Emerging Trends: Future of Security Services

The security service landscape will shift significantly over the next several years. Product leaders across security technology vendors and service providers must adjust service delivery strategies as buyers seek to shift operational delivery of internal business outcomes to service providers.

Overview

Key Findings

- Business leaders’ increasing influence and impact on buying decisions are shifting the focus from technology to use-case-based outcomes, such as support for a hybrid workforce in a specific vertical industry.

- Service providers are struggling to deliver at the speed of technology innovations, like the use of artificial intelligence (AI) and machine learning (ML).

- Service providers, often seeking best-of-suite platforms over best-of-breed point solutions, will establish partnerships with technology vendors offering vendor-delivered service wrappers (VDSWs).

- Market convergence will drive increased interest in service providers acquiring adjacent and often less mature service providers.

Recommendations

Product leaders responsible for understanding the impact of emerging technologies and trends must:

- Deliver use-case-based outcomes, rather than generalized services available to all markets, by identifying target market segments and maturing service portfolios to meet the needs of those market segments.
Achieve service delivery capabilities, if you are a technology vendor, by implementing the applicable people, processes, and technologies needed to provide a consistent service delivery experience or by acquiring a service provider with capabilities aligned to their product differentiator.

Achieve preferred vendor status and capitalize on vendor consolidation, if you are a technology vendor, by easing integration with other IT and security technology and tools within the environment.

Accelerate innovation, if you are a service provider with legacy services, by acquiring adjacent, more mature, and more enhanced service delivery-oriented providers to adopt their methods over their own.

**Strategic Planning Assumptions**

By 2025, more than 25% of technology vendors will offer a vendor-delivered service wrapper, up from 10% in 2021.

By 2026, more than 50% of service providers will have realigned portfolios to deliver use-case-based outcomes.

By 2028, 80% of security service outsourcing will go to providers delivering use-case-based outcomes, up from less than 5% in 2021.

**Analysis**

**Overview**

The security service landscape is rapidly evolving, and there are several forces driving change and impacting the security service space as a whole. On one end of the spectrum, technology vendors, which historically provided technology to service providers, are creating vendor-delivered service wrappers (VDSWs) around their own technology. On the other end of the spectrum, buyers who historically owned responsibility for delivering internal business outcomes and looked to providers for technology, are now looking to consolidate providers and shift operational delivery of internal business outcomes to third parties. In the middle is a meshing of IT operations and security operations, as growing complexities in technology stacks like secure access service edge (SASE) and zero trust network access (ZTNA) blur lines of separation.

There are four factors driving the significant shift across the security service landscape:
This research will discuss how product leaders must pivot to meet the increasing expectations of their customers at various stages of the technology and service delivery buying cycle.

**Evolution Spectrum**

The shift occurring across the security service landscape is being driven by the changing roles each stakeholder plays and what outcomes they deliver. Traditionally, the vendor delivers the technology, the provider delivers the service, and the end customer delivers internal and external business outcomes. Looking ahead three years and beyond, the following changes across these three stakeholders are taking place:

- **Technology vendors** will continue to move from strictly delivering technology to offering an optional monitored, co-managed, or outsourced level of service delivery.
- **Service providers** will continue to move from strictly consulting, reselling, and integrating technology and managed services to combining the disciplines, by way of partnering, internal service maturity, and merger and acquisition (M&A) to deliver use-case-based outcomes aligned to end customers’ desired internal business outcomes.
- **End customers** will shift focus from primarily delivering internal business outcomes to delivering external business outcomes for new business models.

Figure 1 displays the projected timeframes for each of the three phases in the evolution of security services through 2028.
Phase 1: Vendor-Delivered Service Wrapper

By 2025, more than 25% of technology vendors will offer a vendor-delivered service wrapper; up from 10% in 2021.

Vendor-delivered service wrappers are a result of a technology vendor creating the necessary managed service delivery aspects as an additional option to couple with the vendor's product. MDR, managed endpoint detection and response (MEDR), managed data loss prevention, managed penetration testing, and managed brand protection are examples of a growing number of services delivered by technology vendors on their own products as VDSWs.

