

Managing Security Operations: Towards Integration and Automation



September 2017

An IDC InfoBrief, Sponsored by



Executive Summary

IDC conducted a survey with BT and McAfee to understand the differences between companies' security estates, with a particular focus on end-user views and buyer preferences.

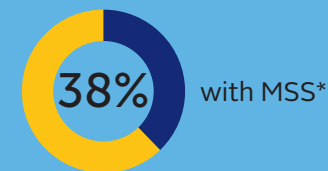
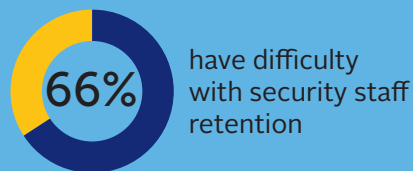
The study addresses a number of topics, including the shortage of security professionals, automation of security processes, the emergence of new technologies, and organisational approaches to GDPR readiness.

The collected data provides a comprehensive insight into the dynamics currently shaping the security market and how technology rationalisation, driven by integration and automation, can help remediate the skills shortage. A focus on the management of security estates will help organisations develop best practices for their security operations.

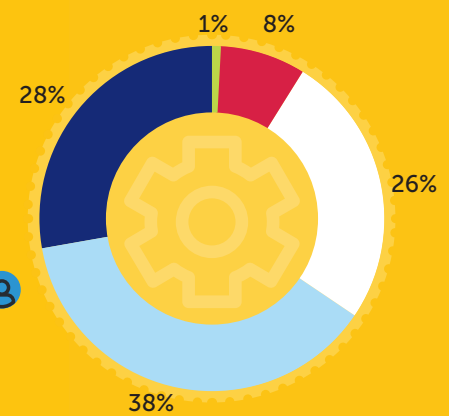


Addressing the Security Gap

As the security skills shortage is felt in all organisations, it is driving the search for operational efficiencies, especially through automation and managed security services.



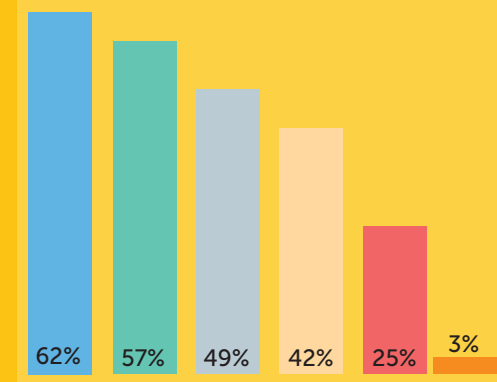
Automation is essential to address the skills shortage. MSS is also growing as a result.



How difficult is it to find or retain skilled security staff?

- very easy
- easy
- neither difficult nor easy
- difficult
- very difficult

What are the biggest issues within your organisation regarding IT security skills availability?



- Retaining talent
- Ongoing training & skills development of existing staff
- Recruitment of talent
- Salary expectations
- Need to hire external consultants
- No impact, we don't have a skills shortage

*Source: IDC WE European IT Security Strategies Survey, April 2017, n=737 | IDC Custom Survey, July 2017, n = 450

Too many products!

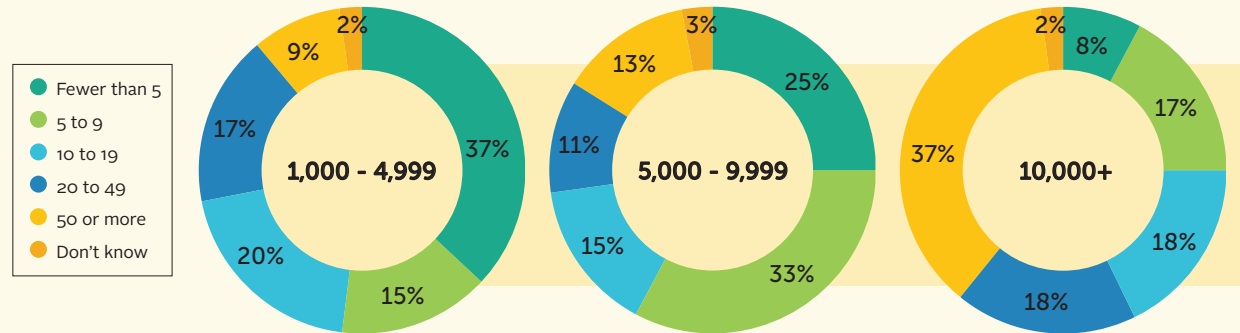


of firms have 10 security products or more deployed in their organisation.

