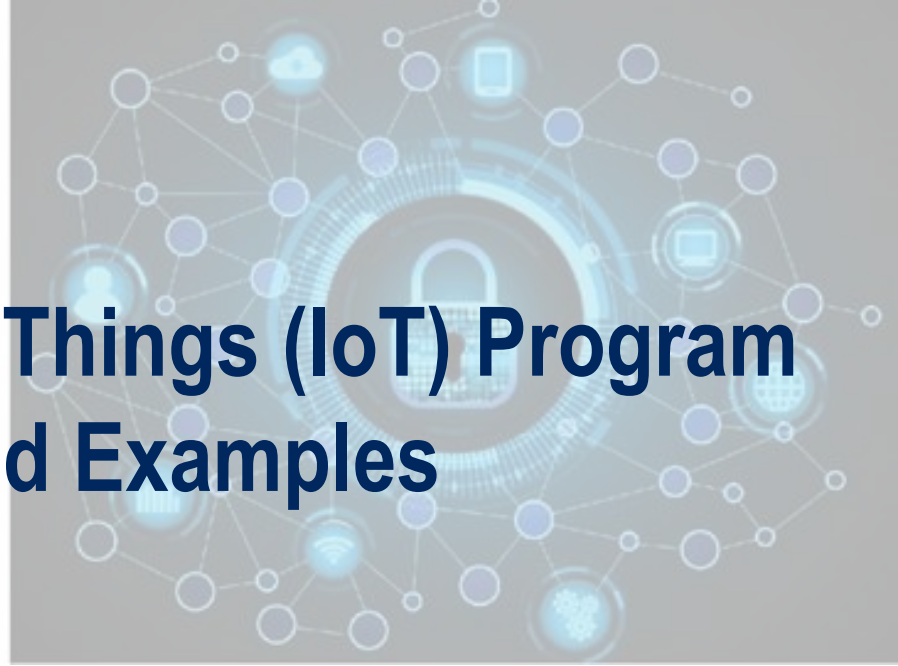


Securing Your Internet of Things (IoT) Program
Three Real-World Examples

A Discussion With Technology Leaders About Smart Communities, Utilities, And Buildings

Welcome!

NFF

SPEAKERS

- Chris Peabody – Chief Strategy Officer, Networking For Future
- Michael Cannon – Chief Technology Officer, Stafford County, Virginia
- Tom Kuczynski – Vice President Information Technology, DC Water
- Peter Burke – Security Technical Solutions Architect, Cisco Systems

NFF

AGENDA

- Speaker Introductions and NFF Overview
- IoT Security Ecosystem Overview
- Smart Communities Case Study
- Smart Utilities Case Study
- Smart Buildings Case Study
- Questions and Answers – Submit via Chat

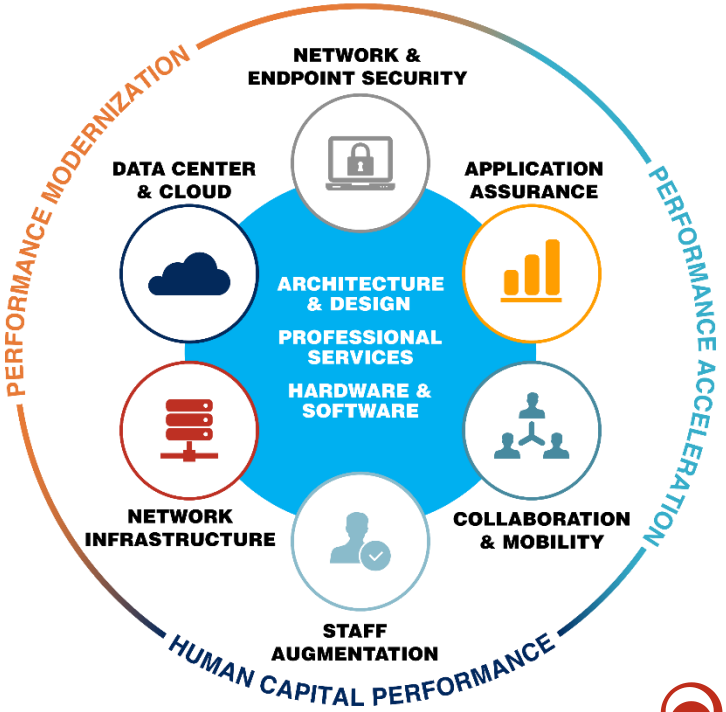
OVERVIEW

Networking For Future, Inc. (NFF)

- Founded in 1996
- Headquartered in Washington, DC
- 130+ Employees
- ISO 9001:2015 Certified
- 77% of workforce hold industry certifications

Offering a performance-focused approach to delivering transformational IT business solutions.

IT Business Solutions



OVERVIEW

Strategic Partners

- Cisco Gold Integrator Partner
- NetApp Gold Partner
- VMware Enterprise Partner
- Splunk Partner
- Microsoft Partner
- Gigamon Partner
- Riverbed Premier Partner
- Aternity Partner
- IET Corporation Partner
- F5 Networks Partner
- Citrix Silver Solution Advisor
- CoreSite Partner
- TRAXyL Partner
- CoastTec Partner
- Catapult Partner

Strategic Contract Vehicles

- GSA Schedule 47QTCA21D0047
- District of Columbia Supply Schedule
  - MOBIS and ITES
- Maryland Education Enterprise Consortium (MEEC)
- Maryland Consulting and Technical Services (CATS+)
- Fairfax County Public Schools
- Maryland Department of Information Technology (DoIT) Hardware Master Contract
- Cisco Virginia Association of State College and University Purchasing Professionals (VASCUPP)
- Federal Reserve Board 202000834

