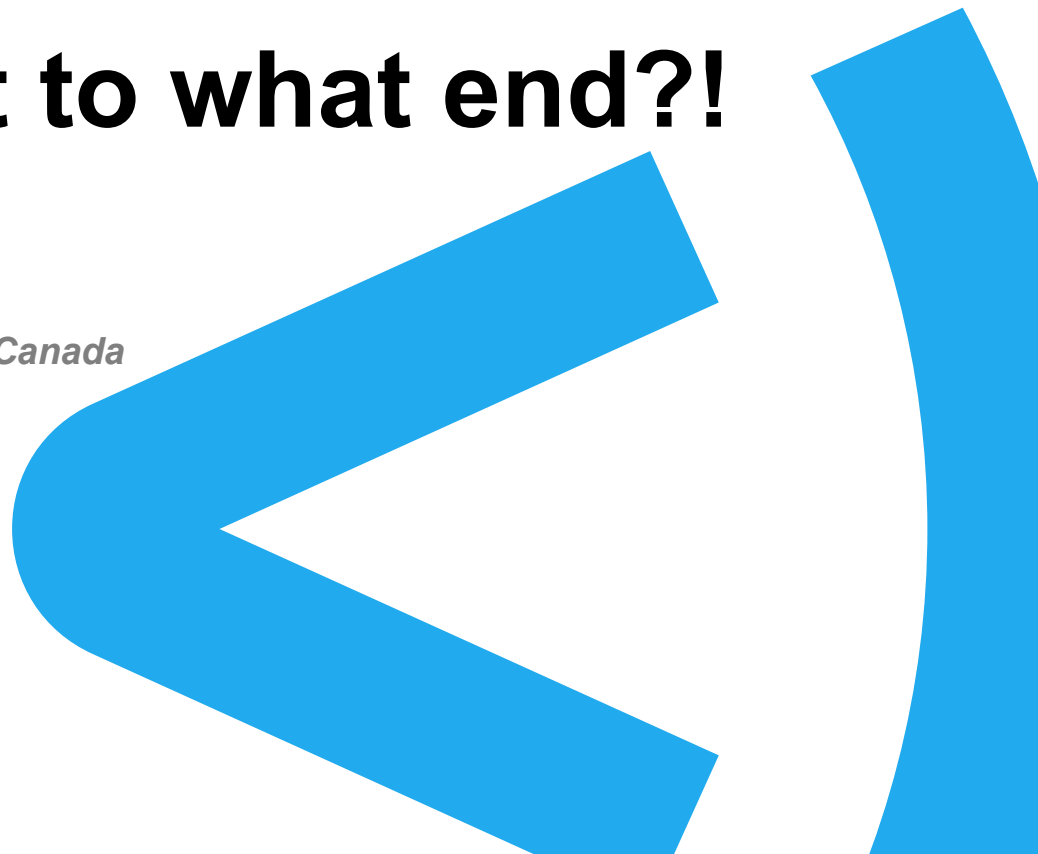# Visibility….but to what end?!

Shane Coleman, CISSP

Systems Engineering Director, Central US & Canada

shane.coleman@forescout.com

(cell) 312-402-0072

Short Vendor Obligatory Pitch

AKA

Shane, why are you qualified to discuss this topic?

FORESCOUT

SCALE

73M+
Total Device capacity sold

2M+
Devices in a single deployment

8M+
Devices in Device Cloud

SCOPE

3400+
Customers in over 80 countries

23%
Of the Global 2000 largest enterprises

Customers in All Major Industry Verticals

VALUE

Visibility
Discover 30% more devices on average

Time-to-Value
65 days – average time for visibility roll out

80
Net Promoter Score
(above security industry average)

Unique, Comparative or Holistic Differentiators

FORESCOUT
CONNECTED DEVICES GROWTH

Agentless — Any device: open/closed, cloud, managed, IT, OT, data center, virtual, campus

Multivariate — Multiple visibility techniques: not reliant on a single approach

FORESCOUT
INTER-CONNECTED

Heterogeneous — Any network type: campus, data center, cloud, and OT

Scalable — Any size network: from thousand to millions of devices

FORESCOUT
AUTOMATION

Take Action — Take action: segment or block

Orchestrate — Coordinate: with all major cyber tools

DEVICE VISIBILITY & CONTROL PLATFORM

eyeSight

eyeControl

eyeExtend

eyeManage

eyeRecover

Platform Capabilities

DEVICE VISIBILITY

ASSET MANAGEMENT

DEVICE COMPLIANCE

NETWORK ACCESS CONTROL

NETWORK SEGMENTATION

INCIDENT RESPONSE

Virtual Appliances

KVM
VMware
Hyper-V

Forescout 5100 Series

5110 FS-HW-5110
5120 FS-HW-5120
5140 FS-HW-5140
5160 FS-HW-5160

<) FORESCOUT.