This rises to 73% for larger firms with over 10,000 employees.

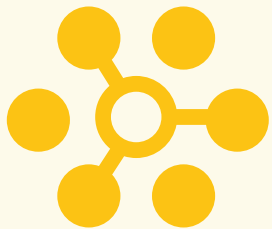
Individual security product types

How many of the following do you deploy in your organisation for IT security?
Individual security product types



The larger the organisation, the more vendors are involved — 14% deal with 10 to 50 vendors!

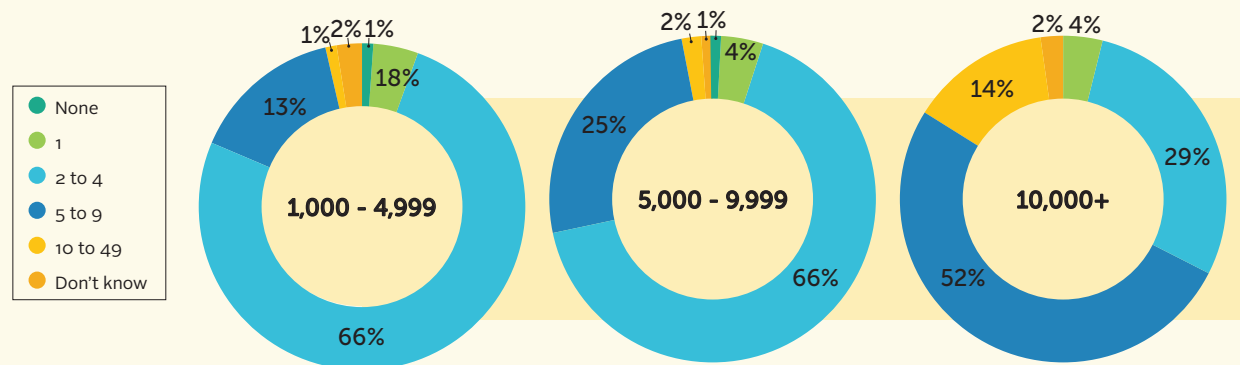
Not (so) many vendors!



Vendor consolidation seems to have already started, as 55% of firms only deal with 2-4 separate security vendors.

Distinct security vendors

How many of the following do you deploy in your organisation for IT security?
Distinct security vendors



Technology rationalisation drives product selection as larger organisations look for ease of integration and fewer products in their security environment.

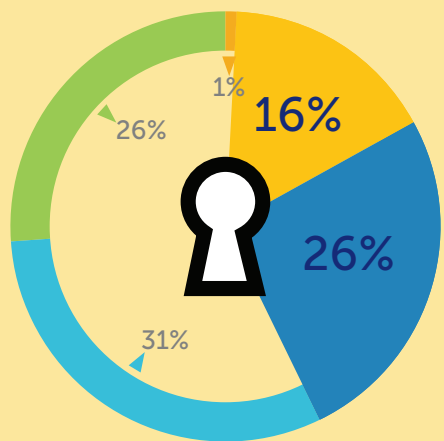


Evolution of product selection towards better integration

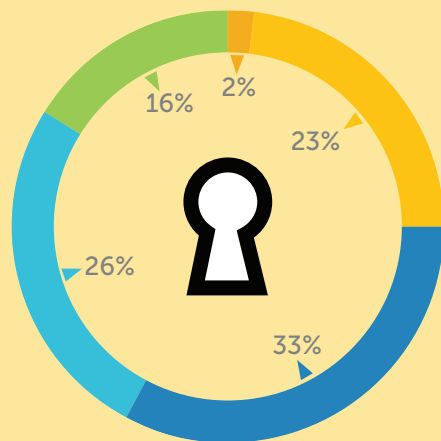


Which statement best describes your approach to selecting a security vendor?

