Antoine Saikaley
Technical Director

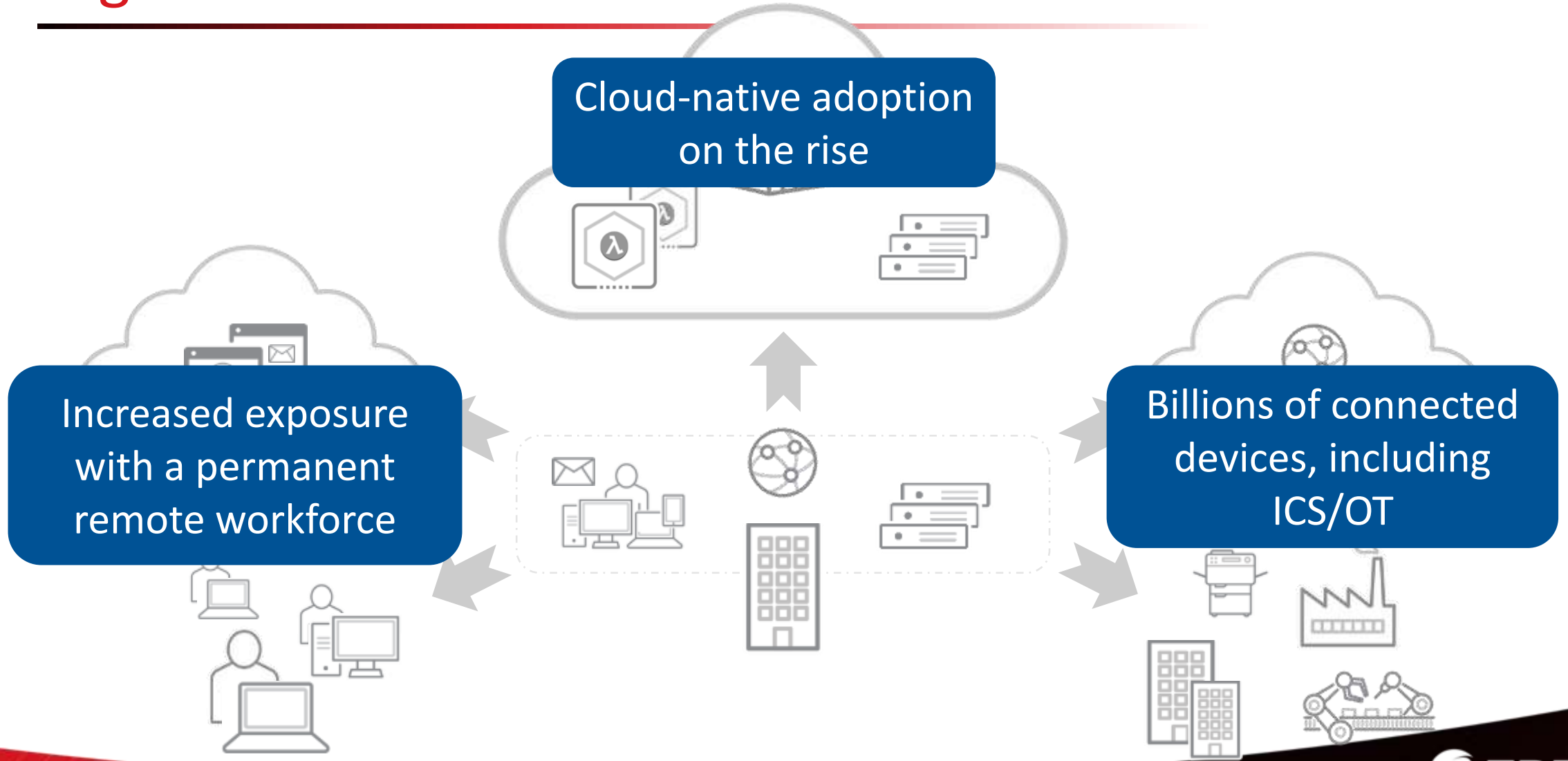
- Oversee the enablement of Trend Micro community members to modernize their cyber security
- 20+ years of diverse IT experience
  - 11 years at Trend Micro
  - Certified Ethical Hacker
- Program Advisor on the Program Advisory Committee to Seneca College
- Simon Fraser University Cloud Security Collaboration

