

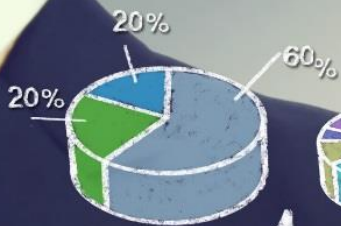
IDEA
CONNECTION



CREATIVITY



WEB



CONTENT



PEOPLE



LIKE

SHARE

SOCIAL

NETWORK

FRIENDS

COMMUNITY



GROUP

FEEDBACK

RESEARCH
INFORMATION
GROWTH

ACCESS

TECHNOLOGY
ANALYSIS
MANAGEMENT

SECTORS 2.0



STRATEGY

SOLUTION

SECURITY



PLANNING

SUCCESS

TEAMWORK



INNOVATION

GOAL

VISION

- ☒ MARKETING
- ☒ TARGET
- ☒ SKILLS

WHO

WHAT


WHERE

WHEN

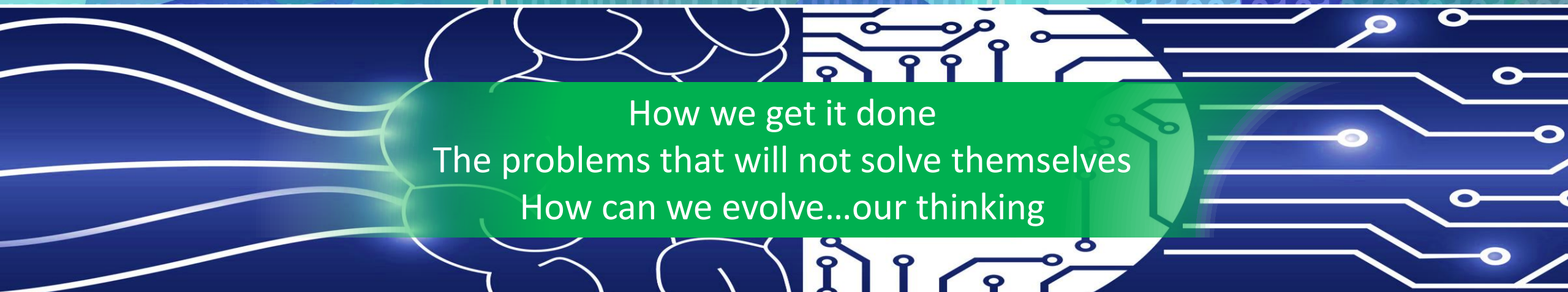
WHY

HOW






Context, otherwise known as my bio
How my career has led me to this presentation
How much cybersecurity hasn't changed in a decade



How we get it done
The problems that will not solve themselves
How can we evolve...our thinking



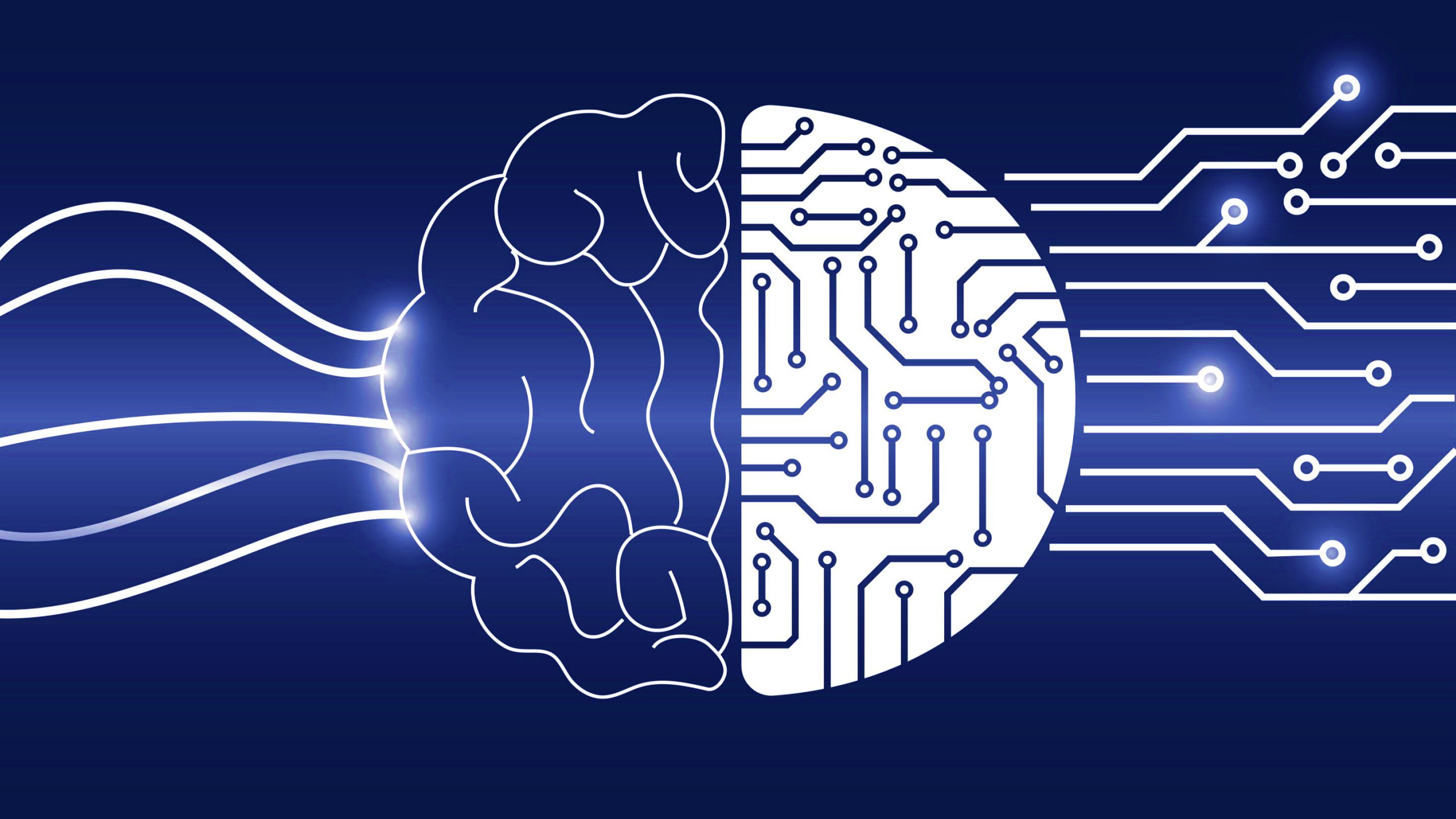
What part does technology play?
What specific technologies will drive change?
How does that affect the way you do cybersecurity stuff?