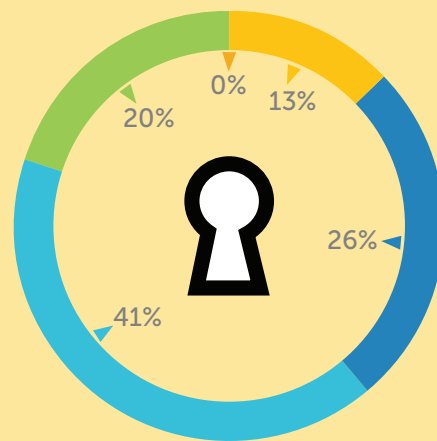
- We prioritise standalone point products regardless of integration concerns
- We tend to buy standalone point products but also look to integration if it makes sense
- We are evenly balanced between products that work together and standalone point products
- We tend to buy products that work well together but still buy standalone point products
- We prioritise management and integration and buy products that work well together



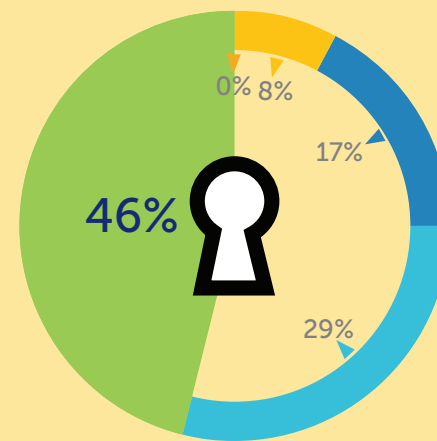
All



1,000 to 4,999



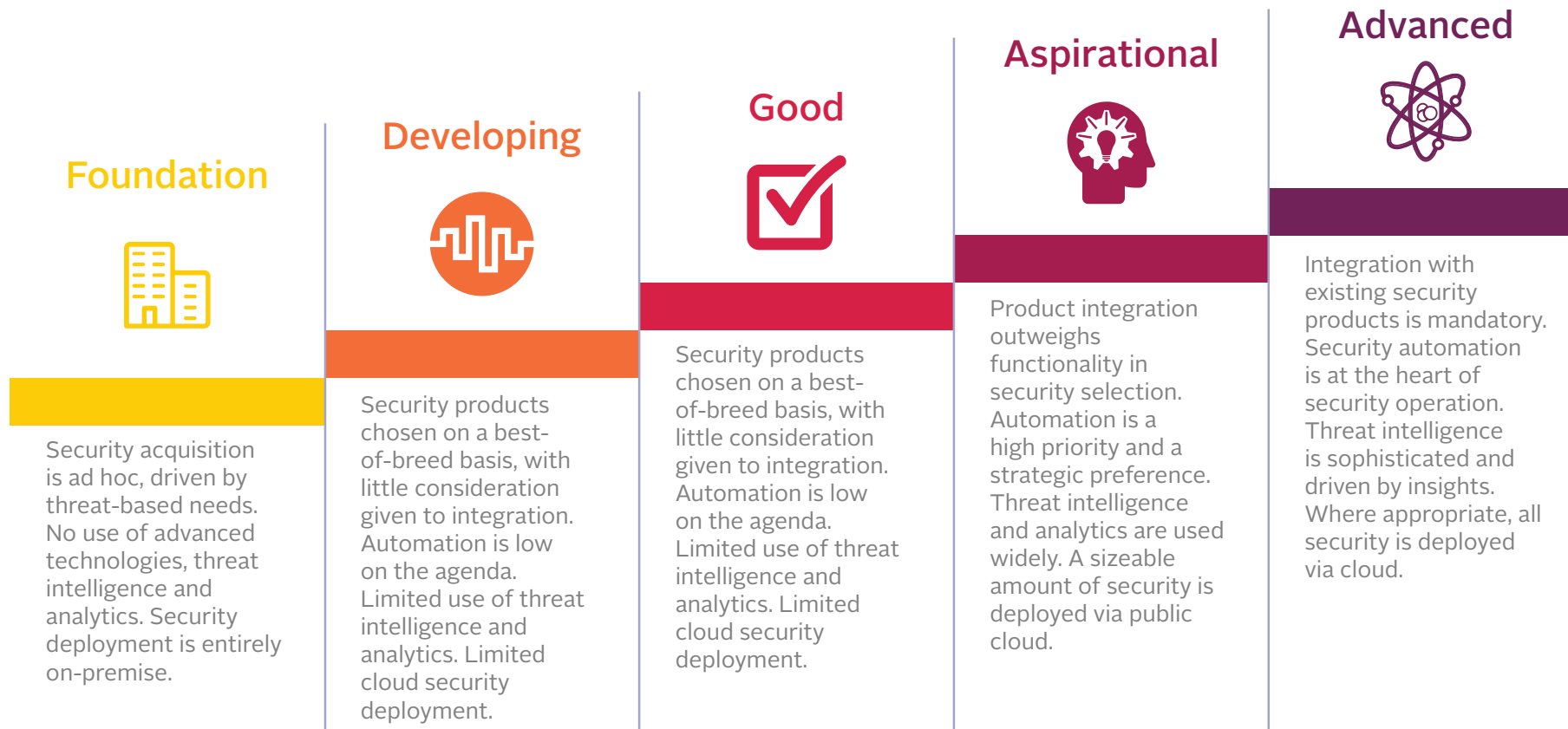
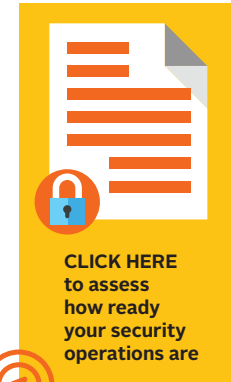
