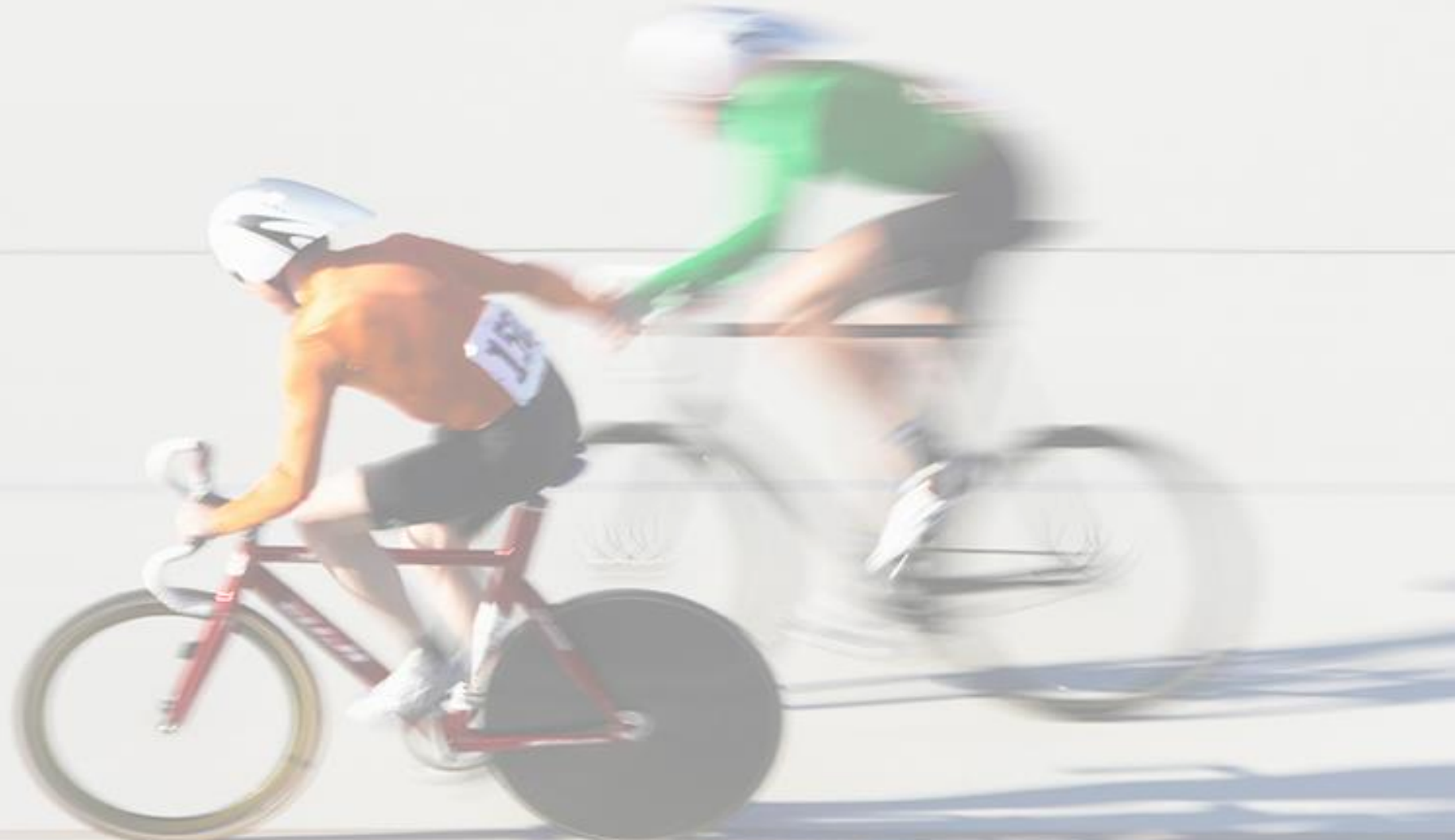


# New challenges **NEW IDEAS**



# Regulatory Compliance with Azure Security Center



## WHOAMI



Bart Verboven



Azure Technical consultant



[bart.verboven@realdolmen.com](mailto:bart.verboven@realdolmen.com)



[bverboven](#)



