5 Things to Know

CONNECTWISE

Jay Ryerse, CISSP
Vice President

SECUR-SERV

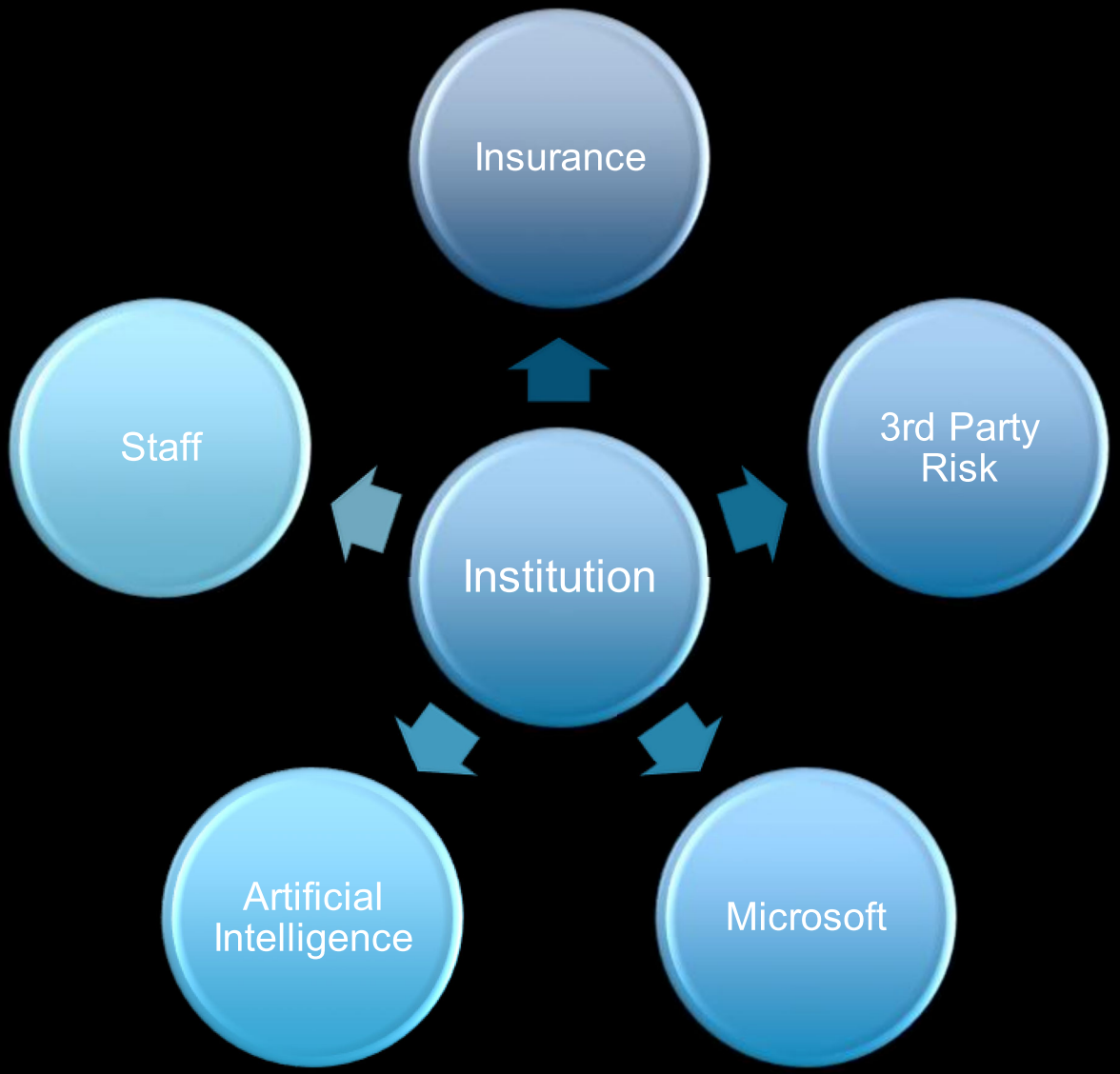
~~5~~ Things to Know

CONNECTWISE

Jay Ryerse, CISSP
Vice President

SECUR-SERV

What are the 5 Things?



SECUR-SERV

- Governance
- Risk Management
- Compliance
- Enablement
- Budget
- Resources
- PPT
- 3 Control Types
- Legacy Systems
- Processors
- Auditors
- Etc.

CONNECTWISE

Expectations

SECUR-SERV

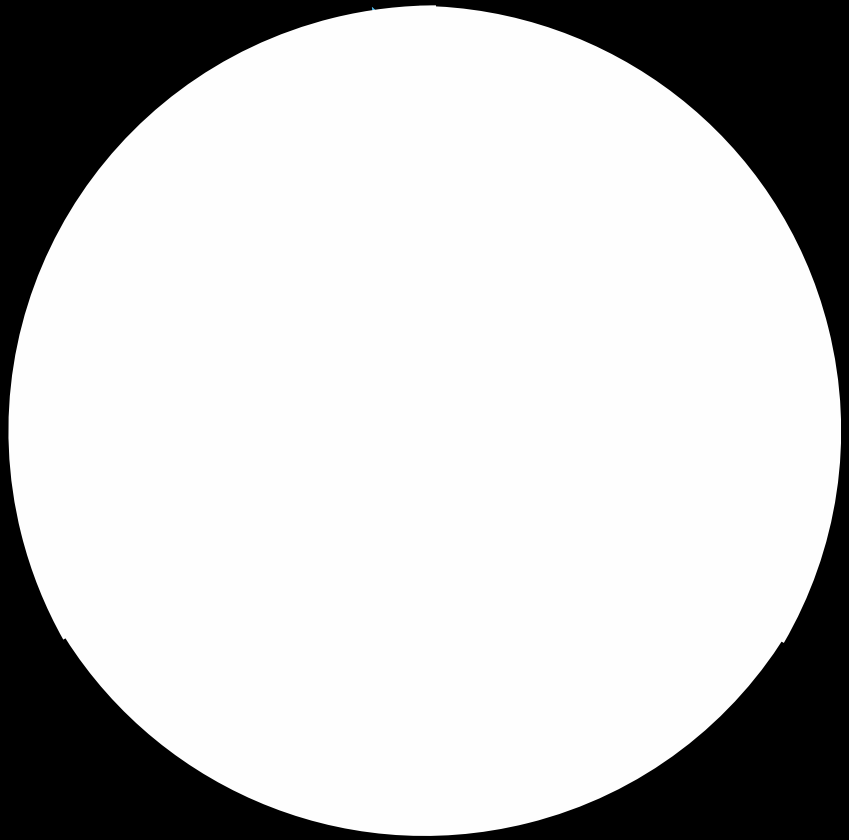
Three Conversations

Hyper Automation

Accelerates the work to be done, minimizes alert fatigue, improves efficiency, and drives an improved quality of service.

