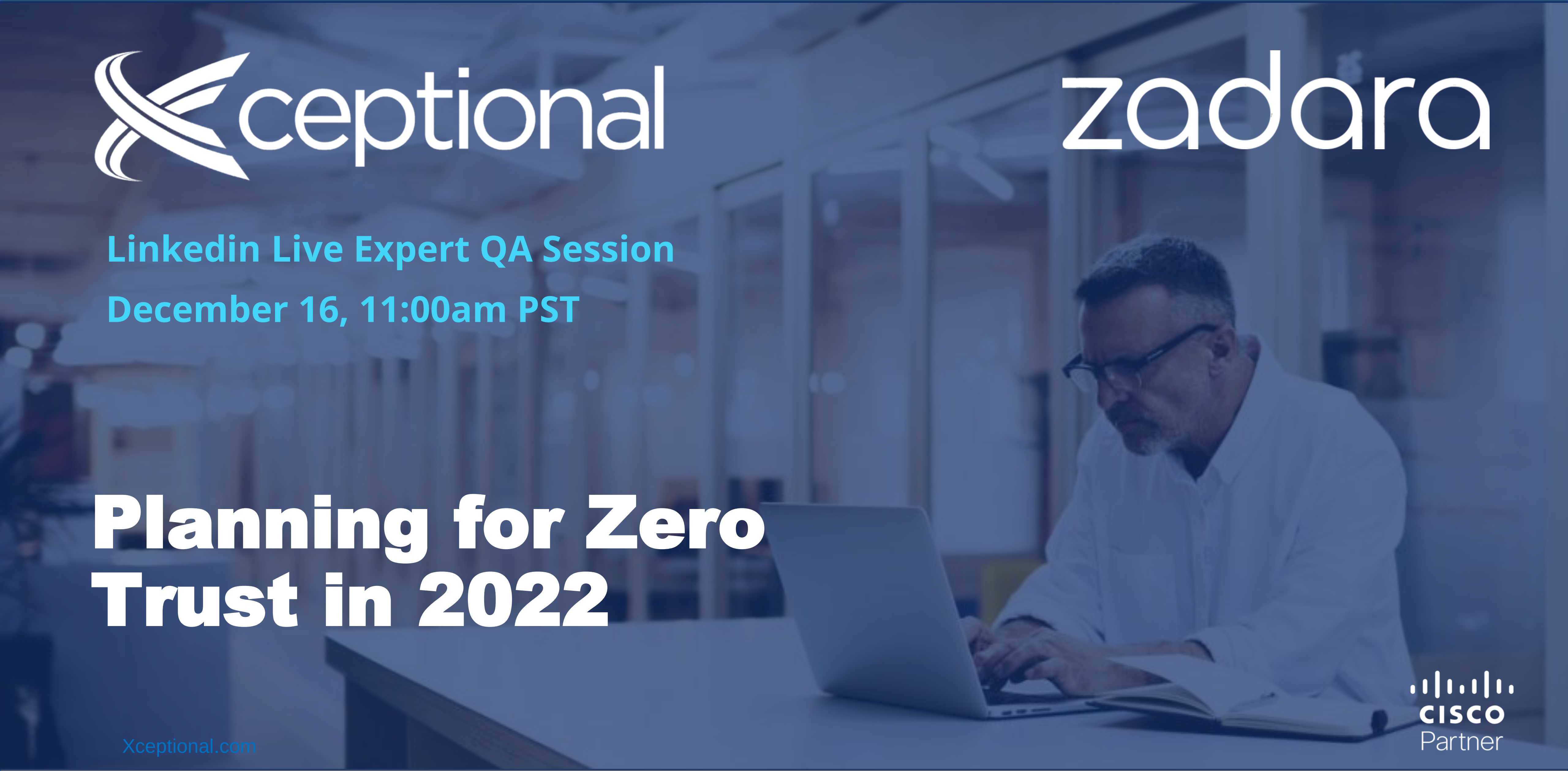
Xceptional

zadara



Linkedin Live Expert QA Session

December 16, 11:00am PST

Planning for Zero Trust in 2022

Xceptional.com

cisco Partner

Session Structure

- Guest Introductions
- Zero Trust Background
- Trends, Current Events
- Zero Trust Readiness
- Planning Best Practices Discussion
- Frameworks, Tools
- Key Takeaways & Wrap Up

Introductions

Xceptional

Host / Mark Dallmeier:

Industry Veteran, Researcher, CSO/CMO for Various Cyber Risk, MSSPs, MSPs.

zadara

Expert / Noam Shendar:

Industry Veteran, Executive VP Global Solution Architecture

DLT®

A TECH DATA COMPANY

Expert / Don Maclean:

Chief Cybersecurity Technologist, Forrester ZTX Strategist

Xceptional

Expert / Chris McKewon

Industry Veteran, Founder & CEO of Xceptional

Zero Trust Background: Why This Matters

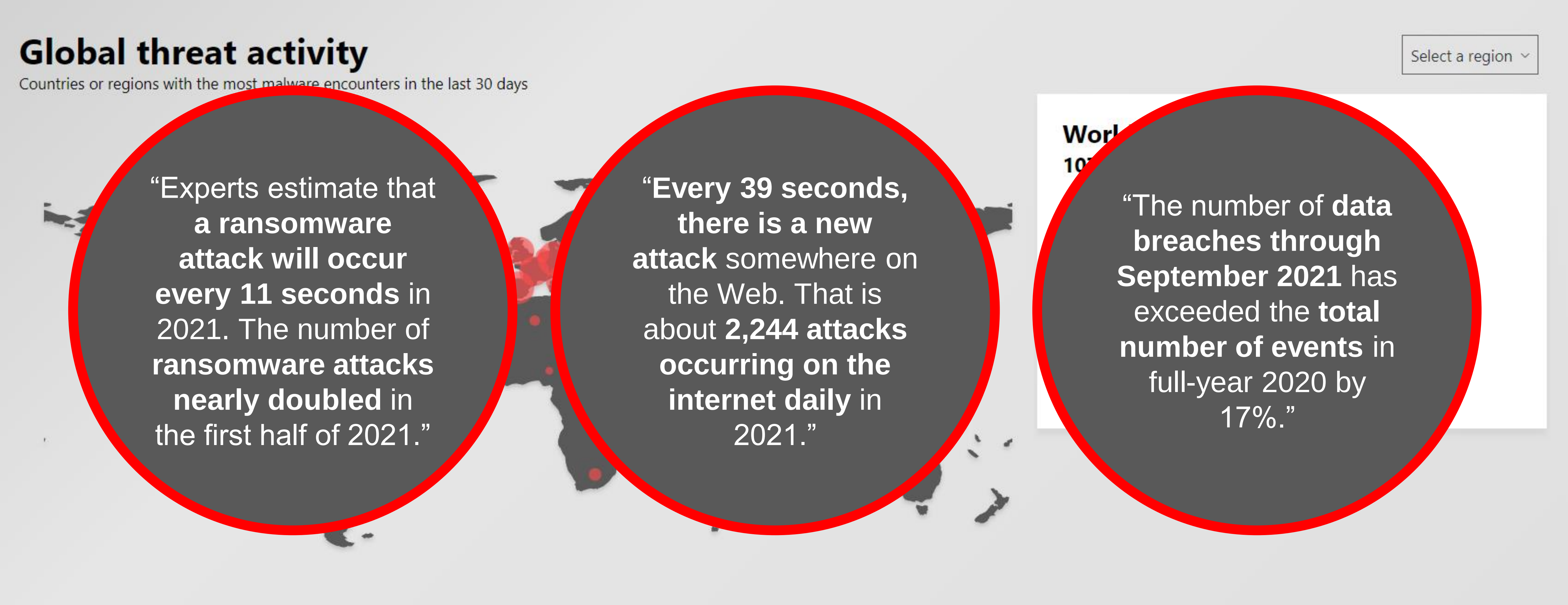
1. **Perimeter-Based Security is Ineffective in the Evolving Enterprise**
2. **Cloud Data Centers Require Shared Security Responsibility**
3. **Third-Party SaaS and PaaS Applications Can't Be Trusted Blindly**
4. **The Internet Network is an Unsecured Network**
5. **Everyone in the Expanding Workforce Shouldn't Have All-Access**
6. **You Cannot Verify the Security Status of All WFH Environments**
7. **BYOD is Not as Secure as Work Devices**
8. **Cyberattacks Are Increasing**
9. **Advanced Persistent Threats (APTs) Are Becoming More Sophisticated**
10. **The Security Stakes Are Higher**

> **"The future of cybersecurity is here, right now. And it is the zero trust security model. The perimeter-based, reactive methods that acted as the foundation of old, traditional security need to become relics of the past. Businesses and governments must be proactive and adopt zero trust now to confidently provide a cyber-secure future to their customers, partners, employees, and citizens."**
>
> *- Satyam Tyagi, Senior Director of Product Management, ColorTokens*

https://colortokens.com/blog/why-enterprises-need-zero-trust-security/#:~:text=%20The%20Top%2010%20Reasons%20Why%20Enterprises%20Need,PaaS%20Applications%20Can%E2%80%99t%20Be%20Trusted%20Blindly.%20More%20

Cybersecurity Trends: Growing Tsunami of Attacks

- Microsoft, National Security Institute, Security Magazine 2021



Global threat activity

Countries or regions with the most malware encounters in the last 30 days

“Experts estimate that **a ransomware attack will occur every 11 seconds** in 2021. The number of **ransomware attacks nearly doubled** in the first half of 2021.”

“**Every 39 seconds, there is a new attack** somewhere on the Web. That is about **2,244 attacks occurring on the internet daily** in 2021.”

“The number of **data breaches through September 2021** has exceeded the **total number of events** in full-year 2020 by 17%.”

