



## PwC Portfolio Rationalisation

### Built for Microsoft Azure and Microsoft 365

Cybersecurity doesn't have to be complex. The objective of this portfolio rationalisation effort is to simplify your portfolio to reduce the cost and complexity of your environment. Every extra tool you have is an extra tool you manage - our clients often have redundant tools that cost them time and money.

#### Rationalise your current technology stack

Utilising a collaborative workshop based approach, PwC's Portfolio Rationalisation holistically assesses your organisation's security capabilities across the enterprise to identify areas of improvement and facilitate the adoption of Microsoft 365 cybersecurity technologies and capabilities to **Utilise**, **Rationalise**, and **Optimise** your cybersecurity technologies.

#### Cybersecurity technology portfolio challenges

- Tools are deployed to "patch" a problem instead of a holistic approach to cybersecurity
- Redundant tools lead to inefficiencies and a variations in user experiences
- Limited communication between technologies inhibit an organisation's ability to detect and respond to cyber attacks



#### Utilise existing tools

- Help leveraging the full potential of tools and optimise your security spend by identifying solutions within your current product stack which are under utilised



#### Rationalise security solutions

- Collaborate with you through interactive workshops to rationalise security solutions to reduce security spend by identifying/eliminating redundant capabilities
- Identify opportunities for integration between your existing technologies



#### Optimise security capabilities

- Through the rationalisation process, PwC will identify opportunities to help optimise the usage of your existing technologies
- Identify which gaps in the current security landscape can be addressed with your existing technology stack

PwC Portfolio Rationalisation can help you assess your organisation's enterprise-wide security capabilities to identify areas of improvement.

## An interactive workshop to Rationalise your Portfolio

### In each session we will help you

#### Understand what you have:

- What tools do you own?
- What they are being used for?
- How mature are your use cases?

#### Uncover the redundancies and gaps:

- Identify redundancies within the current tech stack
- Identify gaps in existing capabilities
- Explore opportunities to increase tool maturity within the current landscape

#### Agree on a unified, future cyber tool vision:

- Simplify cybersecurity tool portfolio
- Optimise cyber technology spend

#### Identify next steps:

- Immediate actions or hotspots that can be addressed right away (1-3 months)
- Longer term priorities (>3 months)

### As a result you will have



#### Current tool inventory:

- What they are used for
- How mature their implementation is
- What the current coverage gaps are
- What additional use case could be leveraged
- How the tool environment could be optimised, rationalised, and simplified



#### Integrated roadmap:

- High level short and long term projects to get to your rationalised cyber portfolio
- Immediate areas for improvement that can be turned around in a short time period
- Identification of long term initiatives and goals



#### Future state vision:

- A shared future state cybersecurity vision with a robust tool portfolio

### Pre-session

- Conduct pre-sessions assessment to understand the domains that client focus on and current state of existing tools

### Portfolio session

- Conduct sessions to Identify the overlaps between client's existing tools and Microsoft technologies and understand how we can help address the gaps and improve the capabilities

### Post-session

- Develop Tools Rationalisation Report to recap and document key pain-points and opportunities

### Let's connect



**James Toulman**  
Director, Cloud Services  
James.Toulman@pwc.com  
+971 56227 1811



**Haitham Al-Jowhari**  
Partner  
Haitham.AI-Jowhari@pwc.com  
+971 56676 1146