Standardization

Simplifies your operating stack and allows you to leverage the technology integrations in a meaningful way.



Consolidation

As IT professionals, we manage too many tools; this impacts efficiency and quality of work, leading to potential burnout from alert fatigue and a reduced quality of service for our clients.

CONNECTWISE

SECUR-SERV

Cybersecurity Insurance

Cyber Insurance (and renewals)

SECUR-SERV


BRIT
writing the future

Are back-up files disconnected and inac

Are back-up files encrypted?

If no to any of the above questions, ple
around security posture and controls:

Click here to enter text.

additional information

please provide any additional information
of these exposures:

Click here to enter text.

Signature:

Print Name: Click here to enter tex

☐ Electronically Signed

CXS5xxxxxxx

Page 1 of 1

BRIT
writing the future

ransomware

SUPPLEMENTAL QUESTIONNAIRE

applicant: Click here to enter text.

communications security

Are advanced threat protection settings enabled for all email users?	☐ Yes ☐ No
Are multifactor authentication settings enabled for all email users?	☐ Yes ☐ No
Are incoming emails and communications filtered for malicious links/attachments?	☐ Yes ☐ No
Are external emails and communications marked to alert users of their external origin?	☐ Yes ☐ No
Have you implemented any of the following controls: DKIM; SPF; DMARC?	☐ Yes ☐ No
Do you conduct regular phishing training and testing of all users?	☐ Yes ☐ No
If no to any of the above questions, please provide additional details of policies and procedures around security posture and controls:	☐ Yes ☐ No

Click here to enter text.

systems security

Have you implemented endpoint detection and response security tools?	☐ Yes ☐ No
Do you have established processes and procedures for rapidly deploying critical security patches across servers, computers, mobile devices and other end point devices?	☐ Yes ☐ No
Are multifactor authentication settings enabled for access to privileged accounts or files?	☐ Yes ☐ No
If no to any of the above questions, please provide additional details of policies and procedures around security posture and controls:	☐ Yes ☐ No

Click here to enter text.

back-up and recovery

Is all system configuration and data subject to regular back-up?	☐ Yes ☐ No
Is back-up access subject to separate access credentials which are maintained separately from common system credentials?	☐ Yes ☐ No
Are multifactor authentication settings enabled for access to back-up files?	☐ Yes ☐ No

CXS5xxxxxxx

Page 1 of 1

communications security

Are advanced threat protection settings enabled for all email users?	☐ Yes ☐ No
Are multifactor authentication settings enabled for all email users?	☐ Yes ☐ No
Are incoming emails and communications filtered for malicious links/attachments?	☐ Yes ☐ No
Are external emails and communications marked to alert users of their external origin?	☐ Yes ☐ No
Have you implemented any of the following controls: DKIM; SPF; DMARC?	☐ Yes ☐ No
Do you conduct regular phishing training and testing of all users?	☐ Yes ☐ No
If no to any of the above questions, please provide additional details of policies and procedures around security posture and controls:	☐ Yes ☐ No

Click here to enter text.

systems security

Have you implemented endpoint detection and response security tools?	☐ Yes ☐ No
Do you have established processes and procedures for rapidly deploying critical security patches across servers, computers, mobile devices and other end point devices?	☐ Yes ☐ No
Are multifactor authentication settings enabled for access to privileged accounts or files?	☐ Yes ☐ No
If no to any of the above questions, please provide additional details of policies and procedures around security posture and controls:	☐ Yes ☐ No

Click here to enter text.

CONNECTWISE

Cyber Insurance (and renewals)

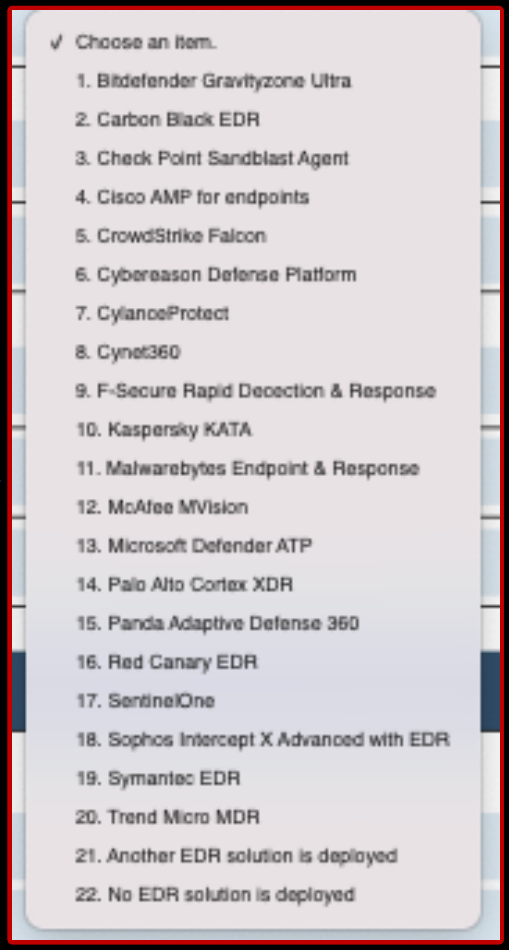
SECUR-SERV

What type of web filtering is used by the applicant?	Choose an item.
How do users access the applicant's network remotely?	Choose an item.
How is remote access to the applicant's network controlled?	Choose an item.
How is Remote Desktop Protocol protected in the applicant's network?	Choose an item.
Which Office 365 security add-ons are utilized by the applicant?	Choose an item.
How often is anti-phishing training conducted for the applicant's employees?	Choose an item.
How is access controlled across the applicant's network?	Choose an item.
How is privileged access to the applications data and applications controlled?	Choose an item.
What EDR solution is used by the applicant?	Choose an item.
What's the extent of unsupported systems and applications in the applicant's network?	Choose an item.
How does the applicant maintain open port hygiene?	Choose an item.
How is Managed Service Provider (MSP) access to the applicant's network controlled?	Choose an item.
What best describes the applicant's patch management procedure?	Choose an item.
What's the extent of the applicant's security events monitoring and logging?	Choose an item.

