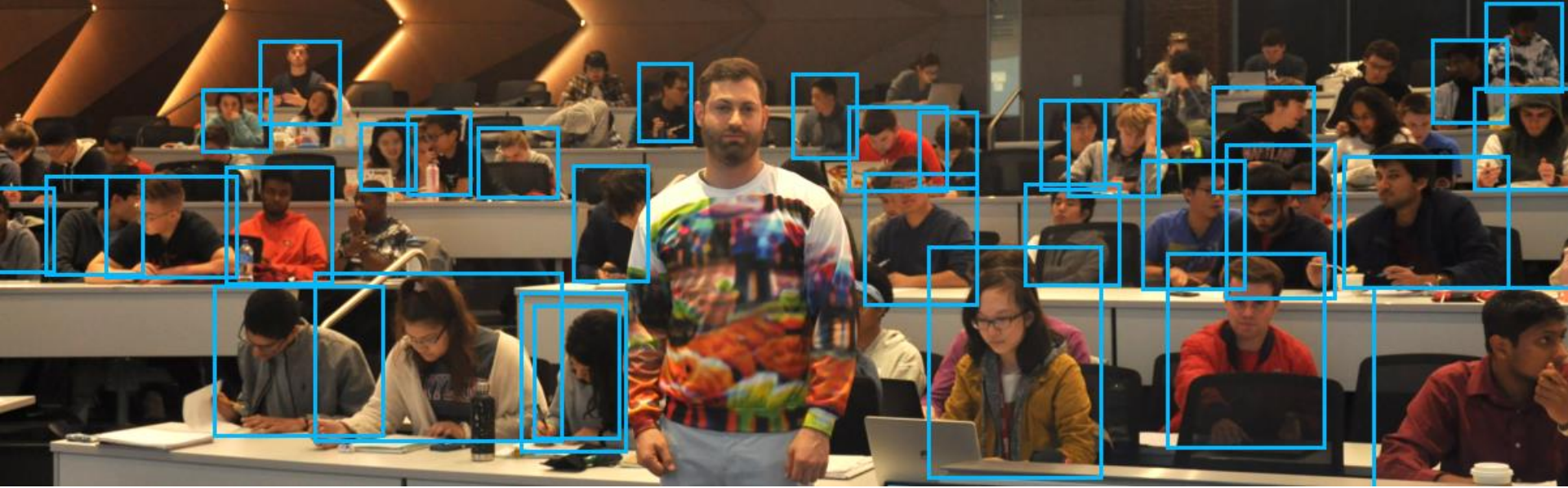
55% of organizations do not have an accurate inventory of assets[3]

The result: Compliance gaps and vulnerabilities reduces overall security posture

The average time to identify a breach in 2021 was 207 days[4]

1. Gartner Predicts., 2. IDG Report, August 2019, 3. ZK Research 2019, 4. Ponemon report, 2021

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public



”Invisibility cloak” https://www.cs.umd.edu/~tomg/projects/invisible/

Know the gaps

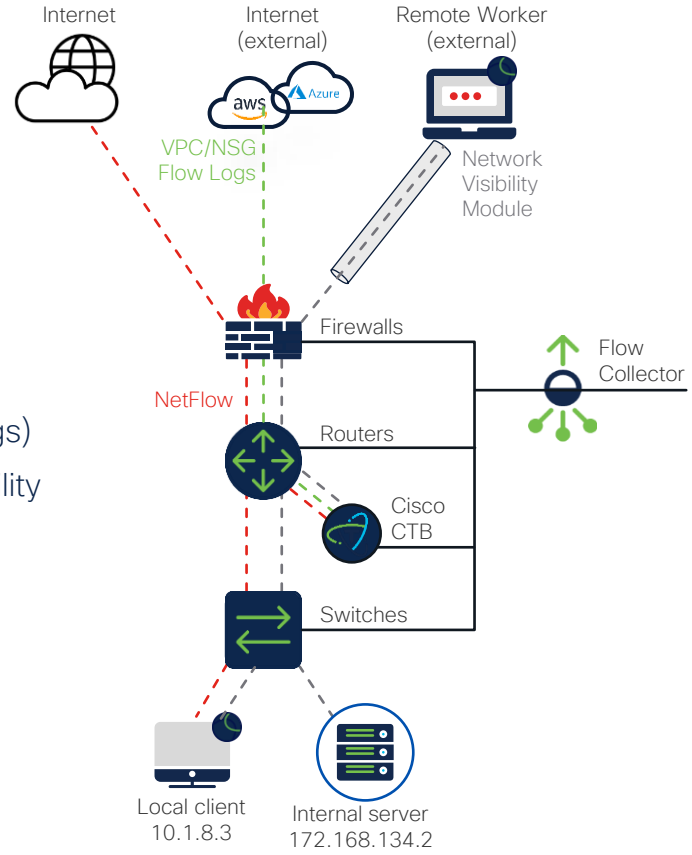
Know the weaknesses

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The network is the source of valuable information

Visibility

- A trace of every conversation
- Agentless information collection
- Remote worker endpoint data collection (NVM)
- Cloud Telemetry ingest (Flow Logs)
- East to west and north south visibility (Cisco FTD logs and NSEL)
- Light meta data collection using the existing infrastructure
- Capture enhanced NetFlow from Cisco ASR, ISR, Catalyst 9000, and Meraki platforms (GTA)



Flow information	Packets
Source address	10.1.8.3
Destination address	172.168.134.2
Source port	47321
Destination port	443
Interface	Gi0/0/1
IP TOS	0x00
IP protocol	6
Next hop	172.168.25.1
TCP flags	0x1A
Source SGT	100
:	:
ETA meta data	IDP | SPLT
Application name	NBAR SECURE-HTTP
Process Name	chrome.exe
Process Account User	Acme/john

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Network Analytics (Stealthwatch)

Cisco XDR

Extended Detection and Response with Cisco XDR. Advanced analytics extends local detections with global intelligence and integrations for accelerated response

Multilayered machine learning

Combination of supervised and unsupervised techniques to convict advanced threats with high fidelity

Behavioral modeling

Behavioral analysis of every activity within the network to pinpoint anomalies

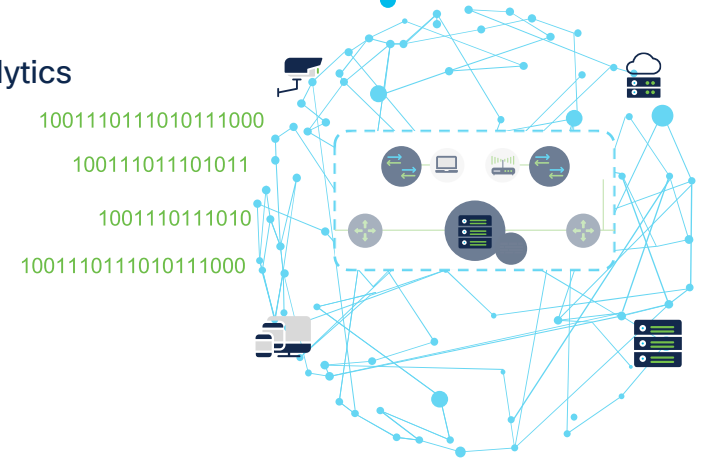
Secure
Network Analytics

Endpoint Telemetry

Device and process insight with flow telemetry from Cisco Secure Client

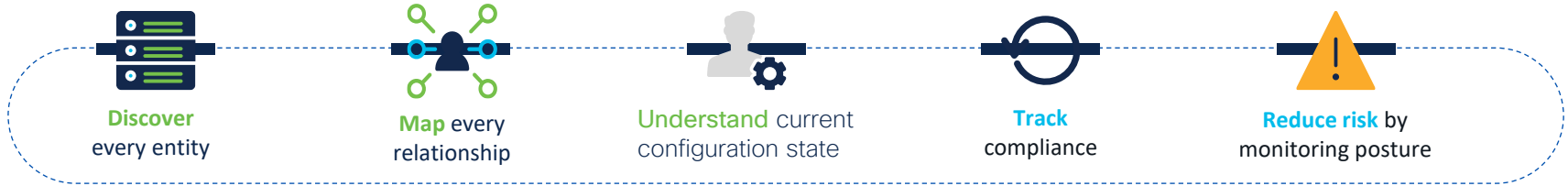
Data collection

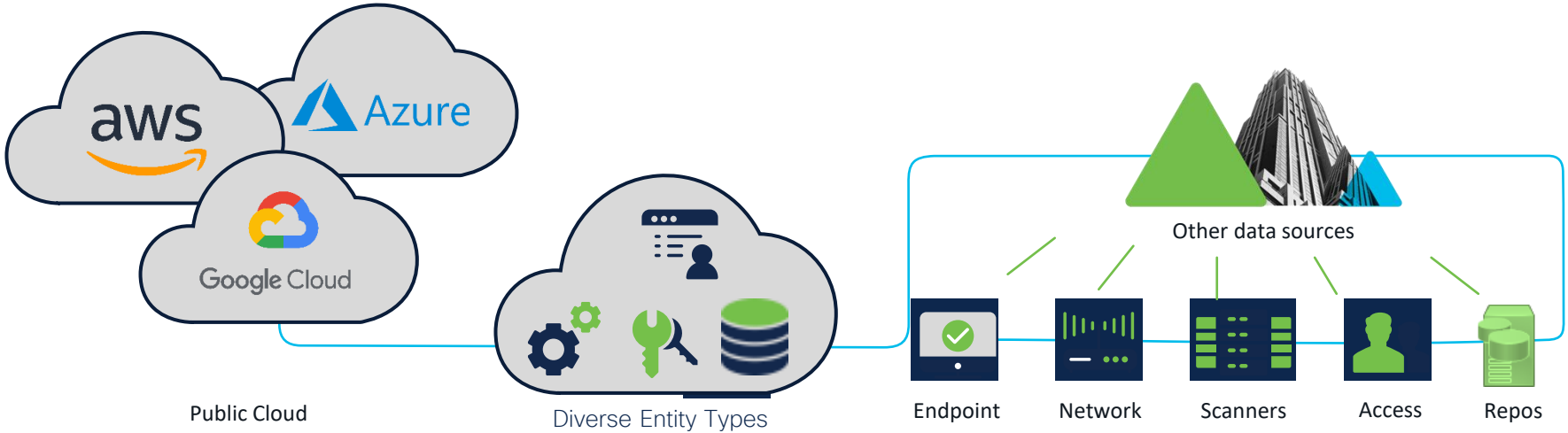
Rich telemetry from the existing network infrastructure including enhanced telemetry for encrypted traffic analytics



