The State of Cybersecurity Integrations

Balancing Tactical Requirements and Strategic Initiatives

2026



synqly™ | We Connect

Table of Contents

Executive Summary 4
Key Findings 5
The Tension Between Strategic and Tactical Decision-Making 6
Setup and Maintenance Drive Integration Complexity and Cost 9
- The Delay in the Setup Phase 9
- Establishing a Partnership 10
- Technical Preparation 10
- Use Case Development 10
- The Long Tail of Maintaining Integrations 11
- The Impact of Changes to APIs 11
- Repeatable Integrations 12
- Outsourcing Strategies 12
- Spotlight: The Emerging Role of AI 12

Breadth and Depth of Integrations Evolve with Product Maturity 13
- Spotlight: The Role of Standardization 14
- The Good: Integration Requirements for a Minimum Viable Product 16
- Spotlight: Improving Integration Value with Promotional Activities 16
- The Better: Data Enrichment for Actionable Detection 17
- The Best: Automation and Go To Market Expansion 18
- Spotlight: Access to Marketplace 18

Conclusion: Critical Success Factors 19



Executive Summary

Cybersecurity teams have been perennially challenged to manage a complex cybersecurity tool ecosystem that adds to operational overhead, a challenge exacerbated by the cybersecurity skills gap. Point-solution islands leave security teams struggling to harmonize inputs and outputs manually as they try to close the critical blind spots in the gaps between controls and disconnected tools.

Integrating these disparate controls is the cornerstone of fulfilling industry promises of convergence to platforms to improve both operational efficiency and accelerate threat detection and response. However, cybersecurity leaders find themselves leery of proprietary platforms that can create vendor lock-in when practitioners also want to use best-of-breed technologies to keep pace with their cyber adversaries.

Simultaneously, cybersecurity product leaders wrestle with the challenges associated with integrating disparate cybersecurity products. They must make difficult decisions about whether to allocate engineering resources to build integrations, especially when considering ongoing maintenance and potential depreciation over time. Some products teams take a myopic view of integration requirements, predisposed to viewing their product as the center of the cybersecurity ecosystem rather than focusing on customer-driven use cases.

Given these dynamics, there is much to be learned from vendors that have effectively balanced competing priorities, tactical and strategic, and managed organizational dynamics to deliver impactful integrations that meet market requirements.