How ForeScout Sees Devices

> DYNAMIC AND MULTI-FACETED

> OVER 20 METHODS

> 76 TECHNOLOGY PARTNERS

> OPEN INTEGRATION

Silent Defense

K

C RADIUS Server

D DHCP Requests

ForeScout CounterACT®

B SNMP Traps

A

E

H NetFlow/SFlow

J

G User Directory

F

I FTP/LDAP Server

Multiple Methods

A Poll switches, VPN concentrators, APs and controllers for list of devices that are connected

B Receive SNMP traps from switches and controller

C Monitor 802.1X requests to the built-in or external RADIUS server

D Monitor DHCP requests to detect when a new host requests an IP address

E Optionally monitor a network SPAN port to see network traffic such as HTTP traffic and banners

F Run NMAP scan

G Use credentials to run a scan on the endpoint

H Receive NetFlow or SFlow data

I Import external MAC classification data or request LDAP data

J Use optional agent

K Deep analysis of over 100 protocols

BUT ENOUGH ABOUT ME...

Goal of Today's Conversation

> **Challenge the way we think of VISIBILITY PROJECTS**

> **Provide momentum-building ideas around REAL BUSINESS SOLUTIONS**

THERE ARE THR33 KINDS OF PEOPLE IN THE WORLD :

those who *make* things happen,

those who *watch* things happen and

those who *wonder* what happened

— Tommy Lasorda

Observations and possible 'future state" of Endpoint Visibility & Control

EXPLODING NUMBER OF **CONNECTED DEVICES**

By 2023, the average CIO will be responsible for more than 3x endpoints they manage in 2018[1]

- › Diversity of IT devices (cloud, virtual, campus, data center)
- › Growth in closed OT devices

EVERYTHING IS BECOMING **INTER-CONNECTED**

By 2021, 70% of OT security will be managed directly by the CIO or CISO, up from 35% today[2]

- › Convergence of IT/OT networks
- › OT network security spend behind IT

ENTERPRISES ARE SEEKING **AUTOMATION**

By 2021, 70% of [large enterprises] will include security automation and orchestration capabilities, up from less than 5% in 2018[3]

- › Willingness to automate
- › Trying to solve network segmentation problem
- › Volume making the "human middle man" impractical

An Exercise in…..SHARING

Care to share your visibility project(s)?

Why is everything so "expletive" hard?!
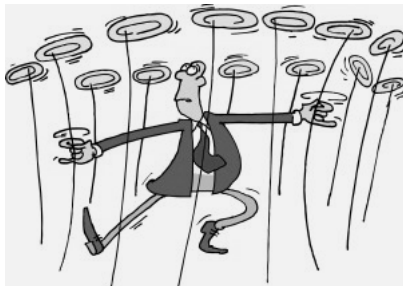## *Organizational Challenges with Visibility Projects*

Visibility?   I can do that!