## WHAT I'M GOING TO TALK ABOUT

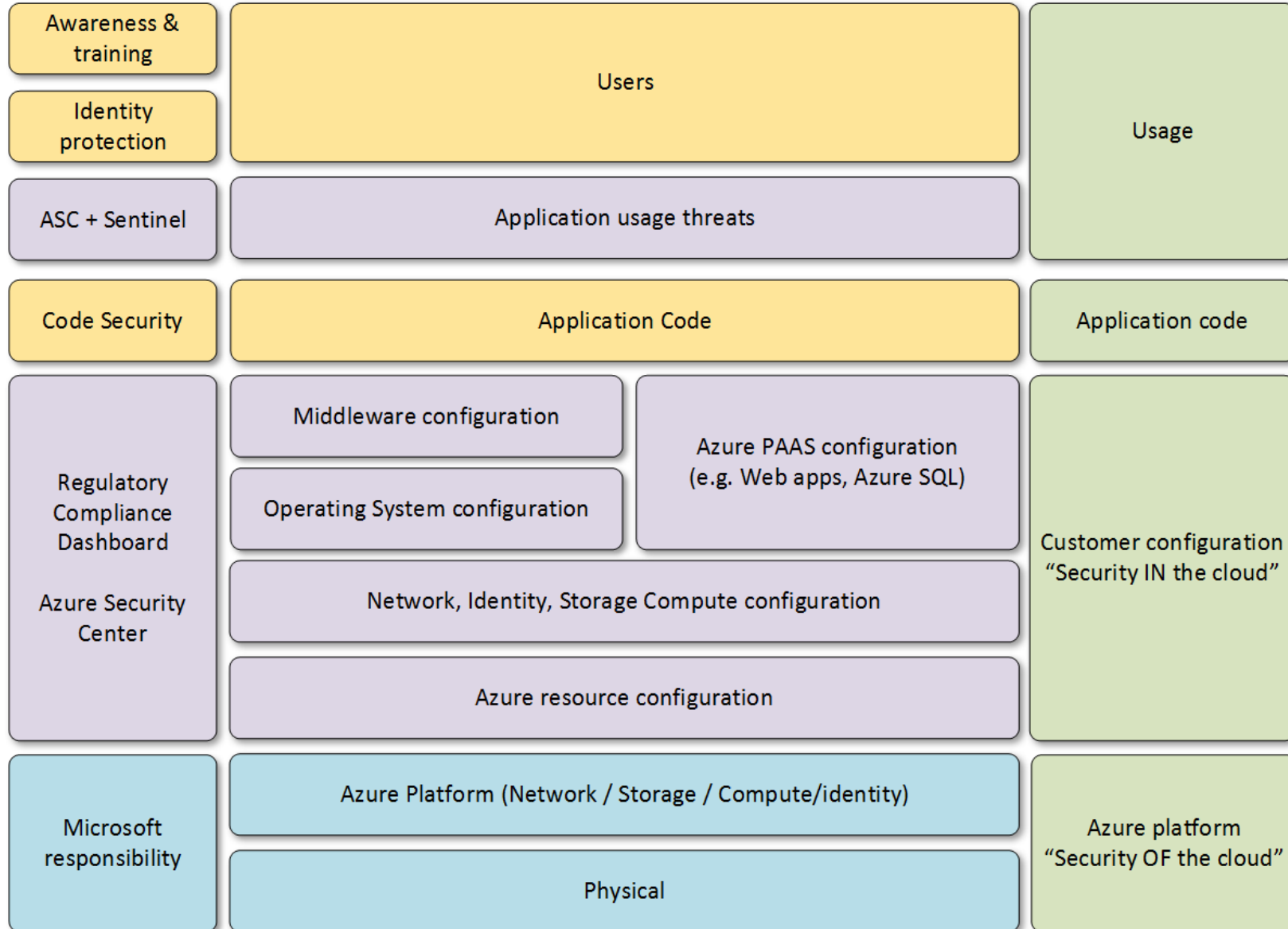
- Security responsibility in a cloud model
- The Regulatory Compliance dashboard
- The technical tracks
- Pricing model
- The Realdolmen approach
- QnA

“Through 2020, 95 percent of cloud security failures will be the customer's fault” – Gartner