Key Findings

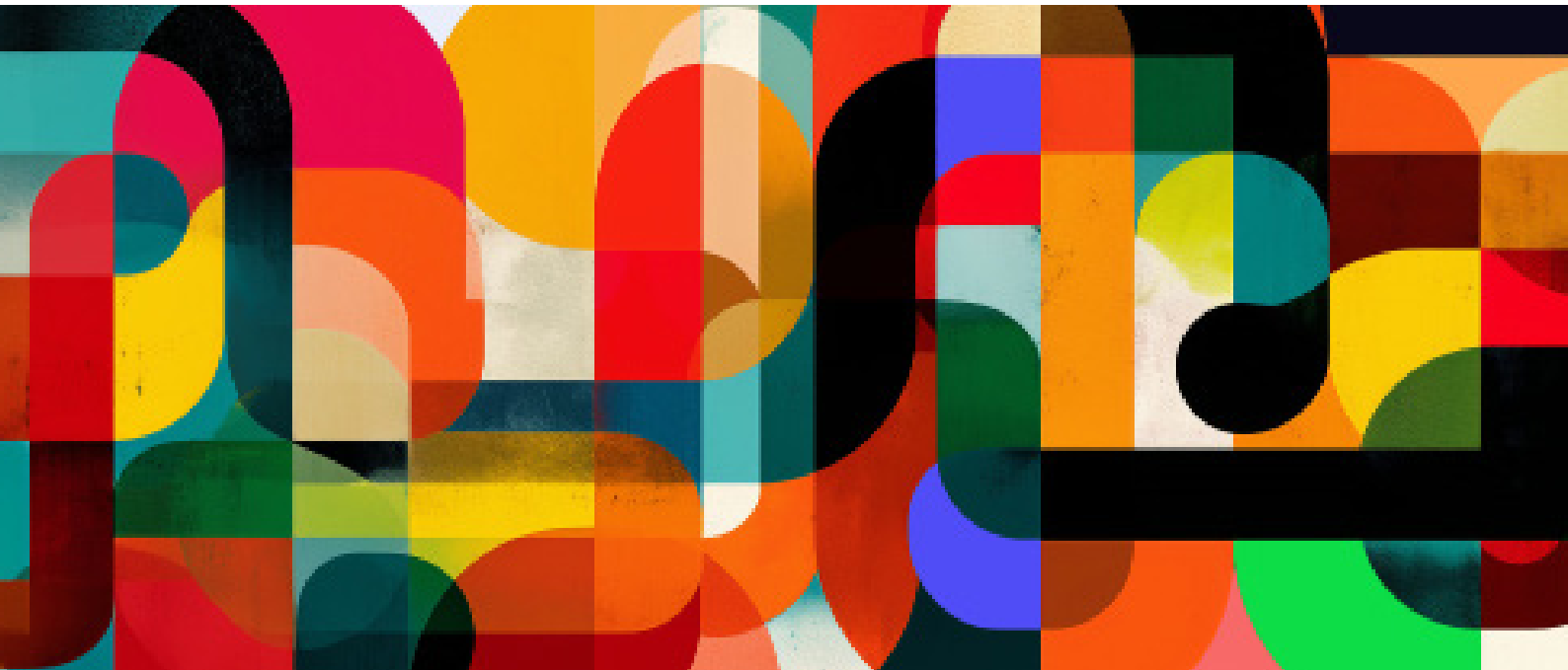
At the end of 2025, over a dozen senior leaders in product management, engineering, alliances, and executive roles from a representative industry cross-section responded to a series of questions about their companies' approaches to integrations with a focus on:

- Integration sources and prioritization
- Calculation and management of an integration's costs and benefits
- Experiences implementing third-party integrations
- Integration monetization and promotion for driving revenue and expanding into new markets

Across large-cap vendors and emerging startups, several patterns emerged in these responses with shared concerns and struggles across the segments:

- 7 of 13 (53.8%) believe that integrations should be strategic
- 9 of 13 (69.2%) mention sales or prospects as the driving force behind building integrations
- 6 of 13 (46%) mention partner alliances as the driving force behind building integrations
- 7 of 13 (53.8%) mention maintenance as a cost consideration for building integrations
- 4 of 13 (30.7%) outsource integration development

Cybersecurity product leaders view integrations as strategic business and revenue enablers, yet resource allocation is more often a tactical decision. From early-stage startups to large-scale market leaders, another theme emerged: the maturation of integrations over time includes functional enhancements to enable more advanced use cases, as well as deeper partnerships to expand market reach.



2

The Tension Between Strategic and Tactical Decision-Making

Perhaps the most salient learning from this study is derived from the first two questions asked of our respondents: the source of integration requirements and whether they felt their organization took a tactical or strategic approach to integrations. It was telling that all product leaders responded with an “all the above” answer to the first question probing the genesis of integration requirements.

All the product leaders we spoke with cited both near-term sales opportunities dependent on a new third-party integration as well as more strategic consideration including integrations to gain access to a partner’s marketplace, as drivers behind their approach to integrations. With the former source being tactical in nature and driven by the Sales team, and the latter sources being more strategic and driven by alliances, channels, and product teams, there are multiple internal stakeholders involved, creating challenging organizational dynamics for some of the vendors in our study.



This feedback serves as both the thesis statement for this report and a call to action for product leaders: **tactical and strategic drivers are not mutually exclusive**, and those vendors can close both tactical sales opportunities dependent on a new integration while also executing a strategic approach realize better near-term and long-term business results.