“There were 1,767 reported breaches in the first six months of 2021, exposing a total of 18.8 billion records. Some industries have experienced 200% - 3000% growth in cyber incidents over the last 36 months.”

https://www.microsoft.com/en-us/wdsi/threats

What Is Zero Trust – Don & Noam

Don:

- A mindset change
- A holistic approach to security
- A means to an end

Noam:

- Making as few assumptions as practical about limitation of access (like a house, there are many ways in)

Problems that Zero Trust Solves

- Disappearing perimeter – no more “moat and castle”
- Growing attack surface
- Inevitable intrusions
- Long dwell times/Lateral movement
  - Bad actors stick around
  - They’ll find everything eventually

What Is Zero Trust – Chris & Mark

Chris:

- A hill that every organization must climb
- Flips the script from access/user centric to security centric
- Identification, Classification and protection of data/information
- An approach that needs proper continual care and feeding

Mark:

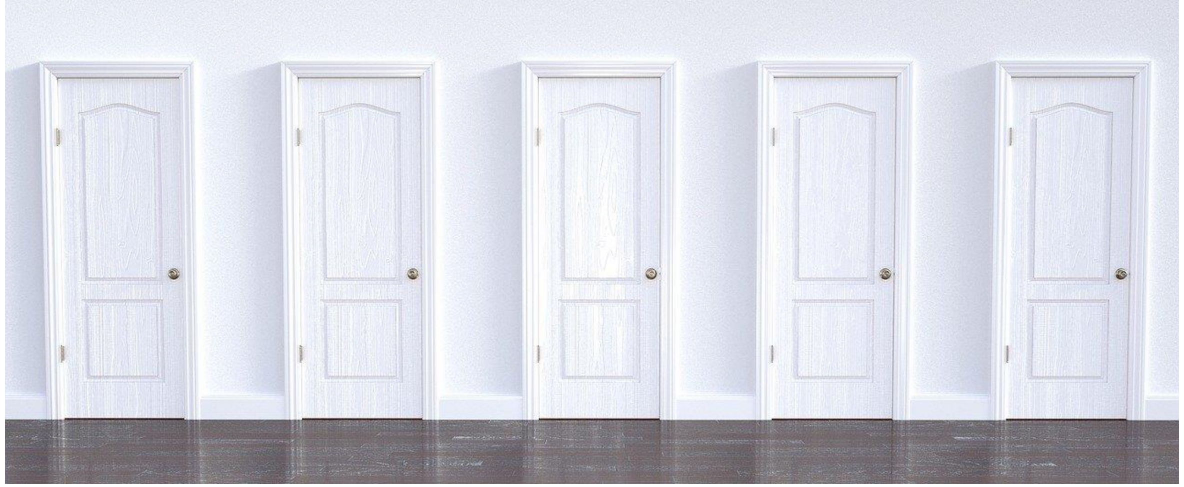
- An opportunity to proactively remove risk from the business
- A giant leap forward in terms of improving cyber hygiene and addressing privacy and compliance requirements

Drivers for Cloud & Zero Trust

Xceptional

BUSINESS SITUATION	IT USE CASES	CYBERSECURITY & COMPLIANCE REALITIES
Growth, geographic expansion resiliency.	**Repatriation** Migrating Data between, Clouds, DCs and Co-Los	**Hybrid and distributed** workforce. **BYOD, home office networks**, shared office networks. **BEC, Phishing, Ransomware**, Data Privacy, **CCPA, NY Reg, Other State, Fed, Industry Regulations**.
Control or contain spending.	**CAPEX → OPEX at the Edge** How do we model Compute & Storage as a Service	**Visibility into risk, cyber and compliance costs**. Consistency of IT services, network-application-data access. **0 IT system and application downtime, disruption**. **No fines, revenue loss** due to lack of regulatory compliance.
Enhance employee and customer engagement, employee productivity.	**Edge & Latency** Needing cloud services closer to the source of data	**Automated, consistent, secured access to IT systems, applications, and data** – when they need it. **Expect data privacy, protection**, monitoring is in place.
Rapid response to market demands and needs.	**Utilize Local partnerships,** Knowledge and Infrastructure for Production, DR & Backup.	**Need a trusted workforce, trusted workplace, and trusted workloads** to enable resiliency, flexibility, and to ensure business continuity.
Architect IT systems and services to support business goals, objectives.	**Technology Refresh** Needing to keep IT resources current at a reduced costs	**Need to address technical debt, remove vulnerable systems** and proactively reduce risks while architecting for the future. **Need to address growing cyber threats** and risks.

Re-Architecting IT for Zero Trust



Traditional Approach:

- Fortify and armor the front door

There's One Problem:

- Once you're in, the place is yours

Zero-Trust Approach:

- Many doors, reasonable security

Advantage:

- Breach a door, the rest are locked

Examples of Zero Trust at Zadara

Segregation of Networks:

