Security Vendor Consolidation Trends — Should You Pursue a Consolidation Strategy?

Published 30 July 2020 - ID G00719769 - 14 min read

By Analysts John Watts, Peter Firstbrook

Overview

As more cybersecurity point solutions come to market, security and risk management leaders have reached the tipping point for vendor integration and management. They must rationalize their information security portfolio to determine if a consolidation strategy or best of breed is the right approach.

Key Challenges

- Organizations find vendor consolidation strategies challenging. Eighty-five percent of organizations currently pursuing a vendor consolidation strategy show a flat or increased number of vendors in the past year.

- Twenty-three percent of organizations planning to pursue a vendor consolidation strategy are expecting reduced spending as a primary benefit, but only 16% of those currently pursuing a vendor consolidation strategy reported reduced spending as a primary benefit.

- Vendor consolidation strategies require at least two years to yield meaningful results. After two years, pressure rises to add more vendors due to leadership changes, emerging threats or gaps within the incumbent vendor landscape.

- About one-quarter of organizations are pursuing a vendor consolidation strategy now, but an additional one-half of the organizations surveyed plan to do so in the next two to three years.

- Organizations expect external factors to impact security functions in the next three to five years, while the internal factors of the Internet of Things (IoT) and cyber-physical systems were the top overall ranked factors.

Recommendations

Security and risk management leaders responsible for infrastructure security should:

- Determine a key motivation for a vendor consolidation strategy upfront. Ensure that cost savings calculations are based on total cost of ownership (TCO), and anticipate transition costs and effort when cost is used as a justification. Security operations efficiency and organization risk reduction are the most sought goals, but can be elusive.
Avoid positioning vendor consolidation as an either-or approach. Instead, segment security tools by segment maturity and integration needs. Consolidate in more mature market segments, and consider best-of-breed products in less mature markets or where unique feature requirements demand it.

Rationalize vendors through alignment of product capabilities matrices to determine if buying strategies favor incumbent products or force a business justification for point solution providers.

Plan a multiyear transition from one strategy to another, working closely with procurement and enterprise architecture teams.

Measure progress toward strategic goals. Avoid simple vendor counts to measure success.

**Strategic Planning Assumption**

By 2025, three-quarters of large organizations will be actively pursuing a vendor consolidation strategy, up from approximately one-quarter today.

**Introduction**

Gartner recently completed a survey of organizations to understand current and future trends in security vendor consolidation. In the survey, we found that more than 85% of organizations that pursue a vendor consolidation strategy find it challenging to reduce the total number of vendors. Gartner client inquiries find that unrealistic expectations, poor planning and asset management, or external and internal factors such as mergers and acquisitions often impede vendor consolidation efforts (see Figure 1).

Figure 1. Expectations Versus Actual Benefits of Vendor Consolidation
Organizations looking to save costs must look beyond simply managing vendor counts to find cost savings through reduced product usage, optimized license counts and a shift to lower-tier product offerings.

Most surveyed organizations expect to see increased operating costs and time spent on integration in the second half of 2020 and first half of 2021, even in the face of the COVID-19 pandemic’s impact on the overall economy. However, cost savings may not be achieved through vendor consolidation strategies. Twenty-three percent of organizations planning to pursue a vendor consolidation strategy are expecting reduced spending as a primary benefit, but only 16% of those currently pursuing a vendor consolidation strategy reported reduced spending as a primary benefit. Often, an organization is not prepared to onboard and consume all the technology at once or retire incumbent vendors completely. Vendors may allow products to be added seamlessly during the life of the contract, but rarely allow them to be subtracted.

The security market is always consolidating, but never consolidated.
Historically, there has been a pendulum of sentiment that swings back and forth between a preference for consolidation and best of breed. The results of this year’s survey indicate a strong interest in vendor consolidation to fewer vendors over the next few years, but this may change as new vendors appear and disrupt incumbents. Long term, consolidating vendors may never be fully complete for an organization.

Analysis

Determine a Key Motivation for a Vendor Consolidation Strategy Upfront

Regardless of which strategy an organization pursues, it must determine the trade-offs involved. Often, the risks are more important to consider than the promised benefits.