Government/IT Career Age 5-47

- Government has been around me my entire life
- Connecting industries through IT
- Cyber professional by chance
- Created something from nothing
- Network Access Control, and a decade of almos
- Visibility and the world of Splunk
- In search of integrated security...

Less Complexity Wins Every Time

- Want things to be better and simpler!
- Know what people want, independent of challenges!
- Get ideas from all around you! (e.g. Is a Zebra really a Zebra?)
- Know where you are and where you need to be!

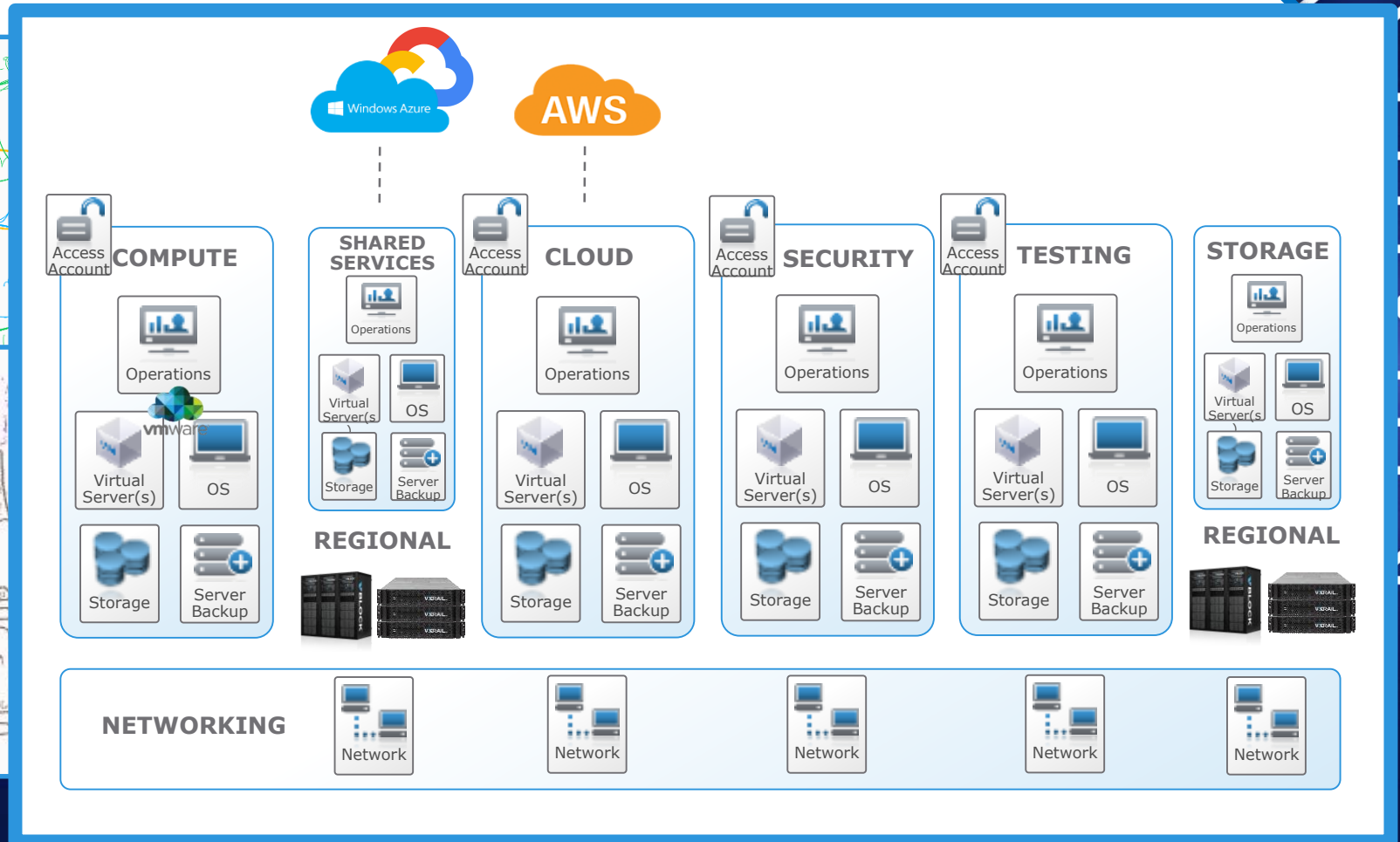




What I think I learned throughout the Cloud First, Cloud Smart, Cloud First, kind-of, maybe if it makes sense, but it depends era

