Security in the IT and Operational Technology Convergence

Christopher Odutola
Sales Engineer

August 2020

SOPHOS

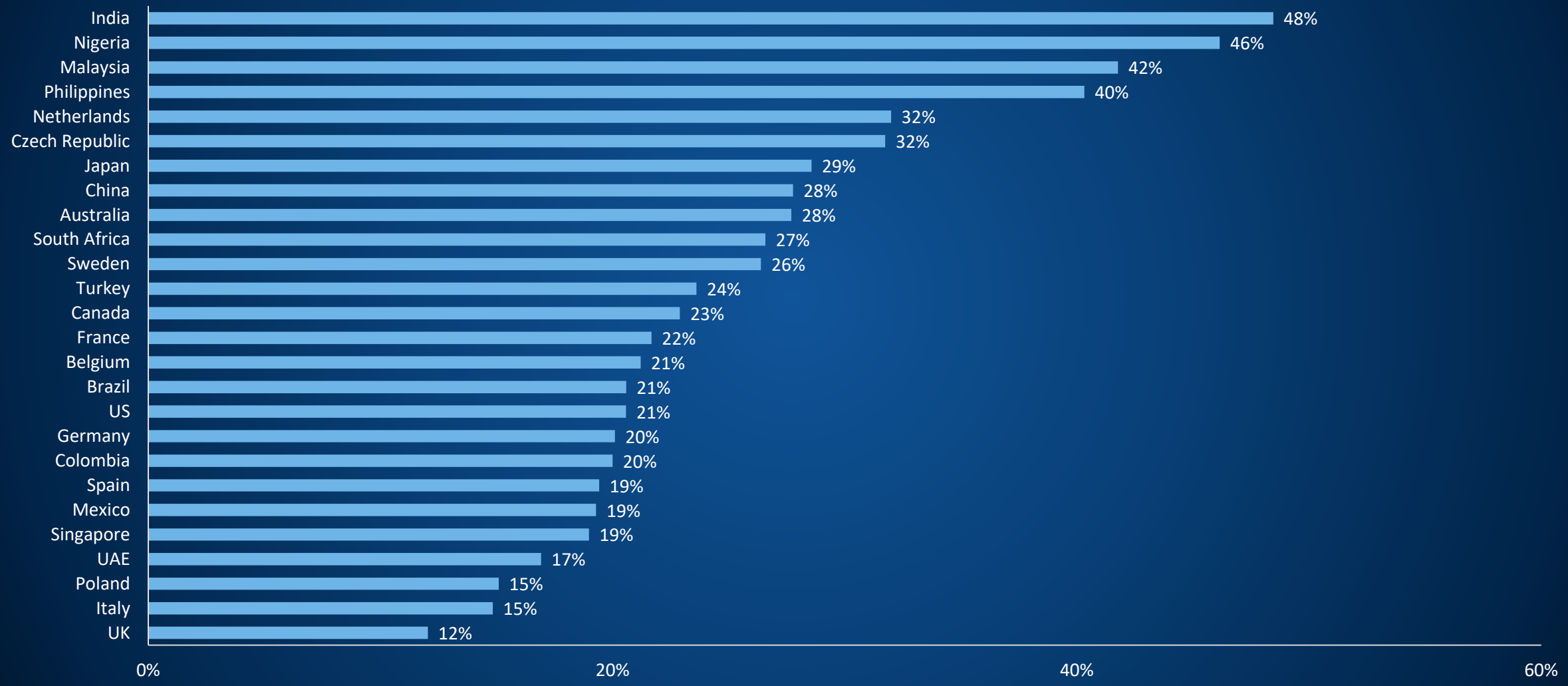
Agenda

- 2019 Review of threats – East Africa
- Overview of IT/OT Convergence
- The Trust factor
- Cybersecurity-as-a-System
- Holistic Cybersecurity Approach
- Conclusion

“There is no technology today that cannot be defeated by social engineering”

Frank Abagnale, security consultant

Percentage of organizations with cloud account credentials stolen in the last year



Has your organization suffered a public cloud security incident in the last 12 months? "Yes, Stolen Credentials".
Base 3,521 respondents

