How does rationalizing cybersecurity tools enhance security effectiveness and efficiency?

EY
Building a better working world

Microsoft

Cybersecurity silos aren't scalable. Complexity adds costs and risk. Simplification is key to strengthening your enterprise cybersecurity posture and supporting the business.

In brief

- Companies strengthen their cybersecurity posture and optimize investment by migrating to an integrated cybersecurity tools platform.
- CISOs can become enablers of innovation while maintaining the security required in an increasingly challenging threat landscape.

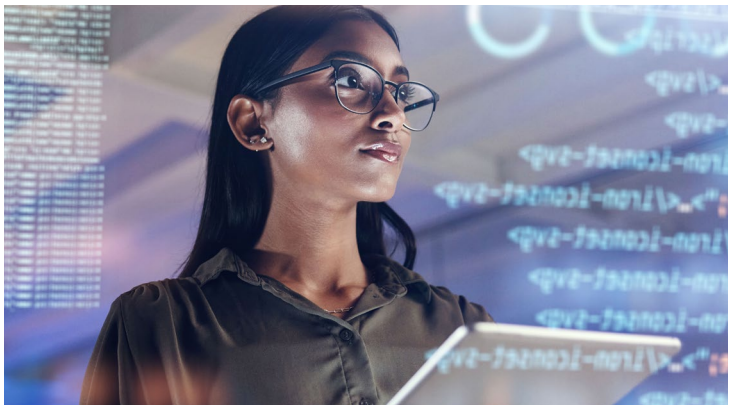
In our experience, many large companies deploy numerous tools from various vendors, often reaching 100 tools from 35 or more providers. This sprawl not only increases costs but also undermines agility and impacts the enterprise risk profile. In fact, many organizations waste significant portions of their IT and security budgets on redundant, underperforming, and complex security tools. Simplifying the portfolio of cybersecurity tools is a critical lever in increasing the value that the CISO can deliver to the business.

Where did all this complexity come from?

The root of complexity often lies in the historical approach of playing catch-up, where SecOps teams added security tools and processes on top of technologies to meet the demands that business leaders feel are critical to their mission. We often see business units "shadow IT" investments in SaaS solutions without fully considering the need for adequate cybersecurity or integration with the enterprise cybersecurity platform.

The unintended consequence of responding to business needs is a patchwork of technologies that are intended to provide a blanket of security over the entire computing landscape, but often failing to do so with cyber-attacks increasing and response times being alarmingly long. This prolonged response time makes the seams in the patchwork between technologies more attractive targets for bad actors.

Today's business environment is only getting more challenging for the CISO. Agility is critical to business success, so the cyber team is expected to adapt at the same pace as the business. The patchwork gets more complex, and, for threat actors, the seams become more attractive targets. Management teams at larger firms are expecting better results, better return on investment, better outcomes and greater resiliency from the billions of dollars that are being spent on cybersecurity technology, people and programs.



The business case for simplification

With the economic downturn and budgets coming under increasing pressure, it's an ideal time for the CISO to start finding efficiencies by streamlining the security tech stack while adding greater protection. We are seeing CEOs, CFOs, the board and regulators put more pressure on cybersecurity teams to demonstrate better outcomes and better returns on cybersecurity investment. The proposed Securities and Exchange Commission rules, titled "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," requires periodic disclosures on an organization's cybersecurity policies, risk management, and the board's expertise and oversight. This underscores the need for proactive cybersecurity risk management.

The traditional reputation of CISOs as gatekeepers ("just say no") is wearing thin and evolving. The C-suite seeks their expertise to move forward quickly and expects the CISO to be an enabler of agility. Embracing simplification paves the way for CISOs to meet these demands and contribute to the overall success of the business.