2. RANSOMWARE RECOVERY INFORMATION

In the event of an infection of the applicant's core network and applications:	
a. How quickly would the applicant's business operations be impacted?	Choose an item.
b. Which percentage of the network could be recovered from a back-up?	Choose an item.
c. What's the applicant's network redundancy?	Choose an item.
d. What's the estimated number of hours to restore the applicant's business operations?	Choose an item.
What best describes the applicant's back-up procedure?	Choose an item.
How often are the applicant's critical systems and data files backed up?	Choose an item.

THE HARTFORD



CONNECTWISE

Cyber private enterprise

Renewal application form

AUS

IT infrastructure and resourcing

Please confirm the name of your managed service provider (if applicable):

What is the approximate number of servers on your network?

What is the approximate number of desktops and laptops on your network?

What is your annual IT budget?

What approximate percentage of your IT budget is spent on IT security?

Is any part of your IT infrastructure outsourced to third party technology providers, including application service providers? ☑ Yes ☐ No

Previous cyber incidents

Please tick all the boxes below that relate to any cyber incident that you have experienced in the last three years (there is no need to highlight events that were successfully blocked by security measures):

☐ Cyber extortion	☐ Data loss	☐ Denial of service attack	☐ IP infringement
☐ Malware infection	☐ Privacy breach	☐ Ransomware	☐ Theft of funds

Cyber private enterprise

Renewal application form

AUS

Please tick all the boxes below that relate to controls that you currently have implemented within your IT infrastructure (including where provided by a third party). If you're unsure of what any of these tools are, please refer to the explanations on the final page of this document.

☐ Application whitelisting	☐ Asset inventory	☐ Custom threat intelligence	☐ Database encryption
☐ Data loss prevention	☐ DDoS mitigation	☐ DMARC	☐ DNS filtering
☐ Employee awareness training	☐ Incident response plan	☐ Intrusion detection system	☐ Perimeter firewalls
☐ Security info & event management	☐ Virtual private network (VPN)	☐ Web application firewall	☐ Web content filtering

Please provide the name of the software or service provider that you use for each of the controls highlighted above:

If you are an Office 365 user, please provide your Microsoft Secure Score *(administrators can find the score using the following link https://security.microsoft.com/securescore)*:

CONNECTWISE

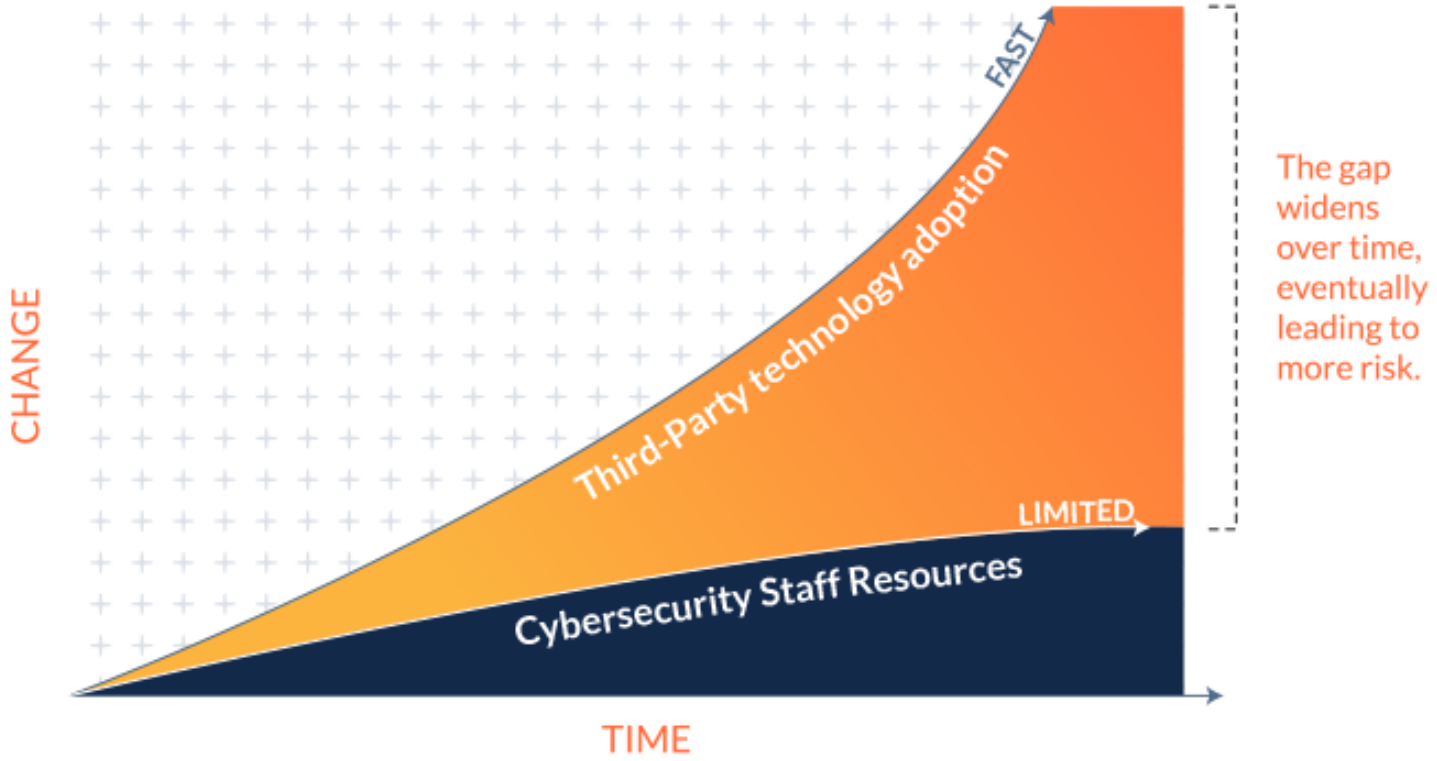
SECUR-SERV

3rd Party Risk

TPRM Dilemma

Third-party adoption has accelerated while risk management resources have stayed the same, or even declined. Risk management professionals must adopt a new way of evaluating third-party risks to sufficiently protect their organizations.

