

# Essential Elements To Achieving Secure Access Secure Edge (SASE)



**Investing In A Long-Term Security Strategy**

# Welcome!

# AGENDA

- **Speaker Introductions and NFF Overview**
- **SASE Framework**
- **SASE Use Cases**
- **Security Transformation: University of the District of Columbia**
- **SASE Trends**
- **Questions and Answers – Submit via Chat**

# SPEAKERS

- **Molly McGuire – Security Sales Manager, Cisco Systems**
- **Mike Rogers – Executive Director, Information Services and Management, University of the District of Columbia**
- **Chris Peabody – Chief Strategy Officer, Networking For Future**

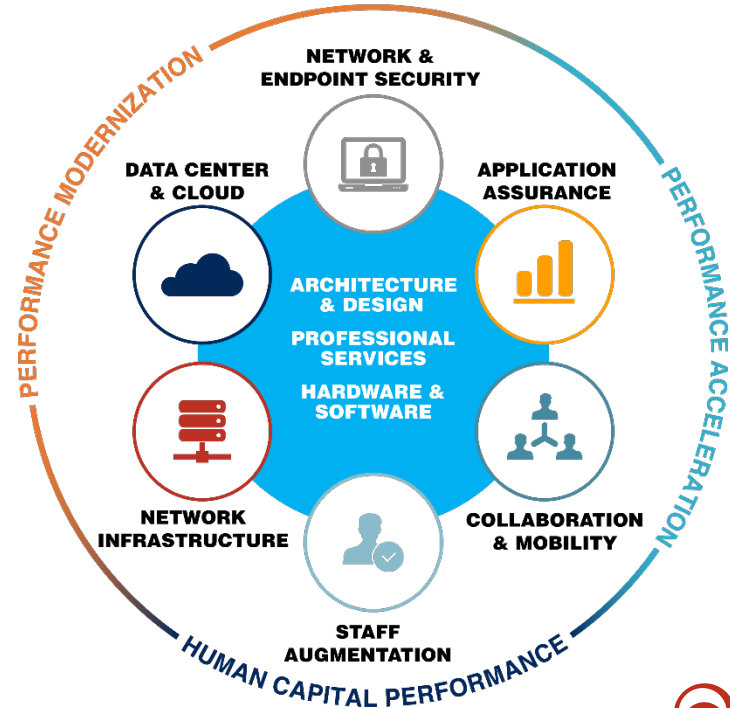
# OVERVIEW

## 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**



# SASE Framework

**Molly McGuire**  
Security Sales Manager  
Cisco Systems

# Essential Elements To Achieving Secure Access Secure Edge (SASE)



Molly McGuire — [momcguir@cisco.com](mailto:momcguir@cisco.com)  
Security Partner Sales Specialist