Problematically, however, when evaluating an integration's costs and benefits, most product leaders have little financial evidence to prove long-term value. According to the interviews, **nine of thirteen product leaders reported having no identified metrics to calculate value.** This inability to clearly quantify an integration's impact on revenue contributes to the tension between ad hoc tactical and strategic business decisions.

Without metrics, organizations are unable to define clear SMART goals for building integrations that would prove their value:

- **Specific:** One-offs based on individual requests without the ability to easily repeat integrations
- **Measurable:** Inability to measure usage or no time to measure usage because each API is uniquely built
- **Achievable:** Inability to scale development strategically
- **Relevant:** Lack of metrics linked to API use or ARR proving revenue impact
- **Time-bound:** Difficulties maintaining schedules when hiring third parties or diverting internal resources

For the product leaders who have metrics around an integration's value, the most common ones were:

- Capturing near-term revenue from the delivery of a deal-driven integration
- Integration-based pricing and packaging model.
- Improved Annual Recurring Revenue (ARR) metrics



SPOTLIGHT: The Impact of Integrations on ARR Metrics

Proving an integration's financial value is indeed a specific product leader pain point not only measuring in revenue contribution to date but also in championing further investments in third-party integrations. An obvious exception to this dilemma are products with pricing models based on data ingestion, although customer perception of such models as punitive are driving vendors to better align pricing units with value propositions. A few research participants who shared that their company can track the integrations in use in production environments noted that when two or more are in use they are "stickier".

Even though most cited a lack of a financial model to measure the return on investment (ROI) for integrations, all product leaders we spoke with agreed that integrations contributed positively to this notion of "stickyness". We discussed this dynamic in the context of Annual Recurring Revenue metrics, arguably the fundamental economic measurements of all technology vendors. There is an understanding that because subscription models put the onus on the vendors to deliver sustained value that integrations which enable compelling use cases can positively impact these business-critical ARR metrics:

- **Reduced churn:** Not only do integrations help reduce losing subscribers to below the industry standard of sub-10%, customer retention enables vendors to up and cross-sell integration-based offerings
- **Renewal rates:** Similarly, given the cost of customer acquisition, integrations also play a role in maximizing renewal rates into the desired zone of 90+% ARR expansion
- **Customer Lifetime Value (CLV/LTV):** Reduced churn, improved renewals rates, and the ability to expand monthly and annual recurring revenue from customers realizing value from integrations maximizes the revenue each respective customer provides over the lifetime of the relationship.

While these are all the fundamentals of ARR metrics, the actionable finding from the research is for those vendors lacking a financial model to measure the financial value of integrations is to put ARR-based instrumentation in place.



3

Setup and Maintenance Drive Integration Complexity and Cost

A clear and common theme from our respondents is that the time and cost associated with third-party integrations are born in the before and the after. That is, **while many shared that their development team could typically complete the technical work for an integration during a two-week sprint, necessary preparation work often resulted in an integration taking a full calendar quarter.** And as one respondent put it, there is then the long tail of care and feeding to maintain the integration.

The Delay in the Setup Phase

Integrations are, indeed, more than a deliverable for the development team and include deliverables for the alliances team as well as technical preparation for the engineering team. More specifically, most respondents noted that after an integration requirement is fielded, appreciable time is required to engage with that third-party vendor, prepare an environment, and develop use cases.

