How can a platform approach for cybersecurity reduce costs and streamline compliance efforts?

EY
Building a better working world

Microsoft

Despite tighter economic conditions and budgetary constraints, business leaders are still expected to protect the enterprise against persistent cyber threat actors while fully complying with an ever-growing list of regulatory requirements. These challenges can be exaggerated by accumulating overspecialized and duplicative tools that add cost and complexity. Instead, leading companies are turning to consolidated data protection platforms to remove duplicate tools, reduce reliance on highly specialized resources and increase program agility to engage the ongoing barrage of regulatory requirements.

In brief

- Leading companies are finding significant business value by migrating from a fragmented cybersecurity toolset to a consolidated data protection platform.
- Asking the right questions is the first step in increasing enterprise cybersecurity while also reducing costs, simplifying regulatory compliance and increasing agility.

According to the World Economic Forum: "Global cybersecurity and privacy regulations, while well-intentioned and seeking to contribute to the daily onslaught of emerging threats … creates complex and costly processes for compliance obligations across industries and makes it difficult for new innovators to become cybersecure." The cost of managing a complex attack surface, the scale and complexity of the cybersecurity tech stack and a skills gap are driving leaders to search for answers.

The hidden costs of specialization

Significant changes in the business and technology landscape have led organizations to accumulate specialized tools to manage newer use cases. The average large company commonly consumes 100 security products from 35 or more vendors. The result is a fragmented, and often redundant toolset that requires maintenance by a substantial operations team. When comparing point solutions, highly specialized tools look favorable on paper, but many desiring "best-of-breed" overlook the impact to operational overhead and total cost. Each incremental tool adds complexity and additional points of failure, increases skill set requirements and lowers program agility. Frequent business and regulatory changes require constant tool reconfiguration and adjustment, bringing organizations face to face with the actual cost of their hybridized toolset.

The average large company commonly consumes 100 security products from 35 or more vendors.

Driving efficiency and security through tool reduction

However, there is good news. The EY organization has helped organizations across multiple industries, achieving average savings of 10%-20% on cybersecurity tool licensing costs, while occasionally realizing savings of up to 35% annually. For other larger companies annual cost reductions are in the millions. Cybersecurity tool reduction is another key metric. In recent engagements we have helped clients reduce the number of tools by an average of 24%, while maintaining the same degree of security.

Potential results

24%

reduction in number of tools while maintaining same degree of security

The EY organization helps companies operating in a Microsoft 365 E3 or E5 environment generate these benefits by transitioning from a fragmented cybersecurity toolset to a cyber strategy that leverages Microsoft Purview and other Microsoft-integrated technologies. The EY organization has a proven and dedicated cyber team with deep experience in helping companies implement and operationalize Purview to reduce the cost and complexity of cybersecurity programs while maintaining compliance. With a clear picture of both the legacy tools deployed and the latest developments in the interconnected Microsoft environment, EY professionals provide a full view of which features have direct parity, partial coverage or are truly gaps to help ensure the development of realistic and executable cost takeout plans that avoid surprises while improving the full scope of security.

Navigating the transition

Together with the Chief Information Security Officer (CISO) and Chief Risk Officer (CRO), business leaders should objectively consider a platform approach with the following four questions in mind:

1. **What are the current pain points in my organization with respect to the security technology stack?** Maintaining multiple tools, integration complexities and establishing an operations team with the right skill sets can be a challenge. Multitool programs require greater effort to provide coverage for regulatory changes and business transformation initiatives. Purview streamlines updates by utilizing a unified data classification library applicable to the entire platform suite.
2. **How effectively is my organization incorporating already-licensed Microsoft Security products?** Microsoft has continued to enhance its cybersecurity capabilities and integrated use cases, and an increasing number of organizations have been integrating Microsoft into their cybersecurity programs, especially in the Purview/Data Protection space.
3. **What do we currently spend on security tools? How can I reduce total cost of ownership (TCO)?** License and maintenance costs, testing and integration costs, and resource costs can multiply across a highly hybridized environment. Organizations are leveraging Purview to simplify and optimize their security and data protection tool kits.

4. **Do our security capabilities provide adequate coverage of current and future on-premises and cloud data usage?** Increasing cloud service consumption and novel data use cases require data protection programs to continually review the coverage they are providing. The integrated data protection capabilities of Microsoft Purview allow for full visibility into your entire data estate. This includes structured and unstructured data, data handling processes, data stored on-premises and in the cloud. Coupled with the other Microsoft Product suites, Defender and Intune, Purview is a cornerstone product suite of the "trust but verify" Zero Trust Model that helps to ensure the strongest approach to data governance and information protection.

For the CISO, Chief Financial Officer (CFO) and CRO, a unified cybersecurity platform offers a variety of value-adding benefits. Operational costs and resource requirements are reduced. Speed to deployment in response to changing regulatory requirements is accelerated. And the cyber team can monitor and protect data security through a single pane of glass. Particularly important: Microsoft's suite of compliance tools makes it easier to comply with data protection regulations and avoid potential fines or disruptions.

Summary

Cybersecurity programs that can run cost effectively and still be compliant are a vital element of the board's concerns about corporate governance and accountability. Business leaders focused on the bottom line should look at cybersecurity programs not as a static expense, but as a cost that can be optimized with an appropriate data governance and compliance solution such as Microsoft Purview. The EY organization's service offering, aligned with Microsoft Purview's capabilities, can help companies transform data governance and compliance from a complex chore to an opportunity for more cost savings, valuable reporting, and accountability, as well as resource allocation that protects the company's valuable data assets.

Contact

Discover how the EY-Microsoft Alliance simplifies cybersecurity to help your organization transform with trust, reliance and resilience.

Nicole Koopman
Managing Director
EY Cyber Alliance Ecosystem Leader
nicole.koopman@ey.com

Authors

Varun Sharma
Principal
EY Americas Cyber Solutions Leader

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

2308-4312966

EYG no. 008663-23Gbl
ED None

ey.com