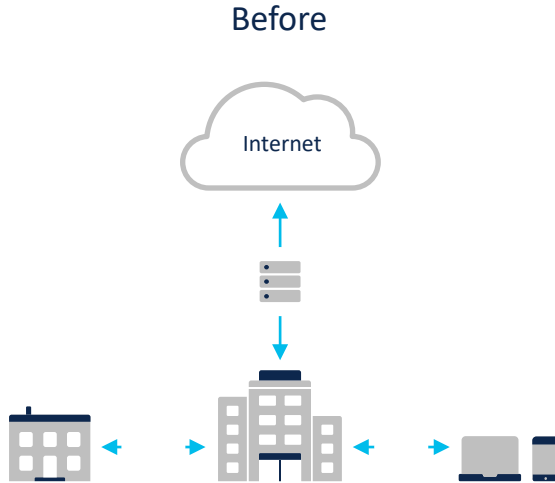


Molly McGuire  
**Security Partner Sales Specialist**

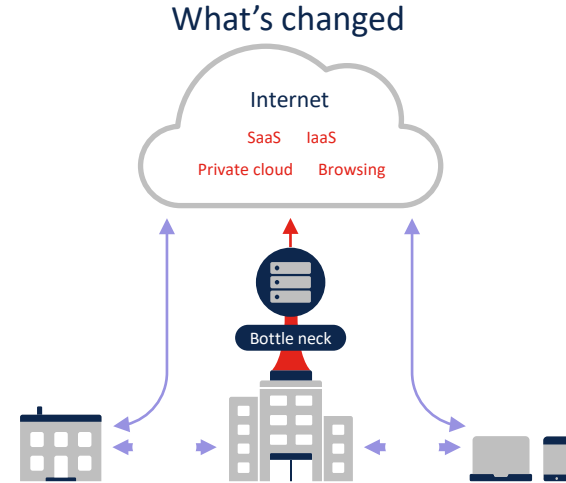
- GSSO Cyber Security Channel Specialist
- Meraki CMNA Certified
- 11 Years in networking and 9 years in SaaS
- Carrousel Museum Board Member
- Volunteers with a dog rescue



# Network transformation



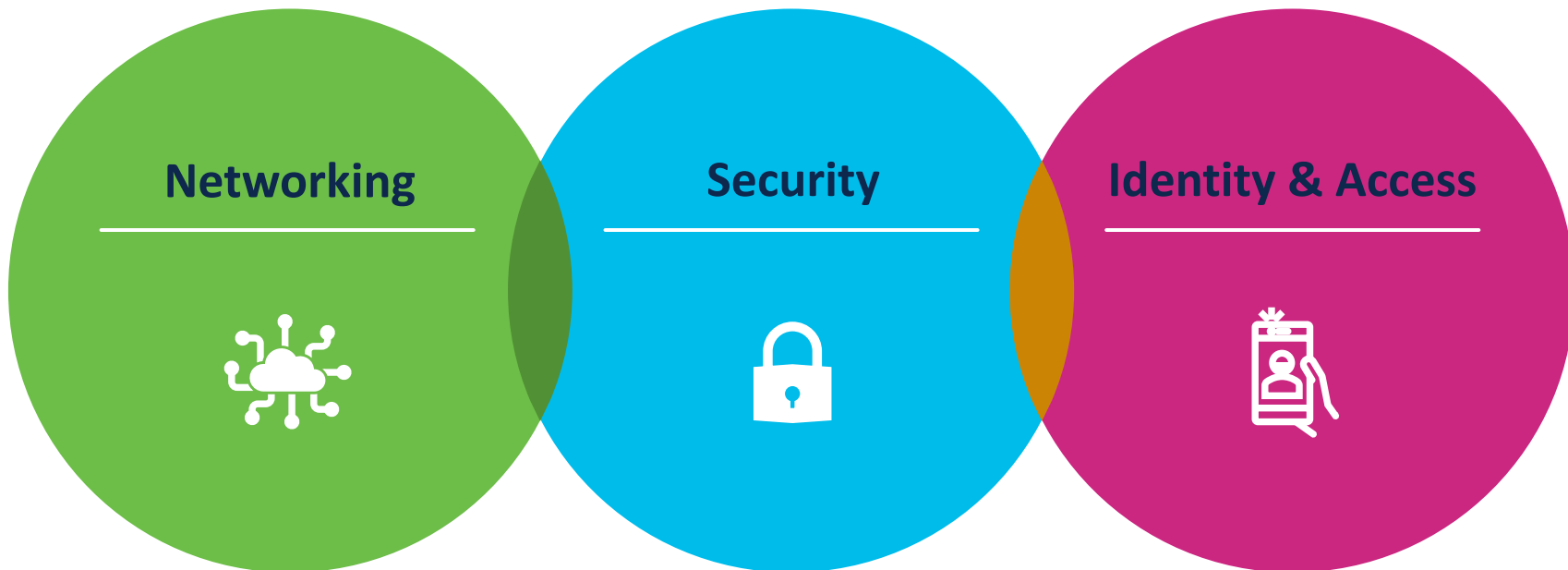
Apps: Hosted in datacenter  
Users: Connected to corporate network to work  
Network: Centralized  
Security: On-premises security stack



Apps: More hosted in the cloud  
Users: More work done off-network  
Network: De-centralized  
Security: Gaps in protection

