Security Integration and Automation: The Keys to Unlocking Security Value

August 2019

Authors
Dominic Trott
Chris Bryan

An IDC InfoBrief, sponsored by
McAfee

IDC #EUR145302619
What Will You Learn From This InfoBrief?

**PART 1**
**INDUSTRY CONTEXT**
Security teams are under growing pressure not just to deliver technical expertise, but also to enable business goals. What factors are limiting the security team from improving its capabilities? And how has the business perception of security changed over the past two years?

**PART 2**
**THE OPPORTUNITY**
The integration of tools and automation of processes for managing security infrastructure provide key means to address these challenges. What benefits can you expect from more integration and automation in security management? What benefits are unlocked as you move up the maturity scale?

**PART 3**
**THE CHALLENGE**
The use and integration of security tools and the automation of security processes are established concepts. How do you compare with industry benchmarks? What are the levels of adoption and maturity? What is the relationship between the automation of process and the use of tools?

**PART 4**
**NEXT STEPS**
Almost unanimously, enterprises plan to increase their use of integration and automation in security management. What are the ambitions driving these decisions? What specific tasks are these ambitions pinned to? What are IDCs recommendations to transform those ambitions into concrete steps?
PART 1
INDUSTRY CONTEXT
Introduction

Security teams are undergoing a reappraisal of their value propositions for the business. Traditional measures of success have been metrics such as threats detected, time to detection, and time to response. These still apply, but increasingly security teams are expected to contribute towards business outcomes such as cost reduction and workforce optimization.

This research shows that the integration and sophistication of security management tools, plus security management automation, can support these goals, with two elements at play:

First, enterprises can target tangible gains via automation and integration. E.g., On average, enterprises can expect to claw back 62 days' effort from the security team by addressing a lack of security management integration.

Second, there is the issue of perception. Enterprises with end-to-end management suites are four times more likely than those reliant on ad-hoc approaches to perceive their IT security as being ahead of their peers.

For organizations that perceive themselves as behind their peers in terms of IT security, or at best in line with them, our research indicates that the integration and automation of security management — a security platform approach — is a key opportunity to change that perception.

Q. How do you think your organization’s information security compares with your peers?

- Similar proportions make use of ad-hoc approaches and end-to-end suites for security management (c. 10%)
- Yet the share of end-to-end suite users that feel their security is ahead of their peers outnumber ad-hoc equivalents by 4:1
- Although less marked than for integration, the same trend applies for automation
- The proportion of those who are fully automated that feel they are ahead of their peers outweighs their fully manual peers by a ratio of 2:1

Source: IDC, Security Policy Survey, April 2019 n=702
Security’s Role in Enabling Business Outcomes

RAISING AWARENESS AND INFLUENCE OF SECURITY

The criticality of security is well recognized, reaching number 1 in the World Economic Forum global risk register back in 2018. Yet the expectations of security teams are evolving. They cannot afford to be perceived as technical experts alone, but must also be seen to support business outcomes.

The good news is that security teams have made progress — with a strong positive shift in the past two years, from being perceived as business blockers by half of enterprises, towards being seen as business enablers by the majority.

But there is room to improve. This study shows how integration and automation combine to create a security platform approach that addresses the challenge.

In this way, security teams and product environments will become more connected, work together better and drive superior results — creating both operational and business benefits.

Q. What is your organization’s general perception of the IT security function?

TWO YEARS AGO

49% saw security as either a blocker of innovation, a compliance hurdle, or a necessary cost

ROLL FORWARD TO NOW

63% see security as either an enabler of efficiency or a driver of competitive advantage

UNLOCK THE OPPORTUNITY!

Source: IDC, Security Policy Survey, April 2019 n=702
Security’s Structural Inhibitors

THE POTENTIAL TO DRIVE BUSINESS BENEFITS BY TRANSFORMING SECURITY MANAGEMENT IS STRONG, BUT THERE ARE SOME KEY HURDLES TO OVERCOME

While the opportunity to drive business benefits through security is strong, there are structural inhibitors preventing this.

Primarily, the nature of security product environments and processes prevent personnel from maximizing the amount of time they spend delivering higher value activities such as responding to threats or building user awareness. Those challenges inhibit metrics such as staff attraction/retention, resource utilization, and cost reduction.