SOPHOS

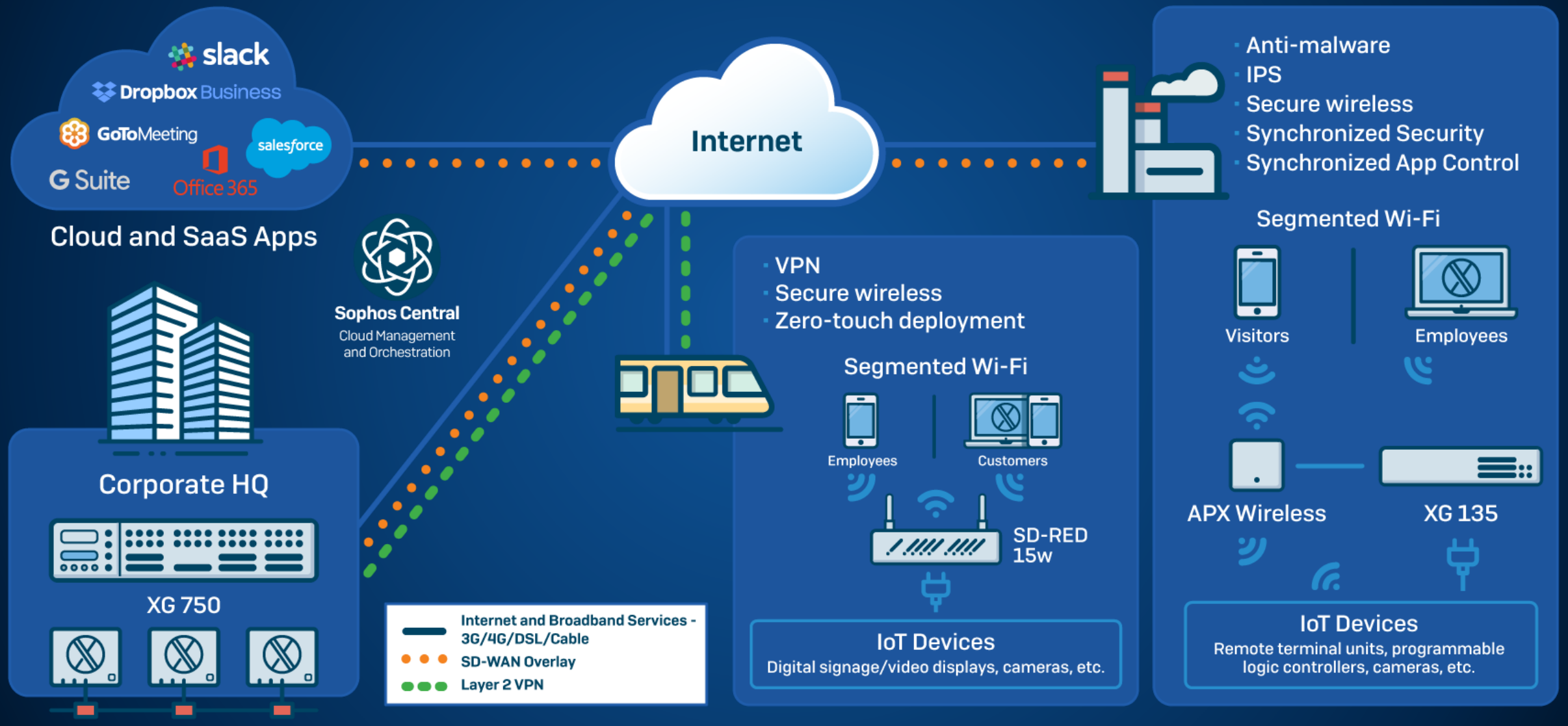
IT/OT Convergence in a nutshell

The integration of information technology (IT) systems with operational technology (OT) systems

IT systems are used for data-centric computing. OT systems enhance manufacturing and industrial operations e.g. SCADA

IT/OT fusion enables more direct control and more complete monitoring, with easier analysis of data, from anywhere in the world

ICSs, Remote Devices & Vehicles



Digital Transformation (DT) - Cybersecurity

Cloud Security is a Shared Responsibility

Security **IN** the Cloud

Host Security	WAF	IPS	VPN	Next-Gen Firewall	Outbound Proxy
Applications and Content					
Network Security	Inventory Configuration	Access Controls	Data Security		

Your Responsibility

Security **OF** the Cloud

Foundational Services

Compute | Network | Storage | Availability Zones

Cloud Provider Responsibility

AWS, Azure, Google

Is SSL Inspection Incredibly Important to IT/OT?

Concerning SSL/TLS Trends and Their Impact

Visibility	Threats	Performance
Google	SOPHOS labs	
80%	**32%**	**96%**
of traffic is Encrypted	Malware and PUA connections are TLS	NOT using SSL Inspection
An Enormous Blind Spot	**Hackers are Exploiting it**	**Organizations are Powerless**