# SASE in three pillars






Securely connect any user to any application with the best user experience



# SASE SD-WAN

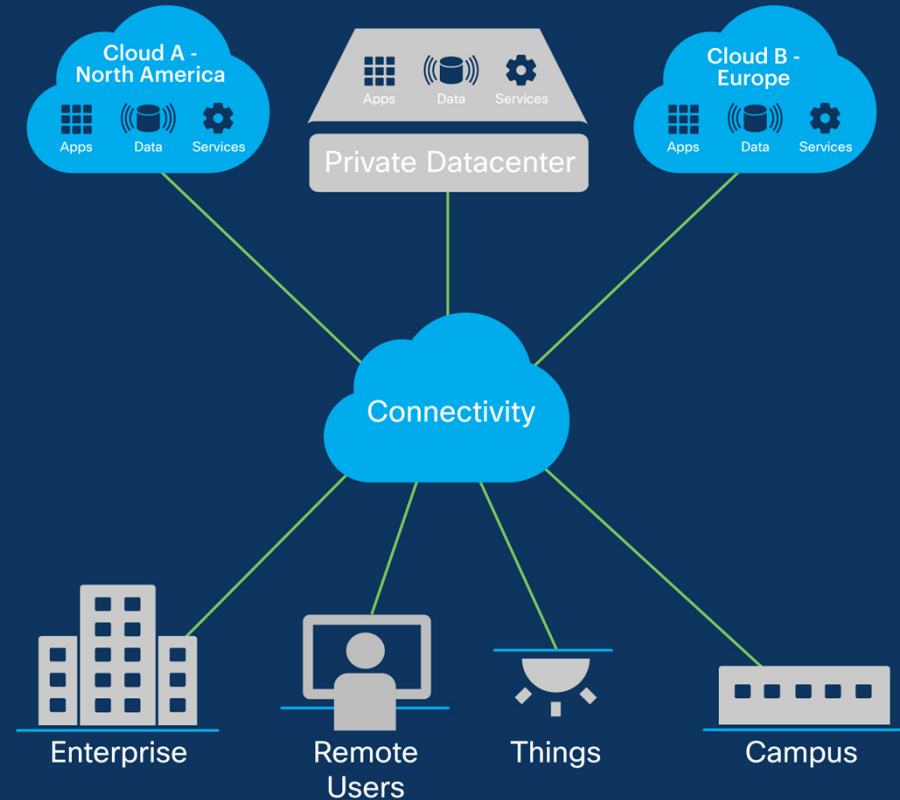


## Secure SD-WAN: Simple and versatile

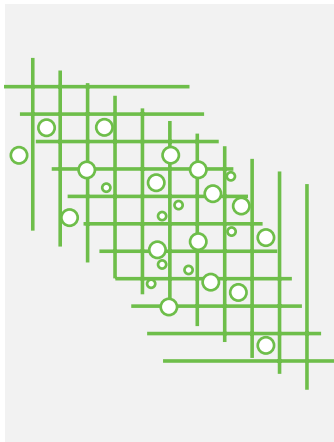
 Automation and Cloud-Based Orchestration 	 Dynamic Performance Routing 	 Analytics, SaaS Telemetry, Smart Thresholds 	 Integrated Security & Macro/Micro Segmentation 	 Middle Mile Optimization 	 Cloud On-Ramp & Multi-Cloud Access 
Zero touch onboarding and provisioning	Predictable app performance and user experience	Proactive network assurance and network operations	Integrated security and network policy controls	Flexible and programmable cloud interconnect options	Single pane of glass cloud networking orchestration

# The Solution

- ▶ Centralize services in the cloud
- ▶ Connect users, apps & data, anywhere
- ▶ Enforce consistent security



# How to SASE



## Inventory

Take a stock check of all vendors and applications, do you know them all?



## Current Strategy

How do you currently connect, observe, and secure/control your branch edges, remote users, and applications?