MAPPING THE DIGITAL ATTACK SURFACE

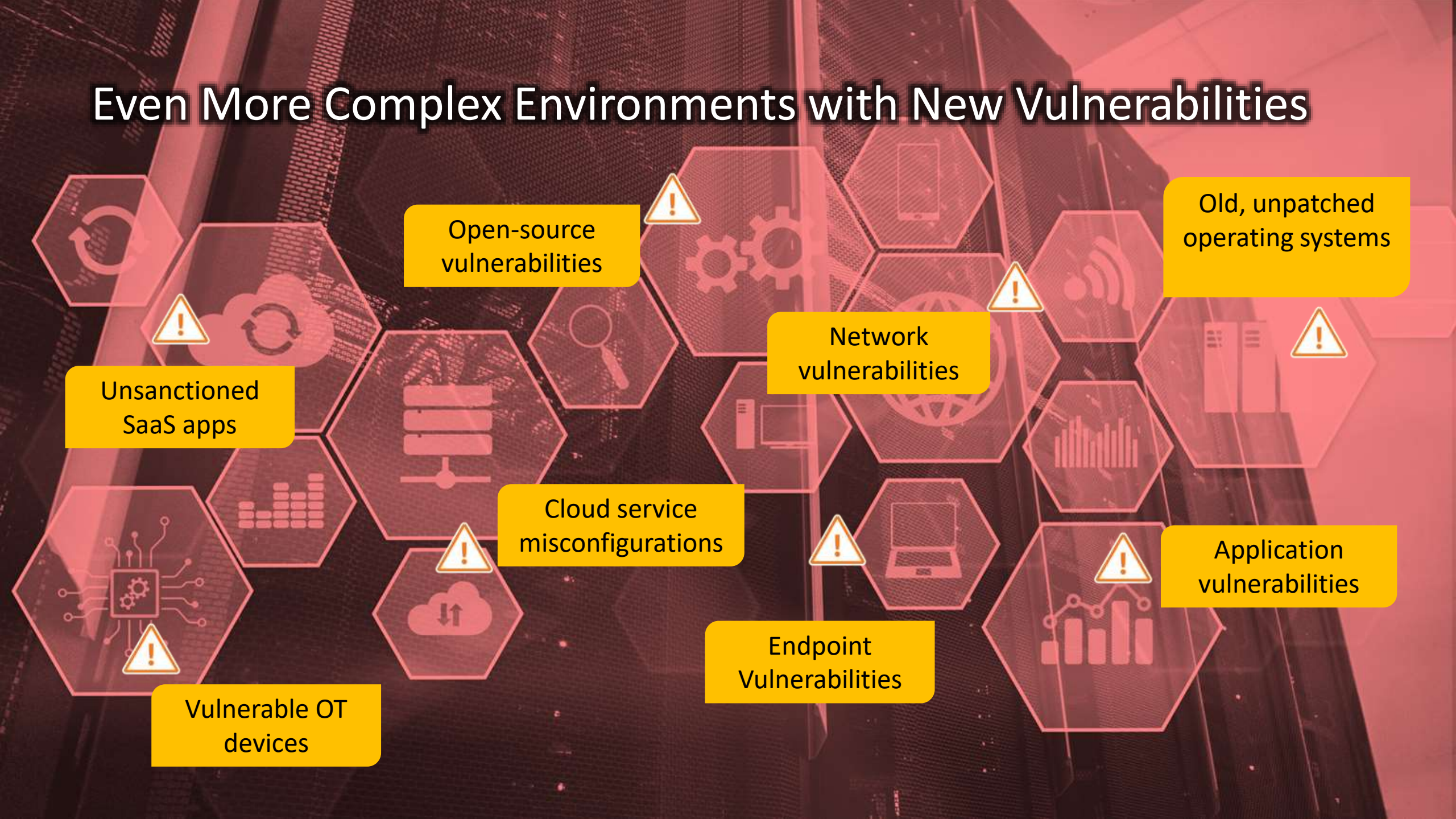
Why organizations are struggling to manage cyber risk and how to build a more risk-aware organization