Establishing a Partnership

All research participants agreed that establishing a technical alliance was an essential initial step to assure not only the successful delivery of an integration but to maintain and support integrations as they get deployed into production environments. These were the basic aspects shared for establishing such a technical alliance:

- Identifying and connecting with the integration product's technical alliances contact who will then introduce their integration development lead
- Completing a legal agreement, typically a Technical Alliance Program agreement (TAP). An important element of a TAP is a Collaborative Support Agreement that provides the process and workflows for the vendors to work collaboratively to address any customer issues that may arise.
- Gaining access to a Not For Resale (NFR) environment to that integrations can be developed and test in a pre-production environment without risk of adversely affecting a customer's runtime environment

Technical Preparation

With a technical alliance now in place, development teams then prepare an environment with the following steps as they concurrently start to define functional requirements that enable key use cases:

- Review the APIs, logs, web hooks, and other documentation
- Set up the environment
- Run an anonymized test case of customer data if the integration involves a data exchange

Use Case Development

The feedback on authoring use cases varied and was another aspect of the tactical versus strategic issue. Some vendors noted they deliver a rudimentary level of integrations to meet the pressure of an in-pipe sales opportunity. Some noted, as discussed below, that such a "good enough" approach had limited appeal over time.

A more strategic approach, albeit more time-consuming, that one respondent called "discovery and shaping" includes:

- Spending time with the third-party product to understand its capabilities before writing the user story.
- Identifying the specific enriching data that enables a well-defined use case, a highly more efficient approach to ingesting irrelevant data
- Actively vetting the use cases with customers to ensure value while sometimes eliminating edge cases that fail to satisfy broader customer requirements. This is one of the key takeaways from the research that highlights the need to balance tactical requirements and strategic initiatives; **vendors who collaborated with a set of customers reported stronger adoption and stickiness versus edge use cases that were provided tactically for a specific customer and did not provide appreciable value beyond a discreet transaction**.

The Long Tail of Maintaining Integrations

Beyond setup and development costs, product leaders cited ongoing maintenance as time-consuming, expensive, and unpredictable. **In fact, twelve of thirteen respondents, 92%, shared that ongoing maintenance is a long tail, variable cost.**

The Impact of Changes to APIs

A primary contributor to the cost of maintaining third-party integrations is the fluidity of the APIs on which integrations are built. While one respondent felt APIs are stable because "APIs are built by developers for developers", a plurality of respondents felt that third-party APIs are too often a moving target. It was not surprising then that unanimously, respondents believed that finding a better way to handle API changes was essential to manage long-tail cost and assure continued seamless operation in production environments.

> *"APIs are a moving target, a very big pain point, and the single largest hidden cost of integrations."*
>
> *Raj Rajamani, former CPO, CrowdStrike*

Many interviewees discussed how such changes to APIs broke production deployments, created customer satisfaction issues, and increased long-term maintenance costs. Some of the challenges that these product leaders identified include:

- Failure to provide API change notifications.
- Failure to update documentation when making changes.
- Log format and schema changes require data remapping.

In addition to creating additional work for the development team, these issues too often created "downstream" production issues for mutual customers. To mitigate the maintenance challenges discussed below, product leaders emphasized the importance of collaborative support agreements with alliance partners to ensure functional continuity and continued customer satisfaction while reducing developer burdens.

Repeatable Integrations

In a few cases, product leaders explained that ingesting telemetry from third-party products to enhance detections was partially replicable within a security control category (e.g., access control or network security) after building an initial integration. However, many respondents noted that because disparate controls within the same product category (e.g., Endpoint Detection and Response) often tag telemetry with different metadata, data mapping to normalize the disparate inputs was still required for subsequent integrations within a product category.

Outsourcing Strategies

Across the respondents, some noticeable differences existed when discussing outsourcing's strategic implications. Some respondents shared that by outsourcing all integration work, they mitigate the ongoing impact on the engineering team, assigning setup, implementation, and maintenance work to third parties. Some felt that working with development firms that have experience with APIs allowed their internal teams to stay focused on core product enhancements. One respondent specifically noted that the company bifurcates outsourcing by managing primary strategic alliance integrations internally while assigning contractors for less strategic integrations. And yet other vendors opt to fund and staff internal teams dedicated to delivering integrations.