- Cloud was the proof of concept that proved a consistent, software-defined environment deployed on uniform, stable infrastructure improves efficiencies that result in direct cost savings and improved security posture.
- Each cloud is different so costs end up relating to first, knowing which is best suited to support the application and secondly, how it interacts with other systems.
- A lot of information is still necessary to make risk based decisions which slows the process considerably.
- We can learn a lot from cloud and implement on-premise as well!

Where we are now...

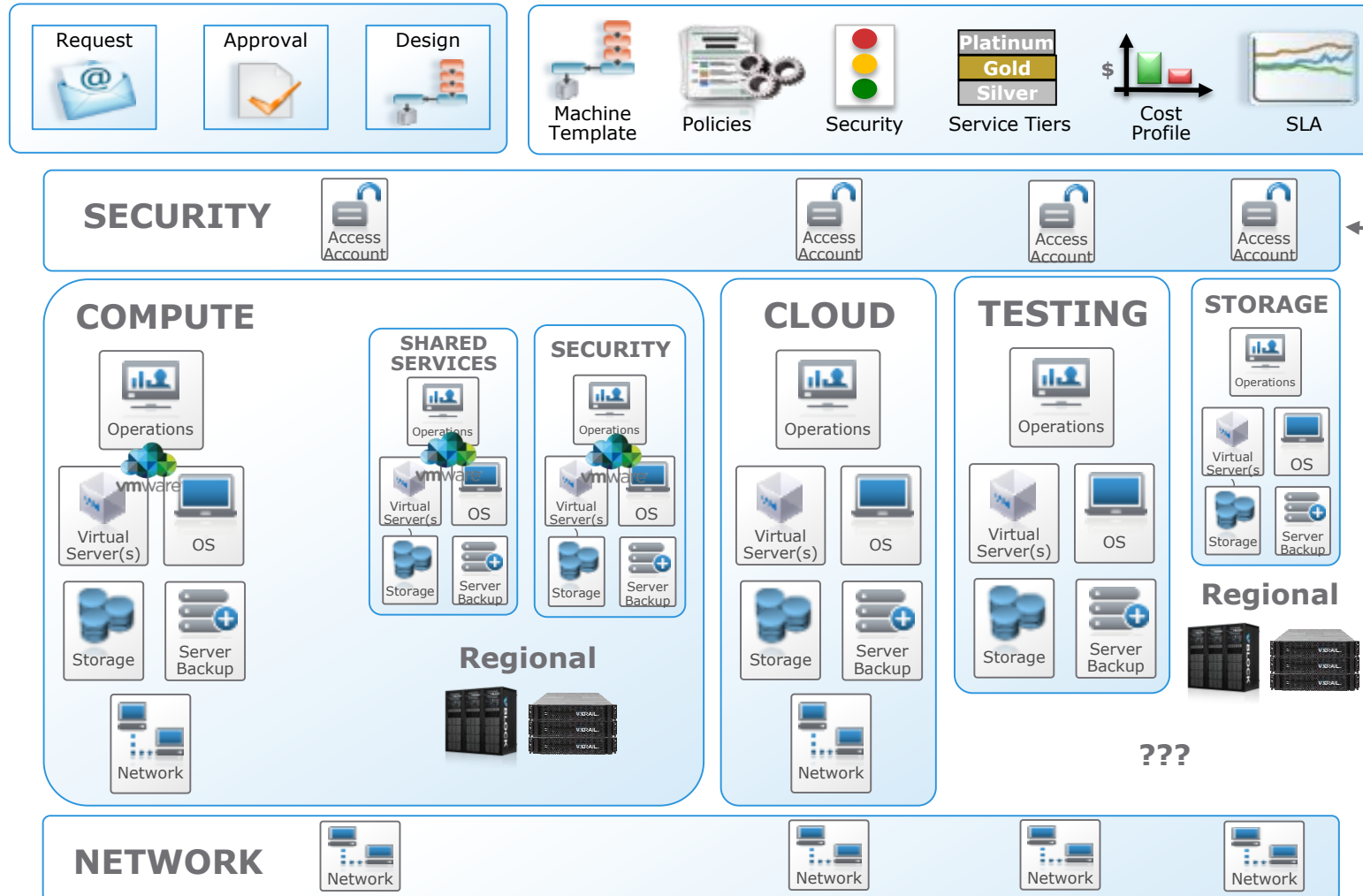


What the next few years look like...



