Fast, Flexible, *and* Sustainable: Bringing *"and"* to Cybersecurity

Automation and orchestration are the trend in cybersecurity operations, but different integration models leave organizations choosing among speed, scale, and time to value.

Organizations already have significant investments in network management, security, and defense products. These products have been purchased over time to meet changing requirements and address changing threats and risks, and they are often updated by vendors to have new or advanced capabilities that organizations are not able to use.

The desire to improve the efficiency and effectiveness of operations centers, analysts, and administrators has led to an ever-growing market of orchestration platform providers. These platforms automate and orchestrate tasks, processes, actions, and operations. They attempt to integrate all your existing investments into one fully functional, adaptive cybersecurity machine. It's too bad that the result often looks more like a game of mousetrap than one of those high-end intelligent buildings. This is because the products these platforms are trying to integrate were not designed, purchased, or deployed with this type of integration in mind.

The good news is that buyer awareness and smart purchasing practices can minimize trade-offs and make the most of new cybersecurity investments.

Previous Investments Can Limit Effectiveness

Vertical integration, proprietary interfaces, and limited-access partner agreements all continue to limit the ability to integrate, and take advantage of, the security tools that organizations *have already bought and deployed.*

Vertical Integration

The business model of tightly integrated, single-vendor tool suites originally offered organizations capabilities that were both automated and sustainable by design. Once customers had bought in, minimal incremental investment in new tools from the suite often provided a quick advancement of overall capability. Over time, it turned out that there was a cost to buying into this business model. No one vendor provides all the tools and products that an organization needs to implement cybersecurity technologies and operations, although certain industry takeovers and buyouts have intended to bring total functionality under single-vendor control. Often the set of products offered and purchased becomes so diverse and numerous that the integration among products lags behind the advancement of features within a product line. In these cases, new capabilities or features need to be added to multiple product road maps, delaying delivery while smaller companies are able to get innovations to market quickly. Customer organizations cannot invest in, deploy, or leverage new products, technologies, or operational best practices without ensuring compatibility with the existing product suite or paying a third-party integrator. Sustainability and ease of automation come at the direct cost of flexibility and innovation. Another trade-off is improved time to value for any of the vertically integrated products versus extended delays in time to value for any other products.

Platforms and Partnerships

Organizations have begun to focus on more timely and measurable return on investment (ROI) for cybersecurity and defense-related purchases. They are investing in products and applications that promote flexibility and interoperability, increasingly judging a product's worth by how many other solutions it connects with or supports. Platforms and limited partnership agreements have become the new business model. Organizations purchase the platform that already supports integration with a majority of their existing products, and the platform vendor adds new products to the road map based on customer demand. Platforms are often designed for a particular process (e.g., incident response) or operational activity (e.g., threat analysis).

Although this business model appears to provide flexibility and sustainability, it often comes (quite literally) at a cost. Many platform providers charge by the integration, effectively forcing an organization to pay more as they connect more of their products together to support enhanced automation. The vendors sustain the integration effort, but the capability

itself is not sustainable because the organization cannot afford to add in new products or automate more actions.

Often an organization has products that are not a part of the vendor partnerships, and therefore the organization is required to create and maintain custom connections for these products. The ease of integration and maintenance for these custom connections is directly proportional to how open, well documented, robust, and stable the application programming interfaces (APIs) are for these products. Lastly, although orchestration platforms provide templates, training, and easier-to-use interfaces, they still require the organization to build out all the automation workflows. The skills to do this work—usually software development or network engineering—rarely match the skills of the people performing the processes that are being automated.

There is a continual balancing act among the ability to automate, flexibility, and sustainability under this business model. For instance, automation and integration may require specialized resources or expensive licensing options. If you have the resources and the product you bought supports easy integration, time to value can be fairly quick. However, if you do not have the resources or you bought a product with a poorly documented or proprietary API such that you need to pay someone to perform the integration, then time to value will be delayed. The good news is that buyer awareness and smart purchasing practices can minimize trade-offs and make the most of new cybersecurity investments.