CISCO TOP-FIVE MID-ATLANTIC SLED PARTNER 2019 & 2020

CISCO OUTSTANDING SOLUTIONS PARTNER OF THE YEAR 2016

Standards American Registrations Authority REGISTERED

ISO 9001:2015

CBE Certified Business Enterprise Program

Inc. 500 | 5000

2016 ICIC INNER CITY 100

HALL OF FAME AWARD

NFF

IoT Security Ecosystem Overview

Peter Burke
Security Technical Solutions Architect
Cisco Systems

Cisco IoT Security

CYBERSECURITY FOR THE INDUSTRIAL INTERNET

BDM overview

Pete Burke
Security Technical Solutions Architect - Cisco
June 2021

Two worlds **converging**

Cybersecurity is the top driver

Context is key to securing any environment

SecOps **lack context** to industrial processes

Security policies implemented without context **cause downtime**

You cannot secure what you don't know

List all the assets you are defending

Spot vulnerabilities to patch

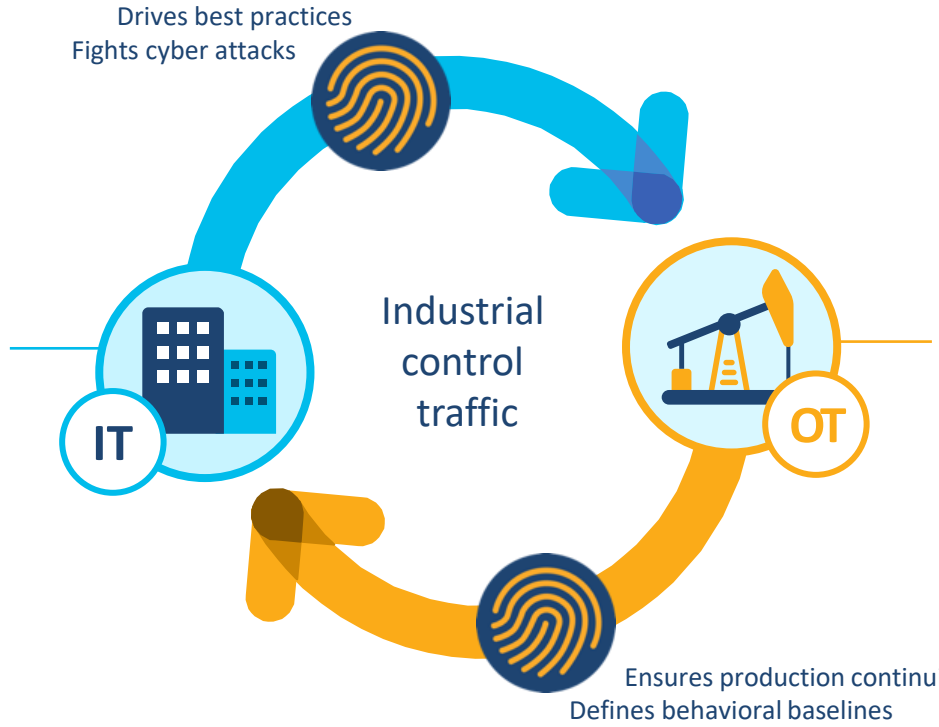
Identify asset communication issues

Detect bypass or leaks in the IDMZ

Build compliance reports

Gain visibility to take corrective actions, segment networks, build security policies and drive best practices

Need visibility to enable **IT-OT collaboration**

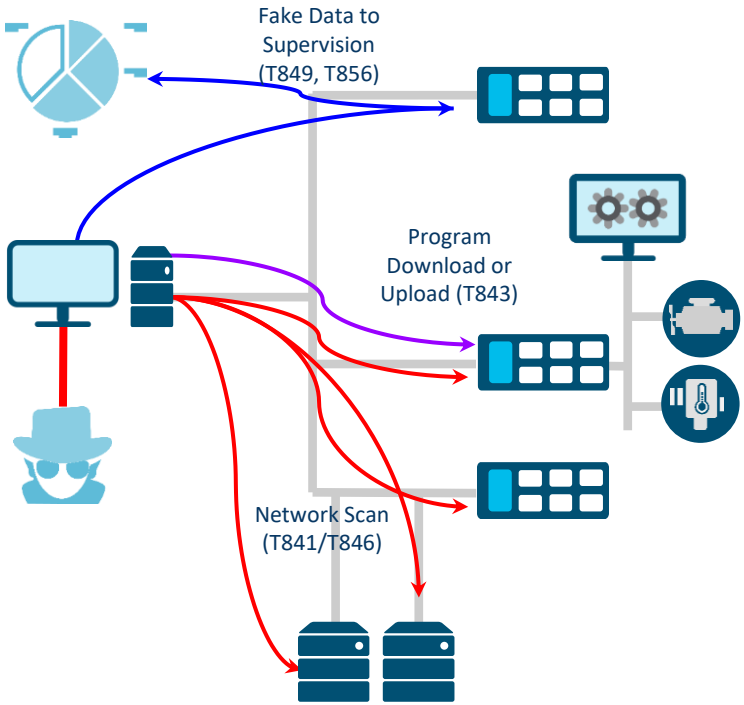


Cybersecurity skills
Network hygiene
Security policies
Detection & Remediation

Industrial process skills
Operational events context
Asset criticality levels
Equipment configuration

Cisco IoT

Detecting OT threats requires understanding IT and OT



How to identify legitimate actions (e.g., Maintenance) and MITRE ATT&CK TTP across dozens of vendors?

- ATT&CK T841/T846
  - Port Scan
  - Network Scan
- ATT&CK T843
  - Change into Control Logic
  - Change Firmware
- ATT&CK T849/856
  - Change into Variables accesses
  - Change into Network Flows

Securing Industrial IoT must address various needs

OT

Gain **visibility** into assets and processes to keep production going and **reduce downtime**