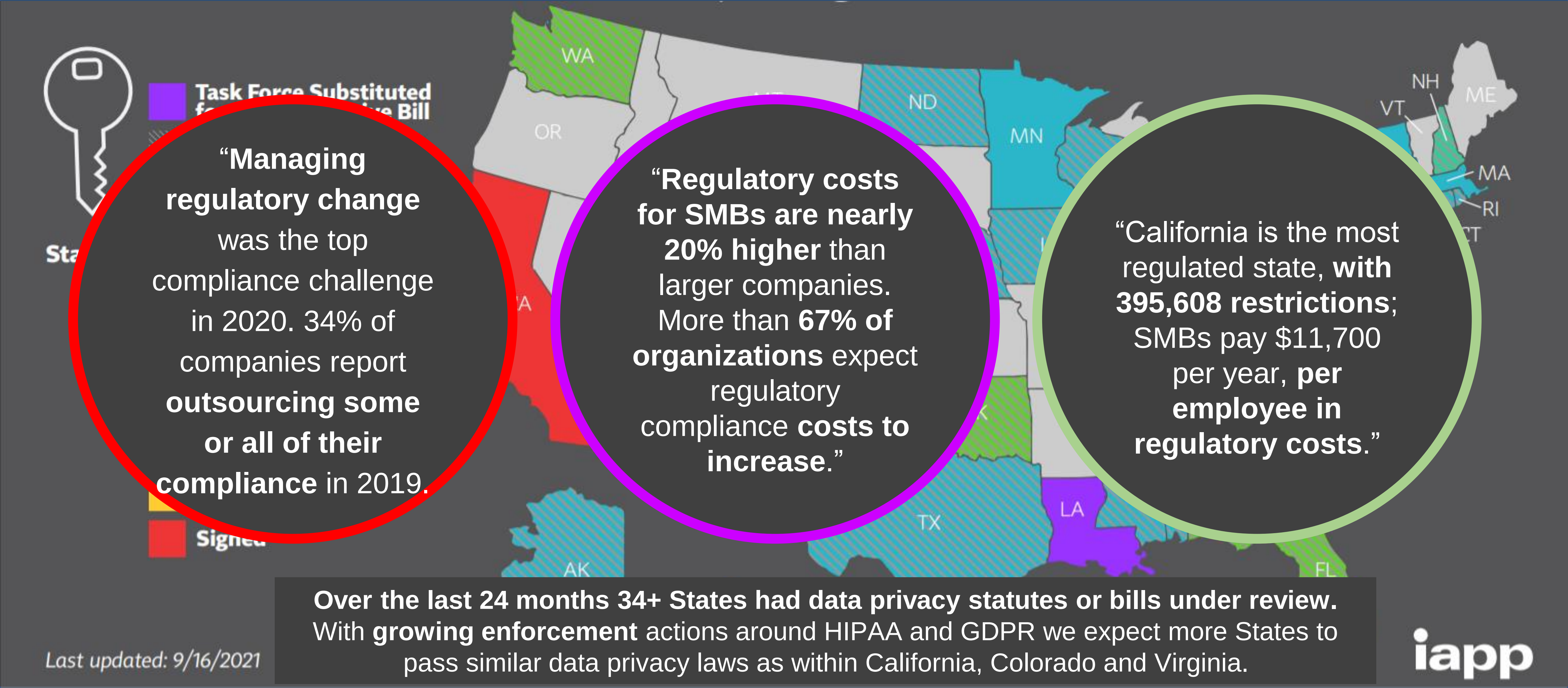
- There is no one big Zadara cloud; rather, Zadara comprises 100s of clouds that authenticate separately
- Even within a cloud Zadara has a separate VLAN for each tenant and a separate a VPC for each compute client
- Each tenant instance and each management/monitoring instance keep its own RBAC system and users/groups

Segregation of Software:

- Zadara uses about 50 different SaaS systems, with no SSO or central directory. Each application requires its own authentication and authorization

Compliance Drivers: Growing Costs, Laws, Regulations

- iapp, Thomson Reuters 2021



“**Managing regulatory change** was the top compliance challenge in 2020. 34% of companies report **outsourcing some or all of their compliance** in 2019.

“**Regulatory costs for SMBs are nearly 20% higher** than larger companies. More than **67% of organizations** expect regulatory compliance **costs to increase**.”

“California is the most regulated state, **with 395,608 restrictions**; SMBs pay $11,700 per year, **per employee in regulatory costs**.”