There are pros and cons to all approaches, underscoring the need to balance tactical requirements and strategic initiatives. Some respondents felt they needed to own integrations to vet, develop, and deliver use cases by interacting with end users. The product leaders whose companies viewed integrations as strategic felt they needed to foster a relationship with their technical alliance partners that could lead to joint go-to-market motions.

SPOTLIGHT: The Emerging Role of AI

Given these challenges, the promise of AI was mentioned by nearly all research participants as a key enabling technology for the future. While agentic AI-driven cybersecurity use cases offer exciting automation capabilities, successful implementations depend on rich integrations.

With the advent of the Model Context Protocol (MCP), organizations can expedite the initial delivery of integrations and keep pace with changes to third-party APIs. Using MCP to connect various AI agents, vendors can provide a variety of impactful use cases leveraging the combination of broader datasets and automation. Meanwhile, engineering and development teams can use the MCP to ensure concurrency with API changes to maintain continued functionality in production environments.

4

Breadth and Depth of Integrations Evolve with Product Maturity



Cybersecurity has long been viewed as a data problem, a reality that an expanding attack surface exacerbates, with security teams requiring more and more telemetry to enable high-fidelity threat detection. And changes to the Tools, Tactics, and Procedures (TTPs) employed by cyber adversaries highlight the increasing dependence on telemetry as malicious actors rely less on malware and more on manual intervention to achieve their objectives. To that point, according to Crowdstrike's 2025 Threat Hunting Report, 81% of hands-on-keyboard intrusions were malware-free, illustrating the need for robust data-driven detection capabilities.

These dynamics have further increased the need for product integrations that both enable detecting threats across multi, hybrid cloud environments and automate the response. Product leaders in our study identified two primary use cases for building integrations with an initial focus on the first representing an initial stage and the latter a more mature stage:

- **Detections:** Deeply integrated insights across complex user identity, infrastructure, and application misconfiguration, vulnerability, device security, network access, and other attack vectors
- **Automated remediation workflows:** Action-based incident response use cases that are more involved and include basic alerting and ticketing to kick off workflows, as well as remediation steps such as disabling and quarantining infected accounts and systems

Many security product leaders find that when making decisions about the integrations to build, they also must make decisions about the data that their solutions ingest or share.



> *Integrations should not mean being a dumping ground for data. It's about being prescriptive to enable specific use cases.*
>
> *Rajan Koo, CTO, DTEX*

Even more challenging, once security product leaders know the data that their solutions need to ingest, they struggle with the various data formats and schemas. 70%, 9 of 13 interviewees, called out a lack of an abstraction layer necessitating bespoke data mapping and normalization. Across all product maturity levels, the lack of standardized data formats and schemas creates a barrier to expanding integrations across solutions and security categories.

SPOTLIGHT: The Role of Standardization

Given the need for data mapping to normalize proprietary data formats to enable detection and follow-on automation use cases, all product leaders agree that standards have an important role to play. As such, there is near-consensus that the cybersecurity industry needs to continue to collaborate on a standard data format and schema for telemetry, similar to the way STIX and TAXII describe threat intelligence.

Respondents also shared various data normalization challenges that increase initial integration costs, delay delivery times, and compound ongoing maintenance overhead. While a few respondents expressed skepticism about using the Open Cybersecurity Schema Framework (OCSF) as a common schema, most believe that as it matures it offers a promising alternative to proprietary data models that can ease data normalization challenges and improve connectivity across ecosystem products.

In a product's early stages, creating a minimally viable product (MVP) that functions as intended is the primary focus. As customers begin to onboard the solution, the product team often finds itself split between adding new features to the core functionality and building integrations so that customers can optimize the solution's value.

At this point, security product leaders must make difficult decisions that can both expand and limit their ability to meet customer needs. Some of these challenges are technical, such as choosing which integrations will appeal to the broadest customer base. Some of these challenges are related to business objectives, mitigating the impact that integrations with competitors can have on future product roadmaps and revenue objectives.