Source: https://www.processunity.com/



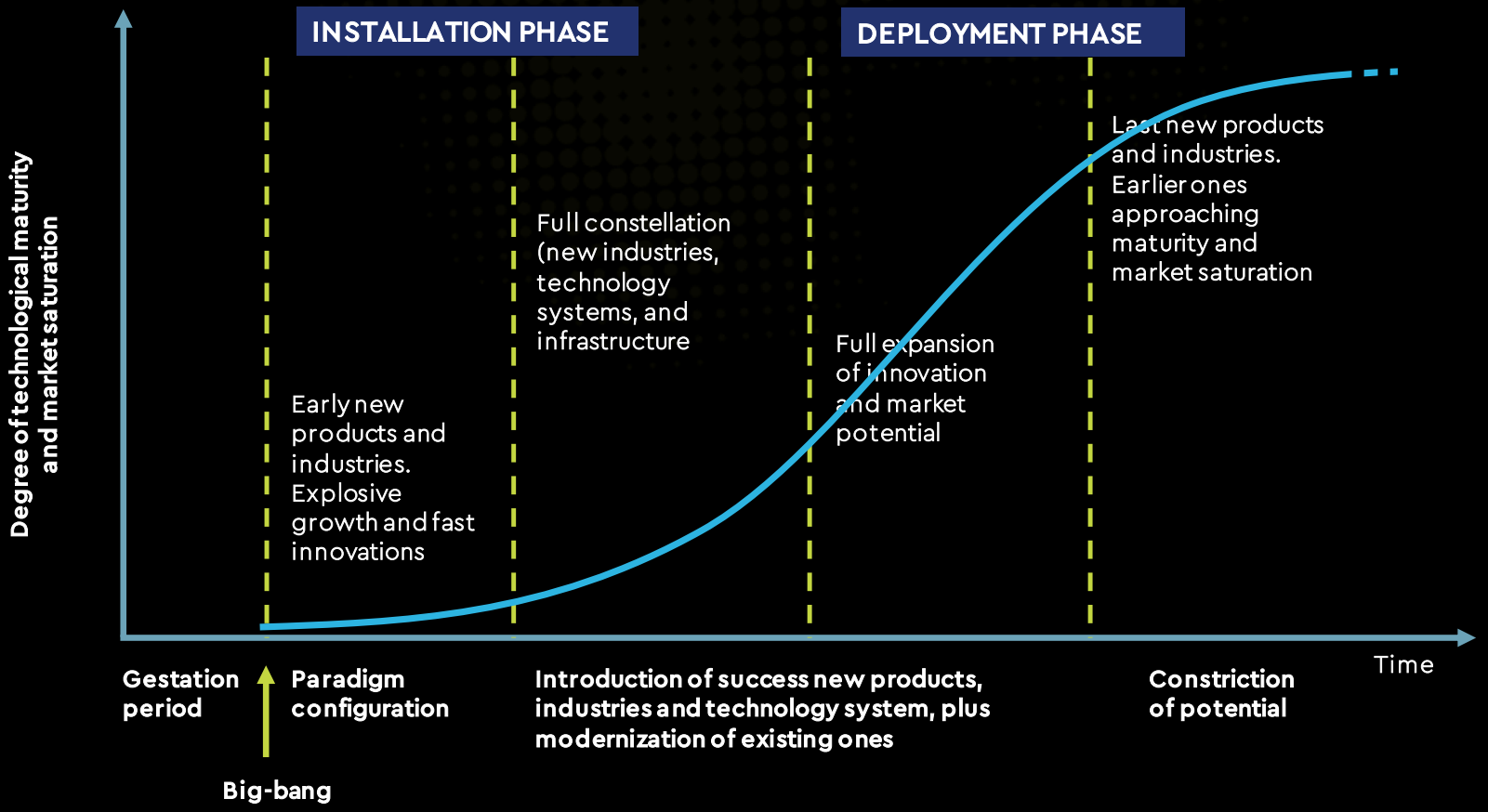
SECUR-SERV

CONNECTWISE

SECUR-SERV

Artificial Intelligence / RPA

Tech Revolution Lifecycle



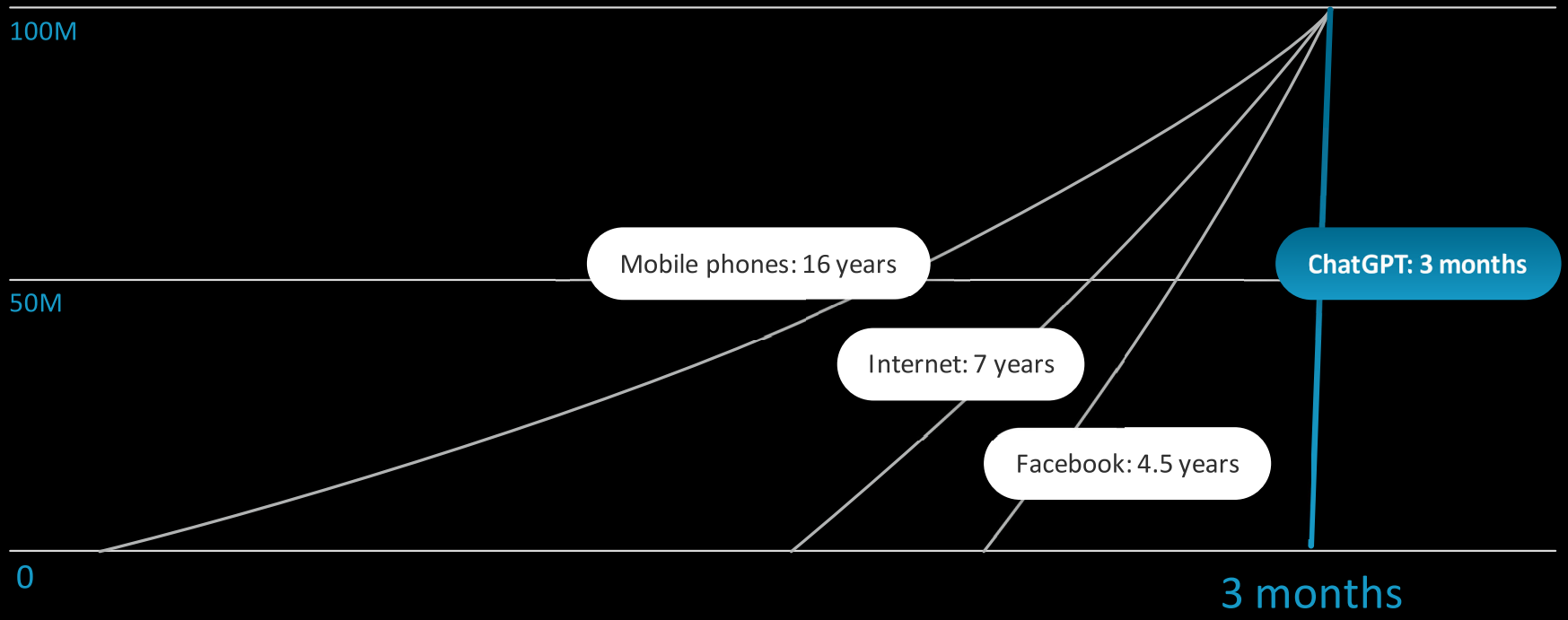
CONNECTWISE

Source: Carlota Perez: Technological Revolutions and

Source: Microsoft New Future of Work Report 2023

Generative AI technology is here.