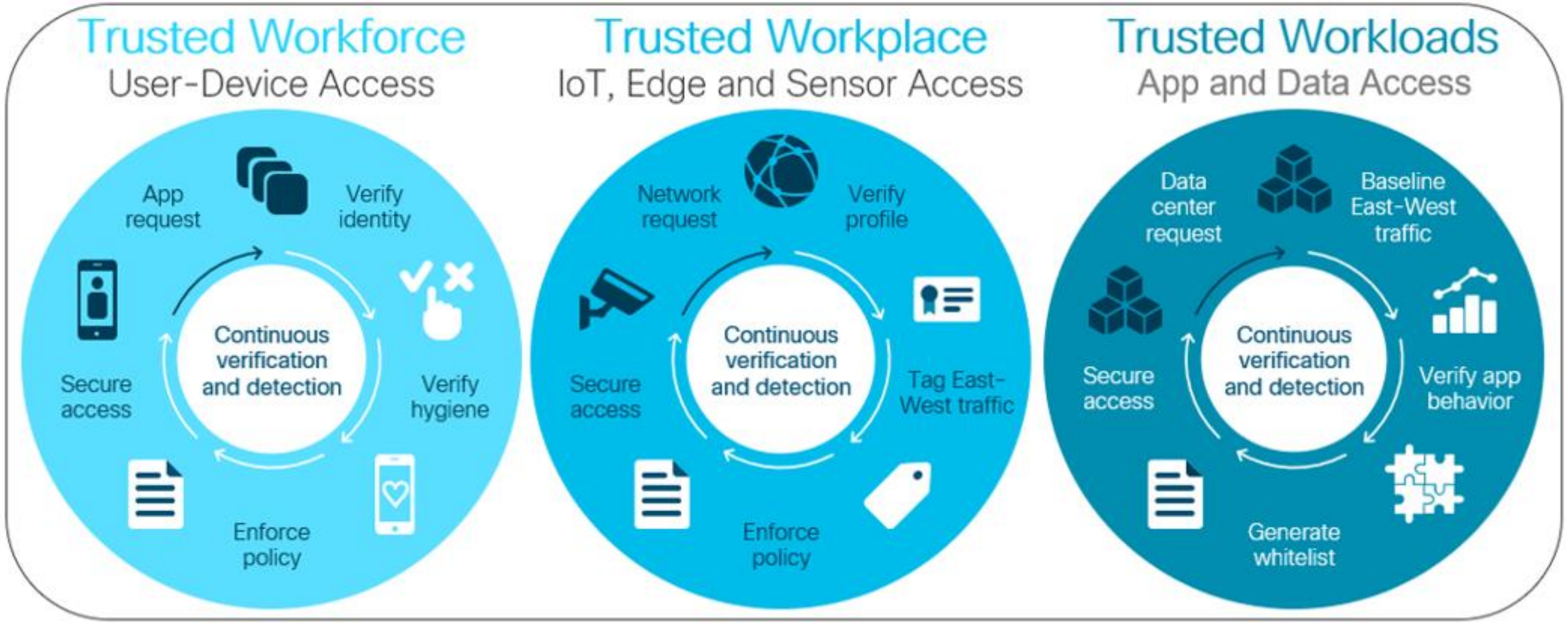
Last updated: 9/16/2021

Over the last 24 months 34+ States had data privacy statutes or bills under review. With **growing enforcement** actions around HIPAA and GDPR we expect more States to pass similar data privacy laws as within California, Colorado and Virginia.

https://www.uschamberfoundation.org/smallbizregs/
https://corporate.thomsonreuters.com/Cost-of-Compliance-2020
https://www.reginfo.gov/public/
https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Zero Trust Readiness (Cisco)

- **Do you have a Trusted Workforce (User and Device) Access process?** Does it drive users to connect to devices and applications securely? Can you verify the user, the security hygiene, and enforce security and access policies dynamically?
- **Do you have a Trusted Workplace (IoT, Edge and Sensor) Access process?** Does it drive users to connect to networks securely? Can you verify the profile, tag the east-west service, and enforce security and access policies dynamically?
- **Do you have a Trusted Workloads (Apps and Data) Access process?** Does it drive users to connect to data centers and applications securely? Can you track east-west traffic, verify application behavior, and generate and enforce a whitelist dynamically?



Panel Discussion & QA

How Should Orgs Approach Zero Trust Pre-Planning?

How Can Orgs Accelerate Readiness?

What Are Best Practices for Zero Trust Planning?

Approach?

How are other organizations approaching Zero Trust Planning and what are the key frameworks being used and activities being driven?

Prep?

Are there approaches or methods that are being used by other companies to accelerate Zero Trust readiness?

Implementation?

How can organizations accelerate through the implementation phase and reduce the risk, cost associated with deploying a Zero Trust model?

Zero Trust Frameworks, Resources

- **NIST SP 800-207:**

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

- **Department of Defense Zero Trust Architecture:**

https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf#

- **NSA Zero Trust Architecture**

https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

- **National Cybersecurity Center of Excellence:**

https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

- **Zero Trust NIST Architecture Blogs:**

https://blogs.cisco.com/security/an-overview-of-zero-trust-architecture-according-to-nist

https://blogs.cisco.com/government/zero-trust-cybersecurity-for-government-part-one

- **Cisco Zero Trust Fundamentals and Pillars:**

https://duo.com/assets/ebooks/zero-trust-going-beyond-the-perimeter.pdf

- **Cisco Zero Trust Framework:**

https://www.cisco.com/c/en/us/products/security/zero-trust.html

Takeaways, Wrap Up

Xceptional

Host / Mark Dallmeier:

Industry Veteran, Researcher, CSO/CMO for Various Cyber Risk, MSSPs, MSPs.

zadara

Expert / Noam Shendar:

Industry Veteran, Executive VP Global Solution Architecture

DLT

A TECH DATA COMPANY

Expert / Don Maclean:

Chief Cybersecurity Technologist, Forrester ZTX Strategist

Xceptional

Expert / Chris McKewon

Industry Veteran, Founder & CEO of Xceptional

Comments, Key Takeaways: Noam, Don

Noam:

- Zero-trust starts with people
- When doing asset discovery/inventory include the cloud
- Many solid doors are better than 1 heavy door

Don:

- People are critical to success
- Leverage all frameworks
- Its about being secure; not Zero-Trust compliant

Takeaways & Wrap Up: Chris & Mark

Chris:

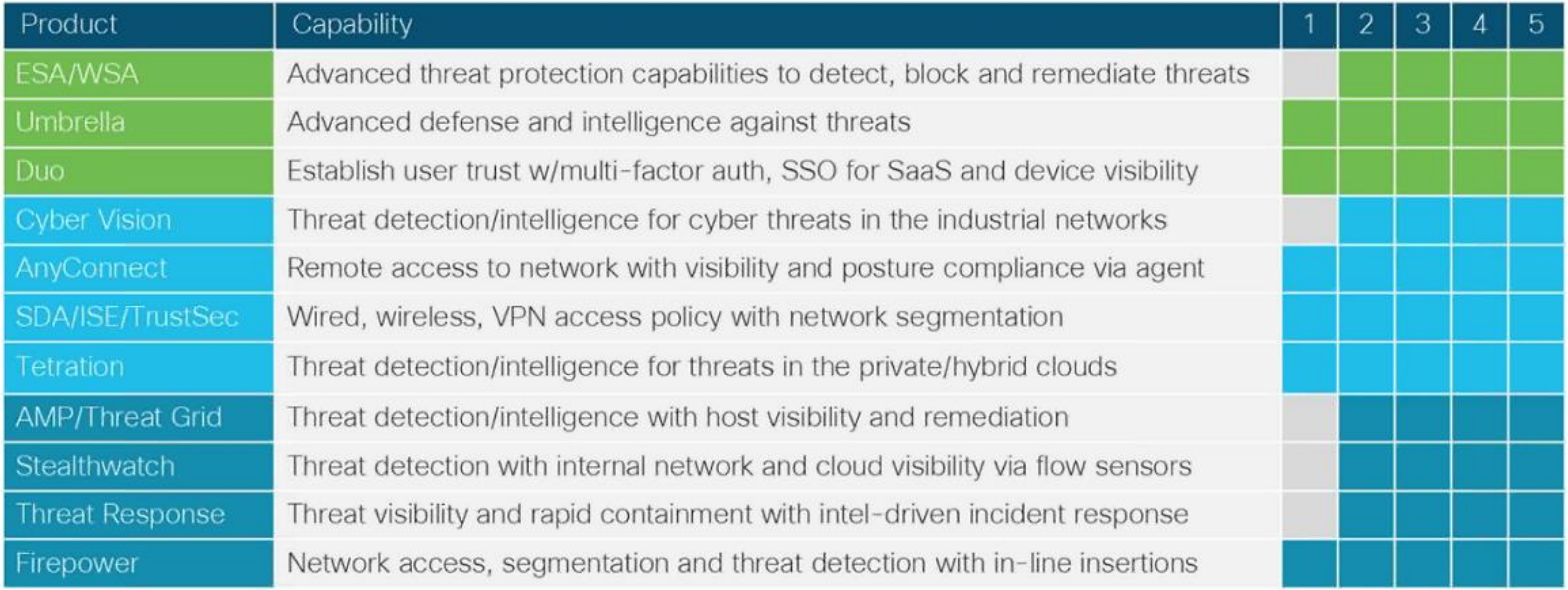
- Communicate, communicate, and then communicate some more
- Don't forget training, end users, administrators and security officers/CISOs
- Automate compliance to the highest extent possible
- Avoid the propensity to use too many tools or create confusion or noise

Mark:

- Leverage industry experts, manufacturers, 3rd party solution providers to accelerate planning and deployment

Cisco Zero-Trust Technology Portfolio

Enabling Basic to Advanced Cyber Hygiene (Supports industry regulations)



		Basic	Intermediate	Good	Proactive	Advanced
Product	Capability	1	2	3	4	5
ESA/WSA	Advanced threat protection capabilities to detect, block and remediate threats		🟩	🟩	🟩	🟩
Umbrella	Advanced defense and intelligence against threats	🟩	🟩	🟩	🟩	🟩
Duo	Establish user trust w/multi-factor auth, SSO for SaaS and device visibility	🟩	🟩	🟩	🟩	🟩
Cyber Vision	Threat detection/intelligence for cyber threats in the industrial networks		🟦	🟦	🟦	🟦
AnyConnect	Remote access to network with visibility and posture compliance via agent	🟦	🟦	🟦	🟦	🟦
SDA/ISE/TrustSec	Wired, wireless, VPN access policy with network segmentation	🟦	🟦	🟦	🟦	🟦
Tetration	Threat detection/intelligence for threats in the private/hybrid clouds	🟦	🟦	🟦	🟦	🟦
AMP/Threat Grid	Threat detection/intelligence with host visibility and remediation		🟦	🟦	🟦	🟦
Stealthwatch	Threat detection with internal network and cloud visibility via flow sensors		🟦	🟦	🟦	🟦
Threat Response	Threat visibility and rapid containment with intel-driven incident response		🟦	🟦	🟦	🟦
Firepower	Network access, segmentation and threat detection with in-line insertions	🟦	🟦	🟦	🟦	🟦