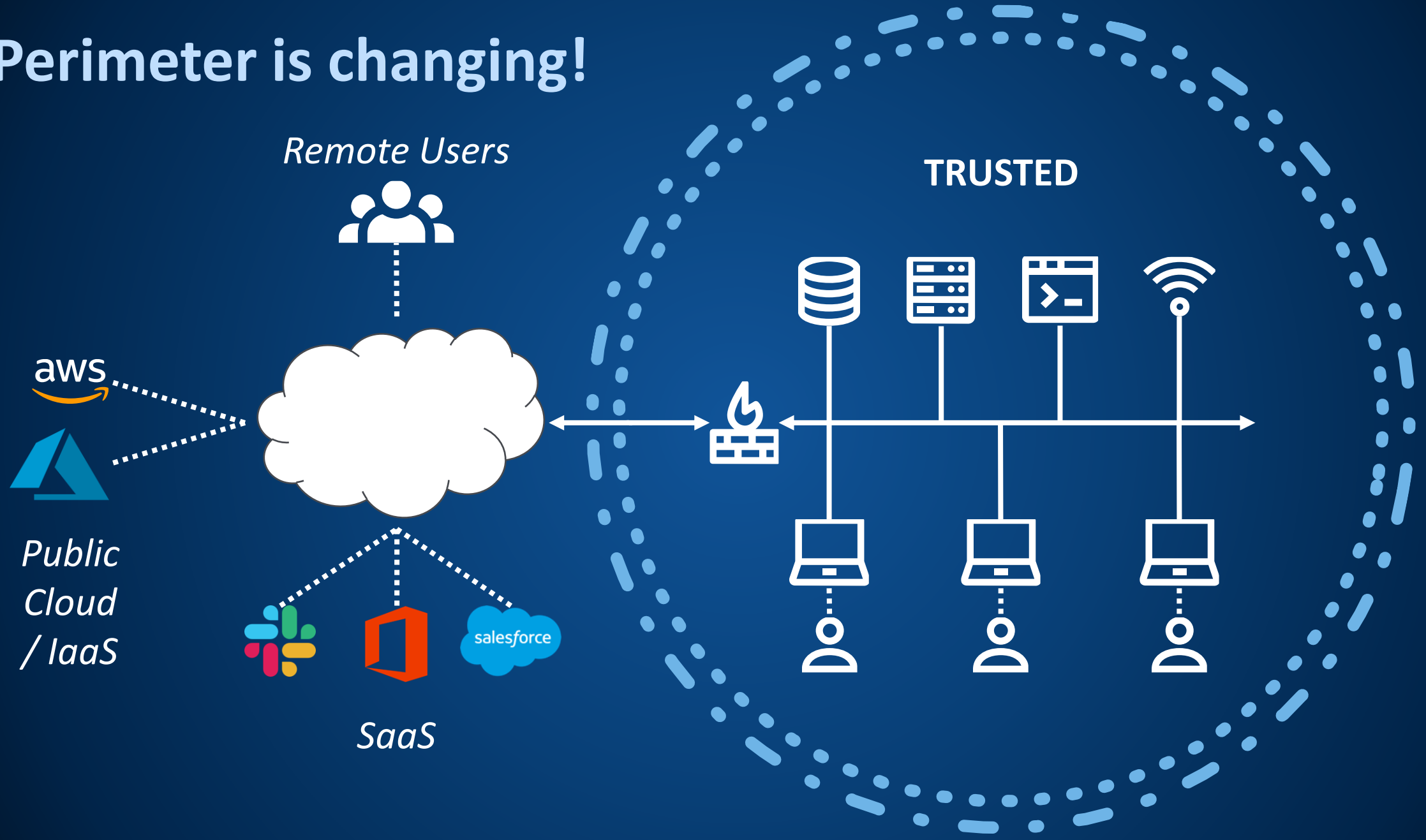
“

Companies need to take a multi-layered approach to data security, from embracing cloud shared security responsibilities and adopting a zero trust model…

”

Frank Dickson, Program VP, Cybersecurity Products at IDC

Perimeter is changing!



Principles of Zero Trust

Trust Nothing, Verify Everything

Always Identify	*Always Control*	*Always Analyze*	*Always Secure*
Secure access to all data and resources by user with MFA	Adopt ***Least Privilege*** model to enforce access control and segment all workflows	Inspect and record all activity and regularly analyze	'Inside Out' cybersecurity focused on data and risk

Cybersecurity as a System – Synchronized Security

ANALYZE

- Discover users, apps, devices, and data – on-prem, and in cloud
- Identify and authenticate in real-time