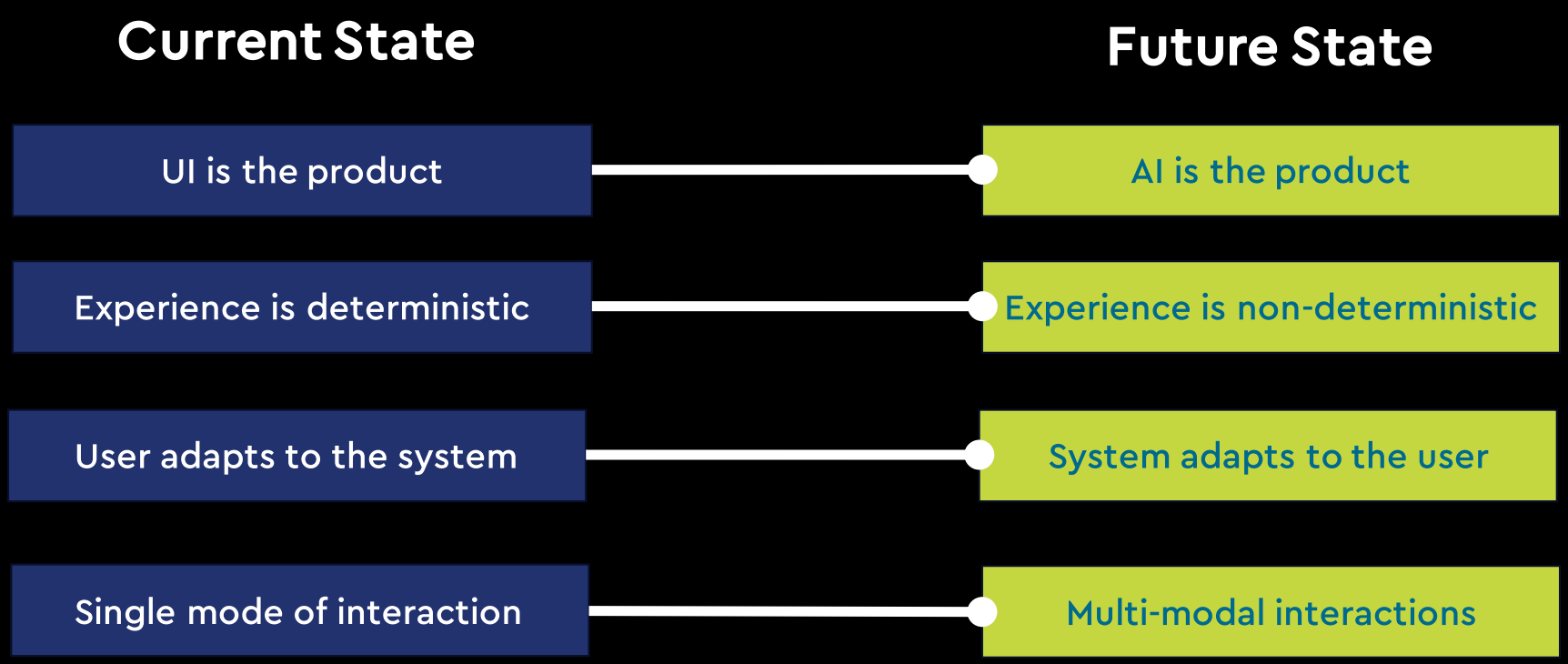
Time to reach 100M users



Source: Microsoft Research

CONNECTWISE

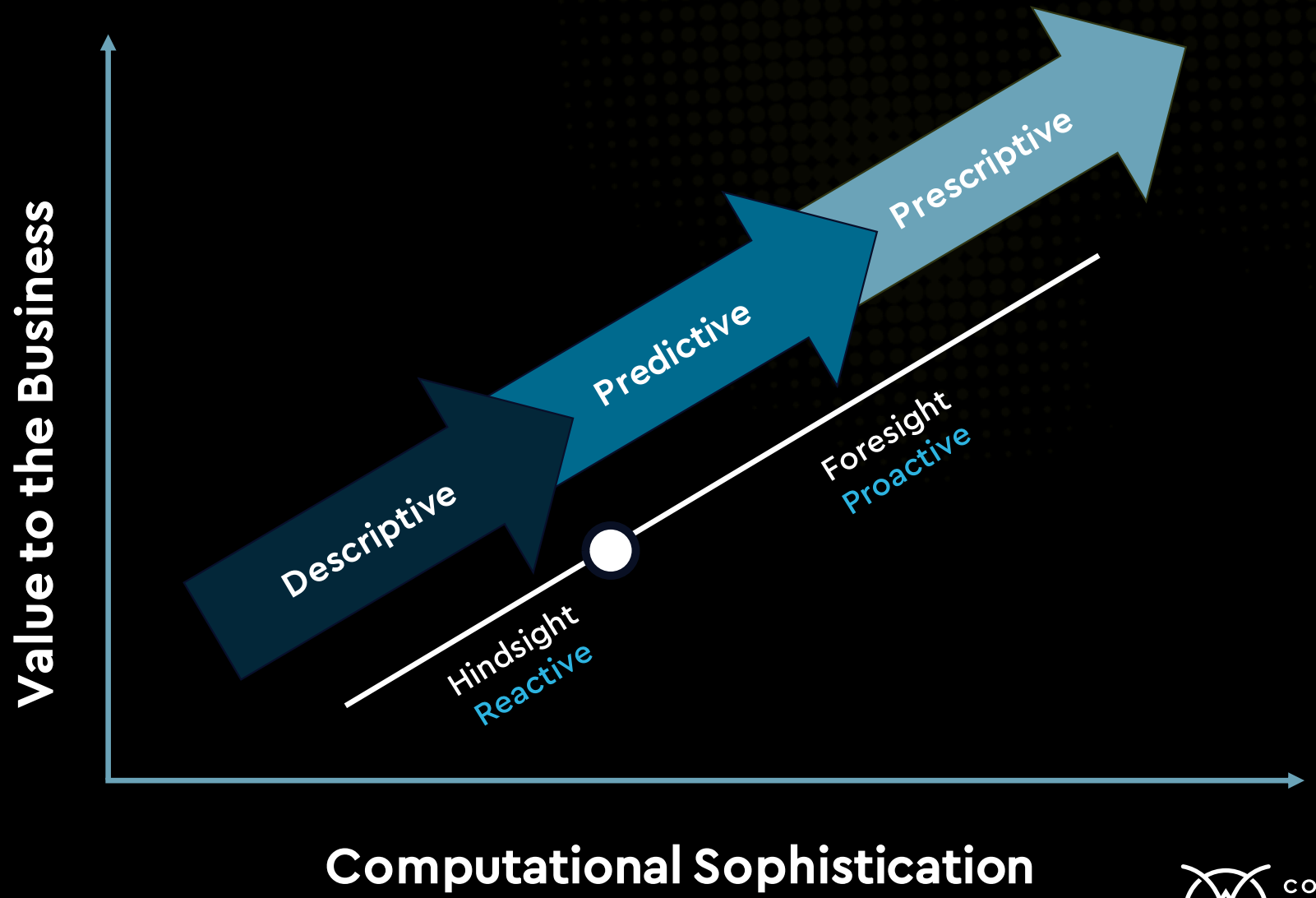
AI-Driven Transformation



CONNECTWISE

Source: Microsoft New Future of Work Report 2023

AI Journey



CONNECTWISE

Source: Microsoft New Future of Work Report 2023

SECUR-SERV

Staffing / Resources / Budget

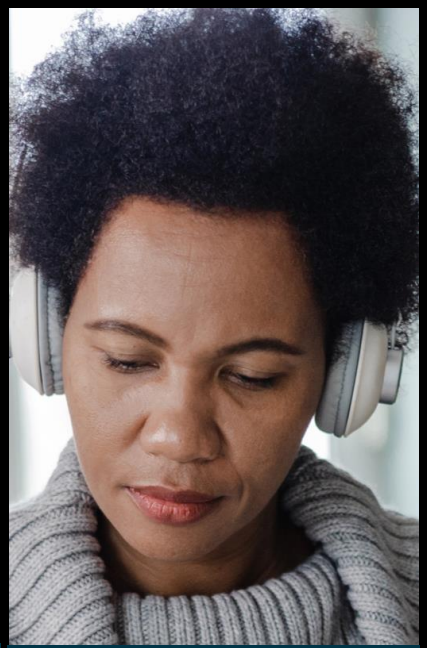
Artificial Intelligence can enhance every role in business; Everyone benefits!

Garret Black
Senior Technician

Exponentially faster time to configure and customize apps with little code experience

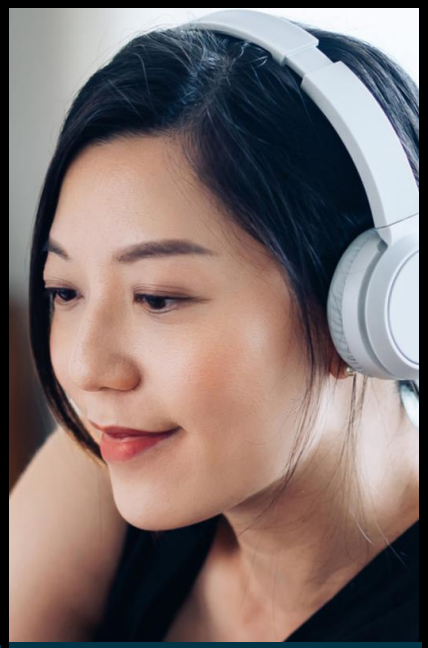
Sahil Ali
Sales

Close more deals and get insights into lost revenue opportunities



Lorena Santos
Finance

Manage cashflow faster and get actionable insights into operational costs



Jessica Cho
Procurement

Exponentially faster time to configure and customize apps with little code experience

Ray Jackson
Owner

Grow the business profitably and obtain unprecedented business visibility

HYPER AUTOMATION USE CASES

Billing, Accounting, And Finance	Procurement And Supply Chain	Talent and HR Management	Sales And Marketing	Project Mgmt. And Service Delivery	Onboarding And Setup	Account Management	CEO, General Management
Reporting and analytics	Product line card screen and select – compliance and certifications	Staff engagement and flight risk assessment	Top sales reps	Exception management	Verticalize Onboarding experiences	Stack alignment and optimization	Valuation and growth analytics
Agreements and service hours reconciliation	Spend analytics and savings opportunities	Tracking staff sentiment and performance	Auto create Initial proposal for discussion	Projects and agreements insights	Meeting agenda and next actions	QBR readiness and client touch points	Forecasting and budgeting optimization
Invoicing, collections and escalation automation	Schedule supply chain, payments and check-in tasks	Competency-based screening of resumes	Sync svc delivery readiness with sales funnel forecast	Root cause analysis And suggested ticket resolution	Meeting notes	User onboarding/ offboarding	Best-in-class compensation assessment
Invoice search and insights	Notify service teams of product availability	Generate interview questions from resume	Highest margin prospects	Ticket assignments, priority, and triage	Sales handoff notification to Service team	Agreement insights and optimization	On-demand analytics and strategy
Client profitability vs. Service utilization	Order insights	Employee onboarding	Visualize next 30 days opportunities	Ticket sentiment and customer email	Craft welcome Email	Client risk and relationship sentiment analysis	NPS and churn drivers