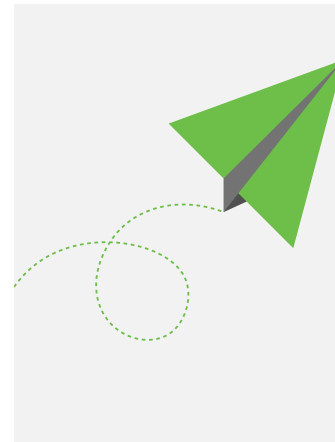
## How do your security and network teams work together

New hires, role changes, is everyone communicating effectively?



## Challenges you have or anticipate having

Remote workers, BYOD, upcoming refreshes in your current architecture?

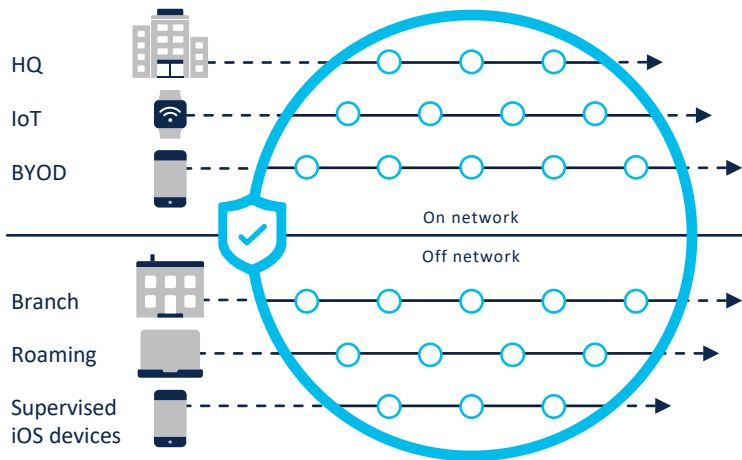


## Solution

Now we can work on a solution to best fit YOUR needs.

# DNS security

- Visibility and protection for all activity, anywhere



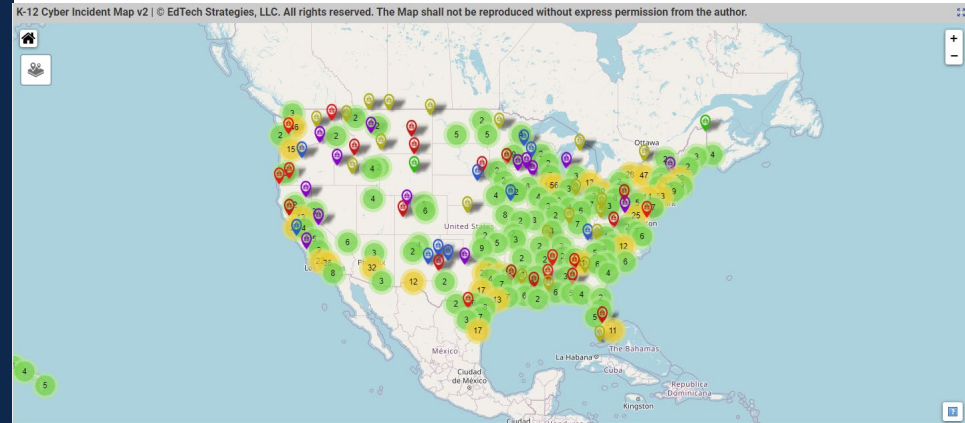
- All office locations
- Any device on your network
- Roaming laptops
- Mobile devices - IOS and Android
- Every port and protocol

