Cybersecurity Portfolio Rationalisation

Optimise security with PwC's Portfolio Rationalisation tool

Limit redundant software and enhance existing applications

Cybersecurity doesn't need to be complex. PwC's Portfolio Rationalisation tool can reduce the cost and complexity of security, by eliminating unused or ineffective tools.

Too many cybersecurity solutions increase the cost and create confusion, while lacking end-to-end visibility, which could impede an organisation from meeting its business goals or responding effectively during an incident.

Rationalise your existing technology stack

PwC's Portfolio Rationalisation service uses a workshop-based approach to holistically assess your organisation's security capabilities, identify areas of improvement, and facilitate the streamlining of your security capabilities.

Cybersecurity portfolio challenges

- Tools are deployed to 'patch' a problem rather than creating a holistic solution.
- Redundant tools create increased operational costs, duplication in licensing fees, require more technical training, skills and experience.
- Limited communications among technologies impede the ability to quickly detect and respond to cyberattacks.

Benefits to rationalisation

Utilise existing tools

- Realise the full potential of existing tools and optimise your security spend by identifying solutions that are under used.
- Identify opportunities to help optimise existing technologies.

Rationalise security solutions

- Rationalise your security solutions and reduce spending by identifying and eliminating redundancies.
- Discover opportunities to integrate existing technologies.

Optimise security capabilities

- Identify security gaps that can be addressed with your current technologies.
- Enhance your Security Team's efficiency and responsiveness with a refined and focused selection of security tools.

PwC's Portfolio Rationalisation tool assesses your organisation's security capabilities to identify redundancies and areas of improvement.

pwc

Using interactive workshops to rationalise your portfolio

In each workshop we will help you:

Explore what you have

- What tools do you own?
- What do you use them for?
- How mature are your use cases?

Uncover 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

Determine a unified future-state for security

- Simplify cybersecurity tool portfolio
- Optimise cyber technology spend

Identify priorities for action

- Immediate actions or hotspots that can be quickly addressed (1-3 months)
- Longer term priorities that can be addressed in more 3 months or longer

Benefit to you

Rationalise, optimise, and simplify security tools

A current tool inventory

- Capabilities of existing security tools
- Coverage of current apps
- Maturity of existing tools
- Additional use cases
- Ability to optimise, rationalise, and simplify existing tools

Integrated roadmap

- High-level view of short- and long-term projects for rationalisation
- Areas for improvement that can be rapidly achieved

Future-state vision

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

Approach

Information Gathering

Leveraging automation, data on your tools is collected and standardised around an industry leading framework to understand your organisations' focus areas and current state of your tools environment.

Scenario Analysis

Facilitated by PwC Cybersecurity Portfolio Rationaliser, Collaborate with you to conduct 'what-if' Analysis and identify how best to utilise your current tools to help address gaps and rationalise solutions.

Strategic Planning

Develop documentation that defines a high level roadmap of remediation and uplift actions that support the objectives identified during the engagement.

Contact us for further information

Craig Maskell, Partner
craig.a.maskell@pwc.com
+64 21 915 380

Mark Hewson, Director
mark.a.hewson@pwc.com
+64 27 283 8475