Most security product leaders hinted at the convergence of a good-better-best or crawl-walk-run approach that applies to integrations, akin to a feature roadmap. However, the onus on evolving along such metaphorical phases is contingent on vetting use cases, often starting with basic alerting and achieving peak maturity with automation. These phases also, importantly, include go-to-market objectives and activities.



The Good: Integration Requirements for a Minimum Viable Product

At the early stage of an integration roadmap, most respondents noted that decisions around integrations related to their security category. For example, Human Risk Management (HRM) solutions and data lake-based Security Information and Event Management (SIEM) solutions rely on data ingestion to provide customer value. For these solutions, integrations are core to their MVP. At this stage, many security product leaders use integrations for basic security capabilities such as alert propagation or basic data integrations.

Some of the primary challenges that vendors providing this first stage identified include:

- Building partnership collaborations with engineers
- Gaining access to API documents
- Validating data
- Proactively identifying and fulfilling customer needs
- Building integrations for brand recognition and product footprint expansion by partnering with market leaders

SPOTLIGHT: Improving Integration Value with Promotional Activities

Across all respondents, product companies share a consistent set of internal and external promotional activities to support monetizing integrations, often externally promoting the integrations with the greatest strategic impact.

The marketing activities typically include:

- Press releases
- Technical content, including a reference architecture
- Webinars
- Customer marketing to promote new integration-enabled use cases

The sales enablement includes activities like:

- Communicating through the sales engineering team's Slack channel
- Using regular sales calls to connect with the entire team
- Providing information to channel partners
- Enabling sales to ask discovery questions about the prospect's use of the third-party product
- Allowing the sales engineers to discuss the use case and deployment models

All respondents agreed that the integrations that garnered more attention were the ones that included go-to-market investments. Organizations validated the value with ARR metrics, like increased customers using the integration or better renewal rates with the product more tightly integrated into their environments.

The Better: Data Enrichment for Actionable Detection

At this stage, security product leaders look to leverage deeper integrations to grow the solution's capabilities to expand the addressable market. Often, decisions are tactical, using customer-driven requirements to win deals. However, this approach may represent limited use cases that have little impact on future deals and allocate resources ineffectively. Many of these integrations focus on improving data, typically enrichment that includes correlation for higher fidelity, actional analytics, and alerting.

Some of the primary challenges that respondents at this level identified include:

- Aligning with product roadmap to reduce customer confusion and limit conflict with potential competitors
- Identifying the product's location within the larger cybersecurity technology ecosystem
- Aligning goals with partners to improve overall outcomes
- Identifying integrations that expand the product portfolio
- Defining use cases to ensure customer and product team alignment and eliminate scope creep
- Identifying key partners with trending products whose technologies will enable joint selling

At this level, promotional activities expand slightly, often including account mapping and joint selling.

> *If cybersecurity vendors are just thinking about checking a box they're missing an opportunity. A good PM will think about the differentiated value a deeper integration can bring customers. For example, data enrichment versus just importing data.*
>
> *PJ Kirner, Founder, Illumio*

The Best: Automation and Go To Market Expansion

In the final stage of maturity, security product leaders have moved toward taking a more strategic approach that maps to business objectives, responds to automation needs, and expands buyer personas. At this level, security solutions can evolve to respond to the more involved action-based use cases. Such evolved integrations are, from an end-user and customer experience perspective, more native vies–a-vies a more tightly coupled user interface that looks and feels the same as the original product and, importantly, often incorporating automation for remediation activities.

As customers expand their buying teams, stakeholders from other business functions need integrations with cybersecurity-adjacent technologies to create value for new buyer personas, like DevOps or SecOps. While many requested use cases come from customers, service providers also work with their own security operations center (SOC) to define, vet, and test integrations. Often, these use cases start with proof-of-concept functionality before becoming product offerings.