Antoine Saikaley

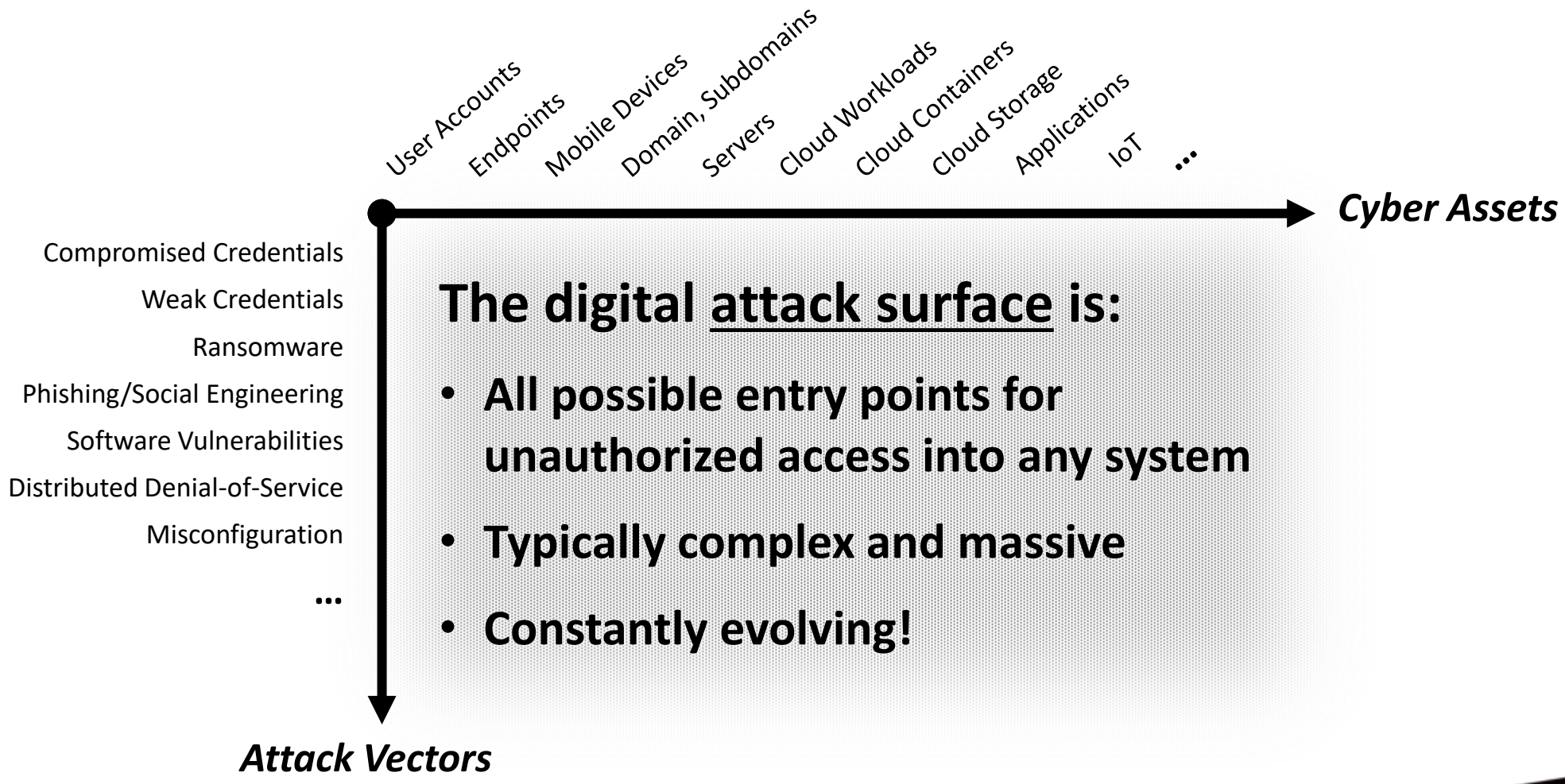
Digital Transformation Continues



Even More Complex Environments with New Vulnerabilities



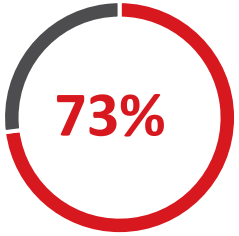
Mapping the Digital Attack Surface – What is it?



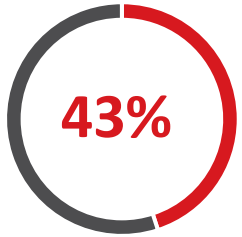
Spiraling Out of Control

Surface states

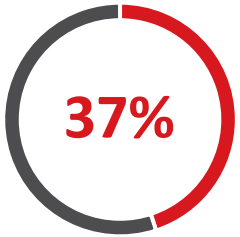
Trend Micro research reveals struggle to control cyber risk against mounting digital attack surfaces.



of global organizations are worried about their growing attack surfaces



admit it is “spiraling out of control”



said it is “constantly evolving and messy

The challenge security teams have:

An attack surface that is expanding out of control

The Visibility Challenge

Low Visibility

62%

said their organizations have blind spots that hamper security

#1 Blind Spot

Cloud assets

#2 Blind Spot

Network assets

#3 Blind Spot

User assets

Key Reasons Why Attack Surface Visibility is so Challenging

Organizations don't have the right tools to gain visibility into all their assets

CISOs and their teams have too many tools, creating information silos

Opaque supply chains

An environment in constant flux: especially in the cloud where assets are dynamic and ephemeral

The sheer size, complexity and distributed nature of modern IT environments

Constant technology innovation, especially from cloud vendors

Business units investing in new products and services without telling IT (shadow IT)

An explosion in remote working endpoints and shadow IT during the pandemic

Why is it so difficult to understand and manage cyber risk?

