synqly™

WHITE PAPER

Solving the Cybersecurity Integration Burden

Reduce Costs, Complexity, and Engineering Fatigue

Contents

Introduction

Between 2014 and 2022, the enterprise security stack grew by a staggering 760% in purchased solutions[1], creating an overwhelming tech sprawl that demands integrated products. To use and operationalize these tools effectively, organizations need trained security professionals and a way to integrate them. To effectively operationalize the wide variety of security tools, organizations of all size require both skilled professionals and reliable integrations. But the ongoing skills gap and limited vendor support for comprehensive integrations mean teams struggle to achieve a fully optimized security environment. In a recent Gartner survey of corporate security teams, 81% of respondents indicated a strong need to integrate security products. Since vendors struggle to support an integrated architecture, many security teams cannot optimize their investments.

Seamless integrations between security products aren't just nice; they are fundamental to extracting maximum value, streamlining data management, and creating a secure environment. Organizations typically respond by either building integrations internally, outsourcing development, or adopting an Integration Platform as a Service (iPaaS). However, each of these approaches comes with distinct trade-offs related to costs, complexity, and resource allocation. For vendors, the pressure to provide these seamless integrations often clashes with the relentless demands of core product innovation. Ultimately, the burdens fall to development teams juggling resource requirements in a complicated space.

Cisco's SVP and Chief Information and Security Officer Steve Martino succinctly captures the customer perspective:

> “*I don't want to spend my time integrating security products., I just want to do security. I tell my team I want to see three things when it comes to a new product:*
>
> - *Make sure it works*
> - *Make sure it gives me complete visibility*
> - *No black holes*
> - *Make sure it's integrated with the rest of our security ecosystem*[2] ”

To better understand the opportunity and impact of a scalable integration strategy, this paper will cover the pros and cons of internal builds, outsourcing, and adopting IPaaS platforms to address growing cybersecurity integration challenges. It will also highlight use cases and key considerations for each.

The Cybersecurity Integration Challenges

Any organization evaluating how to best integrate their security stack typically weigh three primary options:

- **Internal Builds:** Leveraging internal resources and expertise, ensuring control but straining already limited development resources.
- **Outsourcing Integrations:** Contracting third-party developers, freeing internal resources but with compounding costs and maintenance issues.
- **Integration Platforms (IPaaS):** Adopting specialized third-party platforms designed to simplify and accelerate integration development and maintenance that can be hosted, run in your environment, or in your customer's environments.

Understanding these trade-offs is crucial for making strategic integration decisions aligned with organizational needs, budgets, and capabilities.

Security vendors face unique challenges as they strive to deliver seamless integrations while maintaining core product innovation. Regardless of the integration approach selected, development teams grapple with common issues. At a surface level, these teams face issues including:

- **Resource Constraints:** Product and R&D teams typically prioritize core product capabilities, leaving limited internal resources for integration development.
- **Costly Outsourcing:** Relying on external developers is expensive and time-consuming, often leading to delayed integration rollouts.
- **Maintenance Issues:** Once built, integrations frequently suffer from neglect due to a lack of allocated resources for ongoing maintenance.
- **Support Challenges:** Customer support teams often lack visibility into integration usage, failure points, and user impact, complicating troubleshooting efforts.
- **API Complexity:** Learning the nuances of every product API, especially where security solutions are not API-forward and not broadly supported, increases the cost and time required.

The availability and maturity of integrations can heavily influence a customer's perception of a cybersecurity offering. Buyers may start by assessing a solution's core features, but their final decision often relies on whether it functions within their larger enterprise architecture. Tool adoption decisions frequently hinge on which vendor's product easily integrates into an organization's existing workflows and systems. A robust integration stack goes beyond supporting product performance; it serves as a competitive differentiator and a sign of a company's maturity.

All organizations face the same integration challenges. Every company needs to implement security measures to protect sensitive corporate and customer data. Security vendors face additional challenges beyond their own security. A vendor's security solution must integrate easily into their customers' overarching security stack.

From a high-level security perspective, many organizations must decide whether to build their own integrations or outsource that function. Meanwhile, security vendors must make strategic decisions about which integrations to provide customers and how those integrations impact overall revenue. Organizations and vendors need a solution that solves both challenges to build a robust security infrastructure.

The Complexities of Building and Maintaining Cybersecurity Integrations Internally

Building an in-house cybersecurity integration solution has long been the standard approach for many organizations. Leveraging the skills of in-house developers and software engineers, organizations seek to connect all their disparate IT and security technologies so they can ingest, normalize, correlate, and analyze the data necessary to gain insights into their security.