Vendor Consolidation

Vendor consolidation strategies focus on ways to reduce integration and overall security operations complexity. Of those organizations pursuing a vendor consolidation strategy, 41% reported improved overall risk posture of the organization as the primary benefit (see Figure 2).

Figure 2. Primary Benefits From a Vendor Consolidation Strategy
Organizations pursuing a consolidation strategy must justify the value of adding more complexity with point products. Consider point solutions when the primary vendor does not sufficiently meet requirements and favor point solutions that integrate with the primary vendor through partnerships rather than open API integrations, which drive more time and cost through integration activities. In addition, look for vendors offering integration into other vendors’ consolidated management and reporting consoles instead of requiring a one-off management and reporting console.

Fortunately the large security product vendors are starting to deliver on promised integrations into a security incident response capability for organizations that are establishing or redesigning their security operations capability. We call this capability extended detection and response, or XDR. See “Innovation Insight for Extended Detection and Response” for more information on how vendors are moving toward integrated platforms to provide a more broad and integrated security product portfolio for organizations.

A vendor consolidation strategy is not without risks. Those include:
Vendor lock-in and increasing switching costs, leading to supplier apathy or pricing pressure

Increased costs due to shelfware and overlapping software terms

“Check the box” products from vendors missing key functionality

Forced legacy product retirement when acquisitions occur

Lack of product integration, especially when products are acquired rather than built

Corporate merger and acquisition activity that introduces new security vendors to the portfolio

Threat intelligence limited by reliance on fewer datasets and lab analysis

Best of Breed

Organizations looking at best-of-breed strategies are typically looking to solve particular pain points or value the highest security efficacy in each product selected. A security incident might trigger an information security team to search for new products to prevent future incidents. Or an organization may be reacting to changes in the threat landscape and emerging threats, as best-of-breed vendors can be more nimble or offer specialized products to address a new threat. A best-of-breed strategy is not incompatible with consolidation, but it should focus on markets where it is absolutely necessary and should favor vendors with integration partnerships with incumbent solutions to ease the burden of integration.

Most organizations already have as many security products as they can handle and need more investments in people or processes, instead of tools. For example, the Gartner survey discovered that 56% of all organizations anticipated no change or a decrease in vendors next year, despite only 29% actively pursuing a vendor consolidation strategy (see Figure 3).

Figure 3. Expected Change in Elements of Information Security Program in the Next Year
The high-level risks of a best-of-breed strategy include:

- Acquisition, solvency and partnership dissolution risk of smaller vendors
- Excessive time or inability to integrate solutions due to internal resource shortages
- Lack of scale for support and technical resources, especially in worldwide deployments
- Procurement roadblocks to onboarding new vendors
- Overhead required in managing too many vendor relationships
- Lower overall discounting due to lack of volume purchasing from fewer vendors

Avoid Positioning Vendor Consolidation as an Either-Or Approach

Security and risk management leaders must plan for internal and external factors that may impact the strategy. Based on the survey data, external factors are responsible for two out of the top three primary drivers of their information security change in the next three to five years (see Figure 4). Incumbent vendors must keep pace with increasing regulations and external threat landscape.
changes to avoid the need for specific point solutions. For more insights on the current 2020 threat landscape and how it is changing, see “How to Respond to the 2020 Threat Landscape.”

Figure 4. External Factors Impact Information Security

External Factors to Be the Top Drivers Impacting Information Security Functions and Controls of Organizations for Next 3-5 Years
Sum of Rank (1-3) and Rank 1