Source Gartner Reveals Top Predictions for IT Organizations and Users for 2016 and Beyond, October 2015,  
<http://www.gartner.com/newsroom/id/3143718>



# SECURITY IN THE CLOUD IS A SHARED RESPONSIBILITY

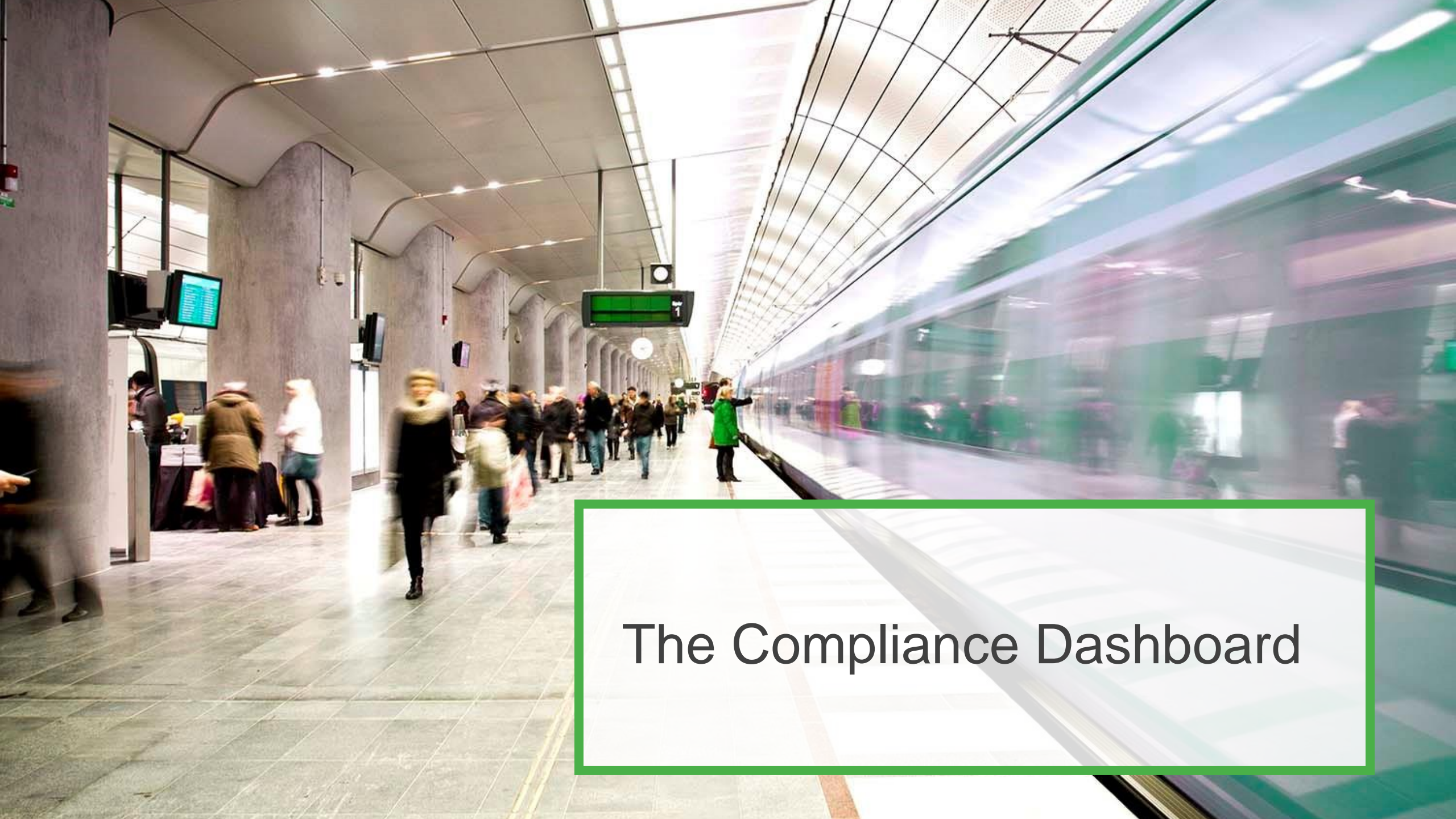


# TRUST CENTER

Global	 ISO/IEC 27001	 SOC 1	 SOC 2	 PCI DSS L1 version 3	 Cloud Security Alliance Cloud Security Matrix	
United States	 FedRAMP	 HIPAA (Healthcare)	 FIPS 140-2	 Life Sciences GxP	 Family Educational Rights & Privacy Act	
Regional	 European Union Model Clause	 United Kingdom G-Cloud	 China Multi Layer Protection Scheme	 China CCCPPF	 Singapore Multi-Tier Cloud Security	 Australian Signals Directorate I-RAP Assessment
Coming soon	 Sarbanes Oxley	 Criminal Justice Information System	 Defense Information Systems Agency L2	 ITAR	 Defense Information Systems Agency L3-5	 ISO / IEC 27018