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Effective cloud security depends on connecting the dots – Secure Cloud Insights



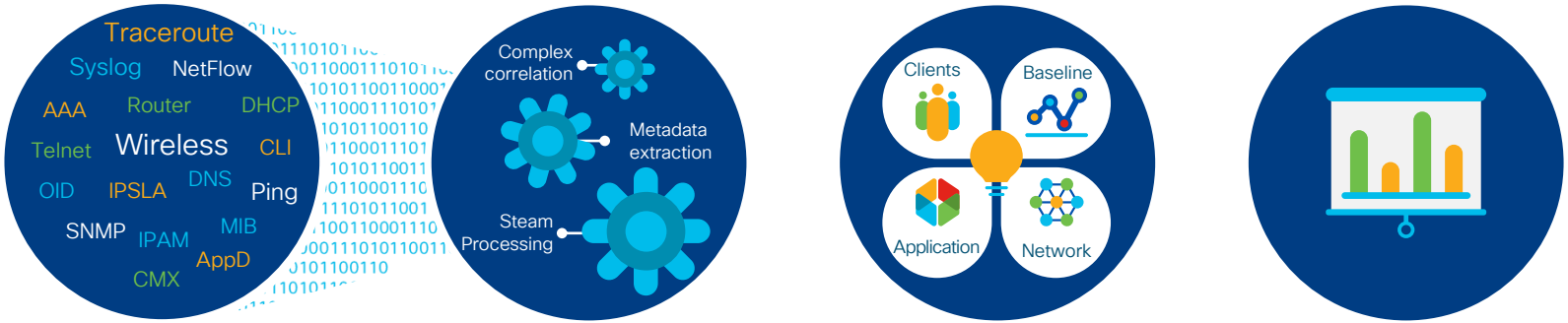


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Management Requires Visibility

DNA center taking network telemetry for network assurance

Network telemetry contextual data | Complex event processing | Correlated insights | Suggested remediation



Everything as a sensor

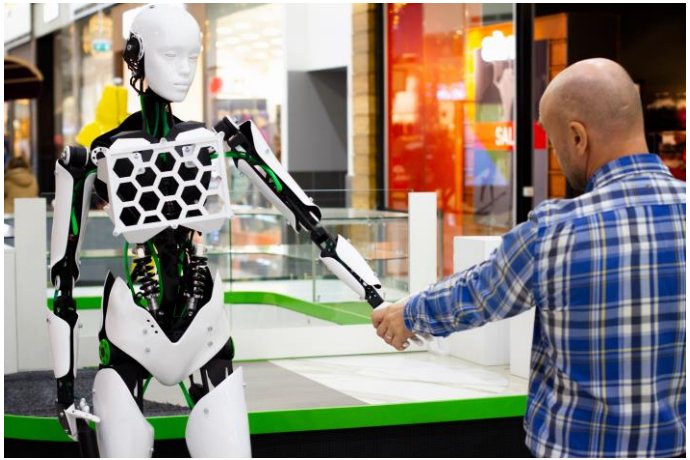
Over 150 actionable insights

Clients | Applications | Wireless | Switching | Routing

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Experiment: AI Visibility

How many of you know The usage of AI within your company?
- Usage of external tools
- Usage within IT system/products?



How would you find out?
- Network/Endpoint traffic visibility
- Cloud/CASB
- DC app visibility

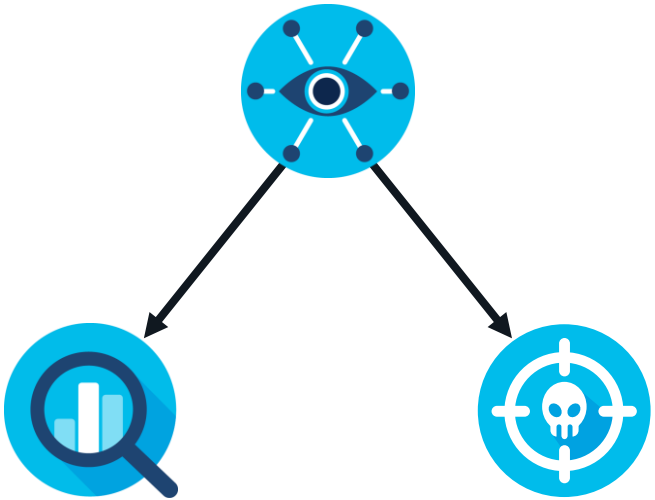
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Industrial Visibility – Cisco Cyber Vision

Visibility helps outcomes for IT and OT

OT cares about Operational Insights

Did this event impact the safety or availability of the system?

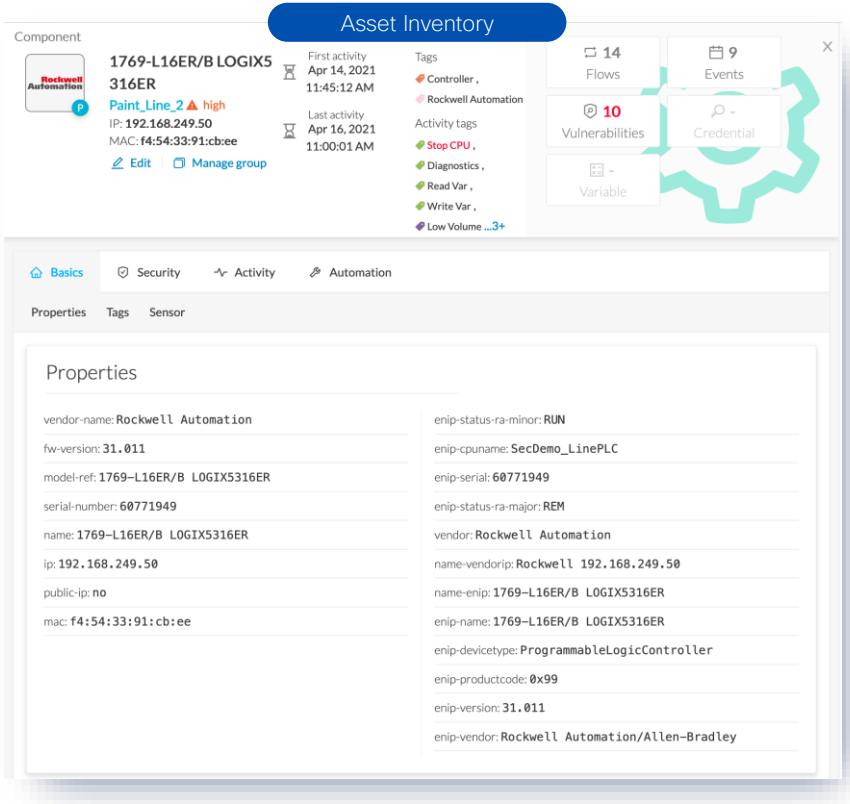


Security cares about Cyber Threats

Is this event a malicious attack on the system?

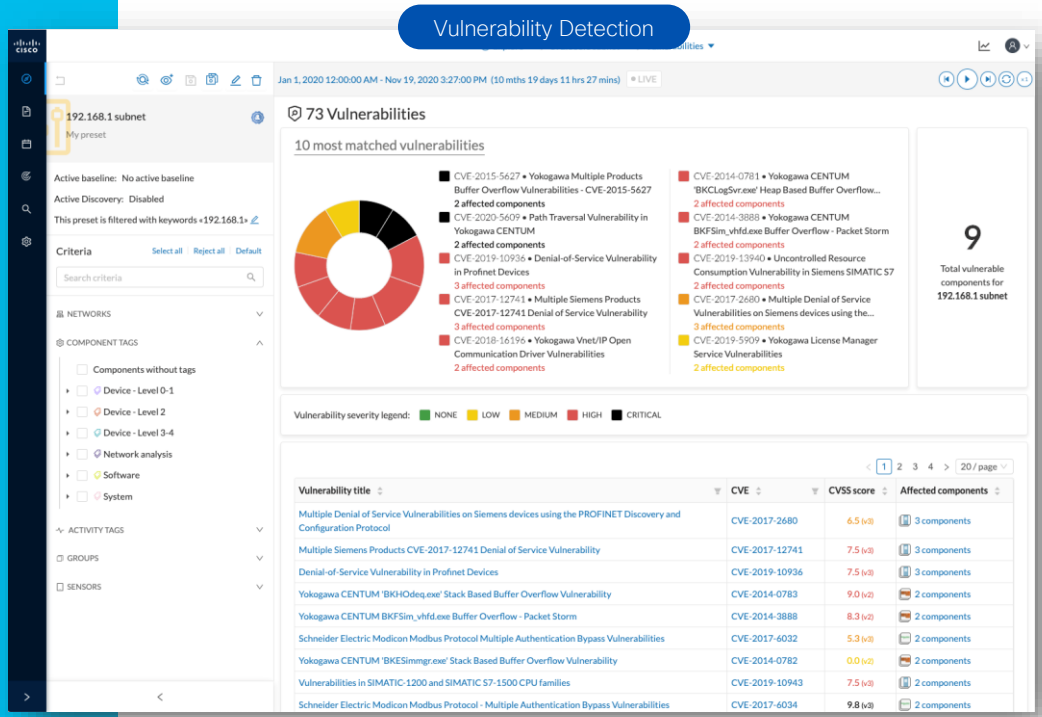
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Industrial Asset Visibility