# SASE Use Cases

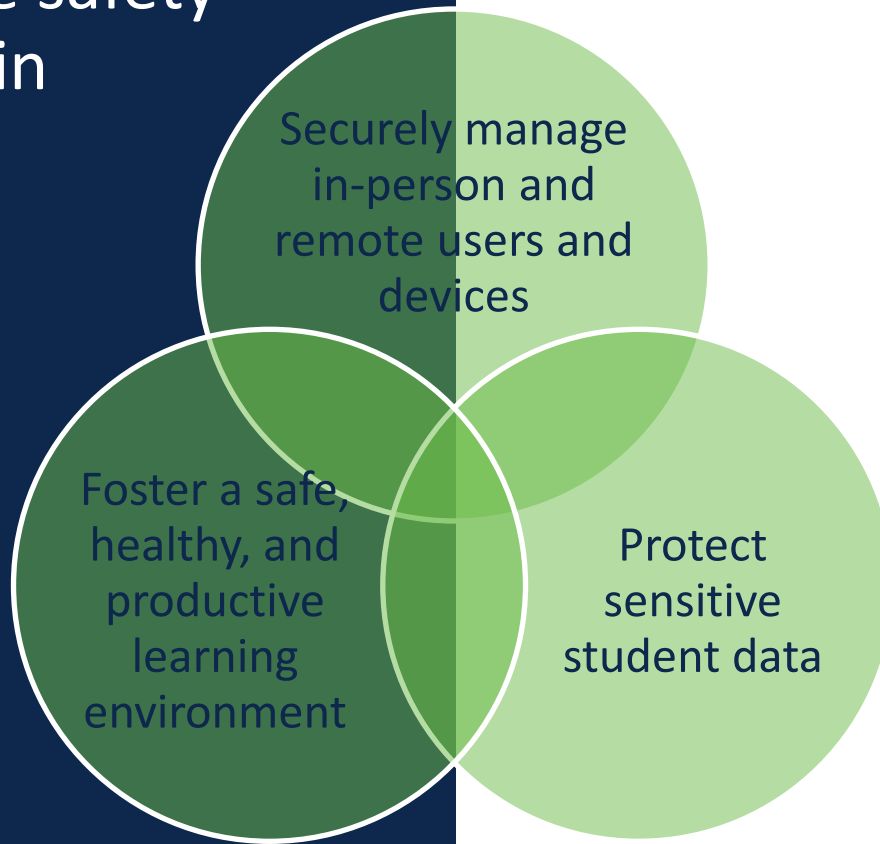
**Molly McGuire**  
Security Sales Manager  
Cisco Systems

# K-12

- In our new world of virtual learning and cloud applications, it's not enough to hand out logins and passwords, considering that 81% of breaches come from stolen credentials.



# Why facilitate safety and security in education?



# Secure remote worker

Lyft deployed Duo and was immediately able to consolidate several projects, such as multi-factor authentication (MFA) and mobile device management (MDM), which reduced their overall total cost of ownership by more than 50 percent



Lyft has a diverse mix of user devices, including MacBooks, Chromebooks, Windows and Linux machines. Some are actively managed by IT, while others are users' personal devices not managed by IT. Device visibility and its security posture was a big gap.



# Security Transformation: University of the District of Columbia

**Mike Rogers**

Executive Director,  
Information Services and Management  
University of the District of Columbia



# Security Transformation: University of the District of Columbia



## University of the District of Columbia Overview

- Established by Abolitionist Myrtilla Miner in 1851
- Only Public University in the Nation's Capital
- Committed to a Mission of Education, Research, and Community Service

## Where We Started Our Security Journey

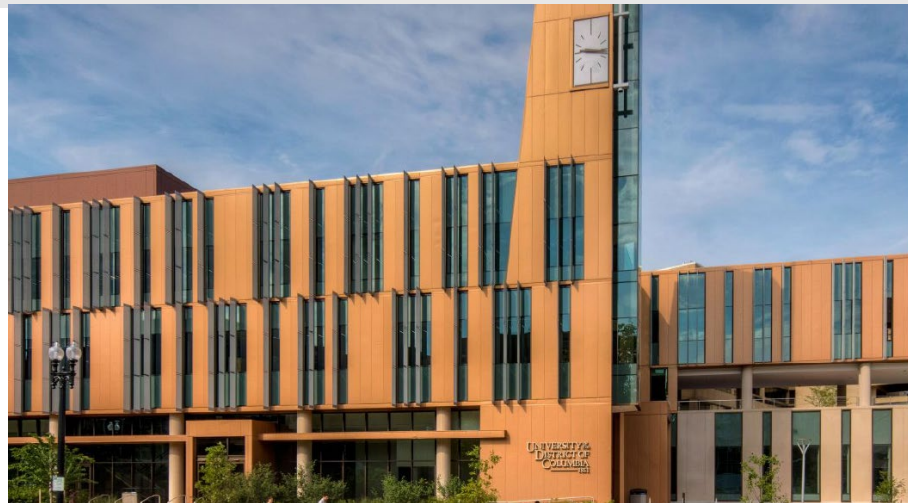
- “Flat” Network – Little to no separation of network users / devices
- No Threat Inspection – Unable to see / address bad actors
- No Identity – Unable to determine who / what is on the network