IT

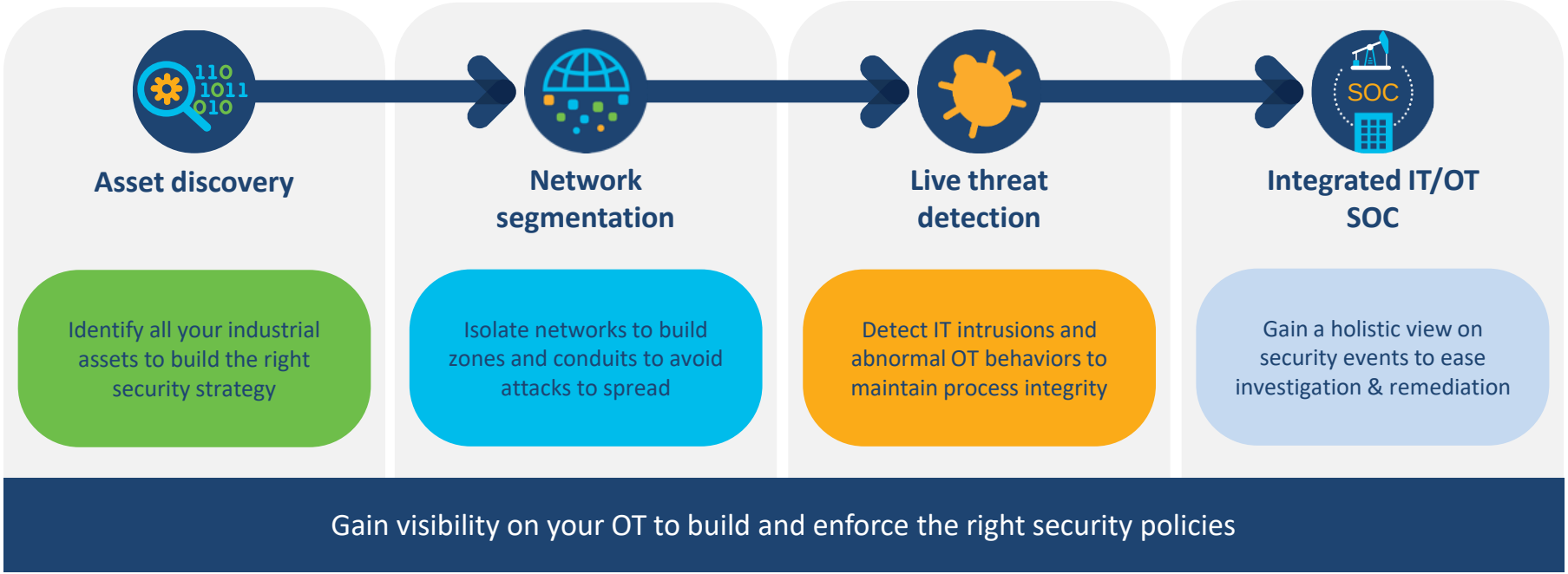
Reduce TCO by eliminating the need to invest in an ever-growing SPAN collection network

CSO

Feed **existing IT security tools** with OT context to build and **enforce OT security policies** that will not disrupt production

The bridge between the enterprise and the line of business

The **4-step journey** to secure your industrial network



Cisco IoT

The **4-step journey** to secure your industrial network

Asset discovery

- Cyber Vision Asset inventory
- Cyber Vision Vulnerability detection
- Cisco CX assessment services

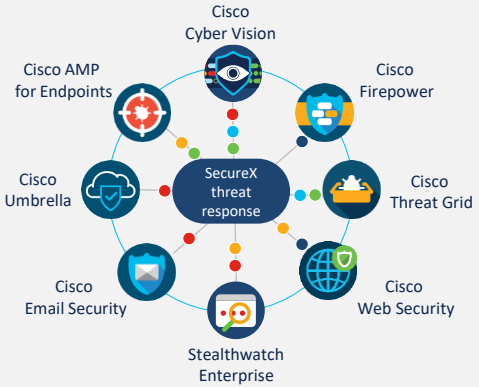
Network segmentation

- ISA3000 Firepower Zone-segmentation
- TrustSec Micro-segmentation
- ISE - Centralized segmentation policy

Live threat detection

- Cyber Vision Anomaly detection
- Firepower/Cyber Vision Intrusion detection
- AMP / Threat Grid Malware detection

Integrated IT/OT SOC



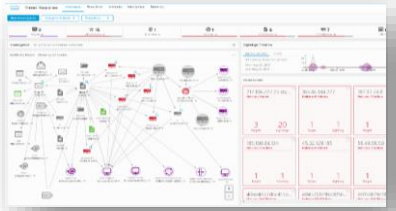
Securing industrial control networks with Cisco

Cisco’s fully integrated IT-OT security solution

Enterprise IT Domain

Investigate and Respond

SecureX



Device Segmentation	Firewall Policies
Identity Services Engine	Firepower Management
Netflow Analytics	Malware Protection
Stealthwatch	AMP
Secure DNS	Network Management
Umbrella	DNA-Center

Powered by Cisco TALOS threat intelligence

Industrial Network

Detect	Protect
Cyber Vision	ISA 3000

Smart Communities Case Study

Michael Cannon
Chief Technology Officer
Stafford County, Virginia

Virginia Smart Community Testbed and IoT Security Use Case

Michael Cannon
Chief Technology Officer
Stafford County, Virginia
June 24, 2021

What is Smart Stafford?

Stafford County, Virginia is becoming an interconnected community, joining the smart community movement and will leverage smart use technology to benefit our residents, businesses, and visitors.

Why become SMART?

- Broadband everywhere-all citizens connected
- Reduces traffic congestion
- Cuts energy consumption
- Attractive to new business ventures and interests
- Improves community safety along with vehicle and pedestrian safety
- Market attractive living for GenXers and others

How have we established Stafford as SMART?

- Partnership and investment with the Virginia Center for Innovative Technology
- Establishment of Virginia Smart Community Testbed
- Use Cases and Pilot Projects to test and deploy Smart Technology in Downtown Stafford

VIRGINIA SMART
COMMUNITY TESTBED
STAFFORD, VA

Stafford's Benefits

- Stafford will become the "center for cyber" and "smart tech"
- Opportunity for State-wide, National, and International recognition
- Business development opportunities
- Entrepreneurial development opportunities
- Focus on improving quality of life for residents and visitors
- Improves public safety in Government Center campus and beyond