For these organizations, the integration costs start even before development, as companies must obtain licenses to target products and stand these up in lab environments. It then continues with reallocating staff away from core projects. After completing the integration's build, the organization then needs to consider the maintenance costs that begin to accumulate, including:

- Minimizing security risks related to code leakage
- Maintaining complete control over customization
- Seamless integration with existing systems, allowing companies to get exactly what they need without compromise

While internal development avoids immediate external costs, the long-term resource drain can outweigh the advantages.

A Deep Dive into the Ocean of Integration Costs

As divers descend deeper into the ocean, they reveal a vast new world of sea creatures that hide in the dark depths. In many ways, the cost of building integrations internally is the same. The deeper into the process the organization dives, the more it finds new, unexpected costs.

Developing the Integration

Building an integration creates costs, and these costs initially seem to be part of daily operations. And organizations believe they can save money by using existing staff. But by reallocating staff from core product and development work to build any number of integrations, the organization slows down the time to market for its core products and services. Whether developers build customer-facing or internal applications, moving engineers to integration projects means they have less time to spend on their primary job function.

Any organization considering building an integration internally needs to consider additional development costs that can include:

- Developers learning the nuances of every security product's API
- Code and security testing
- Running continuous quality assurance throughout the development process

Continued Availability and Reliability

An integration is only as good as its availability. A service disruption between a security tool and its data source can impact security alert fidelity and create blind spots that can lead to a data breach. Without monitoring availability and uptime, reliability can plummet. A single API change or vendor disruption can have a ripple effect across the security and enterprise IT ecosystem.

While continuous testing can prevent such issues, this process creates an administrative burden as it requires:

- Deploying integration software in a lab environment
- Writing end-to-end tests against it
- Dealing with often flakey and unreliable testing processes
- Documenting the testing processes to comply with data protection requirements

Security and Privacy Concerns
Integrations often transmit sensitive data between systems, raising concerns about access control, encryption, and data privacy. While solutions like access tokens and secure credential vaults can mitigate these risks, implementing them adds to the architecture's complexity and requires a long-term support commitment.

Hosting architecture is critical in ensuring integrations function within secure, regulated environments without exposing sensitive data or creating compliance risks. Engineers must often design integrations whose data protection capabilities comply with strict regulations like FedRAMP, GDPR, and other regional regulations.

Ensuring an integration's security and mitigating cybersecurity risk for all parties extends beyond simple encryption. It requires a comprehensive approach that includes:

- **Code and Infrastructure Security:** Integration code and underlying infrastructure must withstand attacks through secure coding practices, regular penetration testing, and vulnerability assessments.
- **Data Storage and Encryption:** To mitigate unauthorized access risks, stored data protection must include encryption enforced in transit and at rest.
- **Regulatory Compliance:** Integrations must align with frameworks such as GDPR for data privacy, FedRAMP for government-related cloud services, and other relevant security certifications.
- **Credential and Token Management:** Integrations must securely store credentials, with token expiration and rotate policies enforced to prevent misuse. Organizations must create systems to simplify token and credential management, as incorrect and deleted credentials and tokens are one primary cause of integration breakage.

All organizations must ensure their environments remain secure even as they integrate diverse security tools into their stack.

Data Inconsistency and Synchronization Issues
Unique vendor APIs and data schema often create inconsistencies and synchronization problems when integrating different systems. Without proper data mapping, these errors significantly increase organizational costs.

The failure to align various platforms hinders data flows and communication between systems, so any new data update can increase data discrepancies, introduce errors, and delay security responses. Organizations need standardized, structured approaches for security data normalization and exchange, prompting the creation of vendor-agnostic frameworks like:

- OCSF (Open Cybersecurity Schema Framework)
- STIX (Structured Threat Information Expression)
- TAXII (Trusted Automated Exchange of Indicator Information)

However, as organizations remain slow to adopt these standards, many navigate a landscape of inconsistent data sharing that increases effort and costs as they try to build the seemingly out-of-reach seamless security tool.

Navigating Integration Challenges in Cybersecurity

Security vendors may refuse to build integrations for smaller tools even when no business competition exists. Building these native integrations is expensive for the security vendors. They need to manage the development, reliability, and maintenance for each integration they provide. While early-stage companies may invest over $175,000 annually to build out their initial integration programs, late stage and public companies integration investments often exceed $1 million annually. Each integration approach presents distinct advantages and considerations, with trade-offs that depend on the organization's resources, priorities, and long-term goals.