Trend Characteristics

VDSWs, like other managed services, are available in one or more of the three common tiers — monitored, co-managed, and/or outsourced. VDSWs are offered direct-to-market, via channel partners, or both. VDSWs should not be confused with SaaS-delivered platforms or implementation consulting services to deploy a product, both of which result in turning over responsibility for ongoing administration to the end customer upon completion.

The three potential VDSW levels are generally summarized as:
Market Characteristics

VDSWs will cut across most security segments as technology vendors create one or more tiers of managed service deliverables around their technology. Technology vendors creating VDSWs seek to standardize processes and efficiencies around the vendor's technology to standardize outcomes delivered by the technology, including maximizing opportunities to leverage AI/ML. VDSWs also shorten the product feedback loop for technology vendors when the service delivery is in-house, aiding in the stickiness of adoption for the technology vendor and streamlining expertise to enhance customer outcomes and experiences.

VDSWs allow service providers to accelerate time to market with new services while reserving the option to move those services in-house in the future with those investments front-end loaded by previous sales.

- **Monitored**
  - Vendor is responsible for workflows required to ensure timely delivery of notifications to the partner/customer according to the playbook.
  - May or may not include automated or minimal human-based triage by the vendor before escalation to partner/customer for a more in-depth investigation and remediation.
  - Vendors may or may not have access to credentials of covered assets.

- **Co-Managed**
  - Includes everything in the monitored level, plus the vendor and partner/customer share responsibility for technology operation and content development of covered assets. (Example: Vendor is responsible for monitoring, platform administration, patching, and alert remediation, while the partner/customer is responsible for moves, adds, changes [MAC] and report creation).

- **Outsourced**
  - Vendor is responsible for the service delivery applicable to the provided technology, including platform administration, triage, remediation, standards compliance, and reporting, but does not include break/fix services of underlying technology components.
When technology vendors opt for a direct-to-market approach over conventional channel partners, intensified competition will result as technology vendors and security service providers compete for these product-centric services add-on opportunities.

**Product and Service Characteristics**

VDSWs allow service providers to focus internal resources on differentiating the end service delivery to the customer from the original VDSW. For example, where a VDSW is more generalized than specific to an industry or use case, the VDSW will need to be bundled with a service provider's tools and services to deliver a case-based outcome more specific to industry or use case.

Some segments, like MDR, are well-established and consistently growing with many existing and new technology vendors offering a VDSW. Meanwhile, other segments, like managed data loss prevention (DLP), have only a few technology vendors offering a VDSW, and others yet are just beginning to realize the trend. In segments with a lack of VDSWs, technology vendors have the opportunity to gain market share by delivering a VDSW.

**Phase 2: Service Provider Portfolio Realignment**

*By 2026, more than 50% of service providers will have realigned portfolios to deliver use-case-based outcomes.*

Service providers are caught in the middle between technology vendors looking to create more predictable outcomes from the vendor’s technology by employing VDSWs and changing customer priorities from buyers valuing use-case-based outcomes over technical features and functionality. Service providers will establish partnerships with technology vendors offering VDSWs often seeking best-of-suite platforms over best-of-breed point solutions. The desired outcome for the service provider is interoperability and faster time to market.

**Trend Characteristics**
VDSWs allow a service provider to speed time to market with new services by offloading upfront costs, risks, and knowledge gaps to the technology vendor. When technology vendors offer VDSWs, service providers will have near-term concerns, like competing with a technology vendor, and long-term concerns, such as if the technology vendor may eventually go directly after all the customers are on their platform. As service providers better understand the intentions of their technology vendors, service providers will seek partnerships with technology vendors whose intentions are to help mature, rather than compete with, a service provider’s offerings. This is a similar trend to what was witnessed with the advent and maturation of cloud services including infrastructure as a service (IaaS), platform as a service (PaaS), and SaaS.