5,000 to 9,999



10,000+

IDC's 5 levels of security operations readiness

IDC has developed a model to help security executives assess their organisation's security operations readiness through five readiness stages

CLICK HERE
 to assess
 how ready
 your security
 operations are

Organisations integrate their security products to enable the automation of their IT security

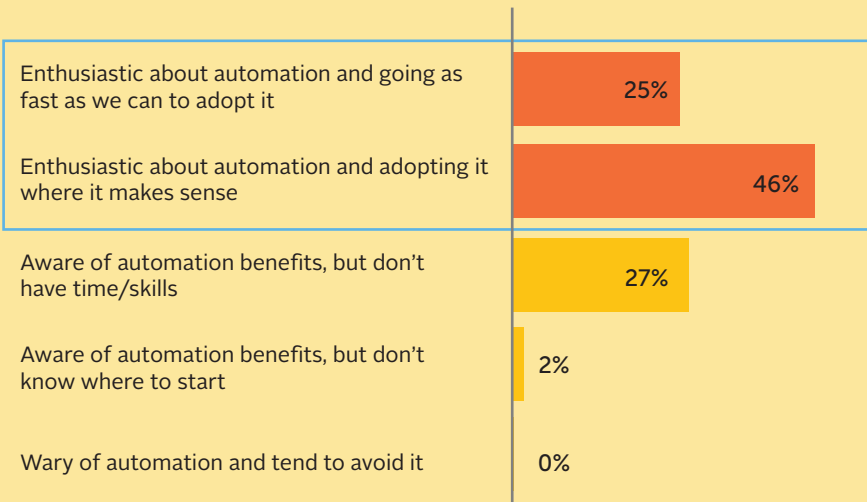
Views of automation among IT security management is hugely positive — over 70% are enthusiastic about mass-scale adoption

Managing endpoint products is the main area for IT security automation, with 85% adoption.