#WhatsNextStafford

Use Cases & Pilot Projects

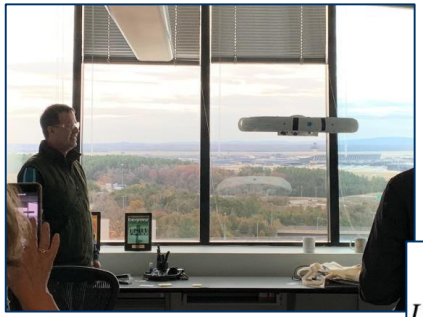
Use Case	Pilot Projects	Timeline and notes
Public Safety	• Use of Drones for Public Safety and Emergency Management • COVID-19 testing in wastewater • Utilize sensors for outdoor smoke and particulate matter • Flood sensors for flood detection	Partnership with Verizon's Skyward software to provide situational awareness in a cloud-based dashboard Utilizing outdoor smoke sensors to detect forest fires and particulate matter. Deploying 15 Flood Sensors throughout the County in flood-prone areas
Cyber Security & Analytics	• Utilize cutting edge blockchain- based military-grade cyber technology • Demonstrate how IoT devices can be secured and protected • Model code and policies for data security and governance	19 cameras deployed utilizing this technology in the Government Center. Also utilizing Iron Yun video analytics software Working with Center for Innovative Technologies and the governance and security of data and potentially storing data in the Commonwealth Data Trust
Connectivity	• Verizon 5G (Outdoor access at government center and testbed • Deploying fixed wireless broadband to unserved and underserved communities	Verizon Small Cell 5G operational in the parking lot of the Government Center and in the Testbed – achieving 2.6 GBS speeds! Utilized cares act and Virginia Telecommunication Initiative grants to partner with fixed wireless broadband providers
Economic Development & Tourism	Green and Renewable, Real-Time Energy Monitoring, Energy - Smart Buildings	In Planning Stages

Drone Alley

Airgility

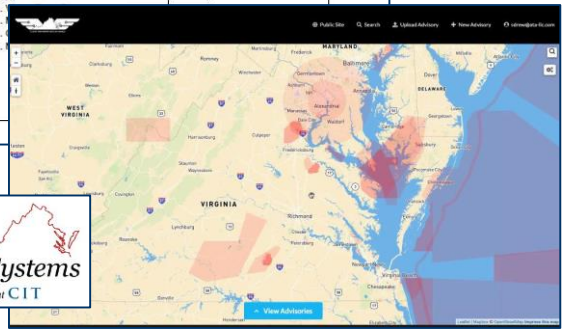
Tactical Van

One Eng Hopper



Skyward

VA-FIX



Virginia Unmanned Systems Center at CIT

Smart Community Testbed Connects Data to People

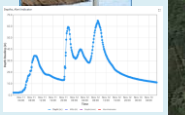
Collect

Connect

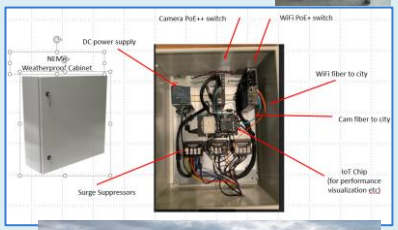
Converge

Correlate

Communicate



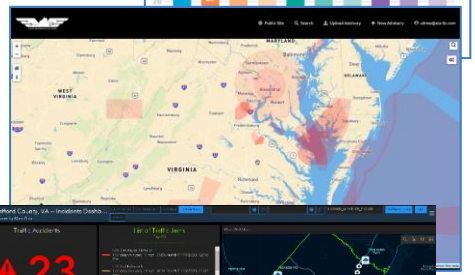
IoT Testbed Rack

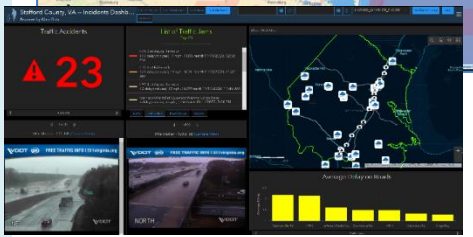


Commonwealth Data Trust

- Overall City Score
- Child Well-being
- Education Quality
- Educational Attainment
- Financial Empowerment
- Neighborhoods
- Health and Safety
- Policing
- Court Reform

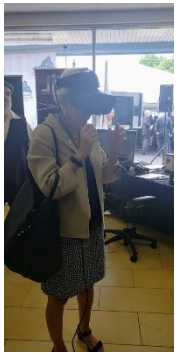
2018 Equity Scores





Security & Privacy

Virginia Smart Community Testbed Launch and Ribbon Cutting
May 25, 2021



Use Case: IoT Security

System Integrator: OST International

Partners

- **Onclave Networks**
- **Axis Communications**

Use Case: IoT Security (continued)

Objective

- **Build a Zero Trust concept for the Testbed that offers greater isolation and containment capabilities than the defense models current deployed on most IT networks.**
- **Based on NIST Special Publication 800-207, Zero Trust Architecture Publication**

Funding

- **The Center for Innovative Technology (CIT) to Onclave to pilot the use of Zero Trust Systems for the Virginia Smart Community Testbed**

Use Case: IoT Security (continued)

- **Two Phases**

- **Phase 1 (August 2020): Establish a pilot testbed at Stafford County Government Center and conduct proof-of-concept penetration testing**