Service providers will continue to combine various technologies to deliver a solution. A need for improved integration will cause service providers to transition business models from vendor-agnostic and best-of-breed technologies delivering managed technology solutions to vendor consolidation and best-of-suite platforms allowing service providers to increasingly deliver solutions in the form of use-case-based outcomes.

Technology vendors will seek to build, buy, or partner with adjacent and complementary vendors to expand integrations and increase their attractiveness to their target markets. Service providers will either seek partnerships with technology vendors that ease the service providers integration burdens or will build integrations themselves between their preferred technology vendors. Ongoing shortages in security and developer skill sets will cause the latter option to be more prevalent in boutique and larger service providers; however, this does not mean boutique and larger service providers will prefer the latter option.

**Market Characteristics**

By offloading foundational service responsibilities to the technology vendor, service providers can differentiate themselves in the market while also increasing customer stickiness and improved retention by focusing internal resources to delivering use-case-based outcomes to customers.

Examples of use-case-based outcomes include:
Service providers will deliver use-case-based outcomes by combining the more generalized services offered in the VDSW with the service provider’s own services, customer portals, reporting and other deliverables specific to the market segments that the service provider serves. This will require those service providers that have historically been generalists themselves to identify their target markets and segments (see A Practical Guide to Market Segmentation) and mature their service portfolios to deliver outcomes specialized to the needs of those markets and segments.

**Product and Service Characteristics**

Blurring of lines between IT operations and security operations from emerging trends like SASE, combined with customers seeking to consolidate providers will drive a convergence between managed service providers (MSPs), managed security service providers (MSSPs) and pure-play MDR providers. MSPs and MSSPs must expand portfolios to cover the other’s respective areas to address these blurring lines. Likewise, they must expand portfolios to address more mature services like MDR. Pure-play MDR providers must expand their portfolios to cover more services conventionally offered by MSPs, MSSPs and security consulting providers or risk losing out in provider consolidation.
Likewise, security consulting services will increasingly be delivered as a continuous service and/or bundled with managed services as providers seek more predictable annuity-based income and buyers embrace the need for more continuous testing, remediation, and guidance over conventional point-in-time activities, driven in part by regulations and by organizational maturity. Examples of these continuous services include virtual chief information security officer (CISO), chief data officer (CDO), and chief compliance officer services, as well as vulnerability assessments and management, penetration testing, breach and attack simulation, and external attack surface management.

Similarly, this transition from point-in-time activities to recurring services will apply to the SI and VAR communities as technology vendors increasingly look to deliver more as-a-service offerings, and the SIs and VARs also look for more predictable annuity-based income streams.

**Phase 3: Use-Case-Based Outcome Delivery**

*By 2028, 80% of security service outsourcing will go to providers delivering use-case-based outcomes, up from less than 5% in 2021.*

Skills shortages, increasing technology complexities, and blurring of lines between IT operations and security operations help drive increasing customer interest in outsourcing to service providers. Buyers, who historically owned responsibility for delivering internal business outcomes and looked to providers for technology, are now looking to consolidate providers and shift operational delivery of internal business outcomes to providers. Security is no exception, and buyers have increasing expectations for security service providers to mitigate risk toward achieving business outcomes and reduce internal workload to resolve security incidents.

**Trend Characteristics**

The lack of skilled security expertise is a significant reason organizations choose to outsource some part of their security operations. This affords the client to offload select functions for various security operations roles and responsibilities to security service providers. The worldwide cybersecurity talent shortage will continue to plague the industry, increasing demand for both VDSWs and their partner service providers to supply the expertise for custom service delivery. Knowledge and understanding of a client’s business and operations to become a true extension of the client security team is a historical challenge service providers must overcome. This is critical to deliver security services based on business outcomes, but it requires effort by the client and the provider to align skill needs, expectations and accountability.
Organizations are seeking more sophisticated security solutions to address complex security challenges. For example, reliance on data science driven threat detection solutions requires advanced technology management and tuning expertise. Many organizations do not employ data scientists or highly experienced detection and automation engineering experts, but VDSWs can solve this challenge because they build the complex security solutions and have access to the back-end code and architecture. This is necessary for customization, tuning and feature enhancement which is an advantage over service provider partners, but it presents opportunities for VDSWs and service providers to deliver customized solutions based on unique client outcomes.