38% said it is simply hard to quantify

33% they don’t have the resources to do so

32% said that they have limited visibility

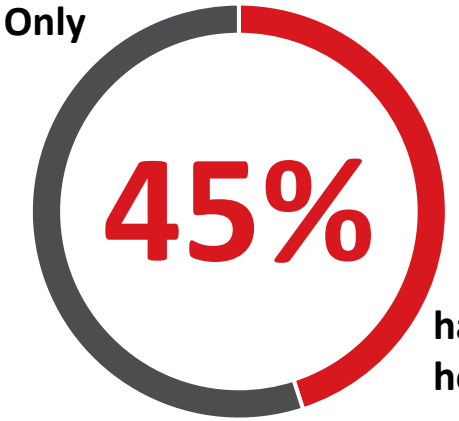
The Problem with Managing Risks

Inadequate assessments

46%

of global organizations believe their method to assess risk exposure is sophisticated

Only

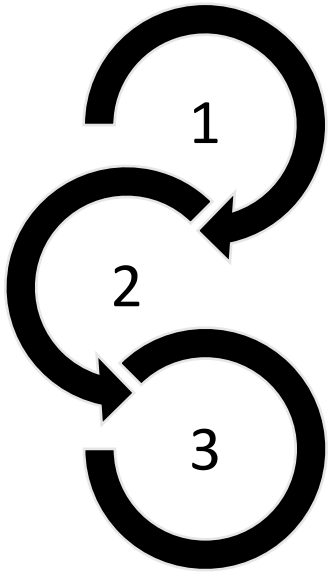


have completely defined how they do so

35%

review/update their exposure on a monthly basis or less

How CISOs Can Build a More Risk-Aware Organization



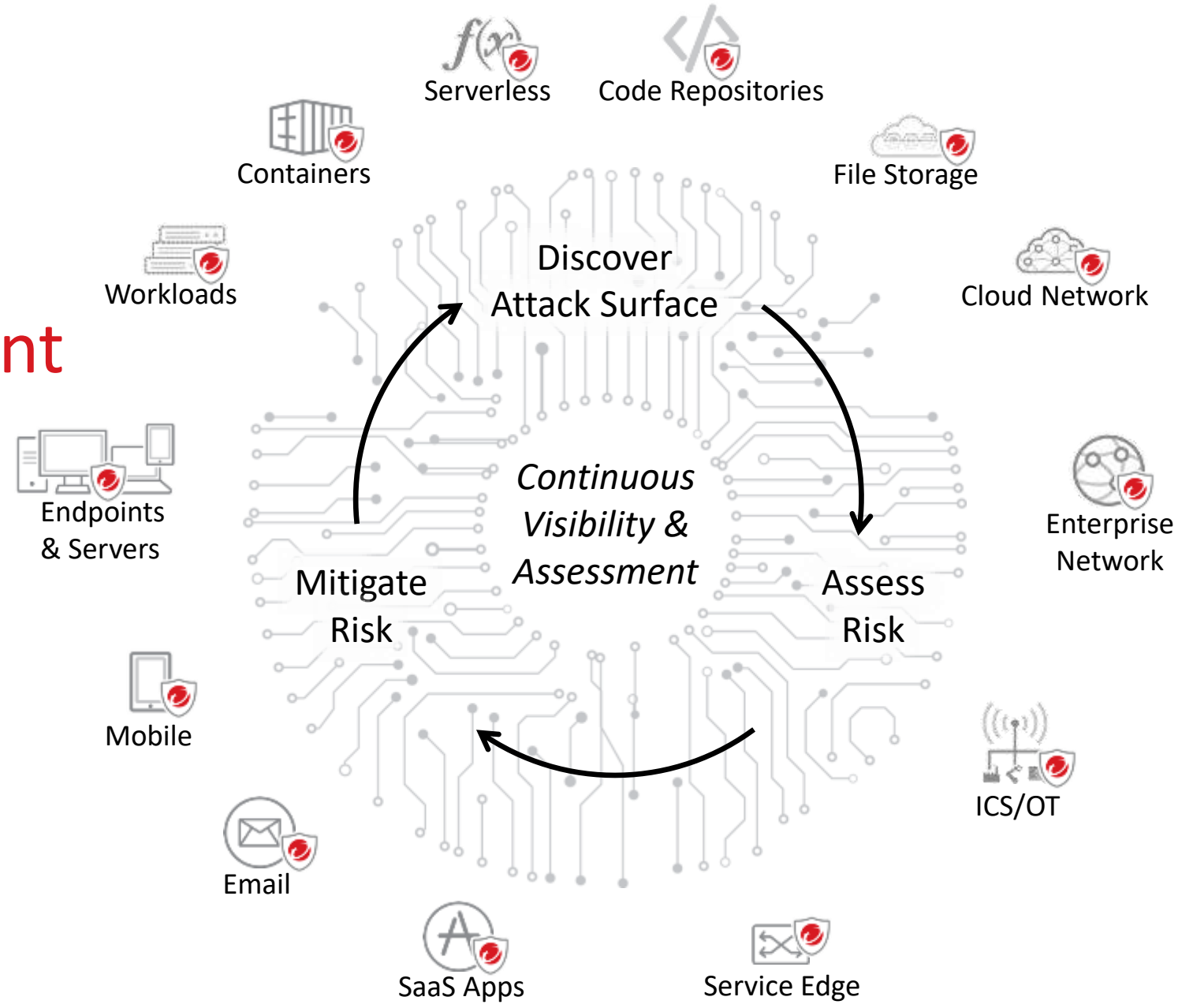
Gain visibility into all assets and attack vectors