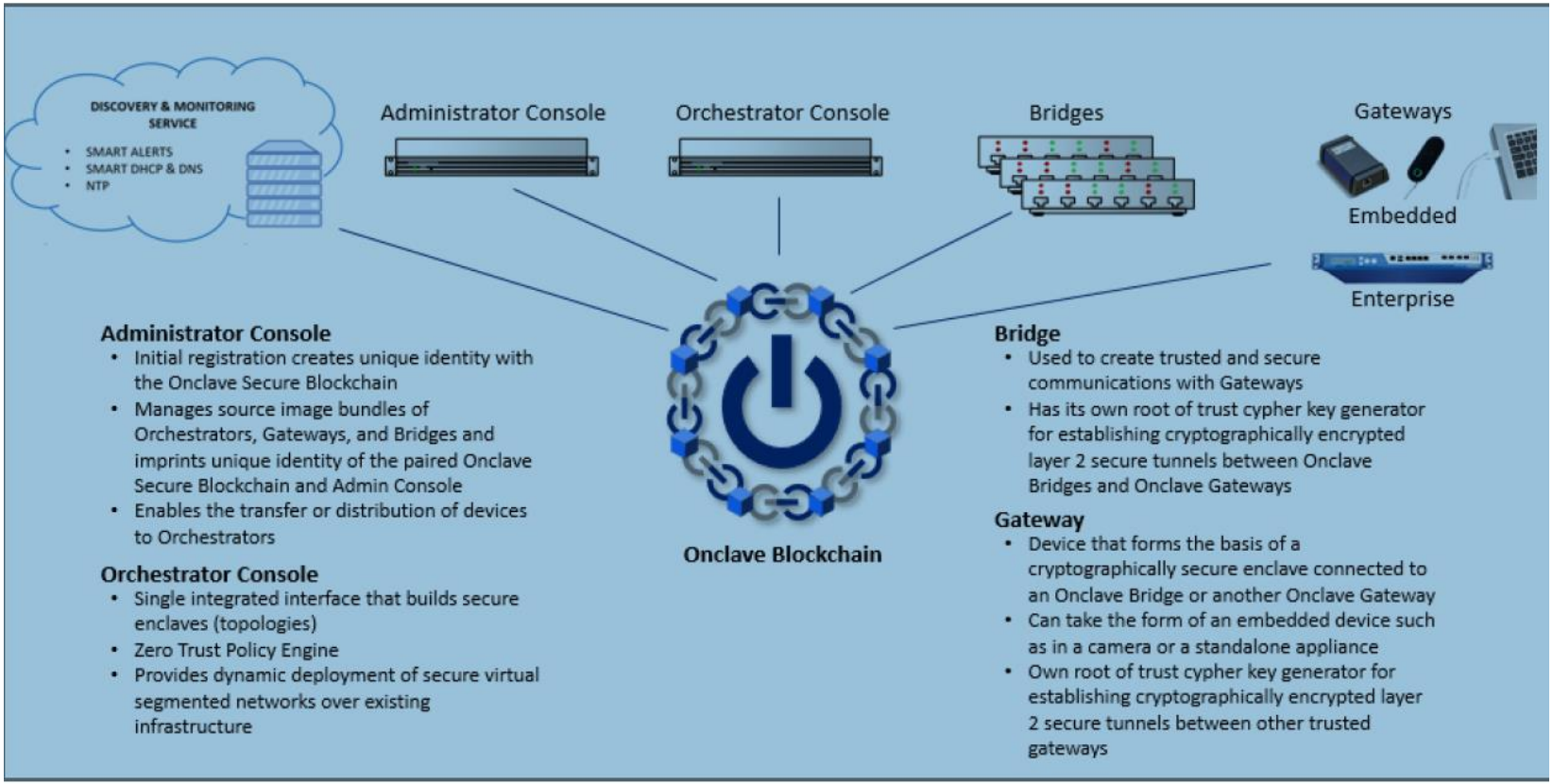
- **Phase 2 (December 2020): Install 19 Axis cameras and migrate the testbed secure IoT configuration to the Stafford IT enterprise**

Use Case: IoT Security (continued)

- The Onclave Networks solution uses a private mult-segment and multi-path blockchain to securely hold cipher keys used in establishing a zero trust environment of all end points within the defined enclave

- Onclave Discovery and Monitoring Services (DMS) uses a dynamics rules engine that monitors all trusted devices based on their common communication parameters before getting trust to each device. DMS detects behavior of trusted devices before granting trust

Onclave Platform Components



Administrator Console

- Initial registration creates unique identity with the Onclave Secure Blockchain
- Manages source image bundles of Orchestrators, Gateways, and Bridges and imprints unique identity of the paired Onclave Secure Blockchain and Admin Console
- Enables the transfer or distribution of devices to Orchestrators

Orchestrator Console

- Single integrated interface that builds secure enclaves (topologies)
- Zero Trust Policy Engine
- Provides dynamic deployment of secure virtual segmented networks over existing infrastructure

Bridge

- Used to create trusted and secure communications with Gateways
- Has its own root of trust cypher key generator for establishing cryptographically encrypted layer 2 secure tunnels between Onclave Bridges and Onclave Gateways

Gateway

- Device that forms the basis of a cryptographically secure enclave connected to an Onclave Bridge or another Onclave Gateway
- Can take the form of an embedded device such as in a camera or a standalone appliance
- Own root of trust cypher key generator for establishing cryptographically encrypted layer 2 secure tunnels between other trusted gateways

Media References

Local newspaper article links:

https://fredericksburg.com/news/local/stafford-opens-smart-community-testbed-to-draw-innovation-entrepreneurs/article_9f634cba-b3c6-5c79-8e9d-b1bcedebf820.html

https://potomaclocal.com/2021/05/26/stafford-county-smart-testbed-opens/

and the DC News 4 Story

https://www.nbcwashington.com/news/local/northern-virginia/high-tech-partnership-could-benefit-stafford-county/2682975/

Questions?

Contact Information:

Michael Q. Cannon
Chief Technology Officer
Stafford County, Virginia
mcannon@staffordcountyva.gov

Testbed Website
https://www.cit.org/virginia-smart-community-testbed.html

Stafford County Website:
www.staffordcountyva.gov

Smart Utilities Case Study

Tom Kuczynski
Vice President Information Technology
DC Water

IoT in Water

"With Opportunities Comes Risk"

Thomas Kuczynski, VP Information Technology

The Promise & Reality

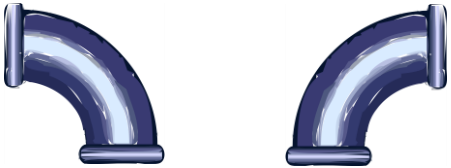
THE PROMISE: The ability to monitor and even control *anything, anywhere at anytime* at a fraction of the cost of traditional legacy technology.

THE REALITY: While this may be true for individual point solutions, in the absence of an Enterprise IoT Strategy, as those solutions expand and data sharing requirements increase security challenges multiply and costs escalate.