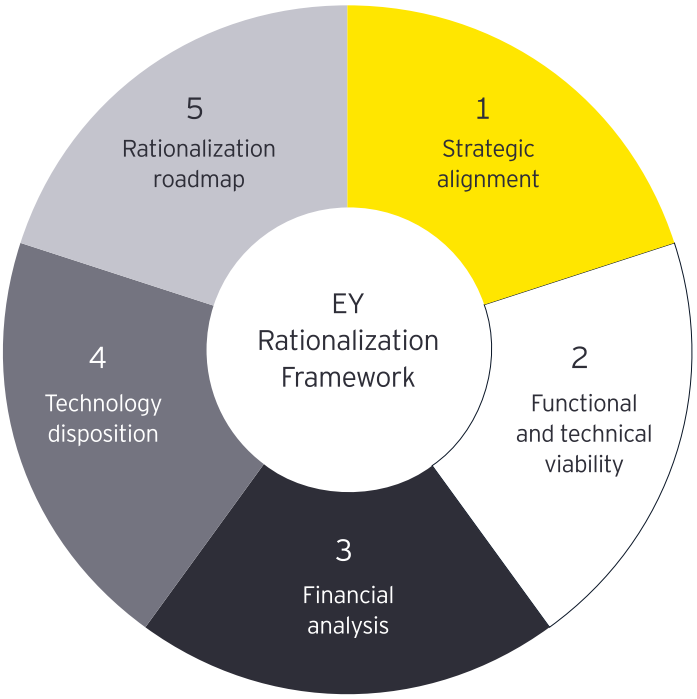
The simplification journey

This journey to security simplification won't come without challenges; it's hard to break old habits, particularly when executives rely on a patchwork of tools, believing that complexity leads to a better defense. But complexity doesn't necessarily equate to greater cyber protection, and spending smart is better than spending big.

Investment will be required over the course of the security simplification transition period as old tools are rationalized and replaced with a streamlined platform. Monitoring and measuring ROI throughout the transition is an essential best practice.

The EY Cybersecurity Tools Rationalization Framework offers a sound security simplification approach, consisting of five key steps with a data-driven analysis foundation, efficiently identifying optimization opportunities across all key business areas.

1. Strategic alignment: Build consensus among business, IT leadership, and the CISO to align cybersecurity costs with corporate strategy, improving the bottom line while serving stakeholders efficiently.
2. Functional and technical viability: Analyze current tools, map to intended functions, identify security gaps, and compare with simplified platform like Microsoft Security and Compliance.
3. Financial analysis: Examine total cost of ownership of cyber assets pre/post migration, including future efficiency, cyber resilience, and enterprise flexibility.
4. Portfolio rationalization: Utilize a security scorecard with pre-determined strategic, technical, and operational fit criteria to guide takeout decisions and gauge alignment with objectives and regulatory requirements.
5. Rationalization roadmap – A detailed timeline of workstream activities required to address prioritized simplification opportunities.



In our experience, large, complex companies find success in their journey when they have a trusted guide alongside. At EY, we help clients in navigating platform migrations through a business lens, always keeping the goal of incremental business value. Throughout the transition, we work closely with IT and business leaders to reduce operational disruptions and help ensure that new technology is adopted consistent with sector, country, and regional cyber and data regulations.

Summary

An unbiased, objective perspective is essential in reducing and consolidating spending on cybersecurity tools while also improving the enterprise's risk profile. The patchwork collection of cybersecurity tools found at many enterprises has become too expensive, cumbersome and vulnerable to attack. In contrast, a unified security stack of complementary tools can strengthen defenses while reducing total cost of ownership. Furthermore, a unified approach can help the SecOps team keep pace with the changing needs of the business, enabling security while integrating new technologies. To reach those objectives, however, the enterprise will have to make data-driven decisions about retiring old tools, which company to partner with, and ensuring that the benefits within reach are achieved.

Author

Dave Burg

Principal
Technology Consulting,
Cybersecurity

Ernst & Young LLP

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

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.

EYG no. 008571-23Gbl

2306-4267154
ED None.