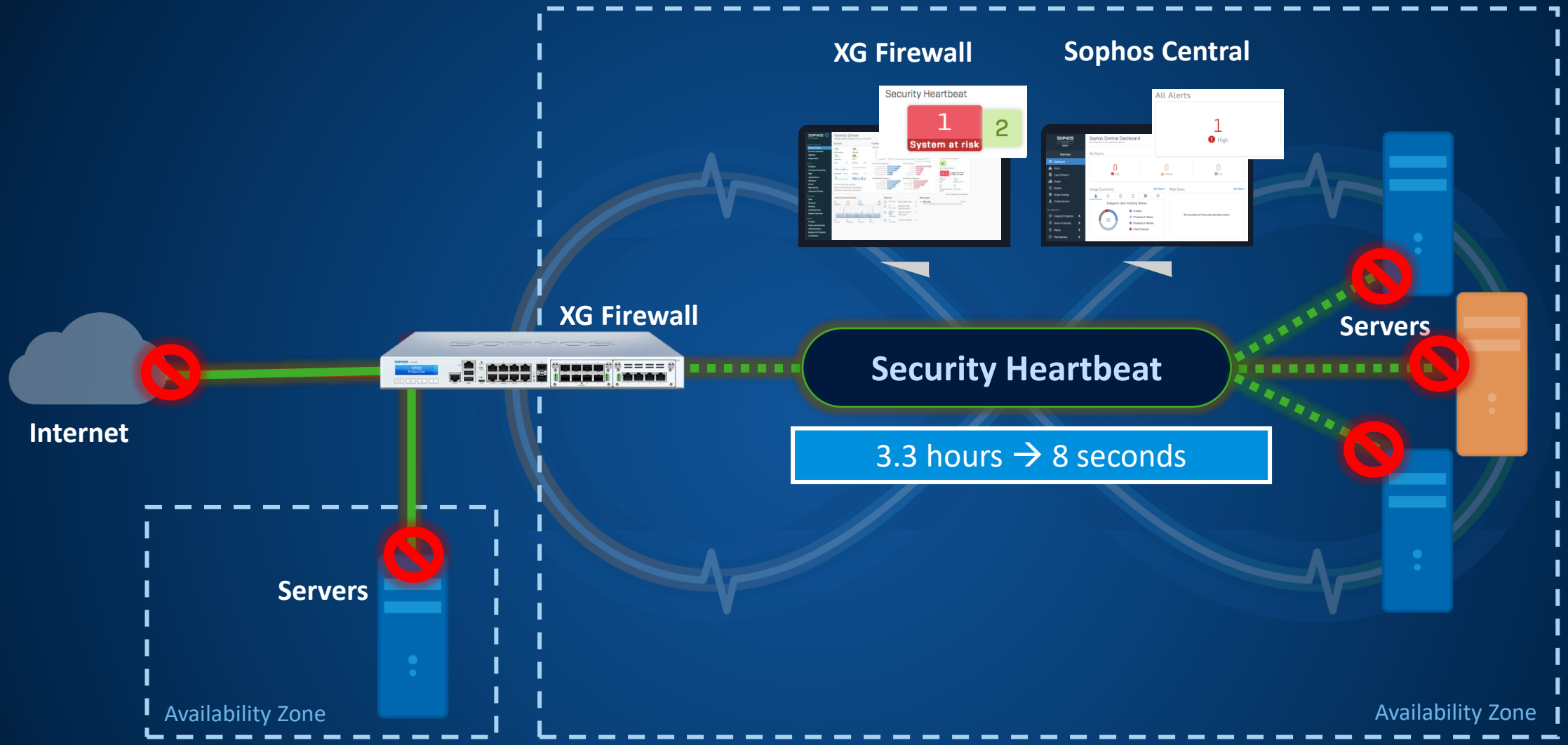
ADAPT

- Dynamic security policies based on threat detection, user behavior, traffic analysis, compliance guidelines

AUTOMATE

- Network and Wi-Fi access control
- Automatic device isolation
- Traffic bandwidth optimization

Automatic Incident Response – Hybrid Cloud Infrastructure



#1 Asset Visibility

#2 Secure DevOps

#3 Continuous Compliance

#4 Close Security Gaps

#5 Visualize Access

SOPHOS

“Embracing change and getting ahead of the curve is the best prescription to be in control of your organization's destiny and avoid being caught off guard.”

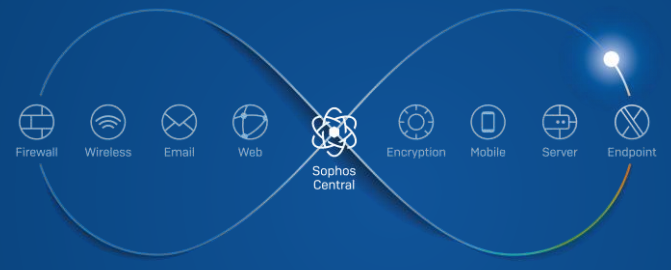
Michael Suby, Research VP, IDC Security and Trust

Holistic Cybersecurity Approach

ZERO TRUST

Cybersecurity Model

Synchronized Security



Cybersecurity System

24/7 Threat Hunting/Response

SOPHOS