Opportunities for IoT in Water

Conservation

Water Management



Leak detection

Conservation

Smarter

Water

Flood monitoring

Pump Station and Dam Monitoring & Control

Water Treatment Monitoring

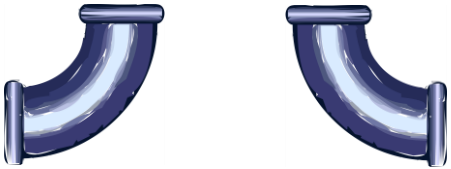
Flow monitoring (COVID)

Process Optimization

Leak Detection

Billing Accuracy

Self-Service



Water Quality

Contaminant monitoring

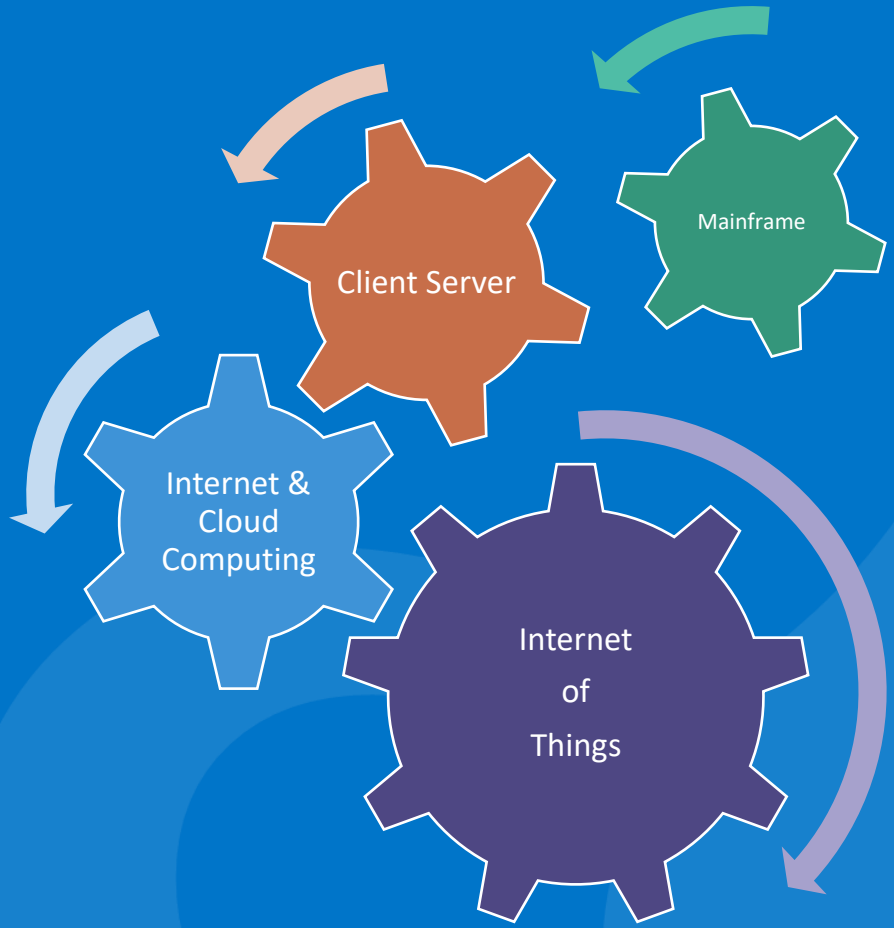
Evolution of IT Security

Mainframes
Proprietary Architectures
Dumb Terminals
Threat Landscape Limited
Remote Connectivity very Limited

Client-Server Computing
Individual Computers
Limited Networking Options
Limited Remote Access

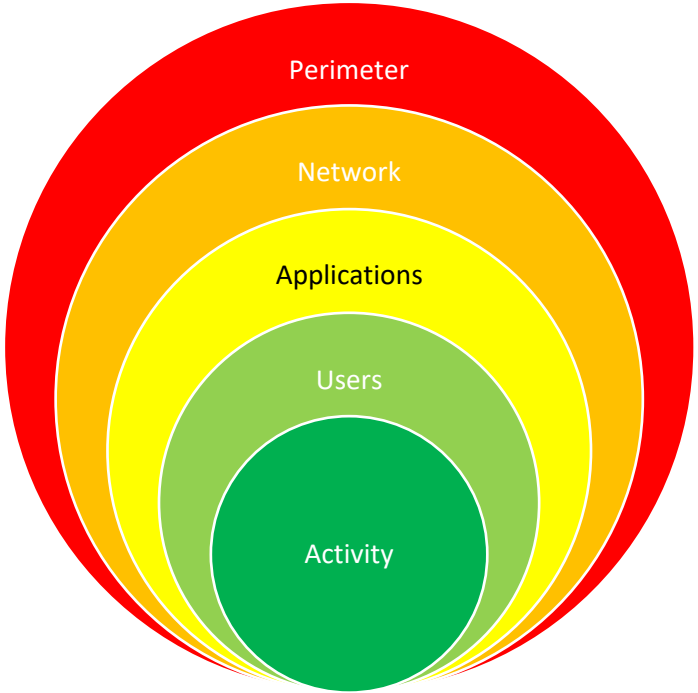
Internet & Cloud Computing
Open Systems
Wired and Wireless Access
24x7x365 connectivity from anywhere