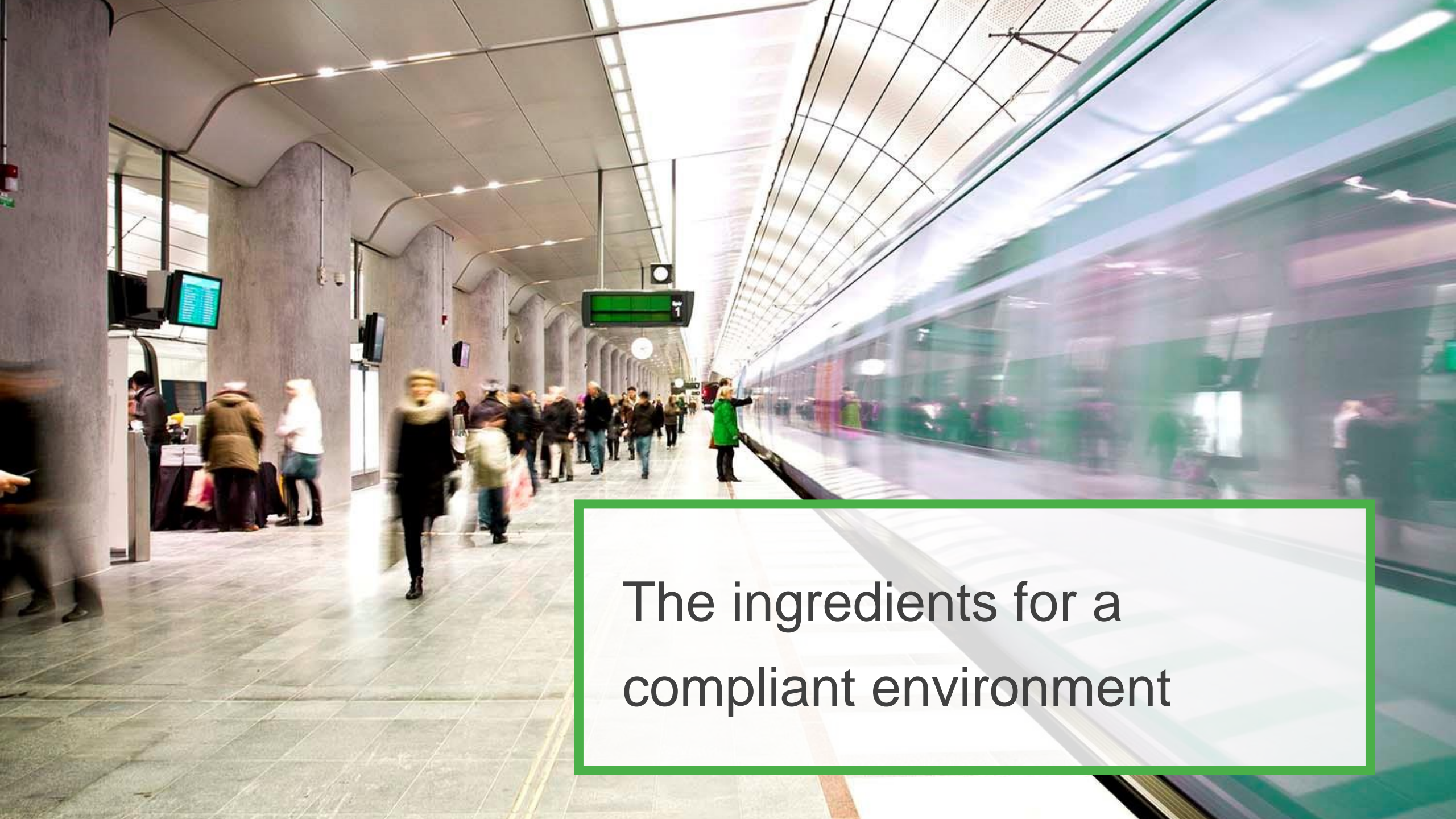






# The Compliance Dashboard





The ingredients for a  
compliant environment



# CONFIGURATION OF AZURE RESOURCES

- Configuration best practices of the Azure Resources
  - ▶ Tied to only resource types you use
  - ▶ ARM based
- Some typical examples
  - ▶ Enforce HTTPS
  - ▶ Use encryption capabilities
  - ▶ Diagnostics
  - ▶ Auditing (e.g. Key Vault access)
  - ▶ CORS restrictions
  - ▶ Remote debugging off for apps



# DATA

- Databases
  - ▶ Data Classification
  - ▶ Set an AAD account as administrator