Outsourcing Integration Development
Outsourcing integration development enables internal teams to focus on core product innovation while leveraging third-party providers' expertise to handle integration workload. While organizations often tout cost savings as a financial benefit, recent analysis shows that organizations only achieve around 25% savings over three years versus hiring an internal development team[3].

Operating and Financial Challenges
Outsourcing is a partnership that relies on establishing a strong foundation of trust and alignment between the external developers and internal teams. To gain the full benefit from the outsourced integration partner, organizations must have clearly communicated:

- Requirements
- Expectations
- Timelines

Further, organizations must have a shared, clear understanding of scope, including technical specifications like

- API integrations
- Data flows
- Security protocols

Outsourcing is far from a set it and forget it process. Organizations must maintain a collaborative relationship throughout the development process to mitigate potential misalignments. Meanwhile, internal quality assurance resources must:

- Test integration quality
- Review delivered code
- Evaluate the integration's security

These management costs increase the overall financial investment for each integration. All organizations must factor these hidden costs into their purchases during procurement.

Operational and Security Risks
Outsourcing often means losing direct control over the code's quality during development and lacking support following release. For all organizations, this lack of control creates operational and security risks arising from:

- API changes that can disrupt security monitoring.
- Creating and updating clear, per-product integration documentation across all updates and releases.
- Ensuring users understand setup requirements, authentication scopes, and connection details.

Outsourcing Considerations

- Is there a dedicated budget for initial development and ongoing management costs that also accounts for potential scope creep, maintenance, and security compliance?
- Are there enough staff to manage the outsourced relationship, including overseeing progress, ensuring quality control, and addressing any issues, adding to overhead.
- Is there internal staff to review and monitor for potential data security risks, including reviewing the integration's source code and all dependencies?
- Will the organization be able to meet its time-to-market needs, including finding an outsourcer, negotiating a statement of work, building the integration, and then doing internal QA on the integration? It is a process that can take as long or longer than internal development.
- How does the organization plan to maintain and support the integration when maintenance and updates are not part of the SOW and minimal support is provided in delivered products?

Integration as a Service Platforms
Integration as a Service Platforms (IPaaS) bridge an organization's security needs and a security vendor's business strategy. Initially focused on business-to-business (B2B) SaaS applications, traditional IPaaS vendors streamline integrations across the enterprise IT environment, enabling interoperability across business operational applications like CRM, HRM, and ERP systems. While some IPaaS maintain limited security product integrations, very few actually address the high security and compliance requirements that come with addressing the needs of security and IT Ops.

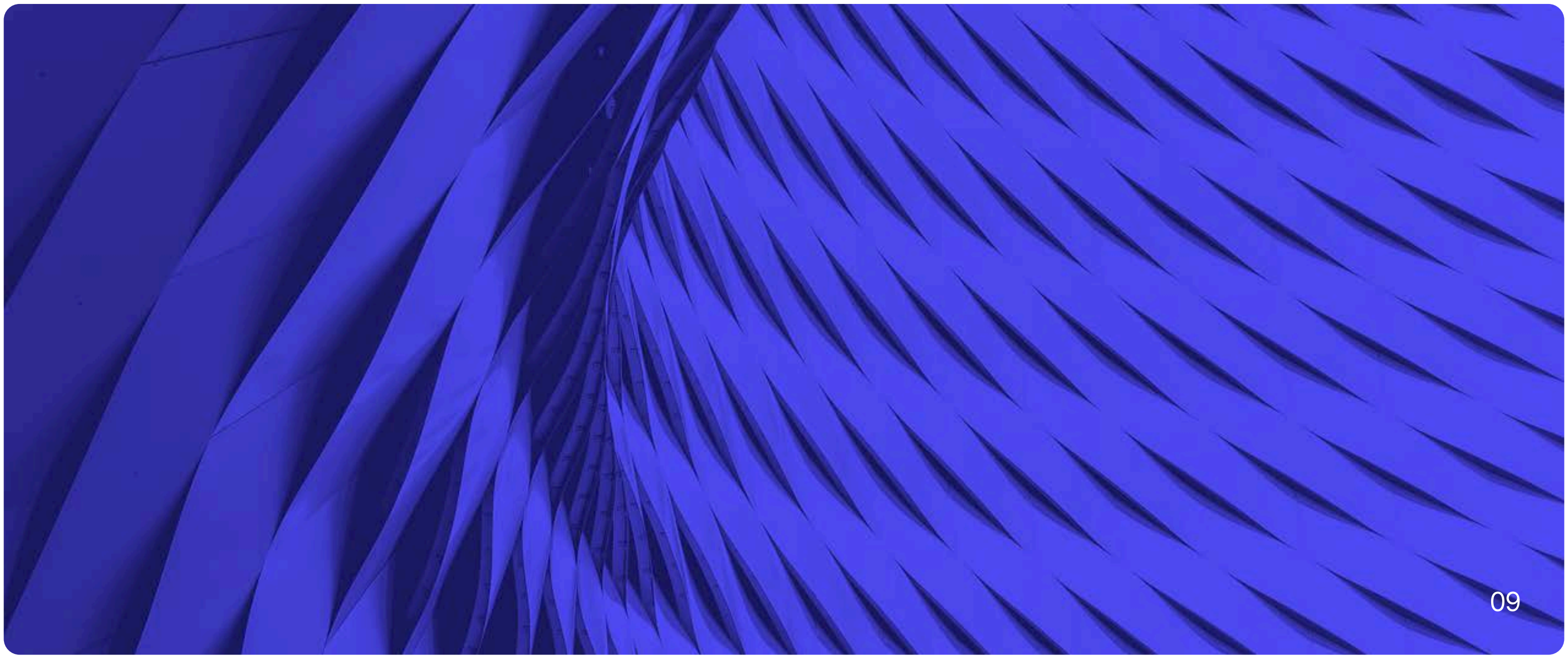
Security-focused IPaaS solutions offer a new opportunity to address complex compliance and security need while supporting business growth. Organizations must ensure that the IPaaS they use truly understand security and IT Ops use cases and are architected accordingly.