Internet of Things (IoT)
Edge computing
Infinite Threat Landscape



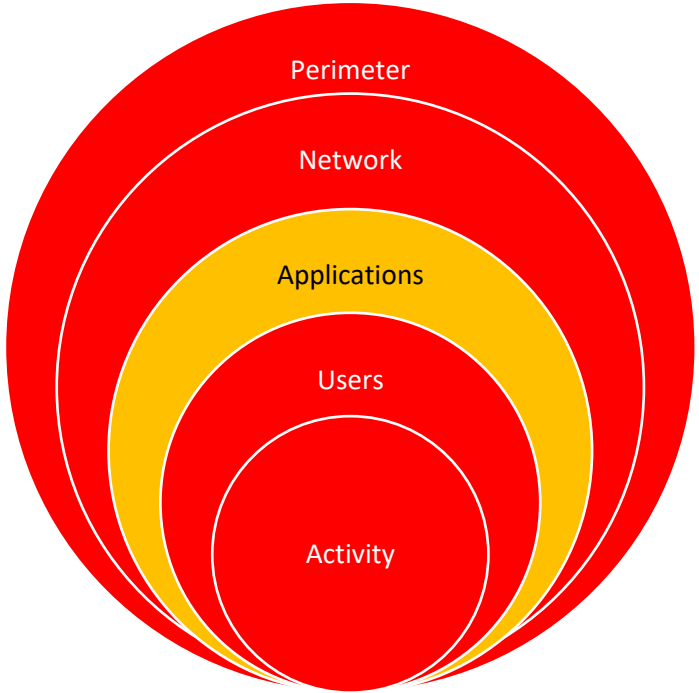
The Lens for Cyber Security has Changed

Yesterday



Outside - In

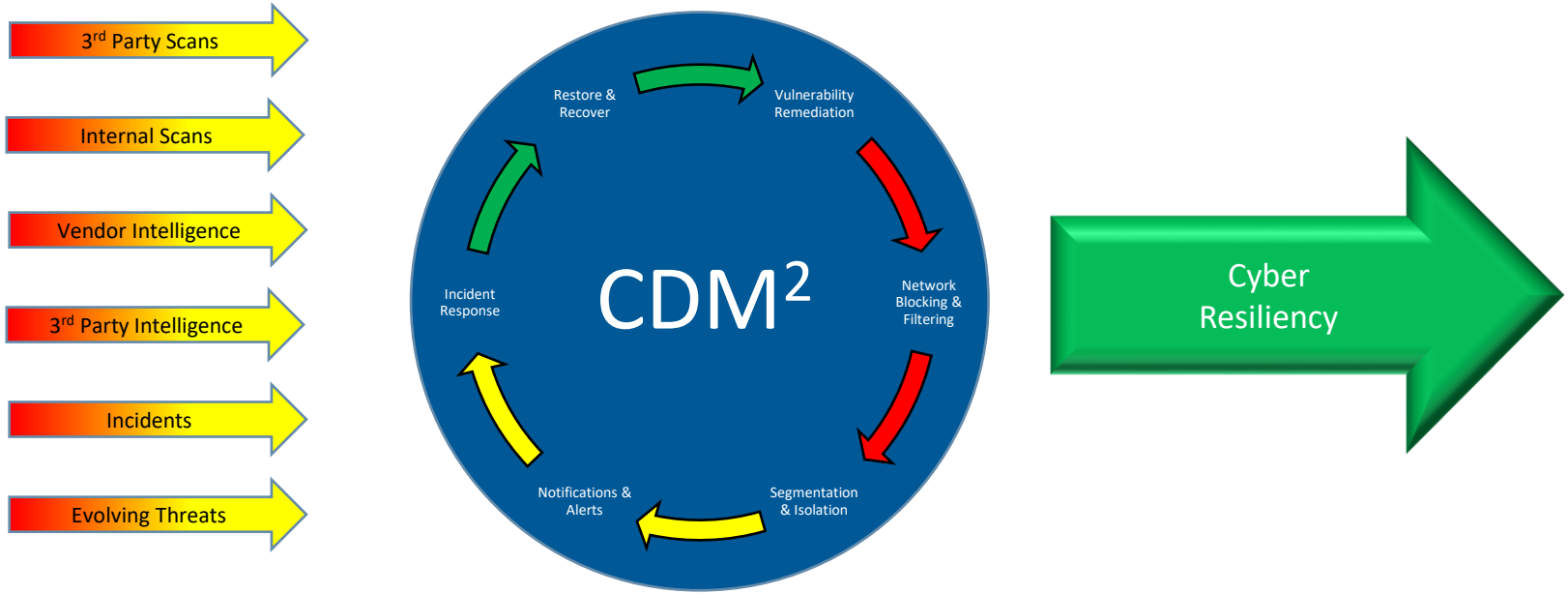
Today



Outside – In & Inside - Out

Continuous Diagnostics, Monitoring and Mitigation

DC Water's CDM^2 program is a dynamic approach to monitor, analyze, detect and mitigate cyber threats to maintain an acceptable ***Cyber Security*** posture. CDM^2 regularly leverages tools, technology and intelligence to identify and prioritize Cyber Risks on an ongoing basis. Prioritizing risks based on potential impacts and mitigating the most significant issues first reduces the likelihood of an incident and helps achieve our goal of ***Cyber Resiliency***.



A Foundation for Cyber Resiliency

Security

Resilience

Know what's on your network

Know who is on your network

Understand your risks and determine what's acceptable

Implement a default deny and least privileged model

Implement multi-factor authentication

Encrypt your data

Implement a Cyber Awareness Program

Monitor your logs for unusual activity

Engage with stakeholders and vendors

Have an incident response plan and test it

Keep your systems patched and up to date

Assess the impact of all new threats

Make sure systems are backed up and backups are stored offline or offsite

Test your recovery capabilities regularly

Specific IoT Cyber Protections beyond the Foundation

- Devices that cannot have their software, passwords, or firmware updated should never be implemented.
- Passwords for IoT devices should be unique per device.
- Self discoverable/configurable devices should always be manually authorized before connecting.
- Never use a default IoT device name and/or password.
- Always patch IoT devices with the latest software and firmware updates to mitigate vulnerabilities.
- Segment IoT devices and never connect them directly to an OT network.
- Understand what and how your IoT devices communicate before deploying them so you can detect future malicious behavior should it occur.

Smart Buildings Case Study

Peter Burke
Security Technical Solutions Architect
Cisco Systems

Smart Buildings

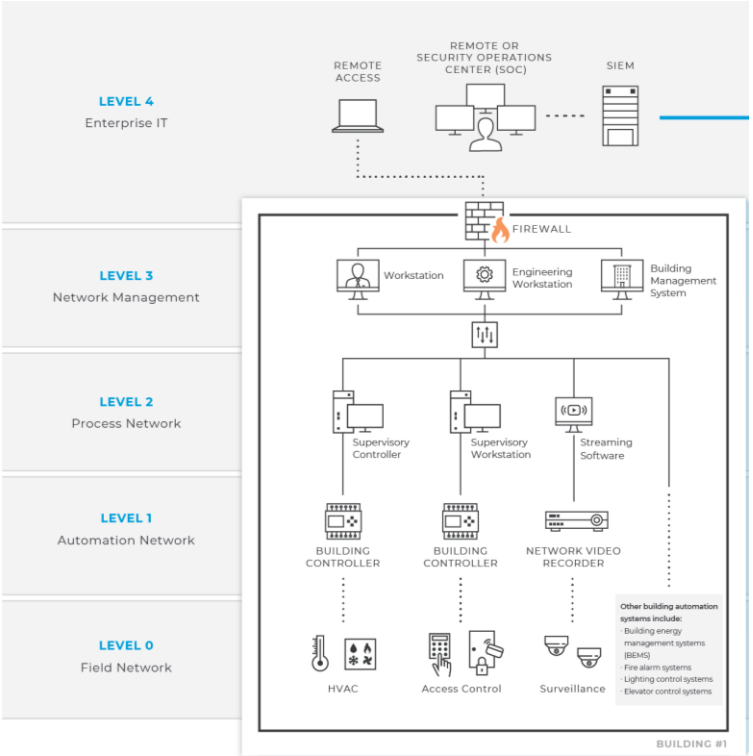
- "By 2028 . . . there will be over four billion connect IoT devices in commercial smart buildings." – Gartner[1]
- Goals
  - Cost savings through increased energy efficiency
  - Physical security
  - Safety
  - Aesthetics/quality of life
- No single vendor will dominate the industry
- Requirement to manage disparate and incompatible systems