Elevated Speed and Precision | Enhanced Productivity | Operational Maturity & Excellence

50%

40%

25%

Profit Increase

Note: Use cases are not exhaustive and actual benefits may vary based on the actual business or vertical market

CONNECTWISE

SECUR-SERV

Microsoft

SECUR-SERV

It was somewhere in the 2001-2003 timeframe when Microsoft stated that they'd become one of the largest security providers in the world.

CONNECTWISE

Microsoft is leading security on the front lines…

SECUR-SERV

Protecting

1M organizations in 120 countries

Analyzing

65T threat signals every day

Tracking

300+ unique nation-states, cybercriminals, and other threat actors

Blocked

70B attacks last year

Source: Microsoft Digital Defense Report, Microsoft Security blog.

CONNECTWISE

Microsoft’s unique ability to address customer needs

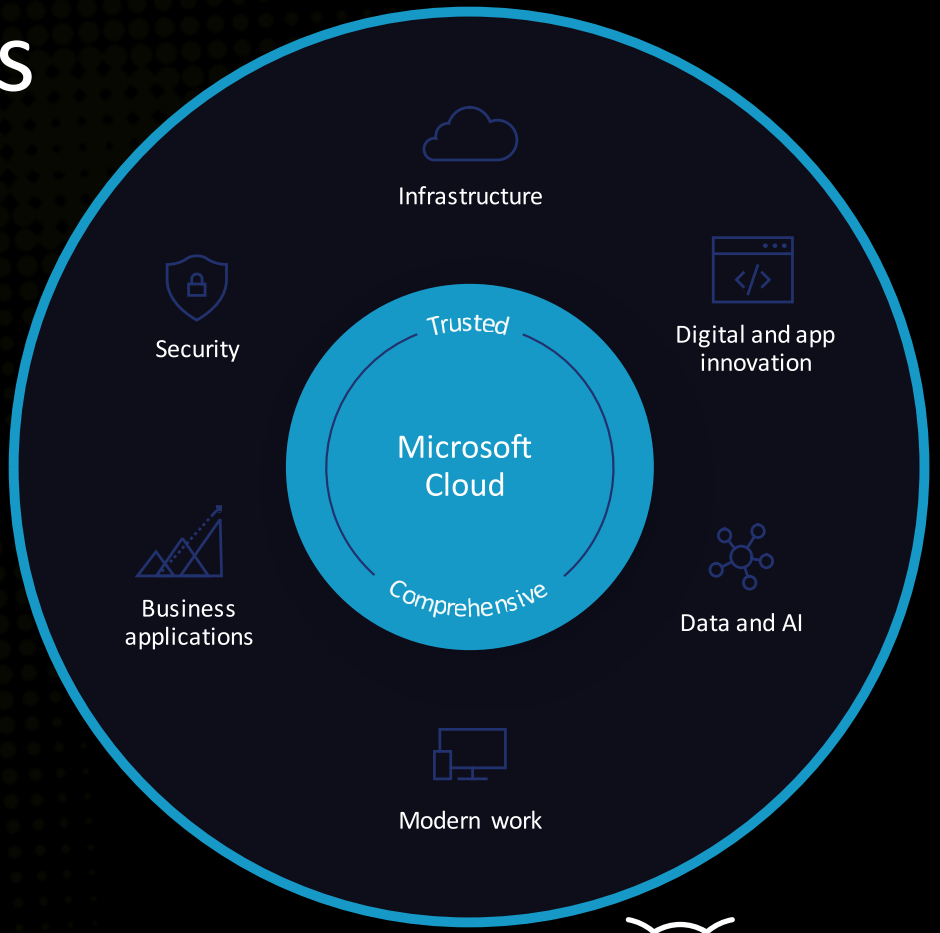
SECUR-SERV

AI Transformation

Deliver copilot experiences across the Microsoft Cloud

Develop the future leveraging Azure AI and the copilot stack

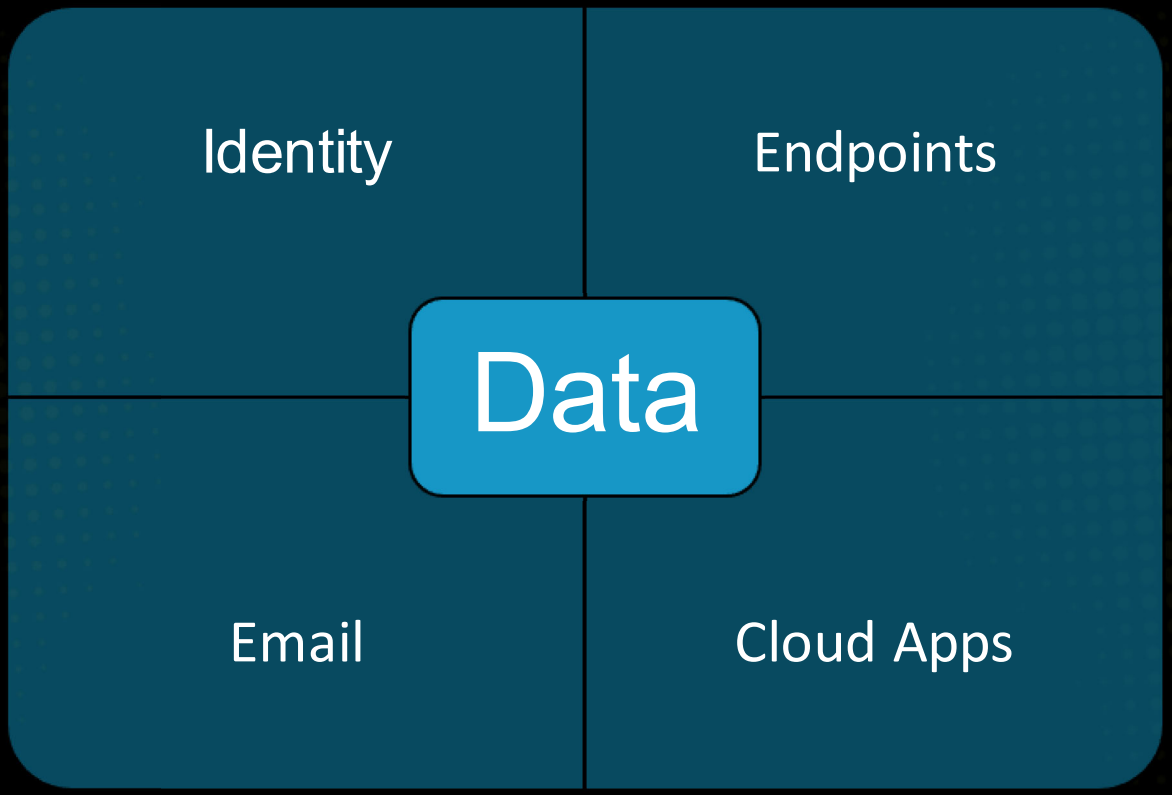
Co-innovate with customers building on the Trust of the Microsoft Cloud