Some cloud native development, software-as-a-service offerings, and "makes sense" workloads.

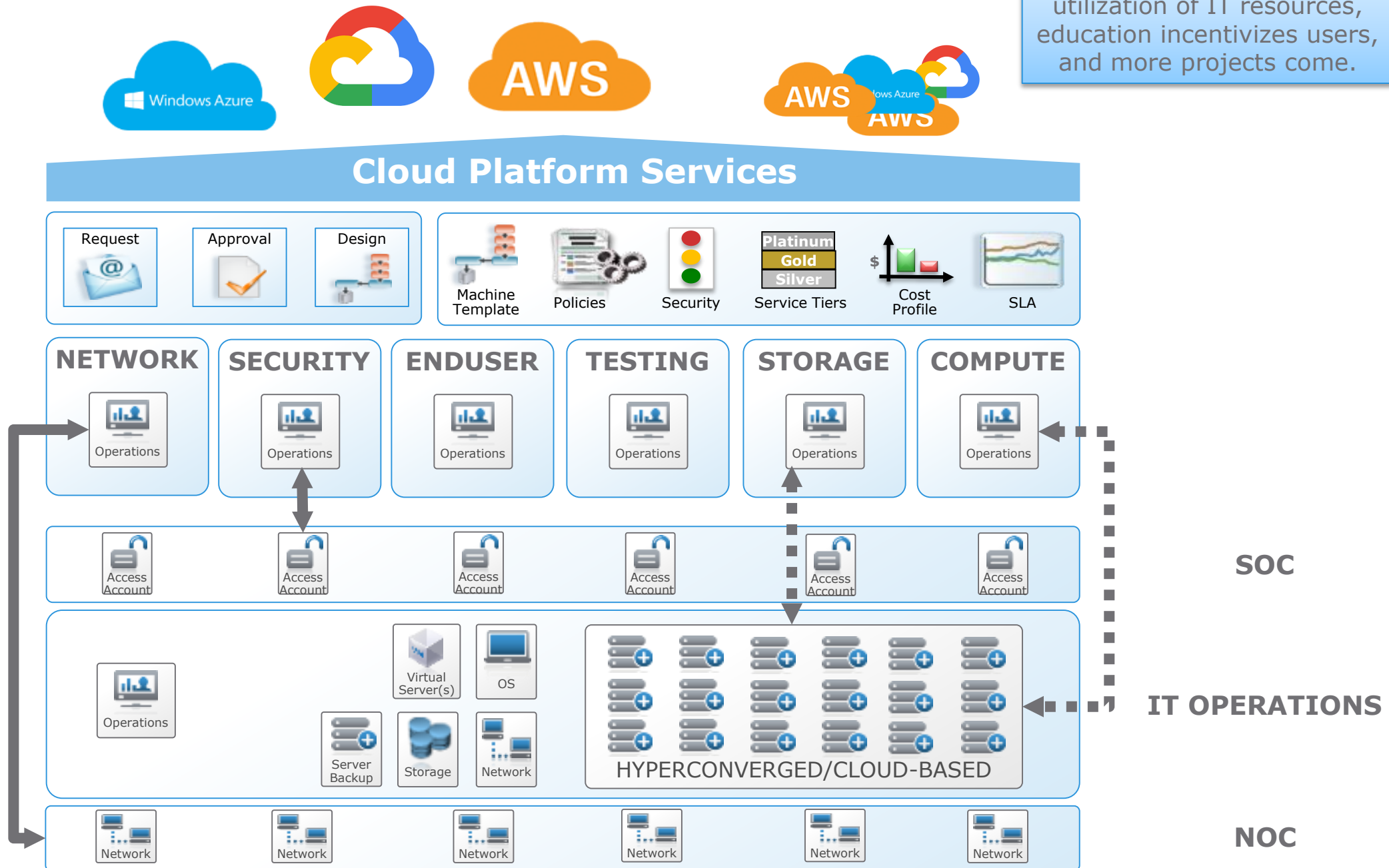
Cloud Platform Services



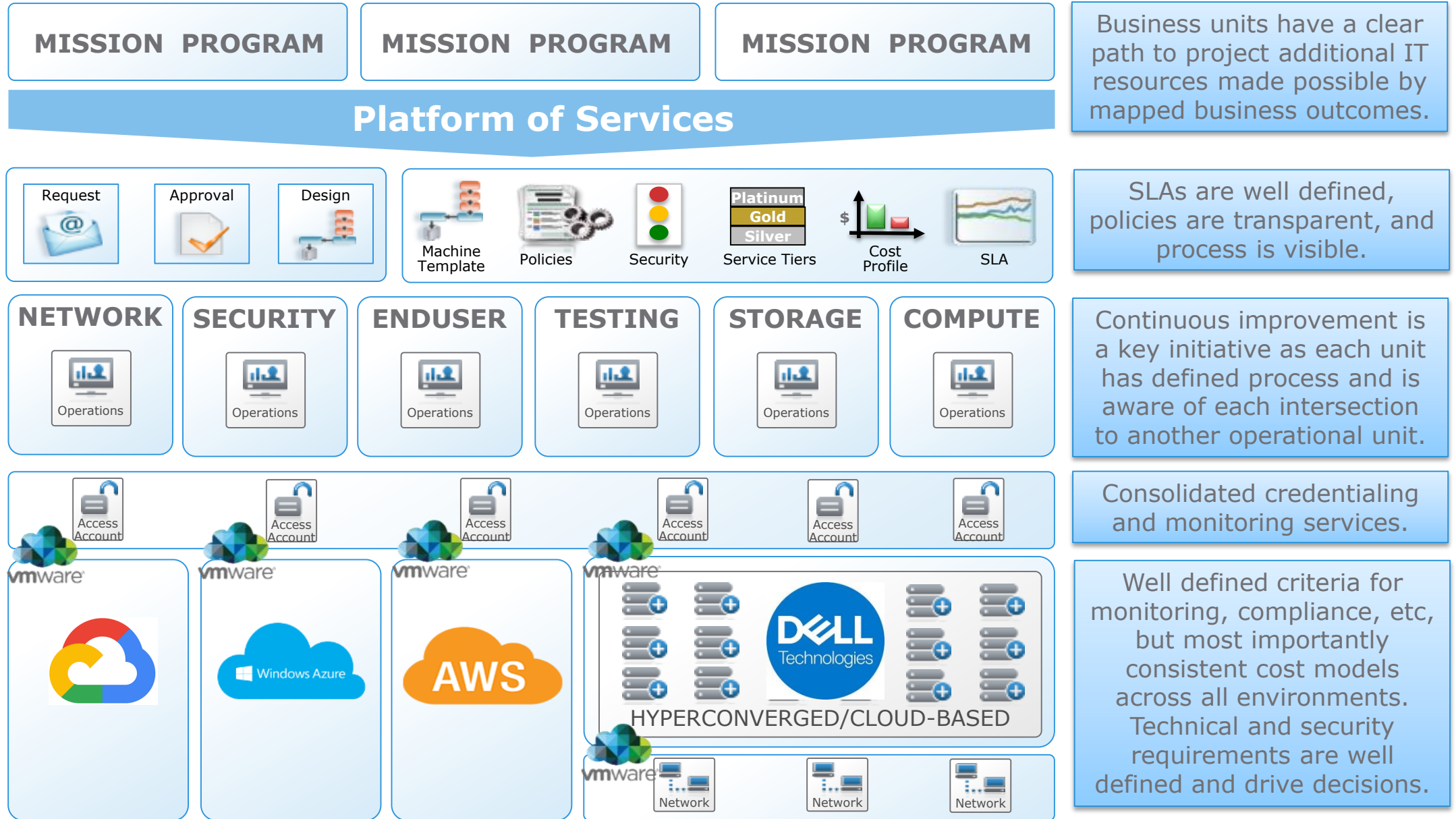
More visibility into access controls across on-premise and cloud assets.

Continuing to consolidate and build toward shared services. Roles and responsibility discussions, SOP.

Upgrades enable optimal utilization of IT resources, education incentivizes users, and more projects come.



And the next few years after that...



Leveraging Data Analytics to Transform Support for the Mission

More and more devices are constantly connected...**More data than ever**

Traditional

- ✓ Intrusion Detection
- ✓ Network Behavior Anomaly Detection
- ✓ Siloed storage, aggregation, correlation, trending, searching, reporting
- ✓ SEM for visibility
- ✓ Point solutions for selective visibility

Mission outcomes



Analytics on everything with fewer gaps

- Datacenter to desktop
- User groups (roles)
- Behavior, e.g. navigation
- Individual behavior



Lower total cost of ownership

- Application performance
- Data management
- Visibility into actual needs
- Weed out old process