Cybersecurity is a distinctive niche within the larger IT function, and organizations must review an IPaaS to determine whether it:

- Operates across public cloud, private cloud, and on-premises environments
- Integrates security and IT operations products running in public cloud, private cloud, and on-premises
- Never stores customer data
- Provides multiple options for management of customer credentials – in the IPaaS vendor's cloud, in the IPaaS customer's cloud, and the enterprise environment
- Implements appropriate security controls to comply with data protection and cybersecurity compliance requirements

Cybersecurity Integration as a Service Platform Considerations

- ✓ Does the IPaaS deliver seamless integrations across a wide range of security tools, including SIEMs, EDRs, identity platforms, ticketing, and cloud security solutions, among many others?
- ✓ Can the IPaaS scale to meet evolving cybersecurity and IT ops needs?
- ✓ Can the IPaaS connect with a broad set of products through a single Integration to prevent building the same integration repeatedly?
- ✓ How well can the IPaaS streamline the integration process?
- ✓ Can the IPaaS reduce development time from months and years down to weeks or even days by providing pre-built connectors and automation tools?
- ✓ Does the IPaaS manage ongoing maintenance, updates, and security patches to free up internal development resources?
- ✓ Does the IPaaS support growing data volumes, evolving security needs, and expanding application ecosystems without requiring extensive rework?
- ✓ Does the IPaaS come with built-in security features like encryption, role-based access control, and compliance certifications, like SOC2 and ISO 27001?
- ✓ Does the IPaaS provide visibility and Metrics for proactive support with faster time to issue resolution?
- ✓ Does the IPaaS support bi-directional integrations, allowing vendors to query data from different systems, push data and alerts to these systems, and take appropriate actions such as forcing a password resent or quarantining an endpoint?
- ✓ Does the IPaaS solution support integrations to products that run in a public cloud, as well as in a private cloud or data center?



The Need for Cybersecurity Specific Integration Platform

While traditional IPaaS providers offer a wealth of options, the capabilities may not align with an organization’s current and future security needs. The traditional IPaaS intends to support traditional tools. To overcome these challenges, organizations should look for a specialized cybersecurity-focused IPaaS that focuses on supporting security tools.

With over 20,000 security and IT Ops products offered by over 9,400 vendors, traditional IPaaS providers do not have the bandwidth, focus, or capability to scale and meet security and IT operations teams’ needs. As the security landscape evolves, using a traditional IPaaS provider creates significant challenges around differences in:

- Security requirements
- Data access and storage policies
- Encryption standards
- Architectural demands

These limitations hinder organizations from achieving the agility and efficiency required to maintain robust, scalable integrations.

A cybersecurity-focused IPaaS acts as the bridge that both organizations and security vendors can use for a cost-efficient, secure solution to their integration challenges. A cybersecurity-focused IPaaS is a transformative abstraction layer that acts as a unifying force providing:

- Scalable and secure integrations
- A wide range of security and infrastructure products
- A single API, built on a platform designed to handle critical data.