Smart Building Technologies and Architectures

- Straddles IoT and traditional OT
- Building Systems Management
  - Smart Lighting
  - Heating/Cooling
  - Fire Suppression & Alarms
  - Earthquake Detection
  - Physical Security Systems
- Connectivity
  - Ethernet (wired and wireless)
  - Serial (RS 232)
  - 802.15.4 (Zigbee, etc.)
  - BACnet
  - LonWorks
- Endpoints
  - Panels
  - Thermostats
  - Sensors
  - Badge scanners
  - Control Servers
  - Workstations
- Example Vendors
  - Johnson Controls
  - Siemens
  - Honeywell
  - Mitsubishi Electric

Smart Building Architecture

- No major standardization between implementations and vendors
- Typically follows hierarchical SCADA model
- Local workstation(s) provided by vendor
- Communication between workstations and panels/controllers via wired/wireless ethernet
- Communication between controllers/panels and physical devices over serial or LR-WPAN (Zigbee, etc.)
- Functionality (HVAC, CCTV, security) may be combined on same network, or segmented back to core



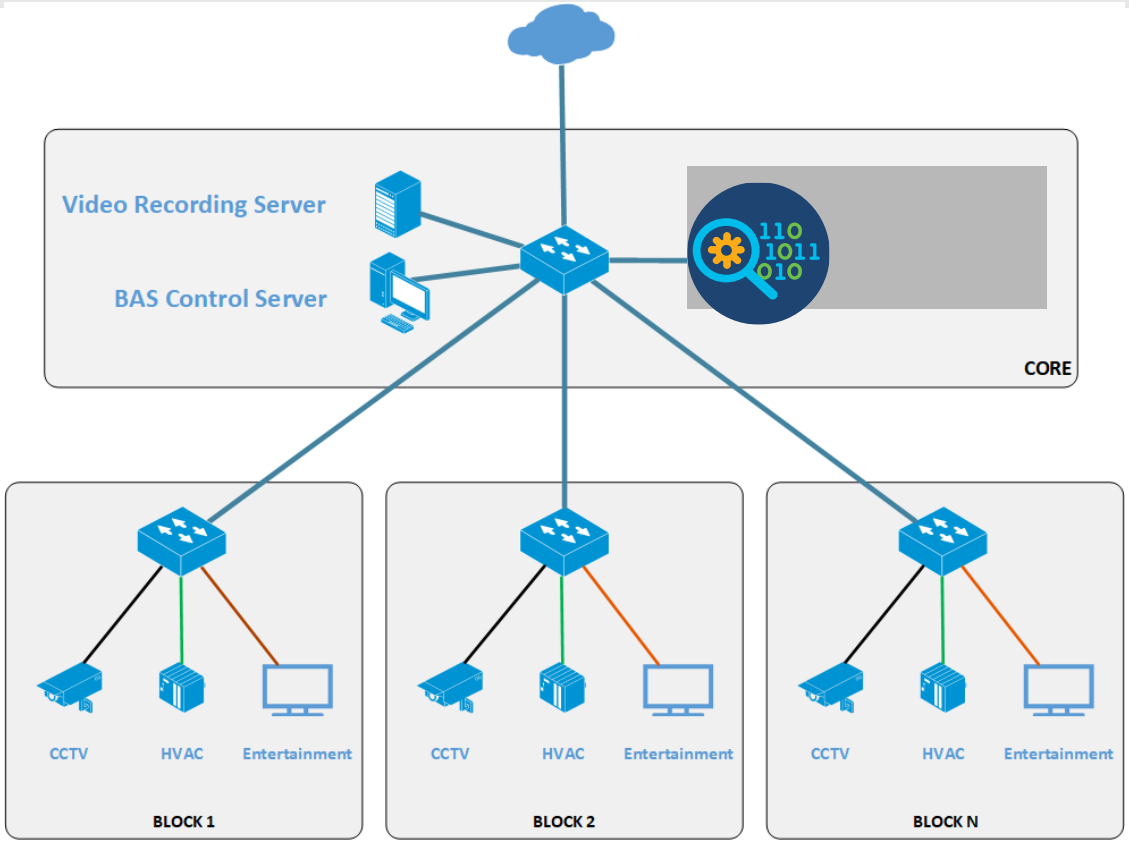
Smart Building Security Challenges

- Dependence on legacy systems that are not routinely updated
- Many different vendors and products in the space
  - Property managers may be responsible for managing dozens of vendors and products
  - Patching and vulnerability management become challenging
- Tenants and previous owners introduce unknown risk
- Companies have historically not placed an emphasis on security governance and management for BAS
  - Lack of proper segmentation
  - Lack of standard IT security controls (NAC, 2FA, IDS/IPS, segmentation, etc.)
  - Systems are still routinely overlooked in security strategy

NFF

Example: Monitoring BAS In a Hotel

- Running all IoT devices on a single physical network:
  - Security Systems (including door locks and security cameras)
  - Environmental systems
  - Entertainment systems for guest rooms
- Collapsed Core design using VLAN segmentation between IoT device types at access layer and routing at core layer
- Nearly all traffic is North-South
- Control system servers located locally
- Can be monitored from a central point (versus in each access block)



Final Thoughts

Questions and Answers
(submit via chat)

Your performance improvement is our measure of success.

Thank You!