Demonstrating Security's Business Impact Through Operational Effectiveness

Dominic Trott
March 2020
IDC #EUR146102020

Sponsored by McAfee™
Demonstrating Security's Business Impact Through Operational Effectiveness

Introduction

Security teams are under growing pressure to enable business goals. There is growing momentum among chief information security officers (CISOs) to reposition their teams' value propositions: away from being technical experts and toward a true business support function that aligns with business outcomes such as cost reduction, risk management, and digital trust.

While an essential requirement to demonstrate the security team's ongoing value and relevance, this transformation is easier said than done. This drives interest in establishing the characteristics that CISOs need to effect this transformation. Engaging with IDC's European CISO panel, two levels have crystallized:

- There are two "non-negotiable" attributes CISOs must already possess:
  1. Technical competence
  2. A controls-oriented, programmatic approach to security operations management
- Beyond that are a range of business-oriented capabilities such as communication, relationship building, financial acumen, and risk management.

As reported in the IDC/McAfee InfoBrief Security Integration and Automation: The Keys to Unlocking Security Value (IDC #EUR145302619), there has been a positive shift in the perception of security. As indicated in the IDC Security Policy Survey, 2019 (n = 702), in 2017, 49% of enterprises viewed security as a blocker. But by 2019, 63% of enterprises viewed security either as an enabler of efficiency or as a driver for competitive advantage.

IDC's research shows that security has made progress in breaking down negative perceptions among the business, and that CISOs have a target set of attributes to develop. But what practical steps can be taken to demonstrate progress along these paths? This report seeks to set out three levels of maturity for security teams to benchmark themselves against. It also uses IDC's research to provide evidence of the business benefits on offer.

IDC's Blueprint for Security Transformation

Security has evolved as a technical discipline, oriented toward the deployment and integration of new technologies in response to the discovery of threat vectors and vulnerabilities as they emerge. Consequently, its operations tend to be inward focused. This is perhaps best demonstrated by the top key performance indicators (KPIs) that security teams measure.
According to an IDC survey of over 750 security leaders across Europe, of the top 10 security KPIs in 2019, all but three are focused on “classic” security measures such as the number of events, the number of known vulnerabilities, and the mean time to detection/resolution of incidents.

These are all important themes for security operations but mean little to business lines. In turn, a focus on these measures helps to perpetuate the status quo of focusing on incremental improvements to demonstrate security’s effectiveness, rather than aligning security with business goals. In fact, anecdotal evidence indicates that this approach helps to foster a culture that treats security as something that stands separate from the business.

This is in stark contrast with the direction of travel of the business reality for security. This is especially the case when considering the opportunity that is presented to security leaders for them to elevate their role and influence by demonstrating the links that do exist, to be a key enabler of what the business and the board want to achieve.

To help security teams and CISOs to take advantage of this opportunity, IDC has developed a three-step blueprint (see Figure 1). This aims to provide a road map for security teams that want to build a more business outcomes-oriented approach to security. It also acts as a benchmark against which security teams can compare their own situation against the rest of the market. Bear in mind that, according to IDC’s survey of over 750 security leaders across Europe, 40% of the market is at stage 1, 38% at stage 2, and 22% at stage 3.

FIGURE 1
Three-Step Blueprint for Security Transformation

- **MAKE SECURITY SIMPLE**
- **INTEGRATE** for effectiveness
- **AUTOMATE** for efficiency (incl. AI)
- **BUT** vendors MUST allay “black box” and vendor lock-in concerns
- **EXTERNALISE** for scale, capability

Source: IDC, 2020
Demonstrating Security’s Business Impact Through Operational Effectiveness

Security Operational Excellence

FIGURE 2
Top Inhibitors of Security Capability Improvement

<table>
<thead>
<tr>
<th>Issue</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security too busy on routine operations</td>
<td>44%</td>
</tr>
<tr>
<td>Security team working on tool management, not security activities</td>
<td>38%</td>
</tr>
<tr>
<td>High levels of demand for new business services</td>
<td>37%</td>
</tr>
<tr>
<td>Management's lack of understanding</td>
<td>36%</td>
</tr>
</tbody>
</table>

Q. What is limiting your ability to improve your IT security capabilities? Please rate each where 1 = no limits and 5 = very limiting. Top 2 responses only (percentages represent proportion of respondents answering 4 or 5 for each theme).
Source: IDC and McAfee, 2019

Integration

A key driver for the top two inhibitors mentioned above is the persistence of fragmented security tool environments, consisting of multiple point solutions that do not work well together. This means security personnel spend all their time integrating and operating security tools, rather than focusing on higher-value tasks.

It is no surprise that IDC’s European security survey from 2019 showed that "unified security" (i.e., rationalizing security product environments and integrating third-party products) is the top driver for security vendor selection. But beyond this, there is broader evidence of interest in security product integration. As shown in the IDC/McAfee InfoBrief, there are multiple benefits:

- The use of an integrated security management system can save the average security team 2.8 working days per week (5.6 FTEs working 37.5 hours a week).
- When asked for their primary operational expectation of an integrated security environment, the top three were faster response (36%), more effective response (35%), and better threat intelligence sharing (29%).
- An end-to-end approach to security management is four times more likely to create the perception that the enterprise's information security is ahead of its peers than with those that take an ad hoc approach.
Demonstrating Security’s Business Impact Through Operational Effectiveness

**Automation**

**FIGURE 3**
Top Expected Outcomes of Security Management Automation

<table>
<thead>
<tr>
<th>Rank</th>
<th>Outcome Description</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>Increase efficiency</td>
<td>25%</td>
</tr>
<tr>
<td>#2</td>
<td>Save time</td>
<td>19%</td>
</tr>
<tr>
<td>#3</td>
<td>Reduce time wasted on low value tasks</td>
<td>13%</td>
</tr>
<tr>
<td>#4</td>
<td>Save money</td>
<td>18%</td>
</tr>
</tbody>
</table>

Q. Why are you intending to retain/increase your usage of security management automation?
Source: IDC and McAfee, 2019

When security environments become more integrated, there is an opportunity to drive more effective automation of security tasks and processes. However, our research indicates the importance of the combination of these two concepts, with automation helping to amplify the benefits that integration offers. As reported in our InfoBrief, 62% of enterprises plan to increase their use of security automation and 88% of enterprises agree that integration will enhance the impact of security automation initiatives.