What is more, they also contribute to the perception of security as a business blocker, preventing security from fulfilling demand for new business services and undermining management understanding.

A security platform approach, combining the automation and integration of security tools and processes, can help to alleviate these issues.

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)

- Security too busy on routine operations: 44%
- Security team working on tool management, not security activities: 38%
- High levels of demand for new business services: 37%
- Management’s lack of understanding: 36%

Source: IDC, Security Policy Survey, April 2019 n=702
PART 2

THE OPPORTUNITY
Enterprises agree that integrating the tools and automating the processes used for security management can be expected to drive benefits. Out of the eleven categories of benefits identified, there were a clear top three. Critically, each of these themes can be linked to those business needs of cost reduction, staff attraction & retention, and resource utilization.

Q. What benefits would you gain from better integration and centralization of your security management environment? [Choose up to 3]

- Reduction of operating costs: 46%
- Improved staff retention: 41%
- Automation of low-value, repetitive tasks: 33%

Source: IDC, Security Policy Survey, April 2019 n=702
Security Management: The Maturity Scale

TWO LENSES FOR MEASURING MATURITY IN SECURITY MANAGEMENT

For the purposes of this study, the maturity of security platform adoption has been measured in two areas:

1. Automation of security management processes
2. Sophistication of security management tools

These have been divided into five steps to show a progression through low, medium, and high maturity levels.

01  Degree of automation in security management

- Manual processes only
- Mainly manual processes (some automation)
- 50:50 manual / automated processes
- Mainly automated (some manual)
- Fully automated

02  Sophistication of security management tools

- Ad-hoc
- Out-of-the-box from existing suppliers
- Blend of out-of-the-box & specialist tools
- Specialized security mgmt. tools
- End-to-end security mgmt. suite

Source: IDC, Security Policy Survey, April 2019 n=702
Security Management Automation: Maturity Benefits

REALIZING BENEFITS BY MOVING UP THE AUTOMATION Maturity SCALE

This analysis was created by measuring the level of emphasis that was placed on the various benefits expected from greater use of automation in security management at each stage of maturity. Identifying where the emphasis for each benefit started to drop gave an indication where a “step change” from those benefits was realized up the maturity levels.

Q. What benefits would you gain from better integration and centralization of your security management environment? [Choose up to 3]

- While there remains a focus at each level of maturity, the most marked “realization” was at the leap from level 1 to level 2:
  - Cutting costs
  - Staff retention
  - Automation of menial tasks

- When moving towards more of a balance between manual and automated processes, enterprises begin to benefit more from improved accuracy in their security activities. This is likely to stem from the minimization of human error that manual processes may encourage.

- Once security management processes are mainly automated, key benefits are realized. First, security staff are empowered to perform higher value tasks. This clearly relates to the automation of lower value, repetitive tasks. As a result of this greater degree of automation, enterprises also see their speed of response improve.

- Where enterprises become fully automated, the impact of integration across the broader security product environment is realized. This is critical, because it backs up the assertion that the full benefits of process automation cannot be realized unless they run within integrated environments.

Source: IDC, Security Policy Survey, April 2019 n=702
Security Management Tools: Maturity Benefits

REALIZING BENEFITS BY MOVING UP THE MANAGEMENT TOOLS MATURITY SCALE

This analysis was created by measuring the level of emphasis that was placed on the various benefits expected from more sophisticated security management tools at each stage of maturity. Identifying where the emphasis for each benefit started to drop gave an indication where a “step change” from those benefits was realized up the maturity levels.

Q. What benefits would you gain from better integration and centralization of your security management environment? [Choose up to 3]

- Significant benefits were highlighted by respondents as they moved from ad-hoc approaches to the use of out-of-the-box tools, these include:
  - Cutting costs
  - Staff retention
  - Automation of menial tasks

- When using a blend of out-of-the-box tools with some specialist management tools, enterprises begin to benefit more from improved accuracy and speed of response in their security activities. This is likely to stem from the efficiencies that begin to be gained from moving towards a smaller number of dedicated management tools, as opposed to “making do” with a wider variety of default out-of-the-box ones.