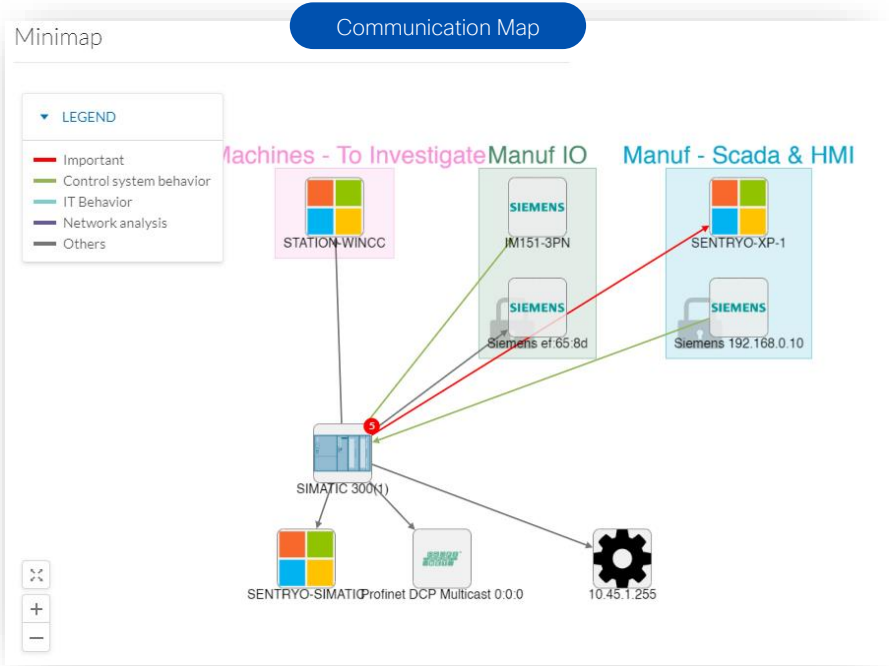
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Asset Vulnerabilities



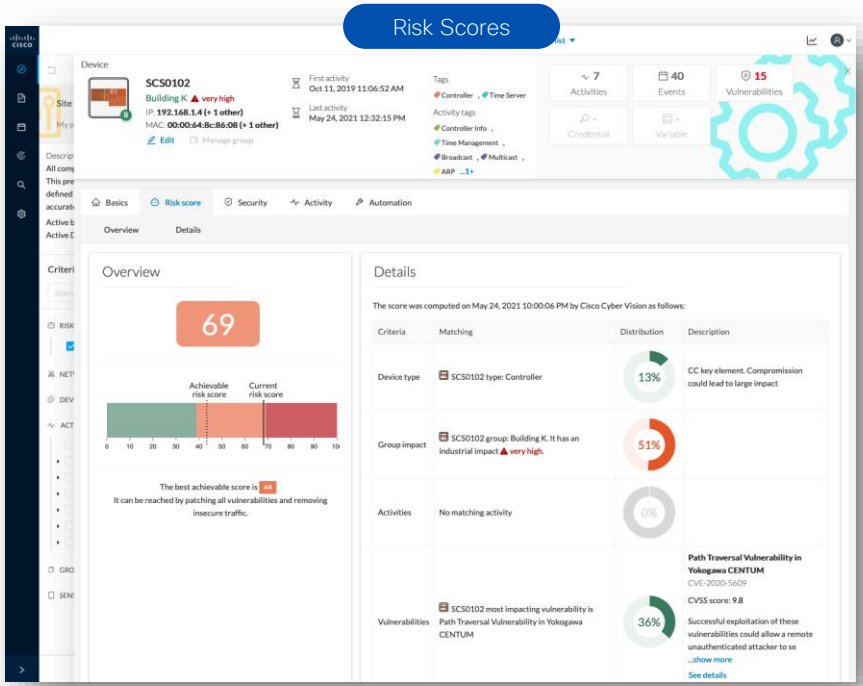
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Communication Visibility



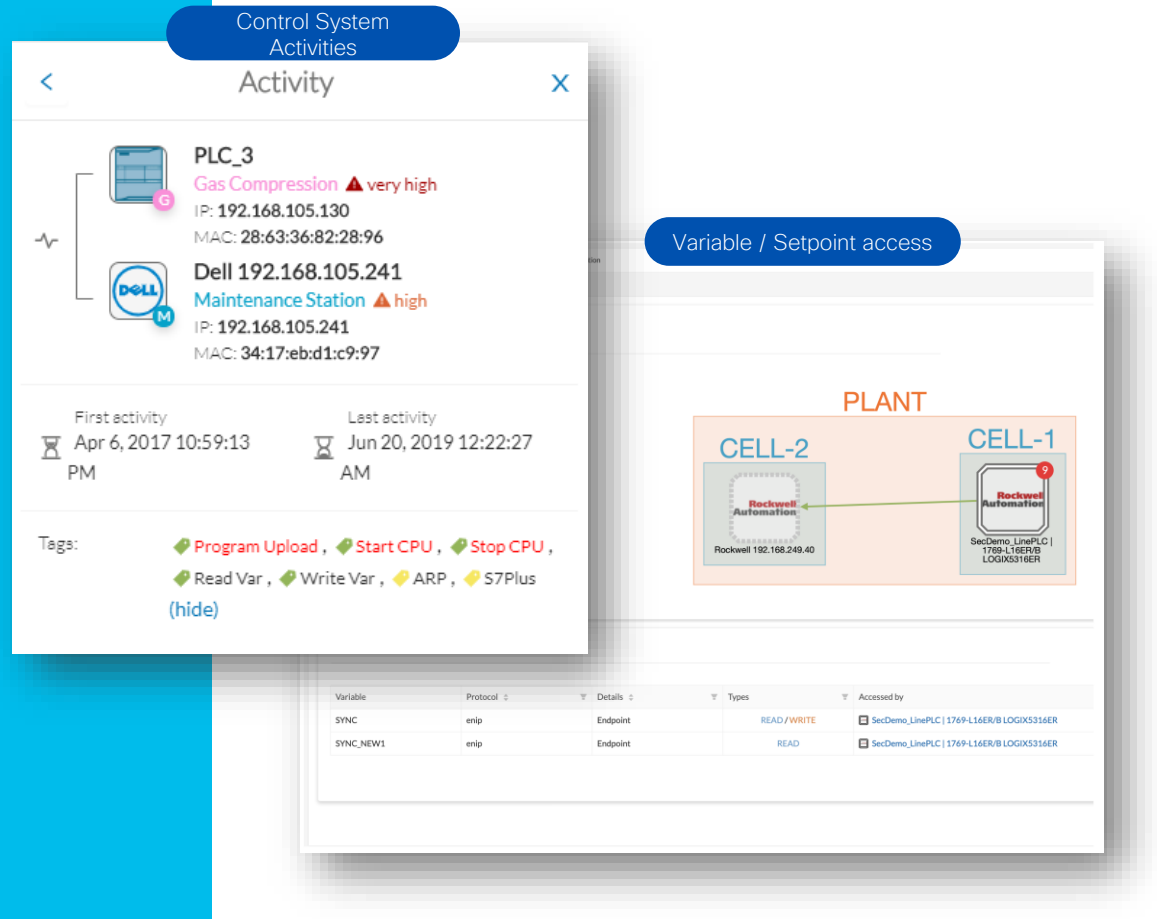
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Risk



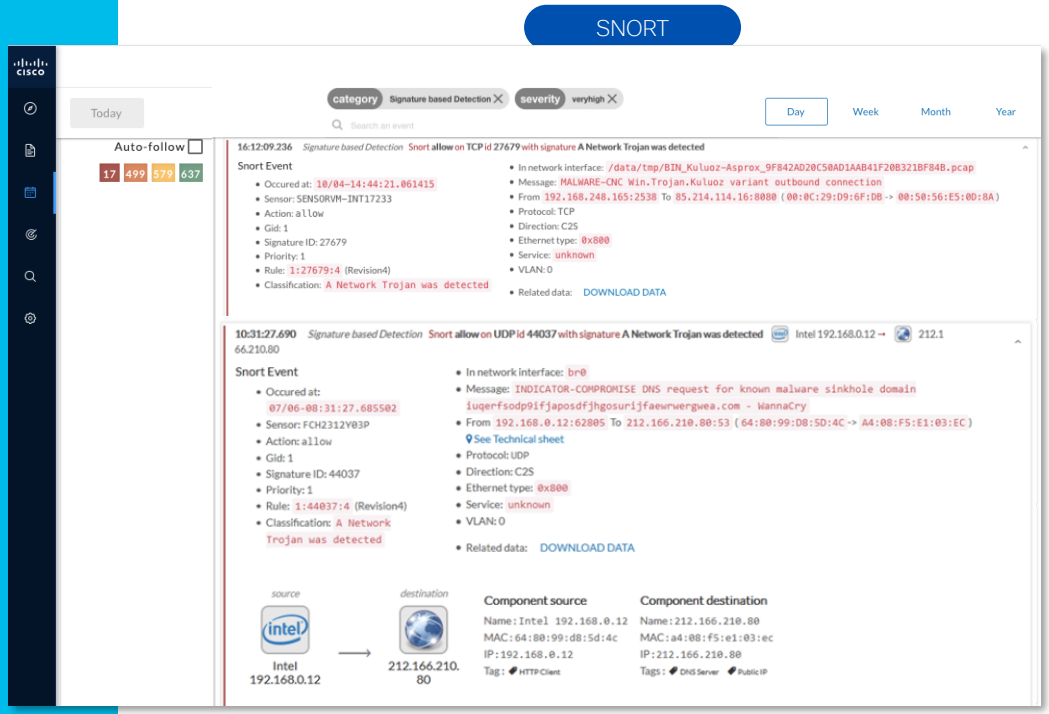
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Monitor