The trend to outsource IT and security functions has resulted in blended offerings from providers. Outsourced IT operations or managed network and service providers are increasingly offering managed security services, which aligns with client demand to reduce the number of vendors they have under management. Security product vendors have constructed mature partner and channel programs for service providers to leverage their solutions in both IT operations (ITOps) and security operations (SecOps) offerings. VDSWs have an opportunity to deliver on niche and specialized services in these partner arrangements, particularly in the following areas:

- Operational technology (OT) environments
- Healthcare and medical device monitoring
- Internet of Things (IoT)
- Advanced analytics and anomaly detection
- Digital risk protection services (DRPS) (see Emerging Technologies: Critical Insights in Digital Risk Protection Services)

Data platforms are increasing features and functionality, either through organic development or acquisition, to offer more holistic solutions that address use cases for multiple parts of the business. This affords service providers the opportunity to deliver on business outcomes throughout the organization. Buyers may invest in a solution or ask service providers to bring technology, which often includes a single platform delivering multiple capabilities, such as:

- Data analytics
- Asset management
Market Characteristics

The security service market has shifted from vendor-agnostic services with an emphasis on compliance and broad use-case deployment to client-environment-focused outcomes and the use of defined technology stacks for service delivery. This approach to service delivery has several advantages:

- Security analyst expertise with a defined tech stack are focused and developed around a finite set of technologies.
- Service providers either own the tech or have a strong relationship with their technology partners to influence features and functionality.
- There is a reduction in noise from sources with limited security value.
- Less time is spent trying to monitor and make sense of everything and focus on what is important for threat detection and client-defined use cases.

Hyperautomation is being exploited by service providers to deliver on client outcomes and make their operations more efficient. This is delivered using a client-procured solution or the service provider using their own solution and even integrating with a client automation environment. Benefits and examples are:

- Integration with client automation processes to achieve business outcomes
  - Unpatched system identification and escalation
  - Cloud environment policy enforcement for new environment creation and resource utilization
Buyers have been putting more focus on maturity of their security programs and look to service providers as a method to fill gaps and/or enhance current maturity levels over time. Service providers must provide evidence of maturity status, maturity improvement over time and alignment to business outcomes.

Product and Service Characteristics
Service providers and VDSWs must implement some core functionality for buyers to shift from internal outcome to external outcome delivery.

Service providers and VDSWs must deliver functionality to measure SecOps success and continuous improvement of security program maturity. Some buyers push for this in service delivery models today, but it will be a commodity expectation to prove value to the buyer. This is not limited to rudimentary SecOps metrics, such as mean time to detect (MTTD) and mean time to respond (MTTR). Buyers will expect demonstrable evidence of their security program improving over time to meet SOCTOM objectives.

More responsibility and access to deliver internal security outcomes mean stringent controls and oversight of what service providers are doing. The details are critical for clients to trust but verify service providers and VDSWs are operating with integrity and competence. Solutions will have to integrate seamlessly with the client environment to enable frameworks like ZTNA or multifactor authentication (MFA) techniques. This implies the service providers will be operating as trusted users in the environment and performing actions previously reserved for system owners.

- Automation of repetitive tasks for incident investigation
  - Decorate indicators with contextual threat intelligence
  - Autogenerate client incident if threat score exceeds a threshold

- Client success management programs to embed as a trusted advisor with the business and client security teams and ensure outcomes are being realized.

- Comprehensive solution mapping during the presales process that utilizes a consultative process to understand the business, target operating model, technical environment details and what the buyer expects from the service.