As the integration strategy matures, the go-to-market level expands, enabling deeper integrations that support reselling, OEM, or licensing agreements. These go-to-market partnerships often include broadening integrations across the partners' portfolio, with multi-product integrations from hyperscalers often tied to marketplace access.

SPOTLIGHT: Access to Marketplace

Increasingly, end users prefer to procure products using the online marketplaces operated by their strategic technology providers, like AWS or Microsoft. For those providers, marketplace purchases deepen the customers' involvement with the ecosystem and provide a revenue stream from partners. Meanwhile, the partners can expand their access to the technology providers' customer base to improve revenue.

54%, 7 of the 13 respondents, cited accessing a partner's online marketplace as a core integration driver.

However, the marketplace promotion and co-selling levels often depend on how deeply a product is able to integrate into a technology provider's overall product portfolio. Since these large technology providers can have a deep, varied product portfolio, building and maintaining a separate integration for each becomes costly and time-consuming, further necessitating a path to monetization.

Conclusion: Critical Success Factors

Security teams and security product leaders are on parallel paths, with **integrations sitting at the intersection of the security team's visibility needs and security vendor's recurring revenue objectives.** And while cybersecurity practitioners also require integrations to address the complexities associated with tool sprawl, cybersecurity product leaders must assess how to leverage integrations as part of their product platform strategy. However, no "one platform to rule them all" exists because organizations have different needs, risk profiles, and environments. Instead, many companies will build an archipelago of clustered security and IT operations tools to achieve operational and efficacy benefits.

These market dynamics require security product leaders build integration strategies to achieve the product maturity necessary for sustained revenue growth. One interviewee explained that integrations at their company were "undervalued" and that the product team, especially engineering, didn't always appreciate the strategic nature of some integrations." A one-off, tactical integration to entice a large customer will be a long-term cost center. However, when viewed as part of the larger product roadmap, integrations enable customer retention and build partnerships.

For smaller vendors and emerging leaders, integrations represent a seat at the table and greater relevancy. As one research participant commented, "Integrations are a necessary evil at worst, and a strategic multiplier at best." At worst, building integrations is a cost of doing business and closing a deal. At best, integrations enable security product leaders to expand their market reach by promoting their solution to their partners' customer bases. within customers' broader cybersecurity ecosystem.