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Detection



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Cyber Vision

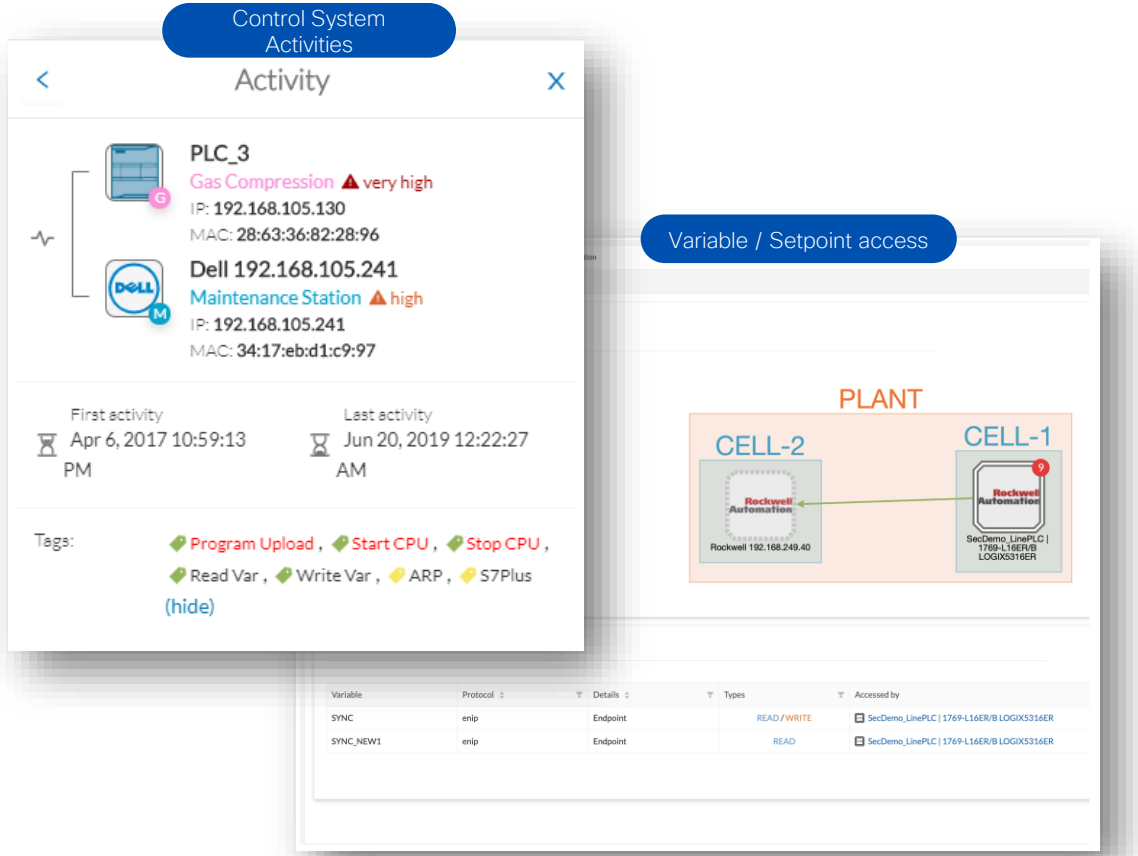
Control System Activities

Track process modifications
Identify configuration changes
Record control system events

Variable Access

See which variables, objects, setpoints are being accessed or modified

Operational Insights



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

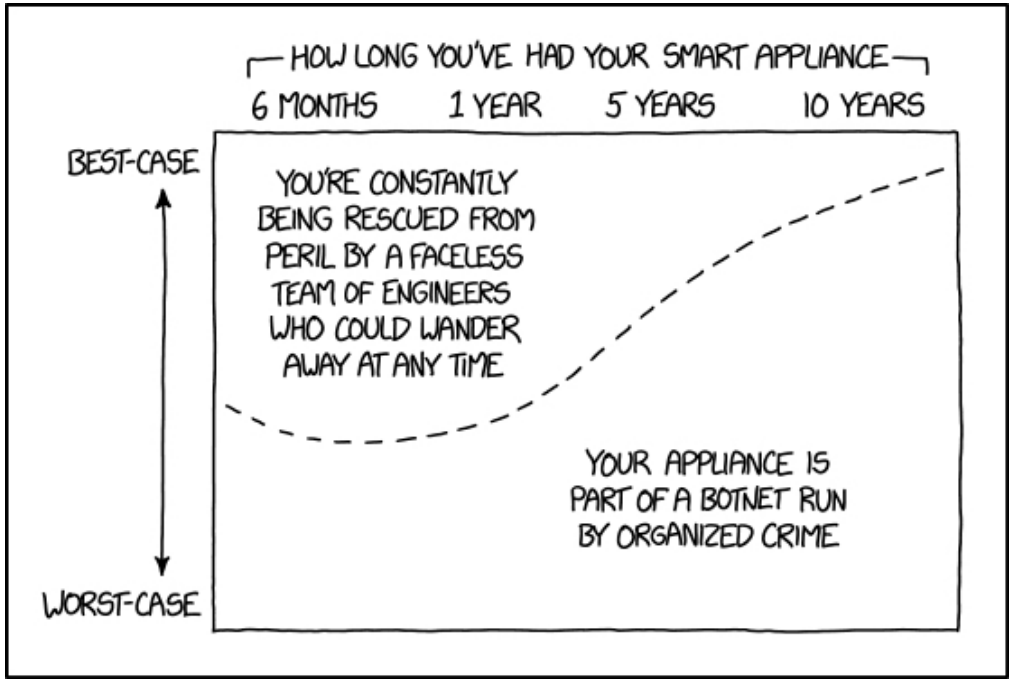
Build visibility in, holistically

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Protection

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Everything is vulnerable



Source: XKCD https://xkcd.com/1966/

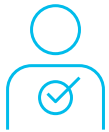
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Leverage visibility to manage risk

Vulnerability

Patch or Mitigate (defend)
Restrict Lateral Movement

Endpoint context



Evaluate Posture & Identity
Contextual policy

Dynamic Policy

Follows the device
Follows the user

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

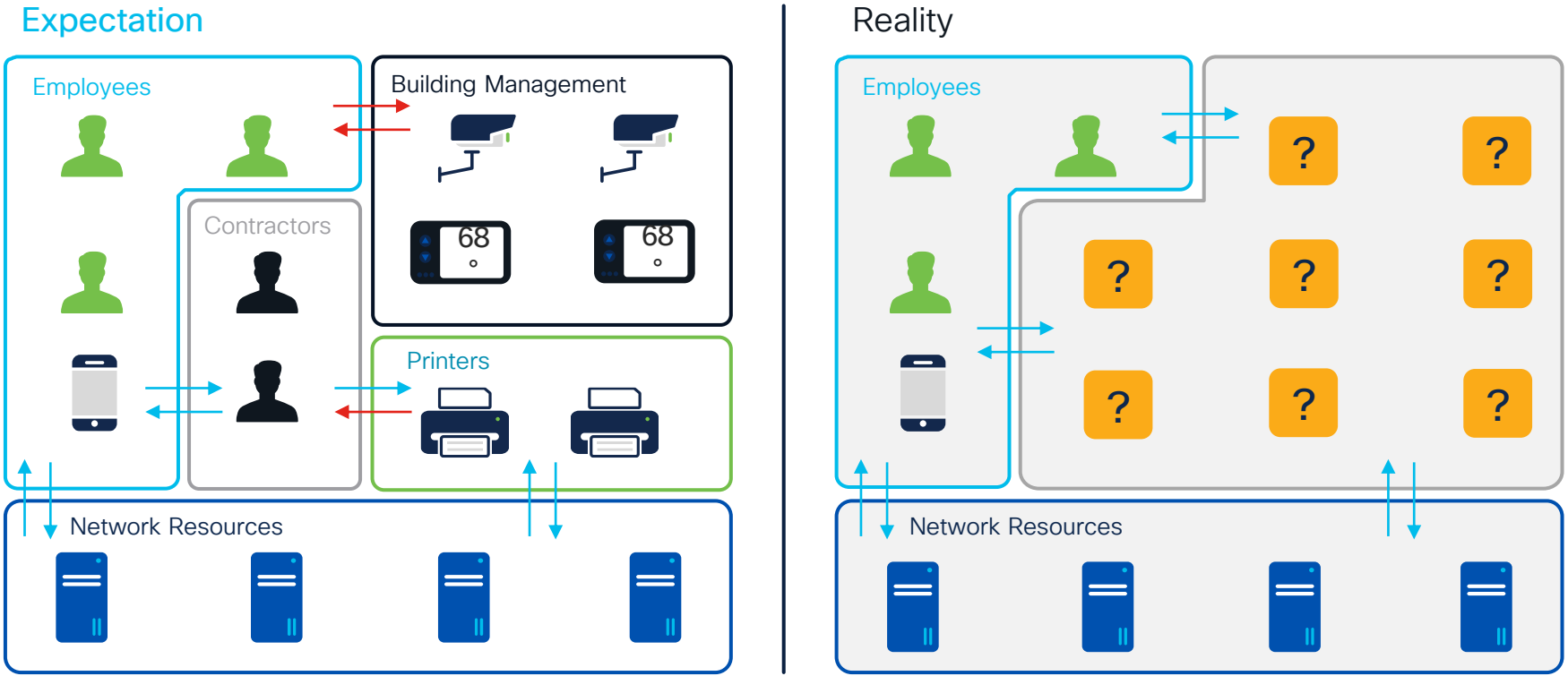
"cisco ise posture кто нибудль сталкивался с этой хуйней? суть в следующем - запускаю впн, а он просит провести проверку в этой залупе, качаю клиент, запускаю проверяет, а сайту с проверкой похуй"