Continue to refine detection / insight

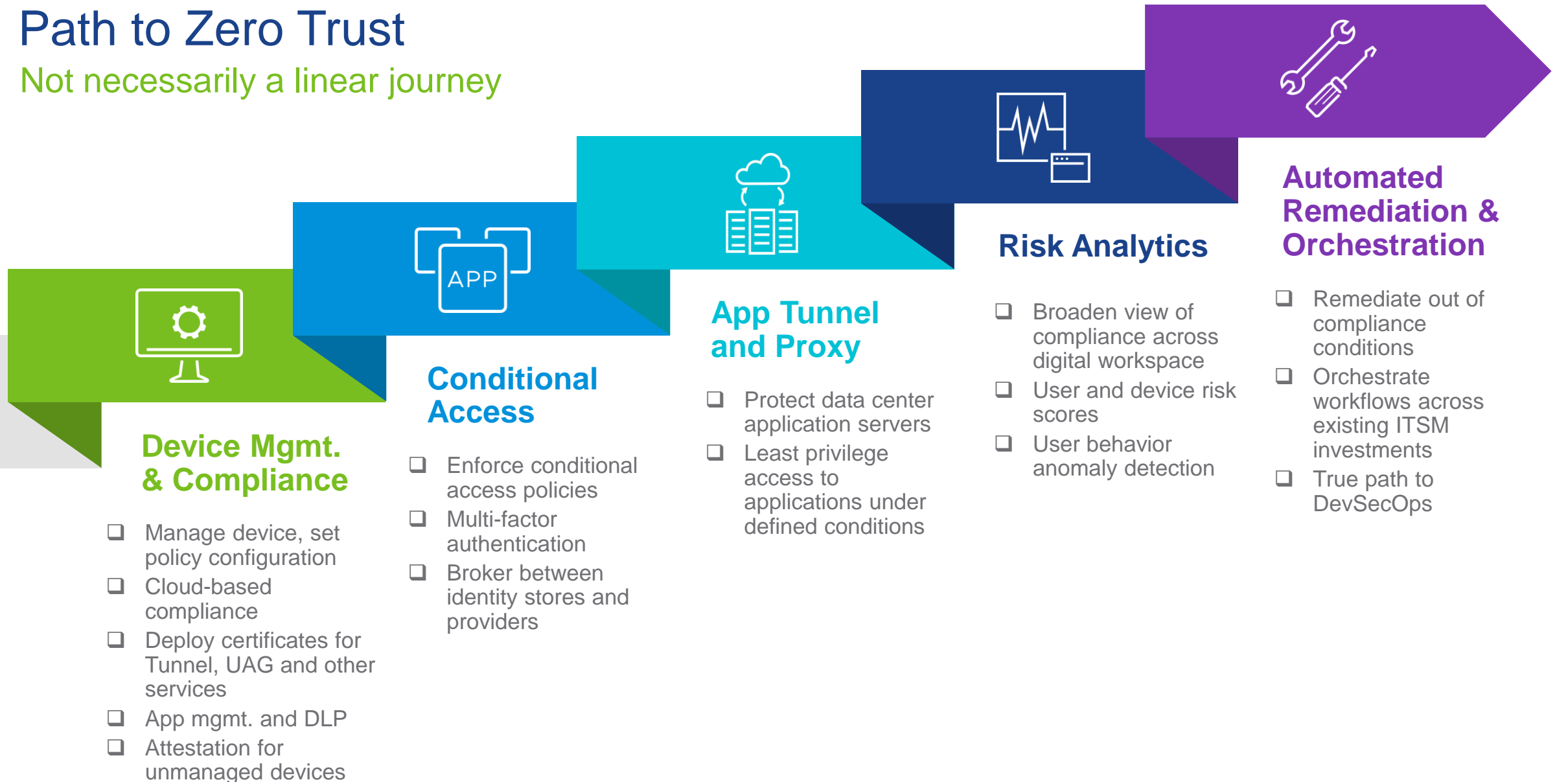
- Shorten timeframes for incident response / fraud
- Analytics, business rules, & predictive

NOT

ENOUGH

Path to Zero Trust

Not necessarily a linear journey



<https://techzone.vmware.com/resource/introduction-vmware-zero-trust>



“I don’t ever really fail. If I fail at making a cake it becomes a pudding.” - Life Lessons from 100 year olds

the longest period of any innovation is the time from brain to mouth to brain... - paraphrasing Elon Musk

How Dell Technologies Became that Partner...

- The relationship began in hardware solutions to provide compute and storage resources that housed application and data solutions.
- Dell expanded its scope through the acquisition of software companies and other capabilities like SecureWorks cyber services.
- Later acquisitions like EMC Corporation, which included a massive portfolio of technology, had critical security solution elements like VMware secure virtualization and EMC DR solutions.

“Dell Technologies has been able to leverage its extensive portfolio of technologies and customer relationships to gain a deeper understanding of the IT challenges facing its customers and develop comprehensive, secure solutions that span from desktop through the data center and into the cloud.”



Dell Technologies Cybersecurity Strategy

- Dell Technologies' cybersecurity strategy and its overarching multi-cloud strategy are simple to understand.
- Leveraging the VMware secure virtualization and cloud management platform that most customers are familiar with today, customers can uniformly deploy IT assets/workloads across each of the major public cloud providers (i.e. AWS, Google, MS Azure).
- Dell and VMware provide a common platform across each environment allowing customers to easily move workloads between environments as applicable, using a common toolset.
- This provides a consistent security model and policy enforcement that is repeatable and auditable vertically through the IT stack and horizontally no matter what environment the workload/data resides in.



What I have learned from the past 5 years...