- Working with buyers to jointly develop a security operation target operating model (SOCTOM) for the organization and aligning it to service provider capabilities to promote long-term renewals.
Market Opportunities

Although VDSWs will be disruptive to conventional channel norms until the channel better understands how and when to partner or compete, the net effect on most service market opportunities will be neutral. Implementation service revenue will see less opportunities as managed and continuous services incorporate implementation costs as part of onboarding or waive implementation fees on long-term contracts. Significant opportunities will exist for both consulting and outsourcing as the evolution transitions to realigning portfolios and delivering use-case-based outcomes aligned to end customer business outcomes.

Opportunities Heat Map

See Figure 2.

Figure 2. Security Service Market Opportunities Heat Map

Security Service Market Opportunities Heat Map

<table>
<thead>
<tr>
<th>Market Segment</th>
<th>Market Subsegment</th>
<th>Phase 1: Vendor-Delivered Service Wrapper</th>
<th>Phase 2: Service Provider Portfolio Realignment</th>
<th>Phase 3: Use-Case-Based Outcome Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Services</td>
<td>Consulting</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Implementation</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>IT Outsourcing</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Other Security Products</td>
<td>Other Security Products</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Source: Gartner
752200_C

Phase 1: Vendor-Delivered Service Wrappers — Opportunities
The most significant market opportunities during the VDSW phase are with the technology vendors. A primary barrier to entry for most products are the buyer’s competing priorities. The buyer may want to acquire a technology vendor’s product, but must balance the burdens of onboarding, integrating, training, operating, maintenance, and continuous improvements related to the technology vendor’s product and the outcomes the product can deliver with other internal initiatives all competing for the attention of the same internal resources. It is a balance of burden versus benefit. Vendors offering a VDSW option can provide a mechanism to significantly diminish the burden on the buyer’s internal resources while also speeding realization of benefits. The reality of both diminishing burden and speeding realization of benefits holds true whether the buyer is a service provider in the vendor’s channel or an end customer.

In addition to lowering barriers to entry for a technology vendor’s product, the technology vendor has the opportunity to generate recurring service revenue. Technology vendors must decide whether the route-to-market strategy is to deliver direct-to-market, via channel partners, or both. This decision is often driven by the determination of whether the desired outcome is to enter the managed service market to purely generate additional revenue via managed service delivery or to lower the barrier of entry for the technology vendor’s product. Those adopting the former are likely more inclined to go direct-to-market, and those preferring the latter are more inclined to choose channel partners. Regardless of desired outcome and route-to-market decisions, it is critically important the managed service arm is designed to be profitable else it will starve for resources needed to continuously mature (see Business Metrics for Consulting and Outsourcing Firms, 2Q21).

As discussed in The Tech CEO Roadmap for Transitioning From Services to Products, creating products and creating services are uniquely different. However, technology vendors that allow the challenges to deter them from creating a VDSW around their product will find themselves struggling to remain relevant in the space. An example of this is illustrated in the EDR market, where EDR technology vendors offering an MDR service via a partner channel or direct-to-market are challengers to the more established EDR technology vendors that do not. EDR technology vendors in the late majority and tail end of the early majority of VDSW trend adopters are finding themselves at the beginning stages of the iterative process of continuous service improvement while those in the innovator and early majority of adopters are accelerating growth by expanding the capabilities of their services via internal innovation, partner integrations, and acquisitions.

**Phase 2: Service Provider Portfolio Realignment — Opportunities**
Most, but not all, of the opportunities in this phase go to the service providers. Those opportunities begin with the ability to significantly speed time to market with new and/or matured services by partnering with technology vendors who offer a VDSW option. When properly structured, these partnerships allow the service provider to onboard new capabilities while minimizing training and integration skill requirements in addition to outsourcing many of the operation and continuous improvement requirements present in any service. Likewise, though the service provider still owns responsibility for integration with internal tools set (examples include remote monitoring and management [RMM], professional services automation [PSA], IT service management [ITSM], SIEM/SOAR, and customer portals), technology vendors equipped to work with service providers will have many of these integrations ready out of the box, further minimizing service provider integration responsibilities. By offloading many of these baseline service burdens to the technology vendor, the service provider can focus resources on maturing service offerings to deliver more use-case-based outcomes in-line with the next phase.