Cisco Zero-Trust Thought Leader

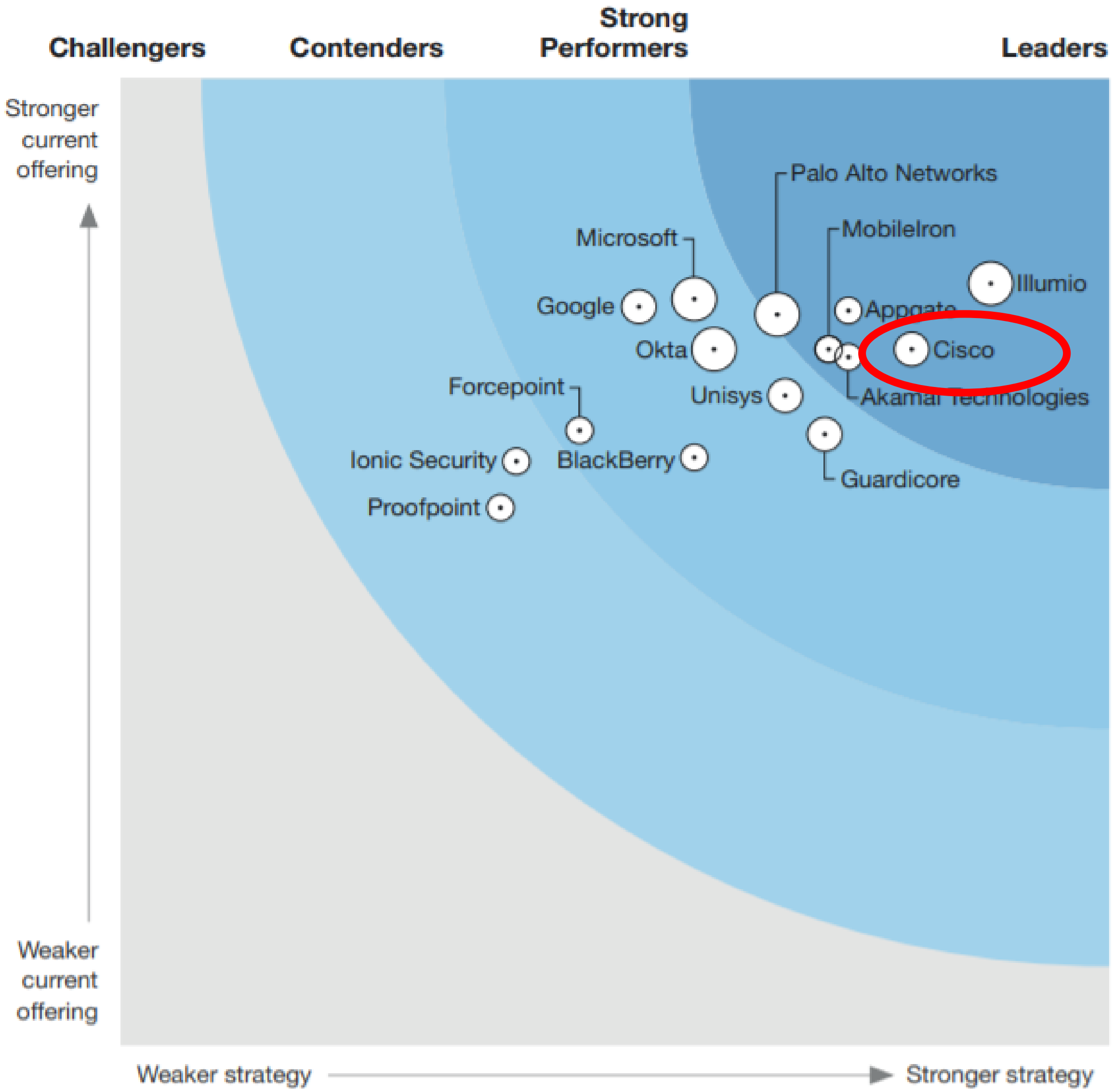
Forrester Wave Report 2020

https://reprints2.forrester.com/#/assets/2/154/RES157494/report

"Cisco pushes the Zero Trust envelope the right way."

"The Duo Security offering has been fully integrated into the Zero Trust-focused Cisco Zero Trust portfolio approach for the Workforce, Workplace, and Workload (WWW). *While the past performance of its firewalls and network security solutions remain powering security operations in the background, the WWW approach based on ZTX is front and center in the vendor's platform, offering integrated analytics and automated decision making and deploying segmentation controls across the entire infrastructure."*

"Organizations that have a well-constructed security apparatus in place and are moving to a more mobile workforce should consider bolstering those capabilities with the ease-of-use Cisco now provides."