<table>
<thead>
<tr>
<th>External Factor</th>
<th>Sum of Top 3</th>
<th>Rank 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT and Cyber-Physical Systems</td>
<td>43%</td>
<td>13%</td>
</tr>
<tr>
<td>Increasing Regulations</td>
<td>40%</td>
<td>14%</td>
</tr>
<tr>
<td>Evolving Threat Landscape</td>
<td>37%</td>
<td>16%</td>
</tr>
<tr>
<td>Security as a Competitive Edge</td>
<td>30%</td>
<td>8%</td>
</tr>
<tr>
<td>Business Leader Seeking Information</td>
<td>29%</td>
<td>8%</td>
</tr>
<tr>
<td>DevOps-Driven IaaS Adoption</td>
<td>27%</td>
<td>9%</td>
</tr>
<tr>
<td>Business Initiatives</td>
<td>25%</td>
<td>6%</td>
</tr>
<tr>
<td>Budget Initiatives</td>
<td>25%</td>
<td>9%</td>
</tr>
<tr>
<td>Mobile Workforce</td>
<td>22%</td>
<td>8%</td>
</tr>
<tr>
<td>Staff Shortages</td>
<td>16%</td>
<td>7%</td>
</tr>
</tbody>
</table>

n = 403, all respondents; excluding don’t know or refused

Q: What are your organization’s top three drivers that are likely to impact its information security function and controls in the next three to five years?
Source: 2020 Gartner Security & IAM Solution Adoption Trends Survey

However, IoT and cyber-physical systems were ranked as the highest overall driver when considering the top three drivers. IoT and operational technology (OT) are very heterogeneous security domains that are not well-suited to standardization unless security architecture is focused on the common network. Other internal drivers such as budgets, business initiatives including mergers and acquisitions, or a move to IaaS and SaaS also can impact a security function. Rather than a rationale for abandoning a consolidation strategy, security and risk management leaders should recognize that rationalizing the more mature and homogeneous security domains can free up time and budget to address IoT/OT security with specialized solutions.

When pursuing a vendor consolidation strategy, onboarding a very specialized point solution must be the exception and not the rule. Organizations must understand whether their business requires specialized point solutions. For example, with IoT and cyber-physical systems, organizations often find that a network access control (NAC) vendor can provide “good enough” coverage by identifying what is connected to the network. In some industry verticals such as healthcare and
manufacturing, specialized vendors that can decode and protect specific devices may be required. Having specialized needs favors a best-of-breed approach. For more insights on NAC, IoT and cyber-physical security, see “Market Guide for Network Access Control.”

Rationalize Vendors Using Frameworks

When choosing a strategy, use a framework to rationalize vendors and set a baseline from which to proceed. This exercise will set the base for current vendor portfolios and how realistic a consolidation or best-of-breed strategy may be.

Gartner speaks with many clients who start rationalization efforts by trying to segment the security market. However, vendor products may not fit neatly into a market segment nor provide adequate functionality. Surveyed organizations indicate that they deploy, on average, about six major products aligned to a market segment from their primary vendor today (see Figure 5).

**Figure 5. On Average, Organizations Deploy Five or More Security Capabilities From Their Largest Vendor**

---

**On Average, Organizations Deploy Five or More Security Capabilities From Their Largest Vendor**

Multiple Responses

- Endpoint Protection Platforms (Antivirus, Anti-Malware, etc.) 40%
- Network Firewall 40%
- User Authentication (Including MFA) 37%
- Access Management (AM) 36%
- Secure Web Gateway 35%
- Endpoint Detection and Response 34%
- Email Security 33%
- Security Information and Event Management (SIEM) 33%
- Cloud Security Posture Management (CSPM) 33%
- Web Application Firewall (WAF) 30%
- Cloud Access Security Broker (CASB) 30%
- Intrusion Prevention and Detection System 30%
- Identity Governance and Administration (IGA) 29%
- Software-Defined Wide-Area Network (SD-WAN) 28%
- Privileged Access Management (PAM) 27%
- Network Traffic Analysis (NTA) 27%
- Security Orchestration, Automation and Response 24%
- Secure Email Gateway 22%
- Distributed Denial of Service Protection 15%
- Other 1%

Average number of mentions 5.8

n = 403, biggest spend information security vendor; excluding don’t know

Q: Which of the following security tools or capabilities have been deployed by biggest information security vendor in terms of budget or spend for the current budget year in your organization?