CONNECTWISE

Key Components

SECUR-SERV

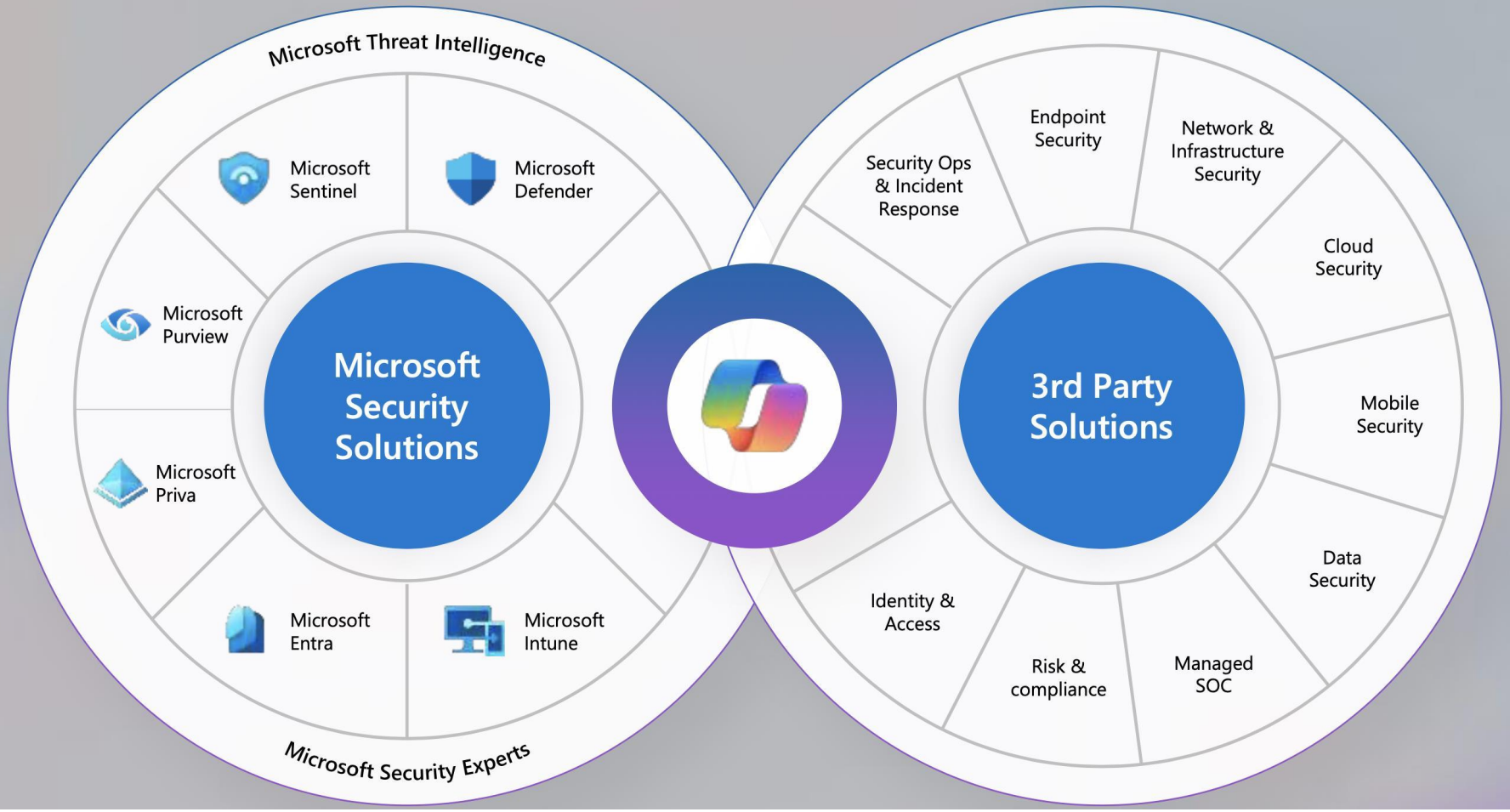


CONNECTWISE

The Copilot for Security advantage

SECUR-SERV

Copilot stitches together information across all security products



Things to Know and Places to Start

SECUR-SERV

- M365maps.com
- Semantic Indexing of Copilot: https://learn.microsoft.com/en-us/microsoftsearch/semantic-index-for-copilot
- Microsoft Security Adoption Framework: https://learn.microsoft.com/en-us/security/ciso-workshop/adoption
- Microsoft Reference Security Architecture: https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra
- Microsoft Copilot Training Material: https://aka.ms/CSPMastersCopilotTechPPT

CONNECTWISE

SECUR-SERV

Thank you!

CONNECTWISE

Jay Ryerse, CISSP
Vice President, ConnectWise
Jay.Ryerse@ConnectWise.com