The most mature organisations with more advanced security product integration are the highest adopters of IT security automation.

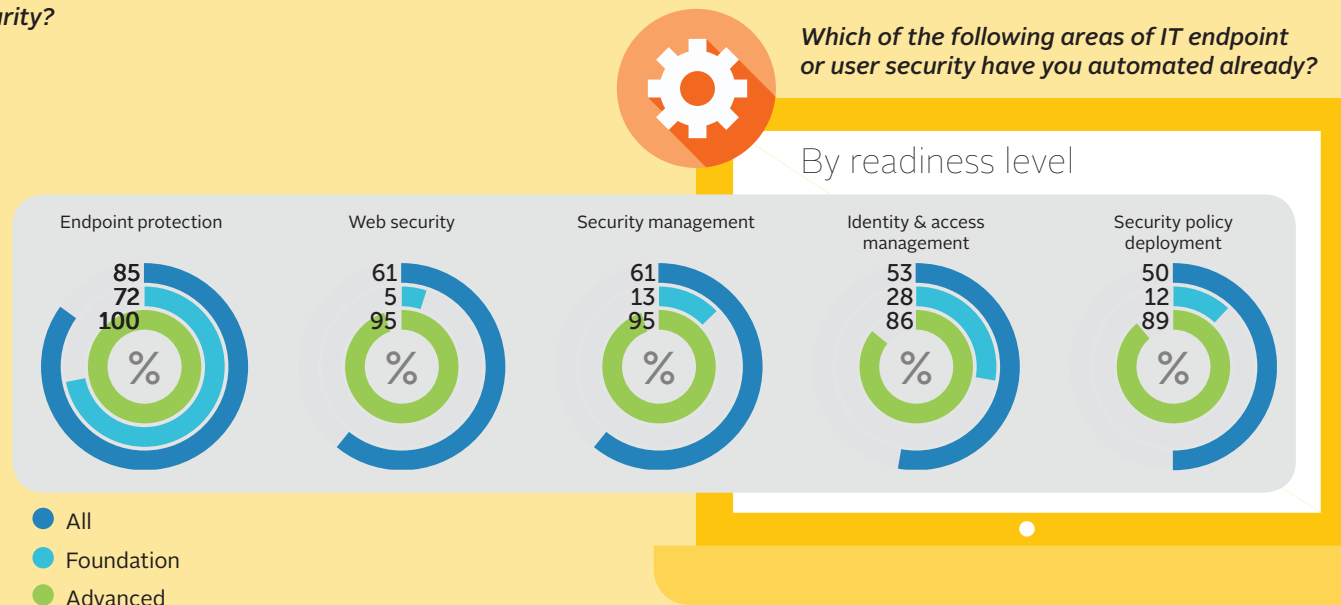


How does your IT department feel about adopting automation to manage IT security?