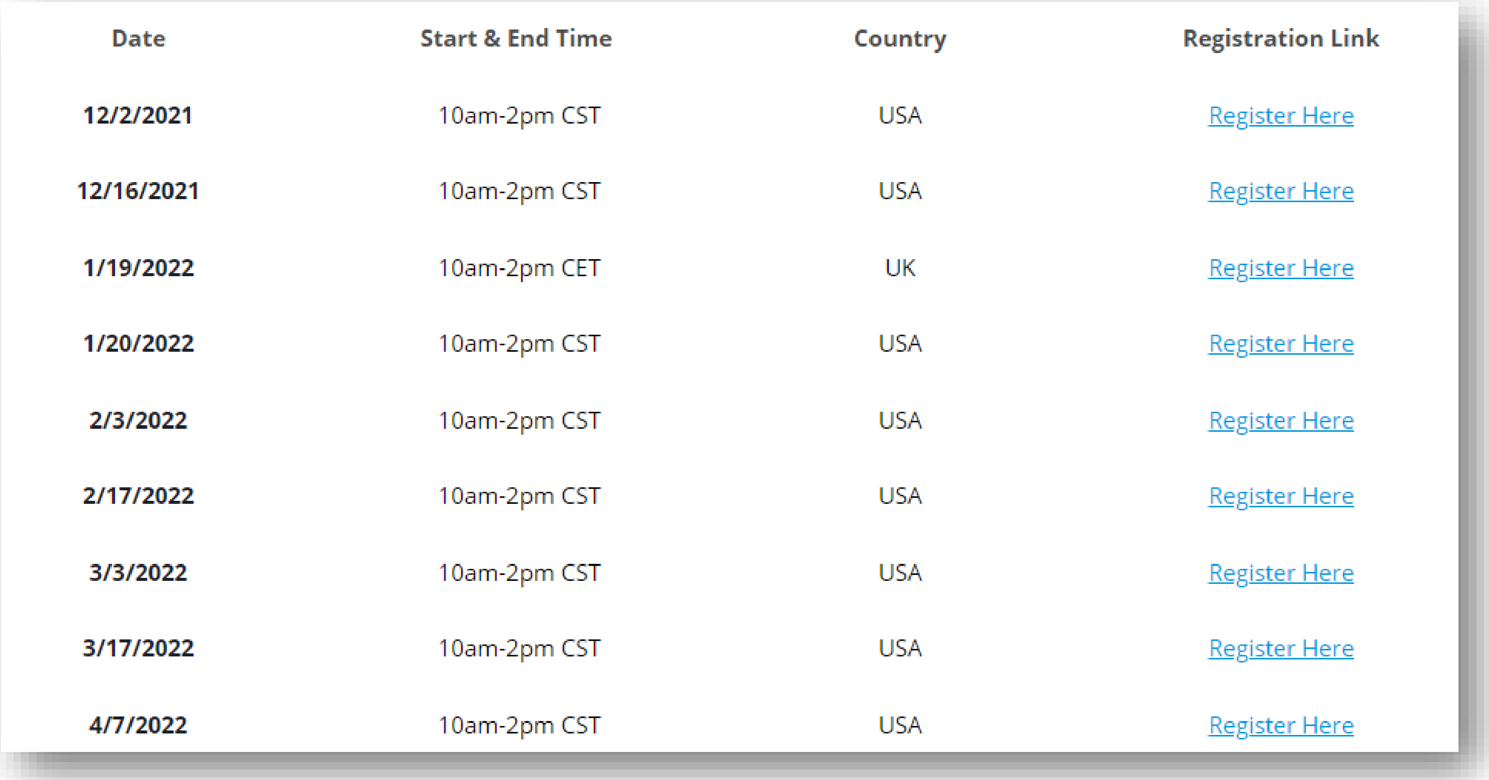
Cisco Zero-Trust Workshops

https://web.cvent.com/event/84f04d16-1486-4555-aeca-43df74102d3c/websitePage:645d57e4-75eb-4769-b2c0-f201a0bfc6ce

Join us for a virtual hands-on workshop to learn how to simplify and accelerate your zero-trust adoption and take your security expertise to new heights.

In this workshop, you will discover how to implement zero-trust to deliver results, integrate zero-trust into your daily workflow, uncover best practices you can use right away, and network with your peers to share strategies, techniques and outcomes.

Engage in a hands-on lab exploring zero-trust use cases, including establishing trust of users & devices, adaptive policies, zero-trust network access, modern application access and Secure Access Service Edge. Discover how to implement technology to accelerate zero-trust adoption.



Date	Start & End Time	Country	Registration Link
12/2/2021	10am-2pm CST	USA	Register Here
12/16/2021	10am-2pm CST	USA	Register Here
1/19/2022	10am-2pm CET	UK	Register Here
1/20/2022	10am-2pm CST	USA	Register Here
2/3/2022	10am-2pm CST	USA	Register Here
2/17/2022	10am-2pm CST	USA	Register Here
3/3/2022	10am-2pm CST	USA	Register Here
3/17/2022	10am-2pm CST	USA	Register Here
4/7/2022	10am-2pm CST	USA	Register Here

How We Can Help = The Portfolio

IT Network & System Architecture, Design, Implementation, Run, Operate, Maintain

Xceptional CARE

- Remote and Onsite Managed Services Support
- 24 x 7 Monitoring and Management of Desktop, Network, Phones, and Applications
- Multiple Support Levels to Fit Your Business, Budget
- Virtual CIO: Quarterly Technology Reviews and Reporting. Includes Strategic IT Planning, Updates to Plans, Standards, Maintenance, and Support Levels

Xceptional CONNECT

- Design, Deployment, and Management of Telepresence and Video Solutions
- Voice, Video, and Web-based Conferencing
- Real Time Communications on all Devices
- Cloud, Onsite, and Hybrid Communications Solutions

Xceptional CLOUD

- Strategic enterprise-class Data Center and Hosting Services. IT Software, Services, Applications, Email, and Network Solutions (Hosting, IaaS)
- Storage Solutions
- Backup & Recovery Solutions (BaaS)
- Compliance as a Service Solutions (CaaS)
- Virtualization

Xceptional NETWORKS

- Networking Solutions Driving Technology and Business Operations
- Routers/Switches
- Wireless Mobility Solutions
- Security Solutions and Security as a Service
- WAN Optimization

QA, Wrap Up & Next Steps

- **QA**
- **Offer: Zero Trust Readiness Assessment**
  - Network vulnerability scan
  - Technology review and evaluation
  - Controls review
  - Summary and recommendations report

info@xceptional.com

Xceptional

zadara

Linkedin Live Expert QA Session

January 13, 2022 / 11:00am PST

Leveraging Cloud to Accelerate Business Growth in 2022

Register Today!

Access more panels, webinars & research:

https://resources.xceptional.com/webinars

Xceptional.com

cisco Partner

Xceptional

cisco Partner

Thank You!

xceptional.com | 858-225-6230