"cisco ise posture who faced this garbage? the bottom line is this - I launch vpn, and he asks to check in this prick, I download the client, I run it, and the site with the check is f#@ed"

Russian/translated chat log quote from Yanluowang leak

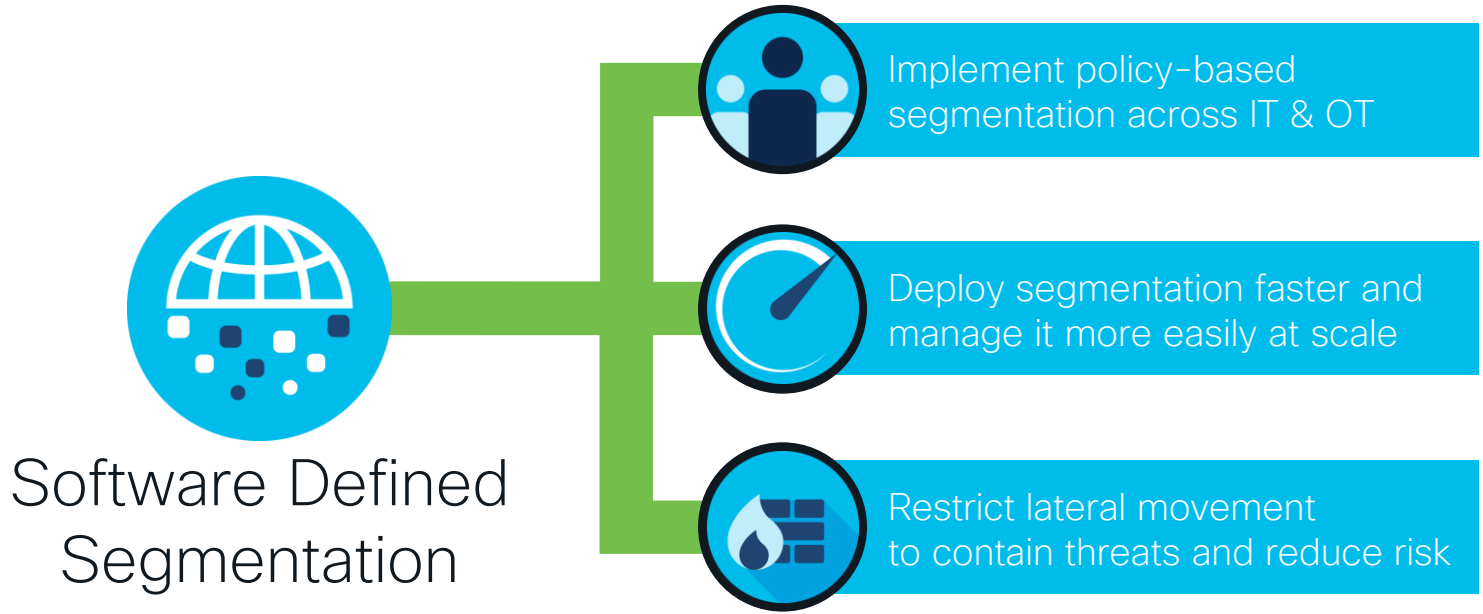
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Least Privilege Access: Expectation vs. Reality



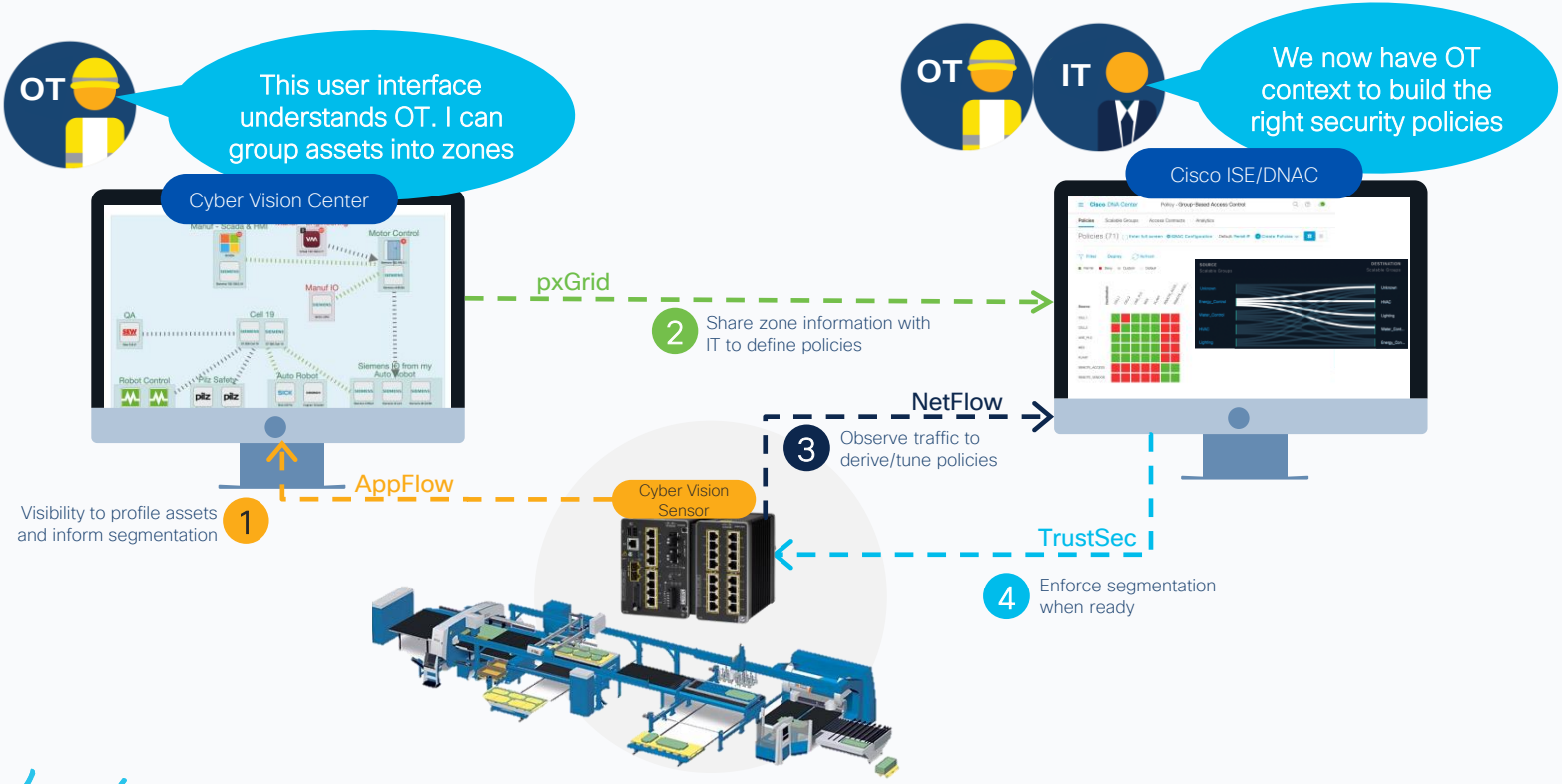
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Protection: As close as possible to the device



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Industrial Network Protection



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Availability

- Do you have the right level of redundancy?
  - Uplink/backhaul
  - Access
- Technology selection
  - Speed
  - Latency
  - Handover (wifi – packet loss)
  - Bandwidth (predictive/standard)

Cisco Ultra-reliable Wireless Backhaul for inshore racing video/social media

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Protecting data with strong user identity