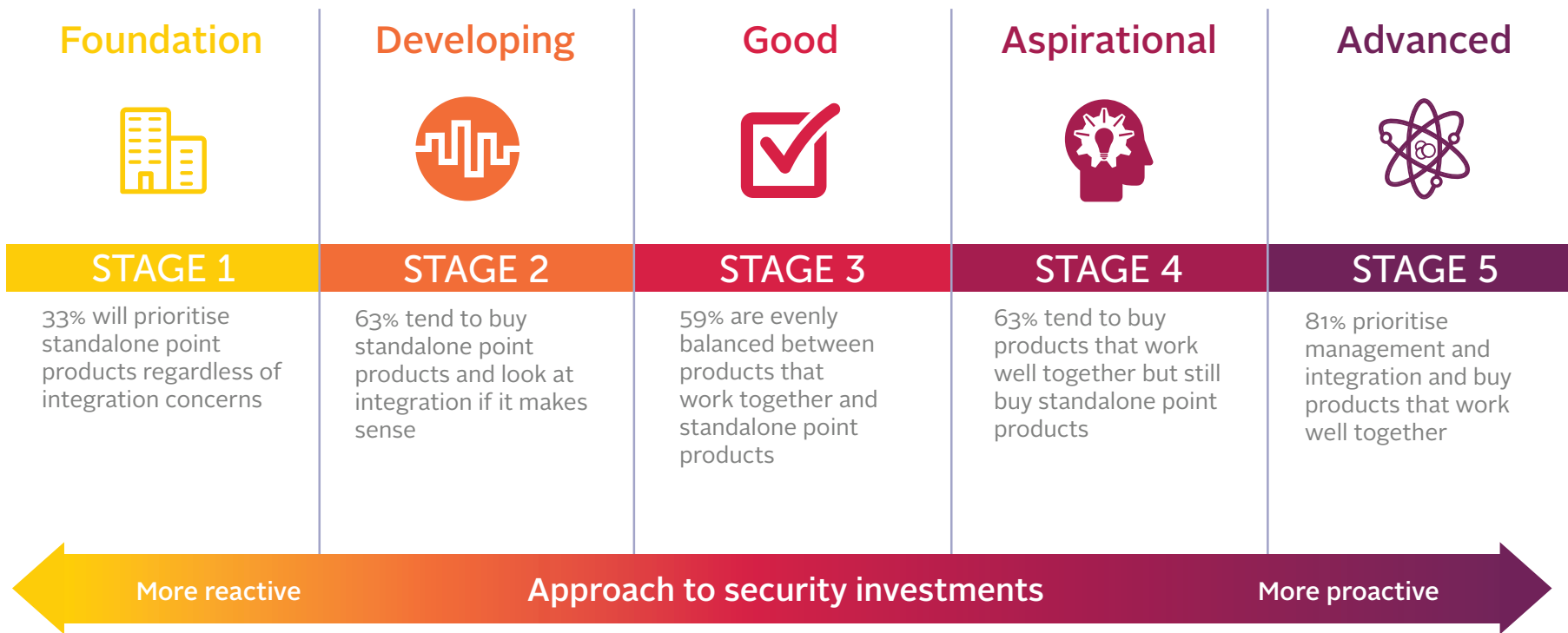


Source: IDC Custom Survey, July 2017, n = 450

Which of the following areas of IT endpoint or user security have you automated already?



Security maturity (or the lack of it) is a driver of the mindset – less mature means more fragmented