## Where We Are Today On Our Security Journey

- Macro and Micro Segmentation
- Threats Mitigated at Multiple Layers (IPS / Malware / DNS)
- End-to-End Visibility of Who and What is on the Network

## What's Left On Our Security Journey

- Utilize Segmentation to Further Restrict Access
- Endpoint Security Management
- Multi-Factor Authentication
- Automation – Turn the data to quick action



## Advice:

- Triage Weak Points
- Get Data First
- Intelligence and Response Come Next
- Make It Easy on Your Users
- Inform, But Don't Spam
- Prevent “Hurdles”

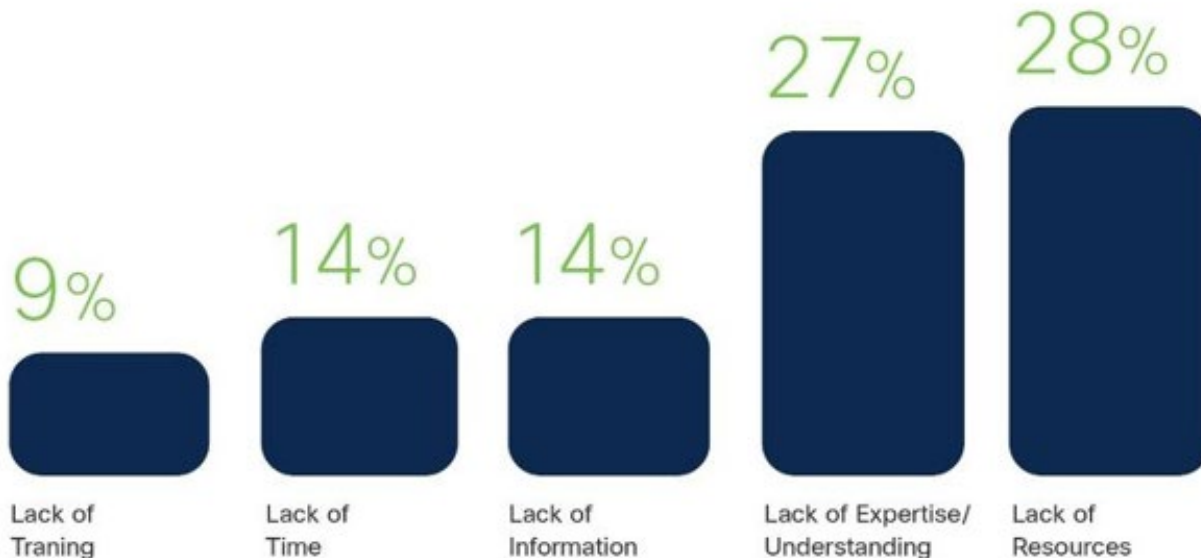


# SASE Trends

**Molly McGuire**  
Security Sales Manager  
Cisco Systems



# Common Challenges for IT teams



81%

of small businesses don't have a dedicated IT person.<sup>9</sup>

46%

of organizations find it difficult to find and recruit qualified security personnel.<sup>5</sup>