This layer eliminates the need for cybersecurity vendors to learn every API while simplifying integration and promoting harmony between cybersecurity and IT operations tools. A cybersecurity-focused IPaaS streamlines security and compliance requirements by consistently applying and enforcing:

- Standardized access controls
- Encryption
- Data governance policies

Ultimately, an IPaaS enables vendor engineering teams to focus on the core product capability for long term, positive impact to the business.

Choosing the Right Cybersecurity Integration Approach

The proper integration approach for any cybersecurity alliance requires a strategic approach that balances financial impact, technical investments, and the final outcome. Companies must carefully evaluate potential integration options by asking two questions:

- Will this approach deliver the outcome both parties need in a reasonable timeframe?
- Does this opportunity have a strong return on investment for all parties involved?

Equally important, all parties must be aligned on how the proposed integration supports broader business objectives and operational needs with technical capabilities that enable seamless, secure, and efficient data connectivity across an integrated ecosystem.

IPaaS: The Future of Seamless Security Integration

Over the past twenty years, cybersecurity vendors and their customers have struggled to find common ground. Organizations need to scale their security stack to respond to the changing threat landscape, which may mean purchasing tools from multiple, historically disconnected vendors. Ultimately, without the ability to integrate their technologies effectively, they still have security blind spots.

Vendors struggle to scale to the meet customer needs, especially when it means a security tool outside their niche. While they choose partners and build alliances, they still face challenges trying to product integrations at the speed and scale that their customers need.

A security-focused IPaaS, like Synqly, is the technology glue that allows vendors to focus on their specialties and organizations to build customized security technology stacks.

These strategic assets enable cybersecurity and IT ops to align technology, product development, and revenue generation goals. By simplifying integration management, IPaaS addresses the key challenges – from concept to maintenance - that engineering and product leaders face with every integration project.

Demand for integrations and alliances increases as the cybersecurity and IT Ops solution landscape expands. For 9,400 security and IT Ops vendors to scale to address these customer needs, they must invest in integrations with a strategic approach that balances technical agility and business priorities. As vendors and customers alike increase their security stack and product lineup year over year, integrations have moved from a luxury to a must-have for businesses as small as Seed Stage to as large as IPO. The need for seamless, scalable, and secure integrations is a critical success factor for vendors and their customers.

IPaaS enables cybersecurity teams, IT operations teams, and their vendors to effortlessly create a robust enterprise architecture with unprecedented speed and accuracy. Integration platforms enable vendors to remain competitive in a crowded market by allowing them to focus on their core value. Meanwhile, security and IT operations can help organizations differentiate themselves with a more robust security posture.

Synqly's IPaaS enables cybersecurity, IT Ops, and security vendors to collaborate more effectively and efficiently by enabling them to build, manage, and scale integrations at a pace that matches current demand. By leveraging an integration platform built specifically for the security industry, all parties gain the speed, accuracy, and flexibility needed to support evolving security architectures, without sacrificing internal resources or business strategies.

Ready to build a healthy, reliable security technology stack relationship?

Learn more at Synqly.com

About Synqly

Synqly is the first AI-enabled Integration Platform-as-a-Service (IPaaS) purpose-built for Cybersecurity, IT Ops, and MSSPs. Our single API streamlines integration development, reducing costs and complexity by up to 90%, without overburdening engineering teams. Synqly's abstraction layer eliminates the need to manage multiple APIs, enabling rapid, seamless integrations across cybersecurity and infrastructure ecosystems. With continuous performance monitoring and Multiplex Connectors, vendors can deploy and maintain integrations faster, ensuring scalable, efficient, and future-proof security integrations.

synqly.com

[1] Cisco. Cisco 2018 Annual Cybersecurity Report. Cisco, 2018, www.cisco.com/c/en/us/products/security/security-reports.html

Panaseer. Security Leaders Peer Report. Panaseer, Jan. 2022, www.panaseer.com/research-reports/

Ponemon Institute and IBM Security. 2020 Cyber Resilient Organization Study. IBM Security, 2020, www.ibm.com/security/data-breach

[2] Cisco. *UK CISO Benchmark Report 2020*. Cisco, 2020, https://www.cisco.com/c/dam/global/en_uk/solutions/security/UK-CISO-Benchmark-Report-2020.pdf

[3] DAC Digital. "IT Outsourcing Costs: How Much Does It Cost to Outsource Software Development?" DAC Digital, https://dac.digital/it-outsourcing-costs-how-much-does-it-cost-to-outsource-software-development/