As with integration, our research shows that several business benefits can be targeted through the automation of security. Interestingly, though perhaps unsurprisingly, these are prioritized higher than more "traditional" (technical/security operational) expectations when considering the drivers for enterprises that are looking to increase their usage of security automation. The top four are shown in Figure 3.

**FIGURE 4**
Top Tasks for Security Management Automation

<table>
<thead>
<tr>
<th>Rank</th>
<th>Task Description</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>Automate security software updates</td>
<td>70%</td>
</tr>
<tr>
<td>#2</td>
<td>Automate discovery of known threats</td>
<td>63%</td>
</tr>
<tr>
<td>#3</td>
<td>Automate discovery of non-compliant devices and workloads</td>
<td>59%</td>
</tr>
<tr>
<td>#4</td>
<td>Push new policy out to devices and workloads</td>
<td>58%</td>
</tr>
</tbody>
</table>

Q. What are your priority focus areas for the automation of security management tasks?
Source: IDC and McAfee, 2019
If these are the top reasons for automating, the obvious next question is where should they be applied. The top four themes indicated by our research are shown in Figure 4.

**Externalization**

As identified in the IDC/McAfee InfoBrief, there is a spectrum of maturity for the deployment of automation tools for security solutions, ranging from ad hoc approaches to end-to-end suites. Every enterprise will have its own "sweet spot" on this spectrum, but broadly there is an opportunity to work with third-party specialists to take advantage of the benefits that integration and automation bring. Enterprises, however, must realize that there are challenges to be considered when launching initiatives in these areas.

Security teams and buyers must be careful to avoid, or at least mitigate, potential vendor lock-in through integration and automation projects. Principles such as "unified security" that target the adoption of technologies that work well in tandem, and the rationalization of security product environments through third-party integration, are central to the value propositions of most security vendors. But buyers must query prospective suppliers over how these concepts benefit the user, rather than driving cross-sales for vendors.

IDC recommends that security teams and buyers test prospective partners around three key criteria:

- First, how well does a vendor's portfolio products work in tandem?
- Second, at the very least, security vendors must show how their own solutions integrate to work together as a whole.
- Third, while this sounds straightforward, market consolidation through M&A means that a "native" integration experience is not always on offer.

The reality of the security products market is that no single vendor can meet all its customers' needs, meaning that security product environments are multivendor in nature. Therefore buyers must challenge vendors on how they can handle integration with third-party products. As a bare minimum, vendors must demonstrate how they've opened their products to integration through APIs, providing an interface for buyers (or their system integrator partners) to bring their tools together.
In an ideal world, providers would be able to go further and demonstrate "native integrations," at least with their most strategic partner in related or contiguous market segments. However, given the complexity and diversity of the security product vendor landscape, a more realistic requirement is to test their commitment to open standards. Given the diversity of the marketplace — even within a single vendor’s portfolio — open standards and integration communities are among the strongest options to enable a "single pane of glass" integration experience, while minimizing the risk of vendor lock-in.

**Conclusion**

There is a clear requirement for security teams and especially security leaders to understand and demonstrate their impact on business outcomes to raise their influence across the organization as a whole. While IDC’s blueprint for security transformation shows that there are a range of methods and maturity levels to do this, for most enterprises the primary opportunity is to strive for operational excellence in their security environment.

The three key pillars of a successful security operational excellence transformation program are integration, automation, and externalization, with evidence-based opportunities to drive business outcomes around cost reduction, operational efficiency, time savings, and staff retention/utilization.

For more insight into where and how these benefits can be unlocked, see the IDC/McAfee InfoBrief *Security Integration and Automation: The Keys to Unlocking Security Value* (IDC #EUR145302619).
MESSAGE FROM THE SPONSOR

There can be little doubt that security transformation is a hot topic or that increased integration and automation can help to advance operational excellence in most environments. However, delivering on the benefits of integration and/or automation is easier said than done.

Companies need to work with vendors that embrace open standards and are actively seeking to provide not just a platform approach to security solutions but a platform without lock-in or dependencies on that single vendor to purchase more and more of their own solutions. No company can offer the best solution in every adjacent market, so you should explore how you can access the best solution from whoever is offering it while still integrating with the rest of the security estate. Ideally, you'll be able to achieve this with a single management console that offers visibility and configuration across these multiple solutions.

We encourage you to find out more by reading the full IDC/McAfee InfoBrief at http://www.mcafee.com/epo-idc-research.

About the Analyst

Dominic Trott, Research Director, European Security and Privacy

Dominic Trott is research director for IDC's European Security and Privacy domain. As well as managing this team of analysts, Trott runs IDC's European CISO outreach program, chairing IDC's European CISO Advisory Board and the European CISO Hub panel. Trott focuses on the top challenges for European security practitioners, including the evolving role of the CISO, security that supports business outcomes, driving efficiency in security through integration/automation/orchestration, and the future of trust.
About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world’s leading technology media, research, and events company.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Global Headquarters
5 Speen Street Framingham, MA
01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com

Copyright and Restrictions

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or permissions@idc.com. Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Copyright 2020 IDC. Reproduction is forbidden unless authorized. All rights reserved.