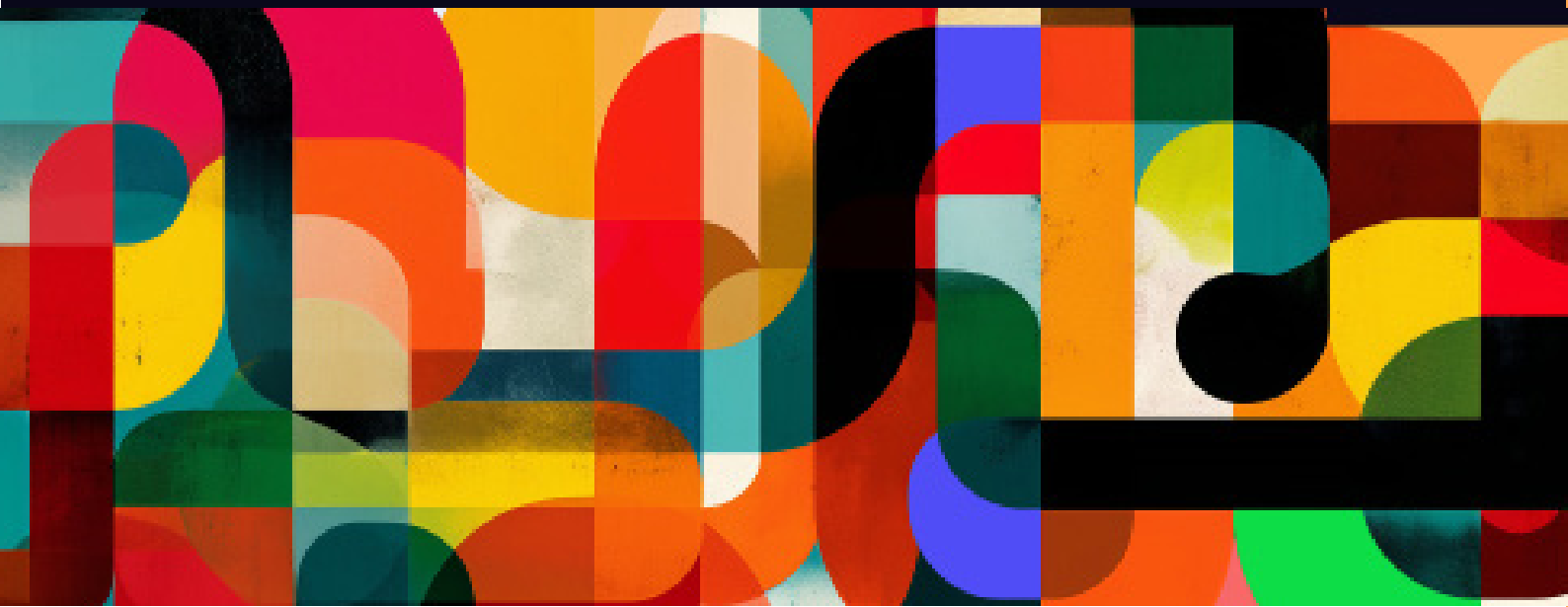


Vendors that can monetize their integrations can build entire revenue streams around the connections, either pricing by API call or data ingestion. This means that for larger vendors, integrations enable them to leverage a platform strategy as a market aggregator to generate revenue.

The charter then embarks on a successful integration strategy with repeatable processes that operationalize integrations and establish key performance indicators. When asked about building such an integration strategy, respondents who viewed their approach a success identified the following activities as critical success factors for evaluating, championing, promoting, and ultimately, monetizing integrations:

- Establish formal programs, like a Technology Alliance Program (TAP)
- Foster a strategic view of the impact of integrations on ARR
- Keep eyes wide open on how to manage integrating with competitors
- Be mindful of the need for an abstraction layer for repeatability
- Monitor shifting APIs and the potential for negative downstream customer impact
- Craft a good-better-best roadmap based on customer vetted use cases
- Crawl-walk-run investments in partner go-to-market promotional activities, sales enablement, or co-selling to maximize integration related revenue contributions
- Seek an approach to integrations which both accelerates time to market while reducing the on-going maintenance cost
- Focus on use case development that provides a customer-centric view of the cybersecurity ecosystem

These best practices shared by our research participants will help guide product leaders at startups, emerging market leaders, and publicly traded companies balance tactical requirements and strategic initiatives and deliver on the collective industry mission of enabling security teams to better protect their organization against a range of threats.



About the Author



Doug Cahill

Doug Cahill is a cybersecurity industry veteran with over 25 years of experience across the cloud, host, and network security domains. He most recently served as Senior Vice President of Analyst Services and Senior Analyst at TechTarget's Enterprise Strategy Group (ESG), where he led the firm's cybersecurity practice and go-to-market consulting for nearly a decade.

Prior to joining ESG, Doug held executive leadership positions at high-growth security startups. He served as CEO of Threat Stack and Vice President of Business Development at Bit9 (now VMware Carbon Black). His career also includes strategic roles at Hewlett-Packard and AppIQ, spanning product management, marketing, and strategic alliances.

Synqly is The Connected Platform for Security, IT, and AI.

Built from the ground up for OEM and enterprises, Synqly's patent-pending data orchestration and normalization layer streamlines product integrations, leveraging a unified API. Synqly delivers the secure integrations that customers demand, continuing to set the standard for scalable and efficient integrations across the industry.

Contact
hello@synqly.com
Synqly.com

synqly™ | We Connect

© 2026 Synqly, Inc. All rights reserverd.