Source: 2020 Gartner Security & IAM Solution Adoption Trends Survey

719769_C
Rather than starting with security market segmentation, begin with the outcome in mind. Start with the business value a capability brings and then align that capability with the products that are in use today from various vendors. From there, you can map out the overlaps and gaps in your existing capabilities to rationalize the vendor products that are currently in use across an organization. This applies to both vendor consolidation and best-of-breed strategies.

Gartner clients use different frameworks for rationalizing vendors, but most commonly custom capability matrices, the NIST Cybersecurity Framework (CSF), and the MITRE ATT&CK framework are seen. Sometimes, organizations use a combination of multiple frameworks to get a more complete picture (for more insights on controls, frameworks and processes, see “Security Program Management 101 — How to Select Your Security Frameworks, Controls and Processes”):

1. Use a product feature matrix to map out vendor capabilities and performance. This can be done using spreadsheets to list out vendors on one axis and capabilities on the other. Each vendor can be rated using a scale showing how “feature complete” they are to meet each desired capability. Capabilities in this exercise are defined by the organization and tailored to its unique needs. This requires more upfront work, but may yield more meaningful results with a customized assessment.

2. Use the MITRE framework to map vendor capabilities to phases of the attack chain. The MITRE ATT&CK framework is often used to map phases of attack. Using this framework can result in a meaningful way to overlay vendor products and capabilities against those common phases. This takes a more process-oriented view of how to rationalize vendors by considering how well each vendor can defend against the common phases of an attacker’s process to compromise an organization. A single vendor with an integrated set of components can be more effective than point solutions, which do not share a single visibility into the attack chain without additional integrations. See Figure 6 for a partial example.

3. Align controls with a controls framework such as the NIST CSF, and map vendor product capabilities to each control area. The NIST Cybersecurity Framework is a popular controls framework that provides another way of visualizing how vendor products help meet the control goals for information security. By mapping vendor products against the relevant controls framework, each vendor and product can be measured against how well it satisfies control across multiple categories. See Figure 7 for a partial example of how an organization might create a heat map based on NIST CSF.

Figure 6. MITRE ATT&CK Framework Example
**MITRE ATT&CK Framework Example**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vendor A Product A</strong></td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Green</td>
<td>Red</td>
<td>Green</td>
<td>Red</td>
<td>Green</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td><strong>Vendor A Product B</strong></td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Red</td>
<td>Green</td>
<td>Blue</td>
<td>Green</td>
<td>Blue</td>
<td>Green</td>
<td>Blue</td>
</tr>
<tr>
<td><strong>Vendor B Product A</strong></td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Red</td>
<td>Green</td>
<td>Green</td>
<td>Red</td>
<td>Green</td>
<td>Yellow</td>
<td>Green</td>
</tr>
</tbody>
</table>

Source: Gartner

719769_C

**Figure 7. NIST Mapping Example**
Partner with procurement and IT asset management teams to build the security vendor product list and keep it up to date. Procurement should have current contracts to know what you are paying for and how much, while IT asset management teams can provide an asset inventory of products owned by the organization. Reconciling these sources of data, along with other sources such as insular knowledge and evaluation of product capabilities by security teams, will build a more complete picture.

Organizations that create a process by which vendor products are rationalized can reuse them in other contexts such as mergers and acquisitions. Keeping an up-to-date product capability matrix helps reduce the extra effort required to gather this information when requested, and can ease the process of reconciling the two vendor landscapes at close. See “Effectively Optimizing Costs in Mergers and Acquisitions” for further insights on mergers and acquisitions.
Plan a Multiyear Transition From One Strategy to Another

Among those surveyed pursuing a vendor consolidation strategy, 83% said they have been doing so for more than a year (see Figure 8). The survey shows that most organizations pursuing consolidation report fewer vendors after Year 2, but organizations pursuing consolidation for more than two years expect to add more vendors.

Figure 8. 83% of Organizations Pursuing a Vendor Consolidation Strategy Have Been Doing So for at Least One Year

Because vendor consolidation or best-of-breed strategies require a multiyear effort, leadership changes will impact the strategy. Setting up processes and policies for internal architecture and purchasing can help vendor strategies survive leadership changes. Work directly with procurement and finance departments as they are often the gatekeepers for new purchases and can prevent deviations from the strategy through approval processes.