  - ▶ Transparent data encryption
  - ▶ Vulnerability assessment
- Storage accounts
  - ▶ Restrict blob access
  - ▶ Restrict account access
  - ▶ SAS tokens
  - ▶ Managed disks

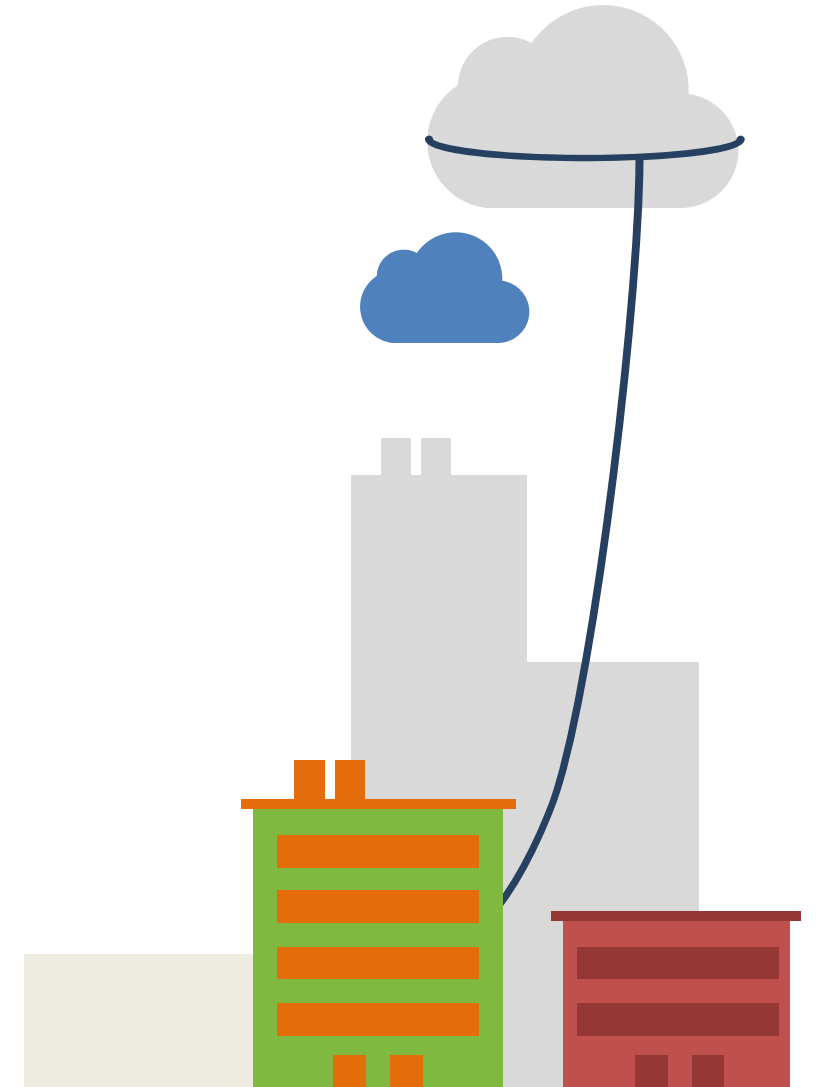




Demo

# NETWORKING

- Implement Network level security
  - Network Security groups
  - Azure Firewall
  - Next Generation Firewall Appliance
- Secure external access
  - Use service endpoints for PaaS resources
  - Built-in ACLs on PaaS components
  - Limit attack surface (e.g. RDP / SSH)
    - Restrict external access in time & have traceability: Just in Time