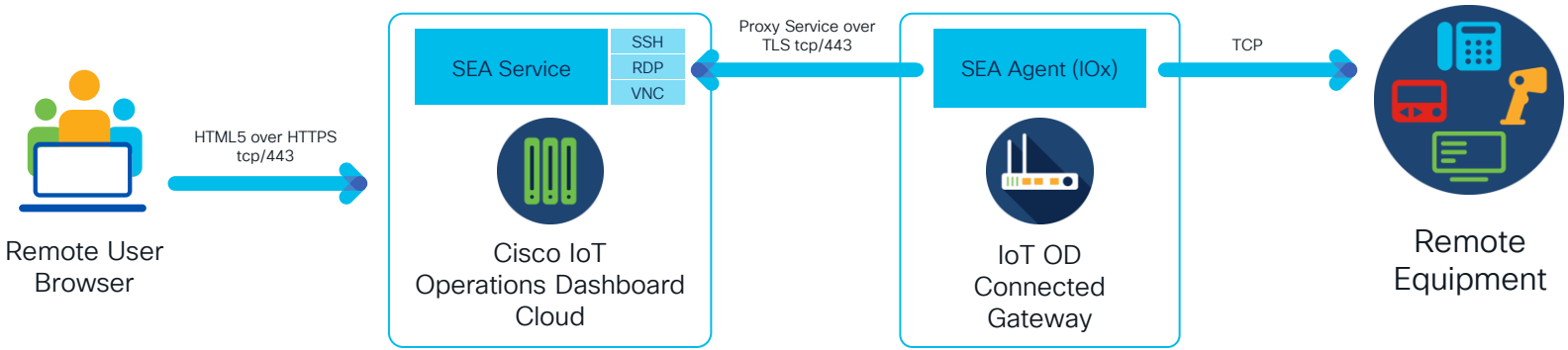
- Globally, ~81% of breaches involved compromised credentials
- The first step towards moving beyond credentials towards password-less, is MFA
- Useability and accessibility drives adoption
- Not all MFA is equal – Fido2
- Goal: Secure every app

- Compromised devices are a vector and can compromise authentication
- Goal: Ensure every device authenticating is secure

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

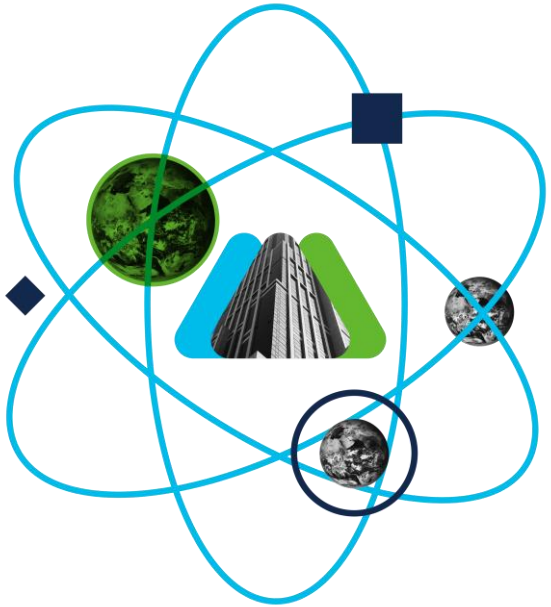
Secure Equipment Access For Remote Assets

- No installation required: equipment access through browser
- Proxy: SEA Agent on Gateway is a proxy over TLS/443
- Isolation: remote user is never directly connected to remote network



The network adds a layer of data protection

- Protecting data as it traverses less secure networks
  - Encryption incl. MACsec/802.1AE
  - Integrity and access control
- Some devices may not offer adequate protection
- Protect the data the devices cannot protect themselves (weak/hard coded/quantum)



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Experiment: Protection

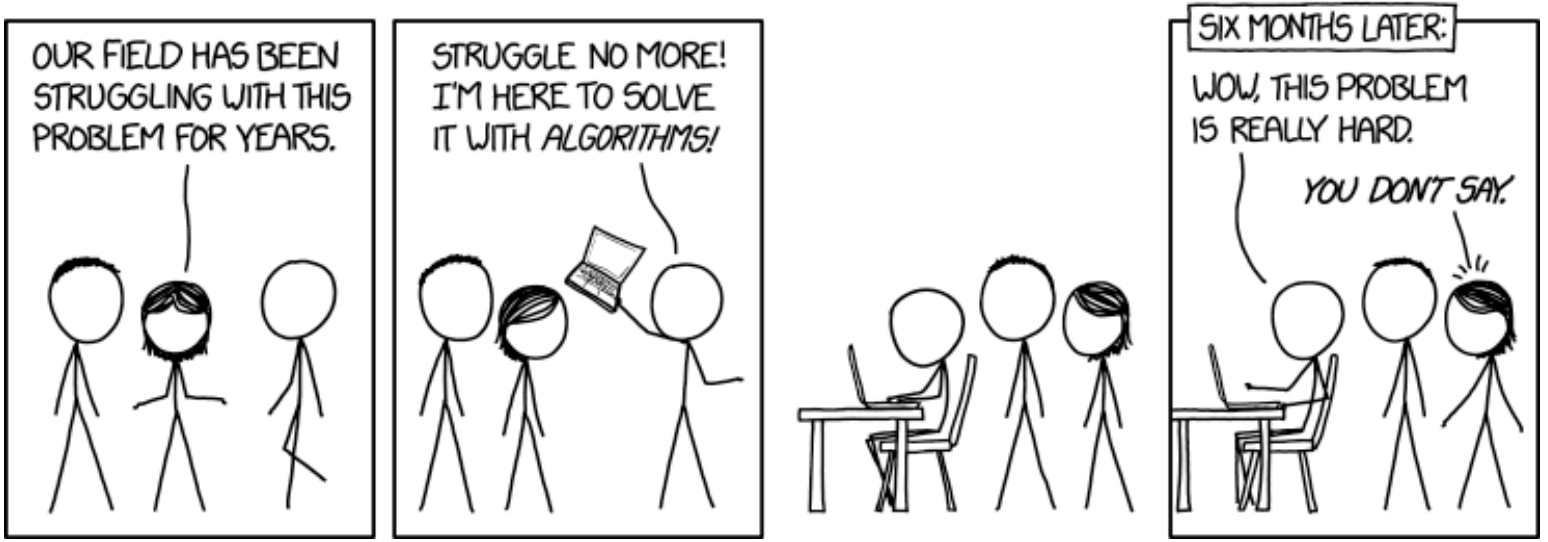
A particular high scoring vulnerability is released. Its remote and affects a lot of devices on your network
- What mitigations can you put in places while you patch?
- How do you protect vulnerable systems in the OT space?
- Some have been exploited, how do you isolate those hosts (IT & OT)

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Protection needs to continually adapt

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Integration and Automation

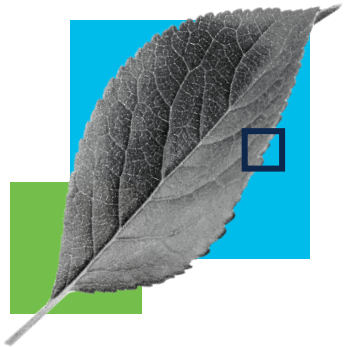


Source: https://xkcd.com/1831/

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Goals of integration and automation

Your tools
simplified

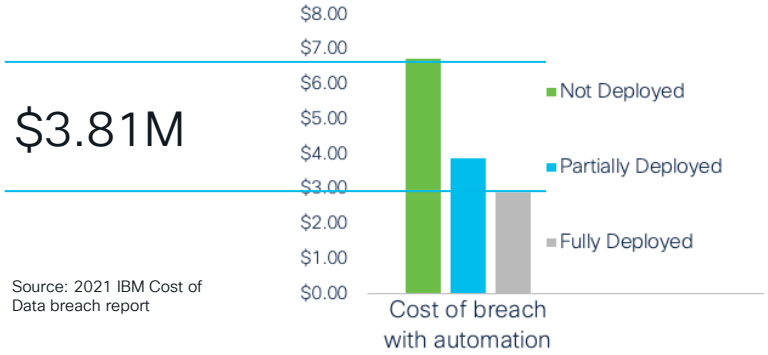


Your response
accelerated

Your resources
efficacious

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Simplification and Integration

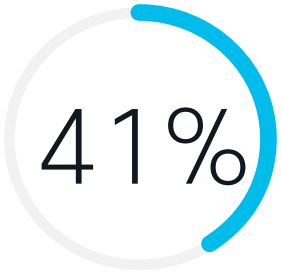


Source: 2021 IBM Cost of Data breach report

2.3M

Additional cost of breach where complexity is high

Source: 2021 IBM Cost of Data breach report



41% engaged more than 10 cybersecurity partners, in a challenging multi-vendor environment

Source: 2019 Cisco CISO Benchmark Study

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

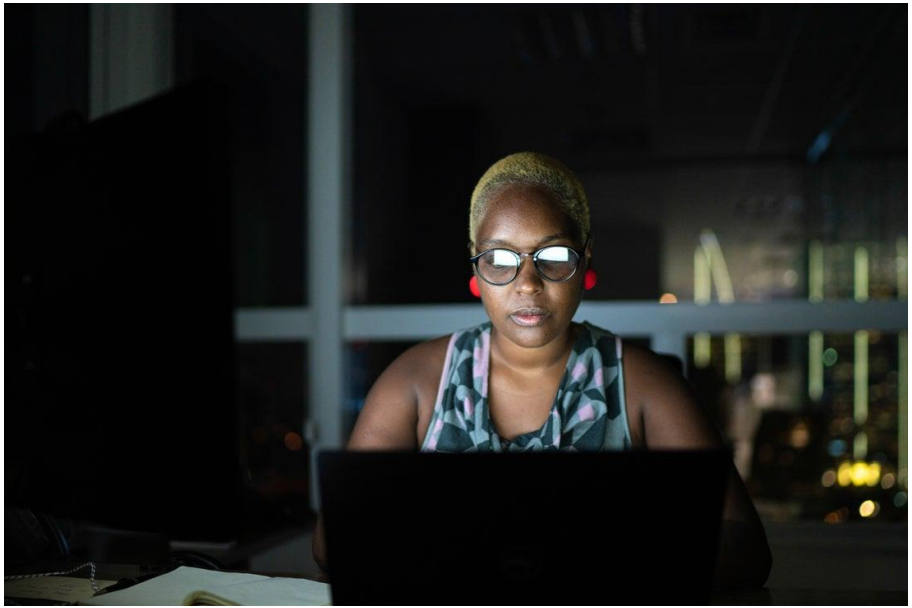
Some Incident Response Goals

Improved detection – Anomaly detection, timeline analysis

Improved response - Automate information to analyst

Improved engineering – Better log injections and health

Improve operational outcomes – “Assistants” training, efficiency and burnout analysis



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Is AI/automation scary in a cyber security context?