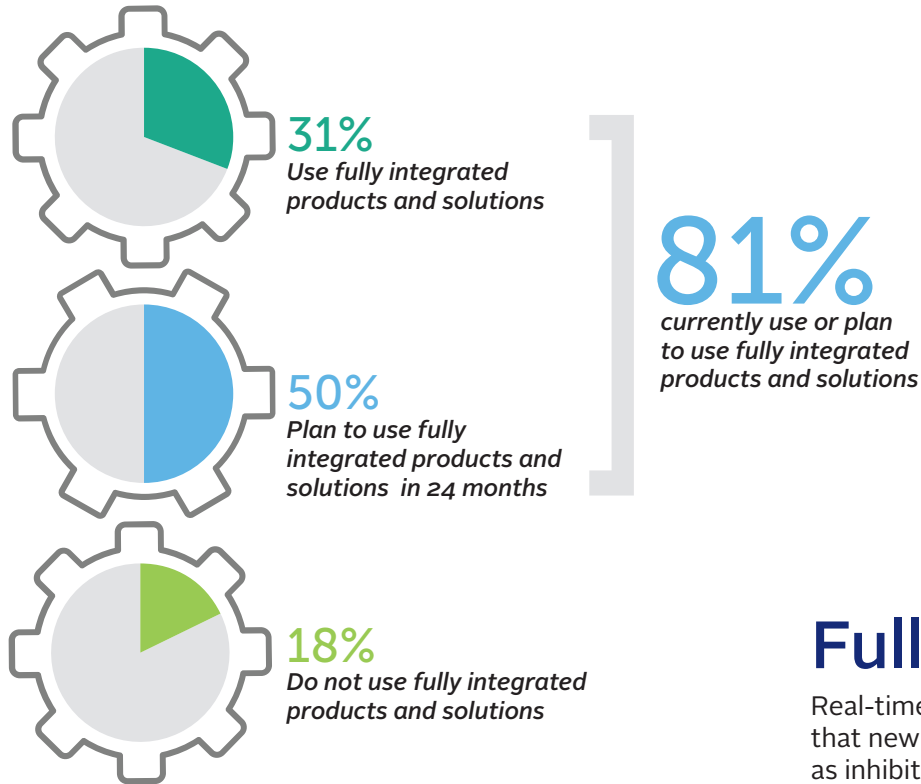



CLICK HERE
to assess
how ready
your security
operations are

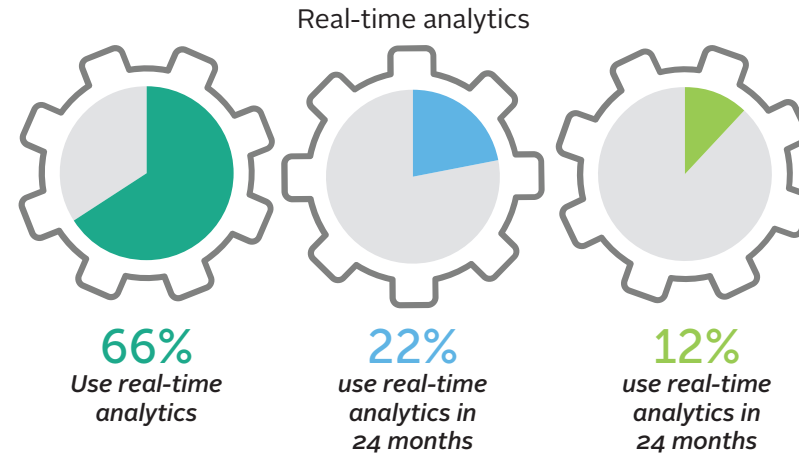


Will emerging technologies exacerbate or solve the complexity issue?

Full integration of products and solutions



Real-time analytics is the most used new technology, deployed by 66% of organisations, ahead of AI, machine learning and threat hunting



Full integration

Real-time analytics adoption shows that new technologies are not seen as inhibitors and can be a driver of integrated technology adoption.



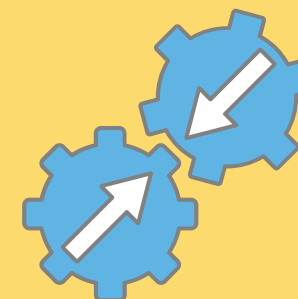
Organisations that don't do full integration will be in the minority in two years' time.



This will put pressure on the acceptance and adoption of emerging technologies that do not integrate well with other solutions (except for real-time analytics, which is already deployed).

Summary

- The skills shortage is a pain point in all organisations. Automation is seen as a solution to this problem.
- Managed security services can alleviate skills shortages, as well as offering pain-free access to integrated and automated solutions.
- Integration is a prerequisite to automation.
- Within two years, integration will be the norm, putting pressure on point solutions that don't integrate well.
- Organisations need to increase the level of integration and automation and have a proactive approach to investment in their security operations, in order to move to a more mature level of readiness.



Call to action

- Assess the complexity of your security operations by determining the amount of separate products and vendors.
- Determine your propensity to buy point solutions versus holistic and integrated security architecture.
- Determine your attitude and readiness to adopt integration and automation in your organisation.
- Consider managed security services as a complementary approach to gaining skills.



Methodology

IDC 2017 Security Survey for BT and McAfee

IDC conducted a survey of 450 global organisations with over 1,000 employees to understand the current readiness of security, and to find out where organisations are focusing their security efforts around automation, integration, threat intelligence and emerging security technologies driving the market.