The cybersecurity portfolio challenges organizations face today

With a consistent flow of new, “best of breed” solutions and an ever-changing set of requirements, managing an organization's cybersecurity tool portfolio has become harder than ever. The diagram below highlights some of the challenges cybersecurity groups face today with their tools:

Underleveraged Tools

Tools that are already purchased, but are not being used to the full extent of their capabilities

Redundant Tools

Multiple tools within the organization that have overlapping capabilities

Incompatible Tools

Tools from varying providers that may be the best of breed, but are difficult to integrate and create a compatible, integrated cybersecurity portfolio

Varied Experiences

Inconsistent user experiences across the enterprise resulting in reduced efficiency and confusion

Leading to: Overspending & Risk Exposure

The challenges facing organizations today has lead to overspending on cybersecurity products caused by redundancies and underleveraged solutions as well as an increase in risk due to limited communication and integrations between products

Low Portfolio Visibility

Lack of understanding of what tools are actually owned by the organization and what capabilities those tools support

Cybersecurity Gaps

Gaps in the cybersecurity program that are not currently addressed by any of the tools in the cybersecurity portfolio

Cyber Portfolio Rationalization – Executive Summary Example

Objectives and Goals of the Project

- Highlight existing solutions where Microsoft E5 security products provide similar capabilities.
- Assess the capabilities and functionality of the overlapping Microsoft E5 security products to determine if they can meet the security requirements of CLIENT.
- Assess current tools against a industry recognized framework to understand where further gaps may exist and how they can be addressed using Microsoft E5 or other tools and solutions.

Key Outcomes

- Some strong security technologies are already present and in use but may not be fully utilized in their current capacity
- Using the NIST framework several gaps were identified which can be addressed by using Microsoft E5, other Microsoft products or through enhancement of available tools and solutions
- A number of capabilities and functionality of implemented solutions was found to overlap with E5 and non-E5 Microsoft solutions providing opportunities for cost and operational efficiency rationalization.

DISCLAIMER:

All results of the Portfolio Rationalization are based on technology, cost, contract and capability information provided in workshops by the client.

Our Approach

1. Data Gathering

Worked with CLIENT to collect current state information across a list of different security technologies.

2. Analysis

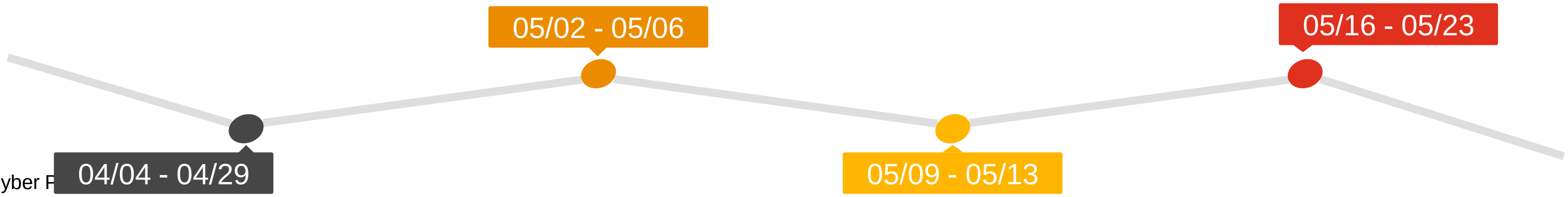
Used gathered information to conduct “what-if” analysis and identify how Microsoft technologies can help to address gaps and rationalize solutions.

3. Review

Microsoft E5 opportunities were reviewed to identify strong overlaps with existing security products.

4. Report

Develop documentation to recap key pain-points and opportunities as well as a high level roadmap representing a potential migration path to the Microsoft security products



3+ workshops held with CLIENT

Potential yearly cost saving of minimum about **400k***

25 security technologies considered

23 NIST security capabilities for holistic view

11 opportunities for rationalization

8 opportunities to transition to Microsoft E5 security solutions

3 additional opportunities for non E5 Microsoft technologies

17 NIST CSF capabilities can be enhanced with MSFT Security

* The estimated saving value only refers to saving opportunity expected from E5 rationalization options and is limited to cost information provided by CLIENT

Cyber Portfolio Rationalization Pricing Options

	Small	Medium	Large
Price	**€50k**	**€80k**	**€140k**
Complexity and Maturity	1. Business operating from a single region 2. Onprem / Single cloud 3. Mature understanding of security tooling 4. Dedicated enterprise security architecture team 5. Good understanding of total cost of ownership and contract duration	1. Business operating from a single region with multiple business units 2. Hybrid Cloud 3. Limited understanding of security tooling 4. No dedicated enterprise security team 5. Limited understanding of total cost of ownership and contract duration	1. Complex global organisation with multiple business units and data centres 2. Multi Cloud 3. No single view of security tooling 4. No dedicated enterprise security team 5. Limited understanding of total cost of ownership and contract duration
Approach	● Client accountable for completing data capture with support and input from PwC	● Up to 4 workshops driven by PwC with SME input to support data capture	● Up to 8 workshops driven by PwC with SME input to support data capture
Duration	● 3-6 weeks	● 4-8 weeks	● 6-10 weeks

Effort