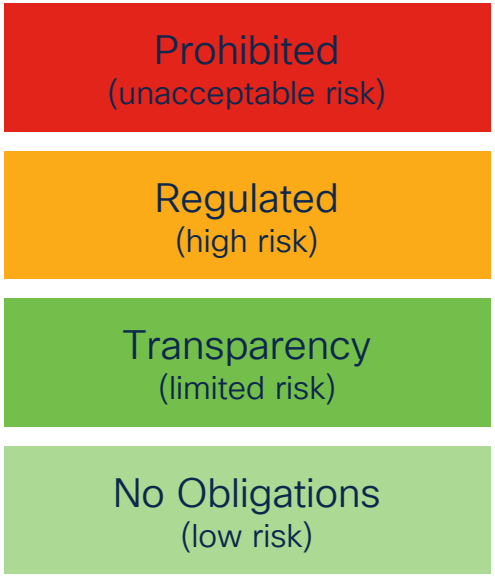
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

EU AI Act

Penalties Up to €30 million or 6% of worldwide annual revenue (€40/**7% for prohibited)**

Purpose: Align development & use of AI with rights of EU individuals

Risk-based Approach



Clear threat to safety, livelihood, & rights
'Real-time' biometric identification in public places
AI systems that exploit vulnerable groups
AI systems that deploy harmful 'subliminal techniques'

Prohibited

Adverse impact safety & rights
Management and operation of critical infrastructure
Biometric identification and categorization of persons
Law enforcement

Registration, Conformity Assessment, & Risk Mgmt

Limited risk to safety & rights
Chatbots
Emotion recognition
Deepfakes, generative AI

Transparency Obligations

Minimal risk

No Obligations

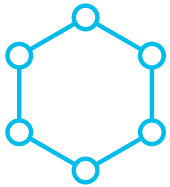
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

But first we must digitise, before we can use AI

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

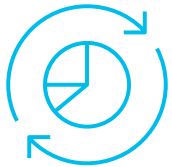
XDR (eXtended Detection and Response)

Integrate your security toolsets



Collection of detections and raw telemetry from multiple sensor technologies across your environment

Application of advanced analytics to the collected and normalized evidence to produce correlated and prioritized detections of malicious activity

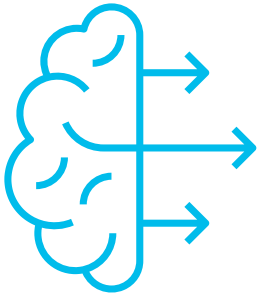


Guided responses across multiple control planes to quickly and effectively contain, mitigate, and eradicate the threat.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Intelligence

Threat Sharing and Blocking



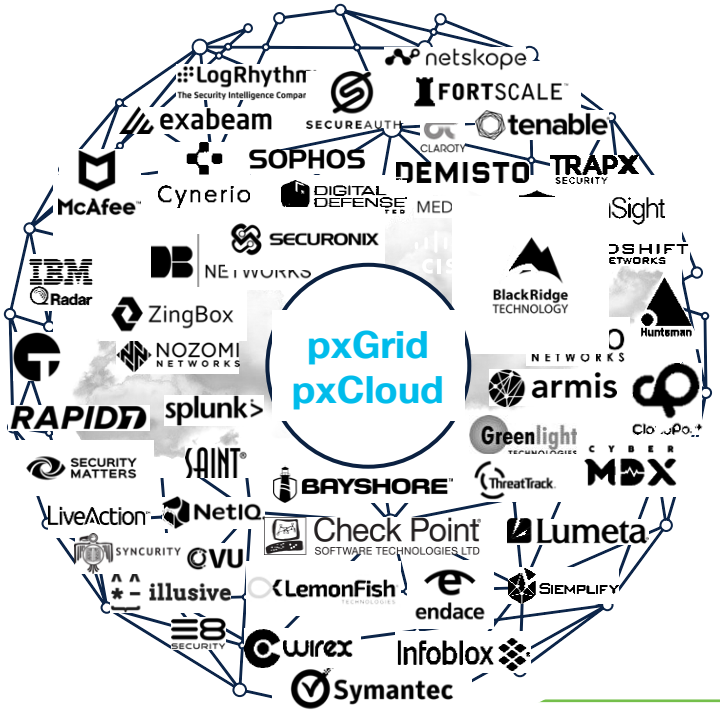
- Use public and private sources of intelligence to achieve better threat identification.
- Create and customize your own feeds based on your environment and needs.

But we need to:

- Consume feeds and distribute to your toolsets
- Gather threat information to share with your communities

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

No-one uses a single vendor



Visibility and automation to other parts of your ecosystem

Integration with 3rd party security products

Cisco Security

Network

Applications

Endpoint

Cloud

XDR

3rd Party/ITSM

Intelligence

Identity

SIEM/SOAR

Your infrastructure

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Integrations for Visibility (ISE)

Medical Devices

Hospital

250+ Medical device profiles

- Pharma-Smart-Device
- Philips-Analytical-X-Ray-Device
- Philips-CareServant-Device
- Philips-Healthcare-PCCI-Device
- Philips-Medical-Systems-Device
- Philips-Oral-Healthcare-Device
- Philips-Patient-Monitoring-Device
- Philips-Personal-Health-Device
- Philips-Respironics-Device
- Phonak-Communications-Device

IOT Building & Automation

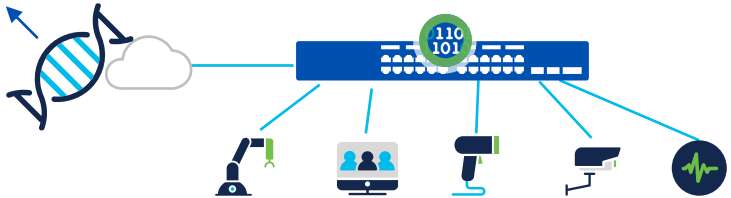
Library

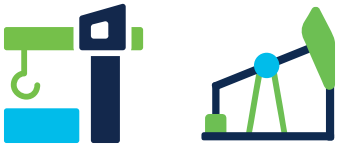
- Siemens-Device
  - Siemens-Automation-Drives-Device
  - Siemens-Building-Device
  - Siemens-Building-Technologies-Device
  - Siemens-Convergence-Device
  - Siemens-Digital-Factory-Device
  - Siemens-Energy-Automation-Device
  - Siemens-Energy-Management-Device
  - Siemens-Home-Office-Device
  - Siemens-Industrial-Automation-Device

pxGrid

Cisco CyberVision

pxGrid





Factory

Industrial Devices

Cisco AI Endpoint Analytics

Profiles IOT devices and sends endpoint labels via pxGrid to ISE for authorization

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Integration and automation summary…

Unlock new value from your existing investments

- From partial awareness to **complete** and **actionable insights**
- From inefficient workflows to the **strength of automation**
- From siloed product usage to **shared context**
- From complexity to **simplicity**

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

We need to be faster

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Network is in and Ideal Position

Network Platform: Security Control and Visibility

Business Applications: Safety, Efficiency, Mobility

Safety and compliance
Passenger experience
Data Operations
Operational Efficiency

Passenger services
Demand management
Predictive Maintenance
Capacity management

Vehicle-as-a-sensor
Weather Detection
Vulnerable road user detection

Traffic signal phase timing, prioritisation, preemption
Roadway Safety
Vehicle automation

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

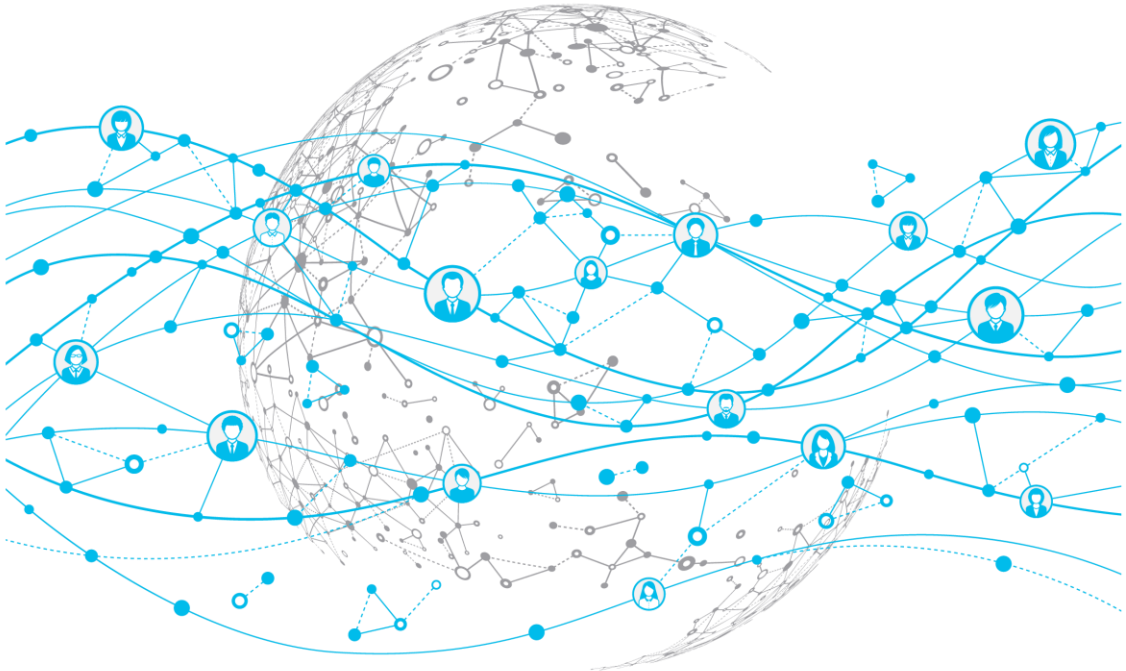
“If you are working at the cutting edge of technology, you may not be interested in geopolitics, but geopolitics is interested in you, and you would be reckless...with your own companies' viability...if you didn’t think about what that means”