Custom Integration

Most organizations have already found a way to integrate some of their cybersecurity products to support automation and enhanced capabilities. Unfortunately, if the one information technology (IT) person who custom scripted this integration departs for another job or decides to retire, the organization can rarely maintain existing functionality. This is a significant problem for organizations that have a large number of legacy, custom-developed, or proprietary products and applications. With a dedicated development staff, be it site personnel or an integration vendor on contract, integration of existing products can be maintained with a surge when there is a product upgrade and/or API update. As for new products, time to value is directly related to priority and ease of integration. As stated previously, ease of integration and maintenance is directly proportional to the openness, robustness, and stability of the associated APIs.

Asking the Right Questions

Does your product have a robust, open API?

- Does your API support all the same functions as your user interface?
- Where is the documentation for your API?
- Does your API documentation contain examples or pseudo-code?
- How quickly is the documentation updated in response to product upgrades?

What is your licensing model?

- What if I integrate more products?
- What if I perform more tasks or actions?
- What if I automate more functions?
- What if I incorporate more data?

What standards do you support?

- For data import and export?
- For networking, communications, and messaging?
- For authentication?
- For cryptographic functions?

Can you support my organizational needs/use cases?

- Can you already do what I need natively?
- Who do you have integration partnerships with?
- What partnerships or capabilities are on your roadmap?

Interoperability: Choosing "and"

As previously stated, organizations are continuing to invest in new products and technologies to improve their cybersecurity posture as well as increase the efficiency and effectiveness of cyber operations. In addition, we have also noted that integration models of existing products may force trade-offs among automation, flexibility, and sustainability, which impacts time to value for any new purchase. However, investing in products that inherently support wide-scale interoperability can minimize these trade-offs and enable a more rapid incorporation of any new product or capability into the existing environment or operations.

Robust, Open APIs

Purchase products that have an API that supports all of the same actions as the user interface. The API-provided functionality should be as stable and consistent as the functionality provided by the user interface. Make sure that the vendor has a well-documented API and that the documentation is openly accessible, easy to understand, and updated whenever the product is updated.

Integration and automation are hindered by APIs that are proprietary, are poorly documented, and/or provide limited functionality.

Support for Unlimited Integration

Whenever possible, purchase products with a business or licensing model that does not limit integration. Make sure the vendor supports integration with products from any vendor, not just their own or those of their partners. Have them demonstrate how to perform a custom integration, taking note of the skill level, knowledge, and time associated with the action.

Beware of licensing models that require you to pay more as you integrate more products, automate more processes, repetitively take a certain action more often, include more users, or handle more data. When it comes to security automation and orchestration (SA&O), organizations often start small and incrementally increase their capabilities as they become more comfortable with automation and the resulting efficiencies. Don't lock yourself into an unsustainable licensing model that will force you to make implementation decisions that limit the ROI of cybersecurity investments.

Support for Standards

Purchase products that import and export data in standard or community-defined formats. Proprietary formats require dedicated resources for parsing, translation, and normalization to support integration and automation. If there are no applicable standards, make sure the vendor is participating in organizations that are attempting to define standards and is willing to conform to the targeted, albeit yet-to-be-defined, standard.

Purchase products that implement standards-based networking, messaging, authentication, and cryptographic protocols as appropriate. Proprietary protocols limit integration and automation and often introduce security issues.

Buy for Success

A change in buying habits may be the single most important factor in implementing a successful SA&O strategy. Purchase only products or services that support unlimited integration and interoperability. Make sure that all desired functionality can be accessed in an automated manner. Avoid proprietary interfaces, schemas, and protocols.

Before meeting with any vendor, document how you want to incorporate the product or service into your operational environment and cybersecurity operations. Explicitly ask whether the product or service is a native part of the vendor's offering. If not, find out where it is on the company road map. If you have to pay someone extra to achieve your operational goals, then you should consider other products or services.

Consider grouping vendor offerings based on support for integration. Standards-based interfaces are the least expensive to work with and maintain. When standards do not exist, robust, open, and well-documented APIs should be the target. Proprietary or poorly maintained interfaces should be avoided whenever possible. When assessing vendor offerings, always account for licensing models. Avoid licensing models where the cost is directly proportional to the amount of integration and automation.