Use that data to continuously calculate risk exposure

Invest in the right controls to mitigate those risks

A more risk-aware organization → A platform-based approach

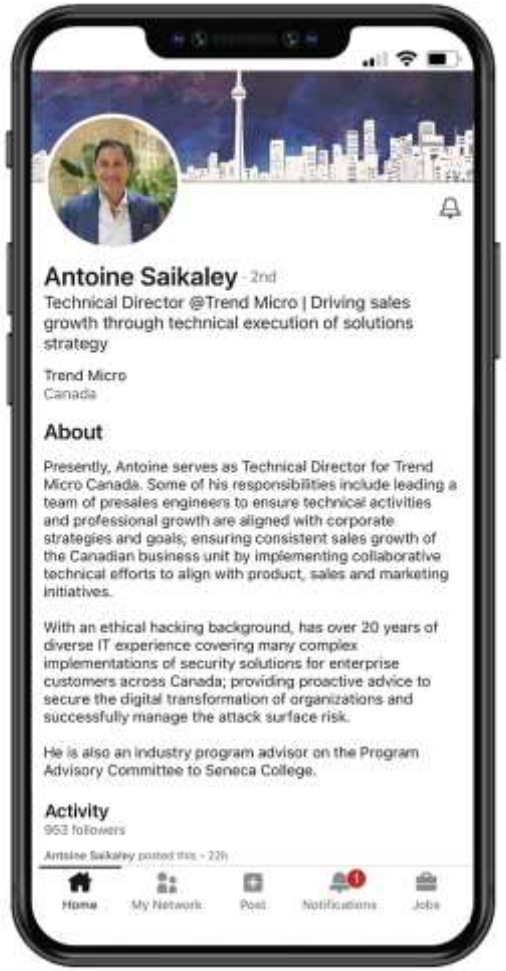
The Attack Surface Risk Management Lifecycle



How CISOs Can Build a More Risk-Aware Organization

01	Formalize cybersecurity	**Formalize cybersecurity** with documentation, KPIs and established metrics. This will help to drive a business risk discussion about cyber.
02	Consider a new role	**Consider a new role** of Business Information Security Officers (BISOs), who can help embed security into business processes and align cyber with business demands for productivity.
03	Restructure reporting lines	**Restructure reporting lines** so that the CISO reports directly into the CEO—this will expose the latter to cybersecurity matters and will help provide more business input for security leaders.
04	Deploy a security platform with XDR/ASM	**Deploy a Sec Ops platform** to correlate and analyze threat data from across the IT environment (endpoints, servers, cloud workloads, networks and email) to provide maximum visibility into threat & risk levels). Alleviates alert overload, increase MTTD/MTTR

Want to continue the conversation about risk?



Add me on LinkedIn!

Antoine Saikaley

647-963-3914

1 Snooker Street

Toronto, ON