Service provider market convergence will drive increased interest in service providers acquiring adjacent and often less mature service providers. MSSPs acquiring MSPs or vice versa, as well as SIs and VARs acquiring or being acquired by MSPs and/or MSSPs will allow higher maturity service providers to capitalize on rapid inorganic growth to quickly mature the service delivery portfolio and expand in an already landed customer base. Not all inorganic growth opportunities belong to the service providers with a higher service delivery maturity. Service providers with legacy services but a more developed business acumen will see opportunities to acquire service providers with a higher delivery maturity, albeit at a premium when compared to their own value. Of critical importance in these transactions is the need for the acquiring service provider to realize that often the lack of internal maturity has come from internal challenges including legacy processes and mindsets that can stifle innovations. Inorganic growth opportunities like these can quickly become an investment of diminishing returns when the acquiring service provider's legacy challenges are applied to the acquired service provider's organization rather than learning and adopting methods utilized by the acquired service provider.

Technology vendors have an opportunity in this phase to increase market share by buying, building, and/or integrating with adjacent and complementary technology vendors. As buyers, both end customers and service providers, continue to consolidate vendors/providers, buyers will seek best-of-suite and integrated solutions over best-of-breed point solutions. Preferred technology vendors will be those that ease integration with other IT and security technology and tools within the environment, supporting efforts toward use-case-based outcomes. Technology vendors that do not will struggle to retain, let alone grow, market share during vendor consolidation.
Likewise, service providers that do not take strategic advantage of opportunities to partner with technology vendors offering a VDSW will struggle to maintain market competitiveness as the speed of innovation continues to increase. Similar to their technology vendor counterparts, these service providers will struggle to retain, let alone grow, market share during provider consolidation. This does not mean a service provider should leverage a VDSW for every service in their portfolio. To take the previously stated “strategic advantage” means to identify portfolio and capabilities gaps and leverage VDSWs for those with heavier burdens to create and deliver. Furthermore, “strategic advantage” means to determine whether use of a VDSW will be short-term, front-end loading investments to move in-house later, or long-term, with no plans to move in-house at a later date.

Phase 3: Use-Case-Based Outcome Delivery — Opportunities

Technology vendors must deliver features in their product to enable VDSW or service provider operations to enable greater responsibility and action in buyer environments. A large amount of it exists today in the form of APIs and SOAR integrations, but the auditing and trust features will likely be under heavier scrutiny. Technology vendors must also consider the impact of regulation on the security industry and requirements, such as national laws on data sovereignty or data protection that dictate where data must reside and how it is handled. Buyer demands for more vendor outcomes will also drive granular controls to reduce likelihood of mistakes being made. For example, two-person integrity validation for taking action in the environment or making environment changes as part of remediation efforts. VDSWs must also define a line of limitations and be clear with buyers and service providers about what they will and will not do as it relates to internal security outcomes. In these instances there must be well defined handoff processes between VDSWs and service providers, or the buyer.

Service providers arguably have the most to gain from the evolution of service delivery models. Buyers demand is increasing for service provider action which means more service tiers and delivery options. Both new and veteran service providers can take advantage of VDSWs and partner programs to implement complementary services or take advantage of industry-leading technology versus organically building solutions and inheriting technical debt. While there are tremendous gains, there are significant risks that service providers have tried to avoid for decades. Disabling a production environment because of a mistake during remediation actions has enormous consequences, but managed network providers have been managing client environments for decades. Security service providers and VDSWs must implement legal protections, and buyers must embrace the possible risks associated with third-party actions to deliver internal business outcomes.
The greatest risk to both VDSWs and service providers is doing nothing to evolve services to meet buyer demand. General security service offerings will become a small niche offering for immature security operations who focus on checkbox compliance delivery. Buyers are exponentially more demanding on security operations than they were even five years ago. Service providers that deliver tailored services based on areas of technology, threat, regional or vertical expertise will win out to address those client-specific outcomes.