Beware of shelfware when signing up for an enterprise license agreement (ELA)
Plan for end-of-life and contract subscription end dates to sequence the transition from one solution to another to avoid shelfware. Set realistic goals and milestones to target those products from vendors that need to be retired based on cost and benefit, as well as current integration status. If a product is tightly integrated into other products, it can take significant effort to fully replace it.

Term licensing forces advanced planning for contract renewals. Replacing products on term licenses must be planned in advance to avoid tough situations where you must renew a contract to keep the service running often with unfavorable terms. Every contract must be tracked against the end-of-life date to allow for sufficient planning, evaluation and transition time.

**Measure Business Outcomes, Not Vendor Counts**

Selecting the right metrics for the right audience to measure progress is important in keeping everyone informed on the success of the strategy. Simply using vendor counts as a metric does not communicate the value of the strategy. Organizations use both qualitative and quantitative metrics to measure the results of their strategy to keep the project on track and make corrections as needed.

Strategically, vendor consolidation or best-of-breed approaches track closely with the Protect the Infrastructure and Manage Operations section of Gartner’s “IT Score for Security & Risk Management.” Use this tool to help baseline and track overall security program maturity tailored to your specific organization.

Tactically, it is important to choose the right qualitative and quantitative measures to track progress (see Figure 9). A few high-level examples of both types of metrics are listed below, which can be used to measure security coverage and operational complexity improvement. More examples can be found in “Security Metrics Catalog.” Also, “Make Operational Security Metrics Work for You” provides more insights into best practices for operational security metrics.

**Figure 9. Example Metrics for Measuring Progress**
Example Metrics for Measuring Progress

<table>
<thead>
<tr>
<th>Desired Outcome</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved Product Effectiveness</td>
<td>Penetration Test Results</td>
</tr>
<tr>
<td>Improved Product Quality</td>
<td>End-User Satisfaction Survey Index</td>
</tr>
<tr>
<td></td>
<td>End-User Satisfaction Survey Sentiment</td>
</tr>
<tr>
<td>Decreased Operational Complexity</td>
<td>Operational SOC Metrics</td>
</tr>
<tr>
<td></td>
<td>Security Team Engagement Survey Index</td>
</tr>
<tr>
<td></td>
<td>Security Team Engagement Survey Sentiment</td>
</tr>
</tbody>
</table>

Source: Gartner

719769_C

Evidence

Gartner’s 2020 Security and IAM Solution Adoption Trend Survey: This study was conducted to learn about which security solutions organizations are benefiting from and what factors affect their choice/preference for such solutions. The research was conducted online during March and April 2020 among 405 respondents from North America, Western Europe and the Asia/Pacific region. Companies from different industries were screened for having annual revenue of less than $500 million. Respondents were required to be at manager level or above (excluding the C-suite) and to have a primary involvement and responsibility in risk management roles for their organization.

The study was developed collaboratively by Gartner analysts and the Primary Research Team that follows security and risk management.

Recommended by the Authors

Innovation Insight for Extended Detection and Response
How to Respond to the 2020 Threat Landscape
IT Score for Security & Risk Management
Security Program Management 101 — How to Select Your Security Frameworks, Controls and Processes

Implement 4 Essentials — NIST Cybersecurity Framework

Segmentation of Technology Vendors Is the Foundation for Effective Vendor Management

Market Guide for Network Access Control

Market Guide for Operational Technology Security

Target Security Metrics at the Right Audience for Maximum Benefit

Recommended For You

Solution Scorecard for Microsoft Azure IaaS+PaaS

Summary Translation + Localization: Market Guide for Industrial IoT Gateways

Summary Translation + Localization: Evolve Your Infrastructure and Operations Organization to Remain Relevant in the Cloud Era

Increase Focus on Data Integration to Surmount IoT Data Proliferation

Explore Unconventional Talent Sourcing Solutions

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."