- Lack of awareness regarding state of technology (e.g. hyper-converged)
- The hard work still has to be driven by the customer internally
- Lack of understanding regarding top market trends
- Not enough structure around conversations
- Metrics don't drive behavior
- Knowledge gap
- No Time





Networking Top 2

- 3-tier to Spine-Leaf
- Separation of Hardware and Software

Enduser Computing Top 2

- Seamless work experience
- How do you deliver your data?

Software Defined Datacenter Top 2

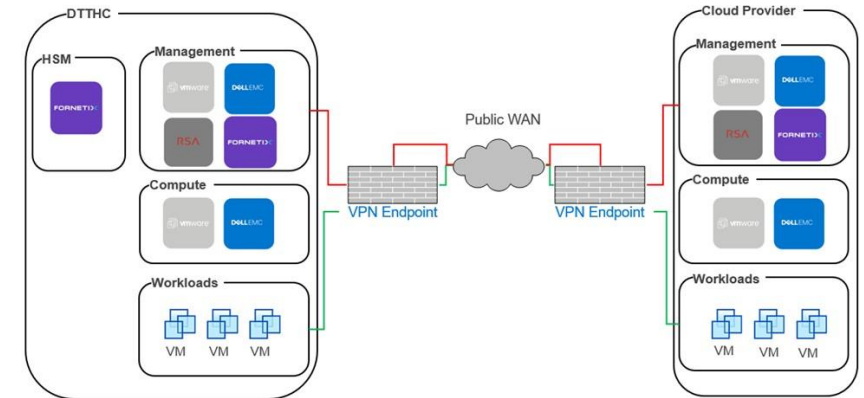
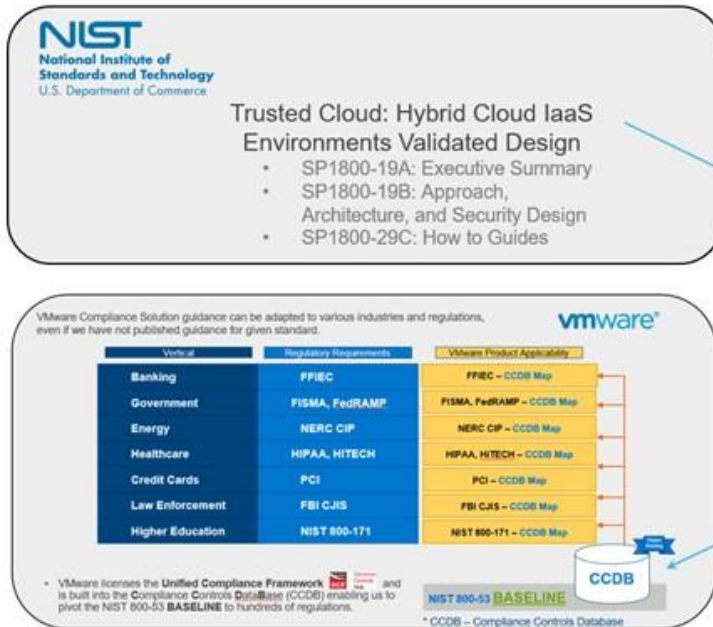
- Knowledge is power via automation
- Show what you know

The Security Stack, Zero Trust Top 2

- Know how you make your decisions
- Operate like part of a business

Dell Technologies Trusted Hybrid Cloud

Dell Technologies has leveraged the secure hybrid-cloud-based architecture developed with NIST to bring to market a solution that can be deployed both in Public, Private, and Hybrid scenarios. The core architecture and components support compliance and operational cybersecurity goals. The solution utilizes best of breed hardware and software from the Dell Technologies family allowing customers to run on-demand configurable pool of shared computing resources within their own architecture.