Ken McCallum, Director General, MI5 (60 Minutes 23 Oct 2023)

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Move toward explicit trust

Supply chain security



Pervasive Security (not enough alone)

Trustworthy Solutions (security controls and checks)

Accountable Partner (H/W, S/W, services and methods)

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

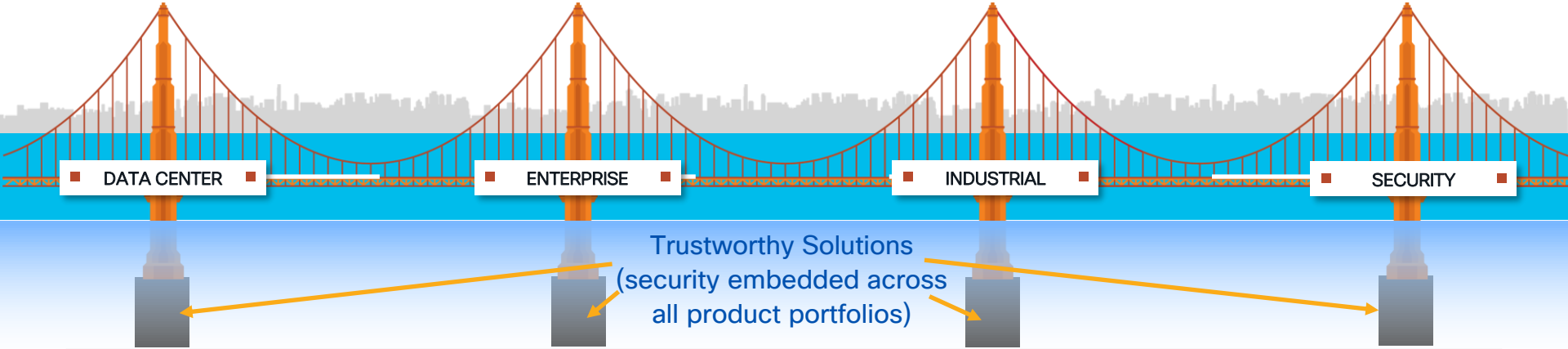
A Trustworthy Solution Is:

Security designed into...

"Security embedded throughout the solution lifecycle and across the Cisco product portfolios"

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Building on trustworthy foundations

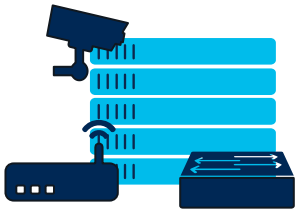


Trustworthy Foundation

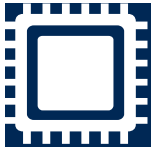
- Secure Development
- Supply Chain Security
- Trustworthy Technologies
- Vulnerability Disclosure
- Rigorous Testing & Assurance
- Data Protection & Privacy

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

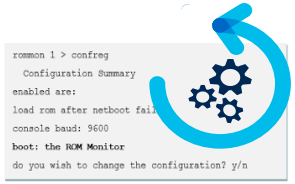
Trustworthy Technologies Protection Scope



Manufacturing

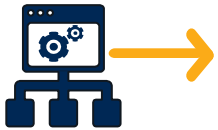


Hardware



BIOS/ROMMON

Software Image



System Booted

Attack Type

Supply Chain Attacks → HW Tampering Attacks → BIOS / Rommon Attacks → SW Binary Attacks → Runtime Attacks

Counter Attack with

Trust Anchor module w/SUDI

Trust Anchor module w/SUDI

+

Secure Boot

+

Image Signing

Runtime Defenses

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Our **Interdependency** with AI **Growing & Getting More Complex**

Our security, is your security

Our privacy, is your privacy

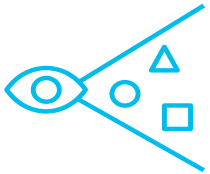
Our resiliency, is your resiliency

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

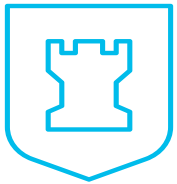
Addressing Business Challenges

Visibility



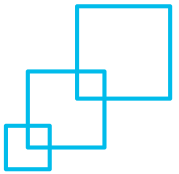
- Detection/Threats
- Operations
- Risk visibility

Protection and Mitigation



- Mitigate vulnerabilities
- Segmentation
- Faster Response

Integration and Automation



- Scale
- Skills
- Compliance

Holistic | **Continuous** | **Fast**

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOT Sessions and Breakouts

- Securing transportation and utilities at scale [BRKIOT-1627]
- Cisco Solutions for Mission-Critical Mobile Infrastructure in Industrial IOT Environments [BRKIOT-2356]
- Using autonomous mining to improve safety and reduce carbon footprint [BRKIOT-1328]
- Improving the IT + OT Partnership Experience to Digitize the Physical World [INTIOT-1103]

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOT Demonstrations

- Cisco Industrial Technologies: The Wall of Solutions
- Securing Industrial Networks: Visibility, Trust, Secure Remote Access - [DEMO-IOT02]
  - Securely manage Who, What, Where and When access is provided to your network
- Scale OT with Cisco SD-WAN – Connect and Manage Remote Assets- [DEMO-IOT02]
  - Manage your Thousands of remote systems securely with SD-WAN
- Industrial Wireless, Anywhere ! -Fixed and Mobile Wireless for OT - [DEMO-IOT02]
  - 5G, Private LTE, WiFi6E, Ultra-Backhaul; choose the best model for your needs
- Unify IT/OT Network Operations – Industrial Ops with Catalyst Center - [DEMO-IOT02]
  - Bring IT-level visibility to industrial operations
- Edge Compute: Process data at the edge with Cisco IOX - [DEMO-IOT02]
  - A Utility case study in action

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Q&A

cisco Live!

Did you know?

You can have a one-on-one session with a technical expert!

Visit Meet the Expert in The HUB to meet, greet, whiteboard & gain insights about your unique questions with the best of the best.

Meet the Expert Opening Hours:

Tuesday	**3:00pm – 7:00pm**
Wednesday	**11:15am – 7:00pm**
Thursday	**9:30am – 4:00pm**
Friday	**10:30am – 1:30pm**

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

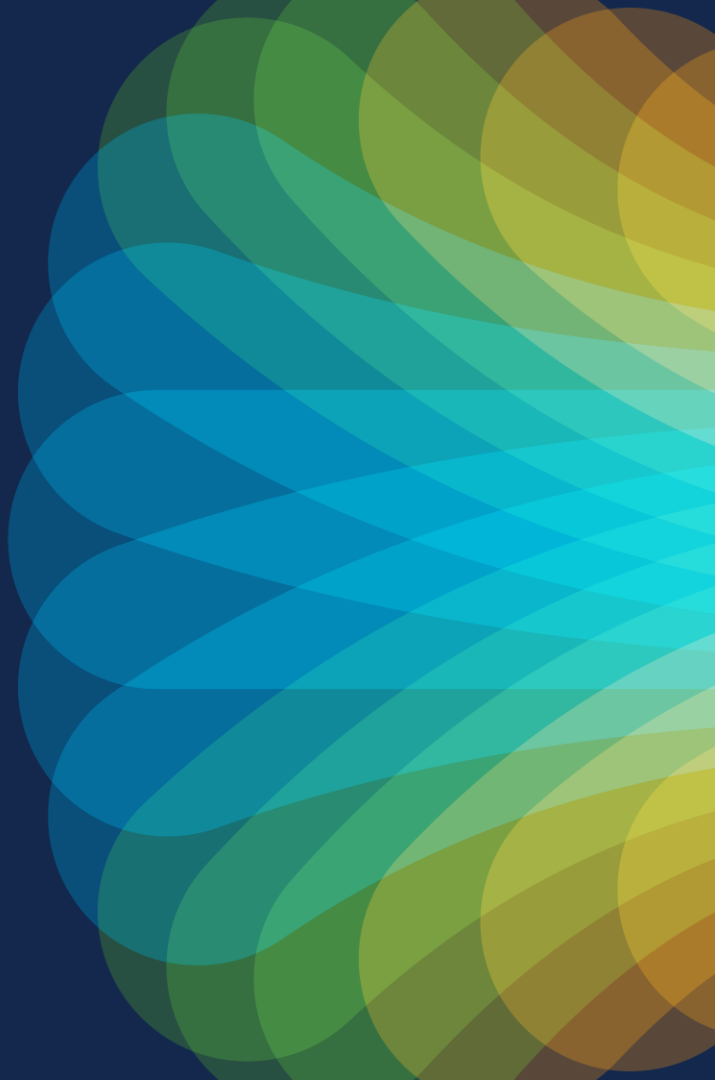
Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The bridge to possible

Thank you



cisco Live!
Let's go
#CiscoLiveAPJC