- Once the management of security has been consolidated around specialist tools, enterprises benefit from more empowered staff. This is linked to staff being freed from repetitive, lower-value tasks that the tools can handle for them. This also explains the realized benefits around vendor consolidation, with enterprises able to rely on fewer, more specialist suppliers. This in turn reduces the burden of supplier management.

- Once enterprises have moved to the use of end-to-end security management suites, they benefit from the resulting product integration. The systems integration burden on security staff falls as they no longer need to “stitch together” a tapestry of management tools with their broader environment of security products. Another benefit realized at this point is central reporting, working through a single system as opposed to multiple tools.

Ad-hoc
Out-of-the-box from existing suppliers
Blend of out-of-the-box & specialist tools
Specialized security mgmt. tools
End-to-end security mgmt. suite

Source: IDC, Security Policy Survey, April 2019 n=702
PART 3

THE CHALLENGE
Security Management — Sentiment for Uptake

**TOOL INTEGRATION AND PROCESS AUTOMATION ARE SPENDING DRIVERS**

There is strong positive buyer sentiment for security platform approaches through both the automation of security management processes and the integration of security tools among respondents to our survey (i.e. the balance between respondents wishing to increase usage and those that want to decrease it).

To arrive at this number, the proportion of respondents planning to decrease their use of the technique was subtracted from the proportion planning to increase it.

For automation, 2% planned to decrease use, with 36% planning to retain the same level of use.

For integration, 1% planned to decrease use, with 45% planning to retain the same level.

**SENTIMENT TOWARDS AUTOMATION**

Q. When it comes to your use of automation for security processes, do you intend to increase or decrease your use of this? (% represents the number answering positively minus the number answering negatively)

+62%

**SENTIMENT TOWARDS INTEGRATION**

Q. When it comes to the integration of security management tools, do you intend to increase or decrease your use of this? (% represents the number answering positively minus the number answering negatively)

+54%

Source: IDC, Security Policy Survey, April 2019 n=702
Security Management — Current Situation

**DIVERSE APPROACHES TO MANAGING SECURITY INFRASTRUCTURE**

Currently, security infrastructure management is fragmented, albeit with “normal” distribution. Roughly equal numbers (c. 25%) sit somewhere in the middle of the security scale, using either out-of-the-box tools from existing suppliers, specialist management tools, or a combination of the two.

Another equal-sized group relies on third parties to handle the task. Much smaller groups (c. 13% each) sit at the two extremes, with either an end-to-end security management suite or entirely ad-hoc approaches.

One point is clear though:

86% of enterprises use tools — of one kind or another — for security management

Q. What is your primary means of managing your IT security infrastructure?

Source: IDC, Security Policy Survey, April 2019 n=702
Security Integration — Current Situation

**MIXED APPROACH TO INTEGRATION AND RATIONALIZATION OF TOOLS**

Yet there is clear recognition of the problems that a lack of integration brings:

- Overall, enterprises believe there is a **16%** likelihood of error due to a lack of integration in security management tools. While this may sound small, any chance of error has the potential to be devastating.
- **75%** believe that over 5% of the security team's time is wasted due to lack of integration.
- With the average security team consisting of 5.6 staff, that represents a potential claw back of **62 working days annually for the security team** through full integration.

**Q. Has your organization already begun the integration and rationalization of tools in your security environment?**

Of the enterprises surveyed, **ONLY 54%** have begun integrating and rationalizing tools in the security environment.

Source: IDC, Security Policy Survey, April 2019 n=702
Integration Amplifies Automation

Integration Amplifies Automation

AUTOMATION OF SECURITY MANAGEMENT IS ALREADY AN ESTABLISHED CONCEPT

Q. To what level have you adopted automation in your IT security management?

- Entirely automated: 27%
- Mostly automated: 26%
- Mostly manual: 23%
- Entirely manual: 14%
- Strive for a balance: 15%

There is clear recognition of the benefits that automation brings to integration:

- 62% of enterprises plan to increase their use of security automation.
- 88% of enterprises agree that integration will enhance the impact of security automation initiatives.