# IDENTITY

- Multifactor Authentication
  - ▣ Free for global admins
  - ▣ Will be enabled by default coming up
- Segregate your duties ....  
... but not too much
- Elevate access using Privileged Identity Management
- Clean up deprecated accounts





Demo

# OPERATING SYSTEM CONFIGURATION (IAAS ONLY)

- CCE (Common Configuration Enumeration)
- Enforce / Control with
  - Group Policy Objects (GPO)
  - Desired State Configuration (DSC)
  - Azure Policies in preview (~DSC) (GA 08/2019)
- Protection
  - Endpoint Protection
  - Patching
- Both Windows & Linux are checked







Demo

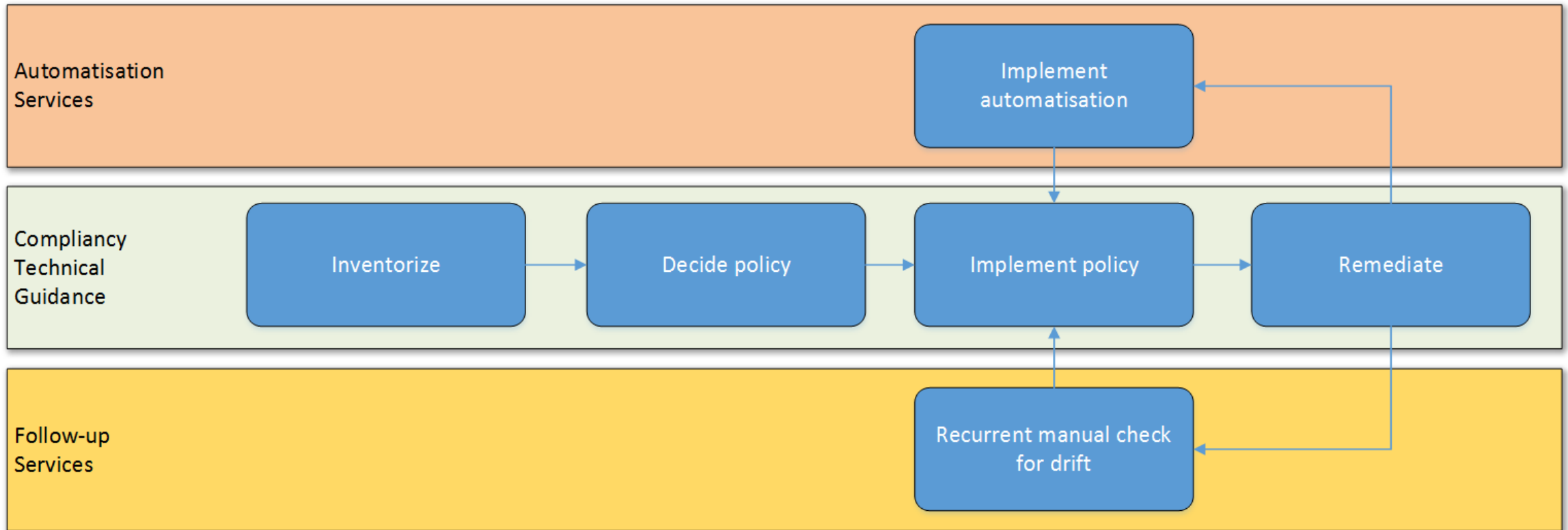


## PRICING MODEL

Free	Standard
Security assessment	Security assessment
Security recommendations	Security recommendations
Basic security policy	Advanced security policy
Connected partner solutions	Connected partner solutions
	Just in time VM Access
	Adaptive application controls
	Network Threat detection
	<b>Regulatory compliance dashboard</b>
	<b>15 USD / Node / Month</b>



# THE REALDOLMEN APPROACH





Questions?

Contact us at:  
[hybridcloud@realdolmen.com](mailto:hybridcloud@realdolmen.com)





Thank you!

Contact us at:  
[hybridcloud@realdolmen.com](mailto:hybridcloud@realdolmen.com)