# Connecting users to applications

---

Users are dispersed — home, branch, and more

82% of workers will work in a hybrid model after 2020

---

Connecting in different ways

93% of enterprises embrace multi-cloud

---

Applications are everywhere

60% organizations expect majority of a



# Cybercrime as a Service



**90%**

of malware use DNS in attacks

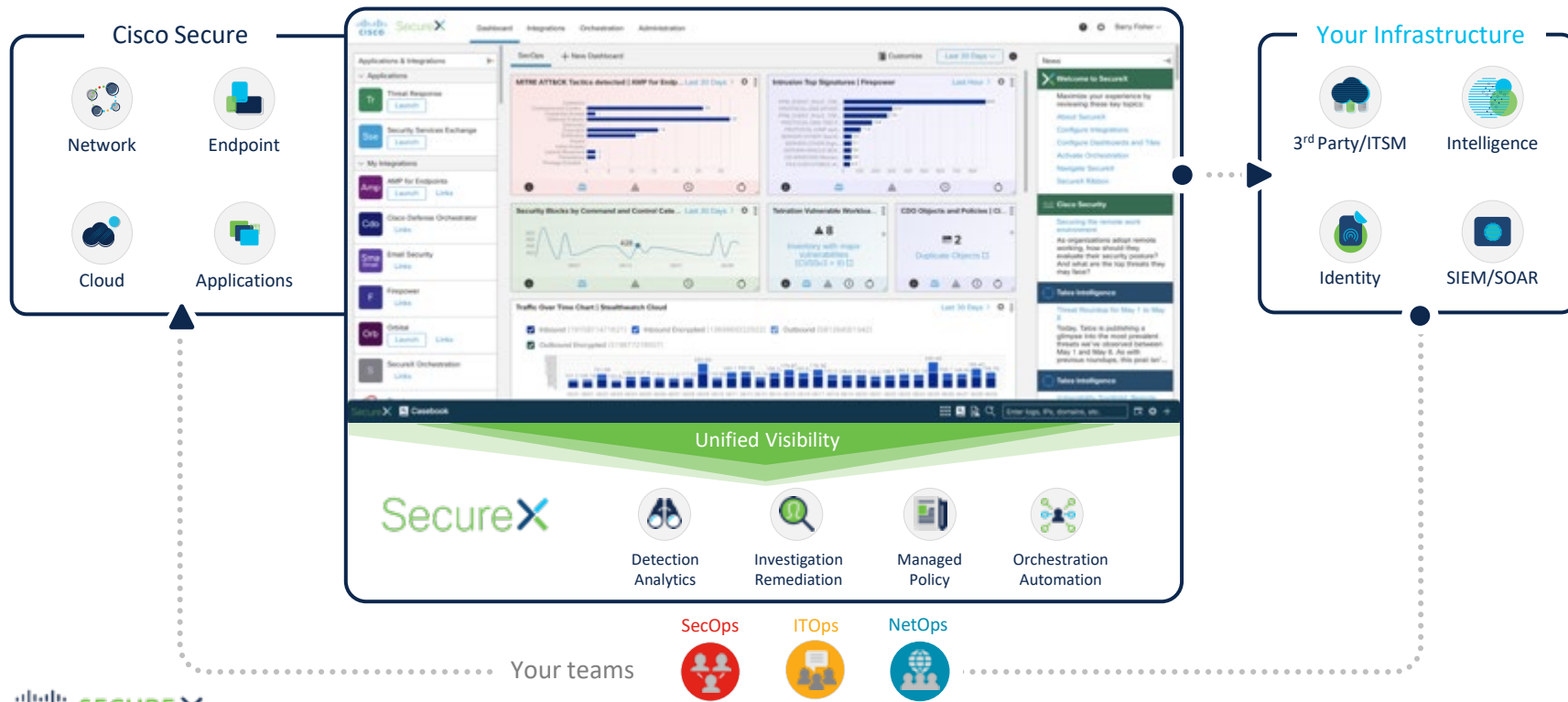
**68%**

organizations don't monitor their DNS



# Introducing SecureX

A *cloud-native*, *built-in platform* experience within our portfolio



# SecureX

## EA Starter



Endpoint  
(Cisco AMP for  
Endpoints)



Firewall



Cloud



Email



## Next Three Products

## Bonus



Cloud  
(Cisco  
Umbrella)



Email



Endpoint



Access (Duo)



Traffic  
or Cloud  
Analytics  
(Stealthwatch)



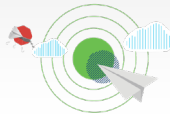
Firewall  
(Cisco  
NGFW)



Cloud



Email



Endpoint



# Final Thoughts

**Questions and Answers**  
(submit via chat)

**Your performance improvement  
is our measure of success.**

**Thank You!**