UNTIL EFFECTIVE SECURITY MANAGEMENT AND INTEGRATION HAVE BEEN ACHIEVED, TO CREATE A SECURITY PLATFORM APPROACH, THE BENEFICIAL IMPACT OF AUTOMATION WILL BE LIMITED

Source: IDC, Security Policy Survey, April 2019 n=702
Don’t Forget Automation in the Cloud

INCONSISTENT SECURITY DEPLOYMENT AUTOMATION FOR CLOUD AND ON-PREMISE

The automation of security deployments for new server builds in on-premise environments is well-established, adopted by over 60% of enterprises.
Yet less than half of enterprises have automated security deployment for cloud workload deployment.
With digital transformation continuing to intensify, failing to automate security deployment for cloud workloads is a missed opportunity.
Equally, enterprises must not assume that cloud workloads are inherently secure.

Q. When deploying new on-premise server builds, do you have automated security deployment capabilities in place?

Q. When deploying cloud workloads, do you have automated security deployment capabilities in place?

Source: IDC, Security Policy Survey, April 2019 n=702
PART 4

NEXT STEPS
Security Integration and Automation: The Keys to Unlocking Security Value

PART 4: NEXT STEPS

Security Automation Goals

MOST PLAN TO INCREASE SECURITY MANAGEMENT AUTOMATION, BUT WHY?

It is critical to note that the top four outcomes expected for security management outcomes are all business-outcome-related, as opposed to security/technical goals. These points came ahead of more “traditional” expectations such as improving security outcomes or reducing the risk of false positives. This shows that security recognizes the need to demonstrate business benefits to support their ambitions. For enterprises considering where to begin with the automation of security management tasks, focusing on addressing the top automation tasks will result in tangible business benefits and should be made an investment priority.

Top 4 Outcomes

Q. Why are you intending to retain/increase your usage of security management automation?

1. Increase efficiency 25%
2. Save time 19%
3. Reduce time wasted on low value tasks 13%
4. Save money 18%

Top 4 Tasks to Automate

Q. Which are your priority focus areas for the automation of security management tasks?

1. Automate security software updates 70%
2. Automate discovery of known threats 63%
3. Automate discovery of non-compliant devices and workloads 59%
4. Push new policy out to devices and workloads 58%

Source: IDC, Security Policy Survey, April 2019 n=702
Security Integration Goals

CLEAR EXPECTATIONS OF WHAT INTEGRATION CAN OFFER

IDC asked what benefits enterprises expected to gain from the integration of security tools. The three responses all relate to saving time for the security team.

This ties to the expectation that the use of a management system will save the security teams’ time:

- Typical expected savings for around half of respondents were up to 10% of the team’s time. This could represent a saving of 2.8 working days per week. Assuming an average team (with 5.6 FTEs working 37½ hours a week).

Q. What is the key expectation/outcome for integration in your security environment?

36% FASTER RESPONSE
35% MORE EFFECTIVE RESPONSE
29% BETTER THREAT INTEL SHARING

BUT these issues represent MORE THAN JUST TECHNICAL IMPROVEMENTS. Each can be expressed in terms of business benefits. For example:

VALUES THAT ARE EASILY UNDERSTOOD BY BUSINESS LEADERS AND THE BOARD

Source: IDC, Security Policy Survey, April 2019 n=702
Key Take-Aways

To maximize its impact, security must work with, and for, the wider business.

Progress has been made — this study shows that perception improved by 12% in the past two years. But there is still room for improvement.

To move further down the path of business enablement through a security platform approach, IDC offers the following set of recommendations:

**Integration and automation** have a strong positive impact on the perception of security. With a lack of management understanding being one of the key limiting factors to improving IT security, this is a key opportunity to forge a common view.

Security must speak the language of the business. **Build a business case for automation and integration by applying the top business metrics** identified in this study (reduced costs, staff retention, resource utilization, response accuracy).

Moving up the maturity chain provides a clear benefits roadmap through both the automation and integration of security management. Identify where your organization sits on this scale and consider the benefits available at higher levels.

The integration and automation of security management go hand in hand — 88% of enterprises believe they drive better results in tandem. Consider how they can work together in your security plans to deliver mutual benefit. Don’t forget that this applies both for on-premise and cloud environments.

The benefits gained from **security automation and integration initiatives map directly onto business outcomes**. Key opportunities include cost reduction, improved efficiency, and optimized staff attraction/retention.
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 Notice

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 2019 IDC. Reproduction is forbidden unless authorized. All rights reserved.