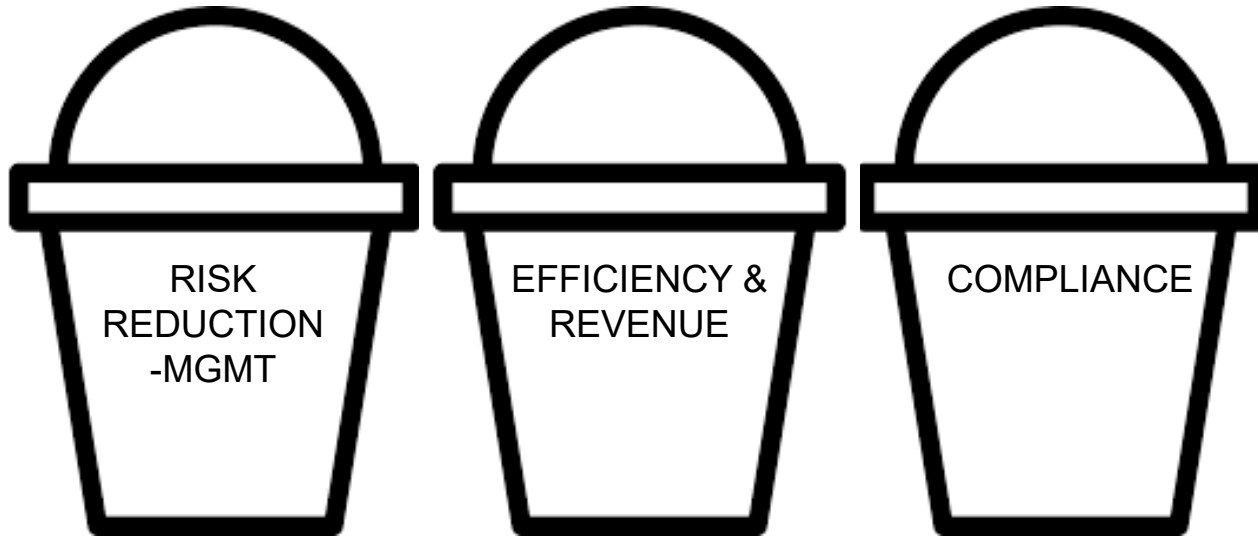Look at me please…

Stop shoving
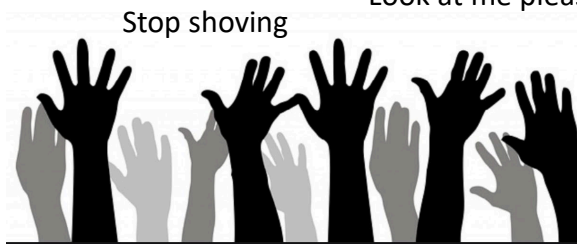
> Visibility is the new 'buzz word'
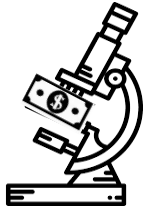
> Project dollars have higher visibility ($ o $$ or $$$)

> So many projects…so little time…

If you could see into the future of your business…

> **What information would cause you to take action?**

RISK REDUCTION -MGMT

EFFICIENCY & REVENUE

COMPLIANCE

So what do you suggest?

"Insert Your Project Management Methodology Here"

What is my current state and the impact to my organization?

- Requirements
- Metrics
- Timelines
- Weight of Alternatives
- Decision Makers

What does good look like for my organization?

FORESCOUT'S CONSULTATIVE APPROACH

- CUSTOMER'S CURRENT STATE

- BUSINESS IMPACT?

TECHNOLOGY AND BUSINESS GAP

REQUIRED CAPABILITIES

& METRICS

- GOALS

- POSITIVE BUSINESS IMPACT?

- Architecture & Statement of Work
- Deployment Plan with timelines & accountability
- Ongoing Manageability Options
- Continual cadence with Account Team

<) FORESCOUT.

Devil in the Details | Metrics to consider

> Mean time to respond or remediate (including audit findings)

> $\$\downarrow$ of cyber-insurance premiums

> $\$\uparrow$ of coverage using same premium amount

> Time to deploy | Time to Value

> % of devices not previously identified/classified

> # of non-compliant devices

> % of audits passed

Showcase your Metrics

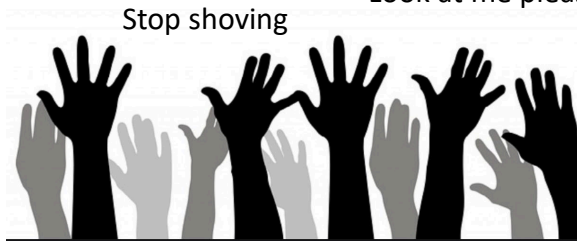# Final Thoughts…

Let's Revisit This Exercise

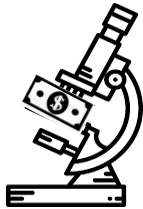**How would you modify your visibility project to highlight its value to your organization?**

Why is everything so "expletive" hard?!

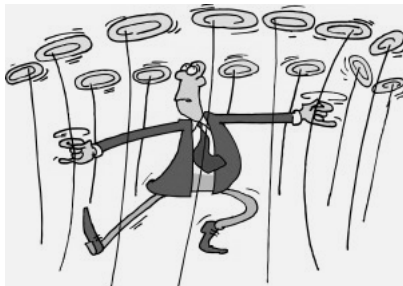## *Organizational Challenges with Visibility Projects*

Visibility?   I can do that!

Look at me please...

Stop shoving

> Visibility is the new 'buzz word'
  – Challenge yourself/team to understand what it means for your company!

> Project dollars have higher visibility ($ o $$ or $$$)
  – Placing business value on projects will GREATLY increase your chance of success

> So many projects…so little time…
  – Prioritize: let your vendors, partners, references do the heavy lifting

<) FORESCOUT.

Final Thoughts for Enhancing-Fast Tracking Your Visibility Project

> **Don't allow "Visibility Projects" to turn so technical to loose the business value**
  - New requirements and capabilities, while 'cool' may introduce more BAD than. GOOD.

> **Keep Asking yourself "Why"?**
  - If you can't find the value, chances are no one else in your organization will either.

> **Identify Internal Budget Owners**
  - What have they looked for when approving projects?

Thank You!