Recommendations to Product Leaders

Product leaders at technology vendors:

- Achieve service delivery capabilities by implementing the applicable people, processes, and technologies needed to provide a consistent service delivery experience or by acquiring a service provider with capabilities aligned to your product differentiator.

- Offer a white-label VDSW to channel partners as an optional add-on to lower the barrier for partner adoption and speed time to market.

- Provide out-of-the-box integration with customer tools and workflows like SIEM, SOAR, XDR, ITSM, RMM and operation automation platforms in addition to mechanisms ensuring you do not limit customer flexibility or conflict with other providers in the environment when delivering direct to market.

- Expand channel conflict protocols to encompass service delivery, including transitions between servicing partners when an end customer desires to change partners while retaining your technology.

- Establish clear responsible, accountable, consulted and informed (RACI) details between technology vendor and service provider or end customer as applicable coupled with well-defined hand-off processes.

- Ensure the VDSW is designed to be profitable to avoid the risk of starving it of resources needed for continuous maturity.

- Deliver features in the product to enable VDSW or service provider operations to enable greater responsibility and action in buyer environments, especially in the realms of audit and trust (i.e., two person integrity validation for taking action in the environment or making environment changes as part of remediation efforts).

Product leaders at service providers:
- Expand portfolios to cover a broader set of managed and continuous service capabilities required to deliver outcomes specific to the market segments you serve.

- Seek and partner with technology vendors delivering service wrappers to speed time to market and address skills and offering gaps. Alternatively, develop required intellectual property (IP) or acquire applicable technology vendors.

- Evaluate partners on product efficacy combined with their ability to deliver details you need to provide specific outcomes to your customers (i.e., data localization, compliance reporting, etc.).

- Transition one-time engagements into recurring services by bundling personnel, applicable security consulting services and customer deliverables (reports, portal, etc.) designed to deliver a specific business outcome (i.e., vCxO services like vCISO, vCDO, vCCO, etc.).

- Deliver use-case-based outcomes, rather generalized services available to all markets, by identifying target market segments and maturing service portfolios to meet the needs of those market segments.

- Accelerate innovation if you have legacy services by acquiring adjacent, more mature, and more enhanced service delivery oriented providers to adopt their methods over your own.

---

**Recommended by the Authors**

Some documents may not be available as part of your current Gartner subscription.

- Emerging Technologies and Trends Impact Radar: Security
- Emerging Technologies and Trends Impact Radar: IT Services
- Emerging Technologies: Critical Insights in Digital Risk Protection Services
- Competitive Signals: Business Metrics for Consulting and Outsourcing Providers, 2Q21
- A Practical Guide to Market Segmentation
- The Tech CEO Roadmap for Transitioning From Services to Products
- Can You, and Should You, Bring in a Virtual CISO?
- Four Tips for a Successful Engagement With a Virtual CISO
Position your cybersecurity organization for success. Explore these additional complimentary resources and tools for security and risk leaders:

**Webinar**
The Gartner Leadership Vision for 2022: Security and Risk Management
Secure your organization’s future with new technology.

**eBook**
3 Must-Haves in Your Cybersecurity Incident Response
Implement cybersecurity awareness with an effective plan.

**Research**
Predicts 2022: Cyber-Physical Systems Security — Critical Infrastructure in Focus
Plan for risks and opportunities within your organization.

**Roadmap**
Protect Your Business Assets With a Roadmap for Maturing Information Security Program
Improve your security for the changing environment.

Already a client?
Get access to even more resources in your client portal. [Log In](#)
Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

**U.S.:** 1 855 811 7593

**International:** +44 (0) 3330 607 044

[Become a Client](#)

Learn more about Gartner for IT Leaders


Stay connected to the latest insights  

© 2022 Gartner, Inc. and/or its affiliates. All rights reserved. CM_GTS_1735200