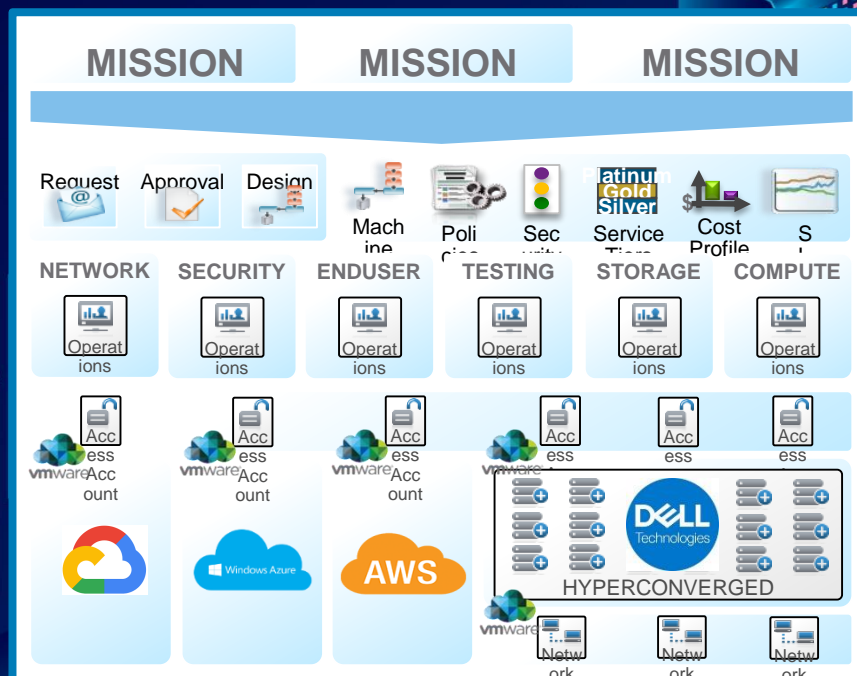


Supports Faster Implementation to Authority to Operate Compliance Goals

The VMware, Dell EMC, RSA, and Fortinet solution components have documented and imported their security control configuration capabilities and practices into the VMware Common Controls Database. This allows for the following:

- Publication of implementation guidance for vertical compliance goals (CMMC, FISMA, HIPAA, EU GDPR, etc.)
- Capability to feed the documentation outputs into a Risk/Compliance Audit tools like RSA Archer
- This can be used to review for drift detection and continual compliance and audit reporting

Know how
you make
decisions!



A portal of services...

Windows Azure



* Example provided is MS Azure

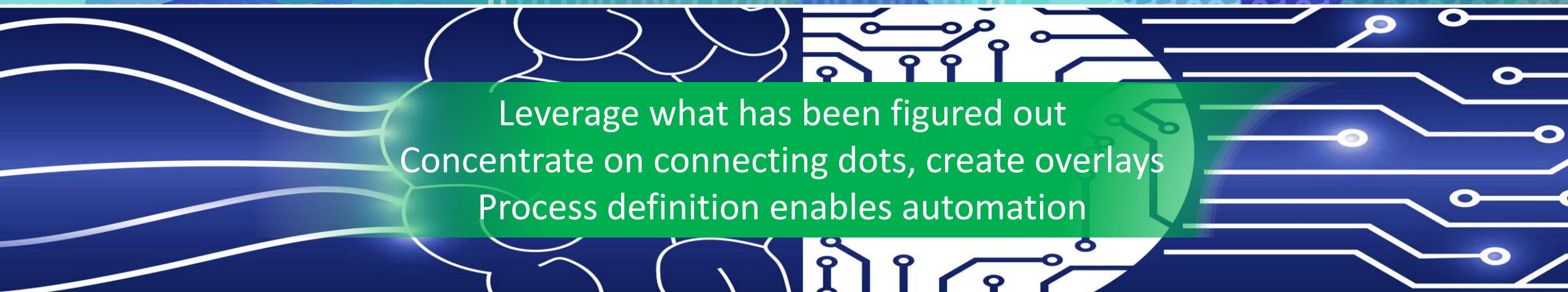
<https://www.delltechnologies.com/en-us/solutions/cloud/microsoft-azure-stack.htm>

Leveraging Data Analytics

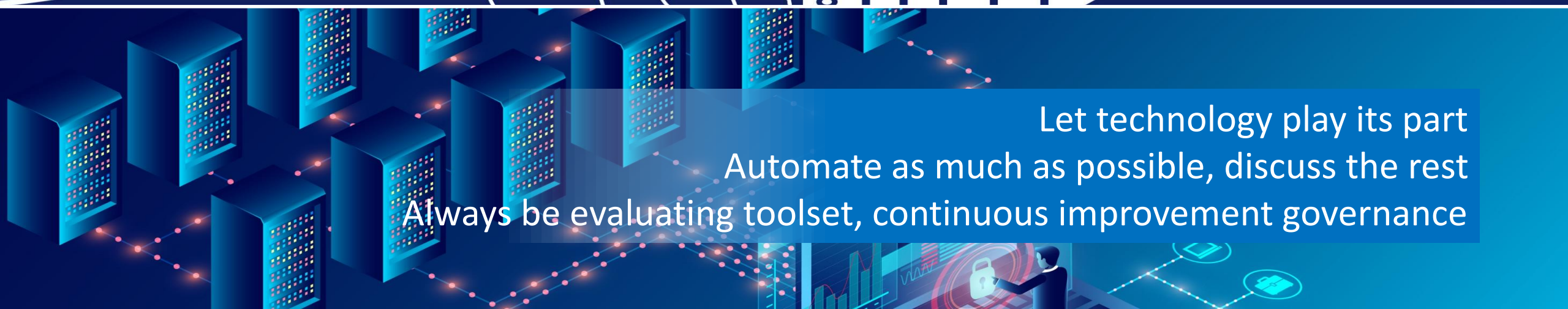




People are always the greatest asset
Continue learning, from everywhere
Practice communication



Leverage what has been figured out
Concentrate on connecting dots, create overlays
Process definition enables automation



Let technology play its part
Automate as much as possible, discuss the rest
Always be evaluating toolset, continuous improvement governance

Bob Nicholson | Bob_Nicholson@dell.com

LinkedIn:

<https://www.linkedin.com/in/bobnicholsonsecurity>