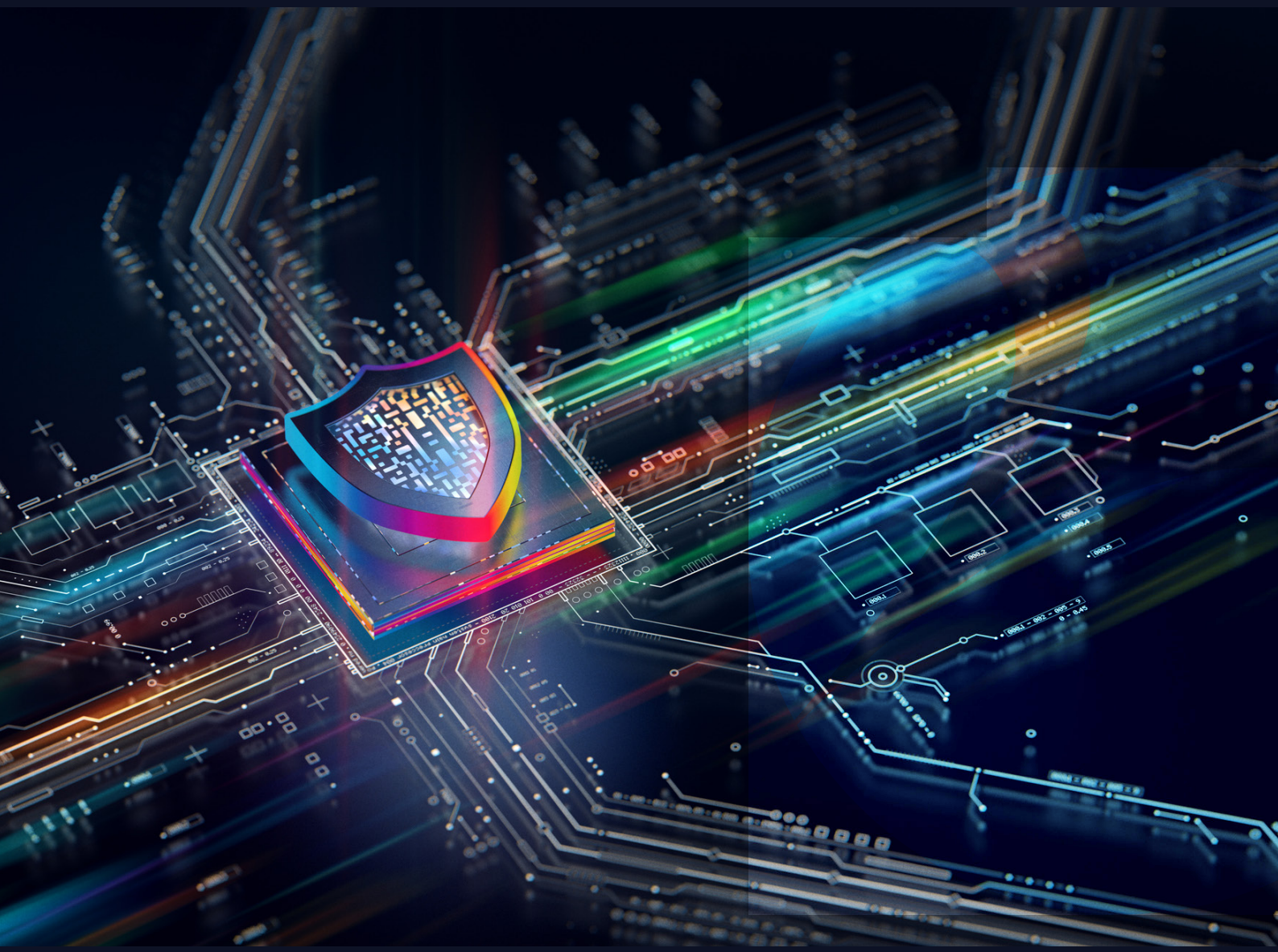
BYTES | Smarter together



Security Survey 2024

By Bytes Software Services
March 2024

Introduction

Thanks to everyone who took the time to help shape this 2024 Security Survey, which focuses on vendor consolidation. By gathering insights into the current challenges and best practices associated with a vendor consolidation strategy, this report aims to shed light on how organisations can drive greater efficiencies and cost savings by having fewer security vendors in their environment.

Here are some of the highlights for the report:

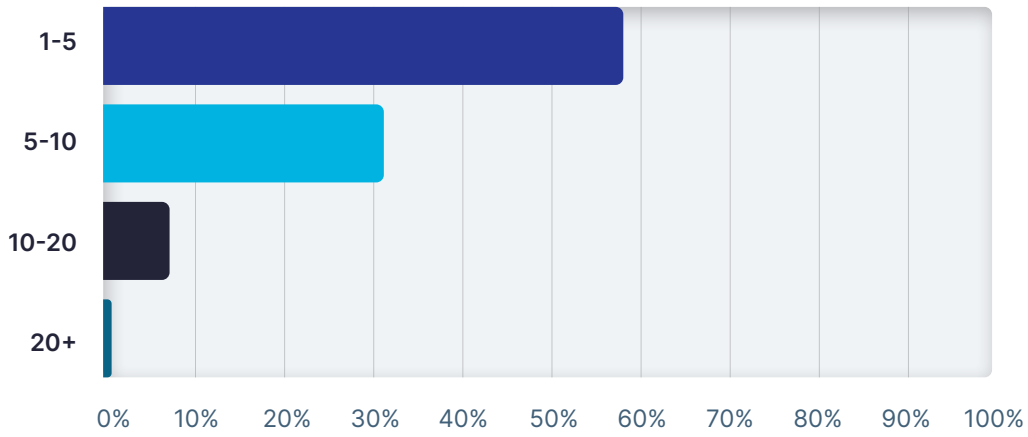
- **Multiple Portal Management** is the biggest challenge organisations face today when managing their security vendor portfolio
- **Delivering cost savings** continues to be a priority for most organisations
- **Vendor consolidation** is on the roadmap for most organisations within the next 24 months

This report includes expert views and commentary from **Luke Kiernan** (Head of Cyber Security at Bytes), **Jacob Ross** (Team Lead - Network Security at Bytes), **Giuseppe Damiano** (Senior Technical Presales Consultant at Bytes), and **Adam McCaig** (Cyber Security Evangelist at Bytes).

If you would like to discuss the findings of this Bytes Market Report with a specialist, or are keen to understand how Bytes can optimise your 2024 Cyber Strategy, reach out to your dedicated Account Manager, or email tellmemore@bytes.co.uk

Q1.

How many security vendors do you currently use in your organisation?



Summary

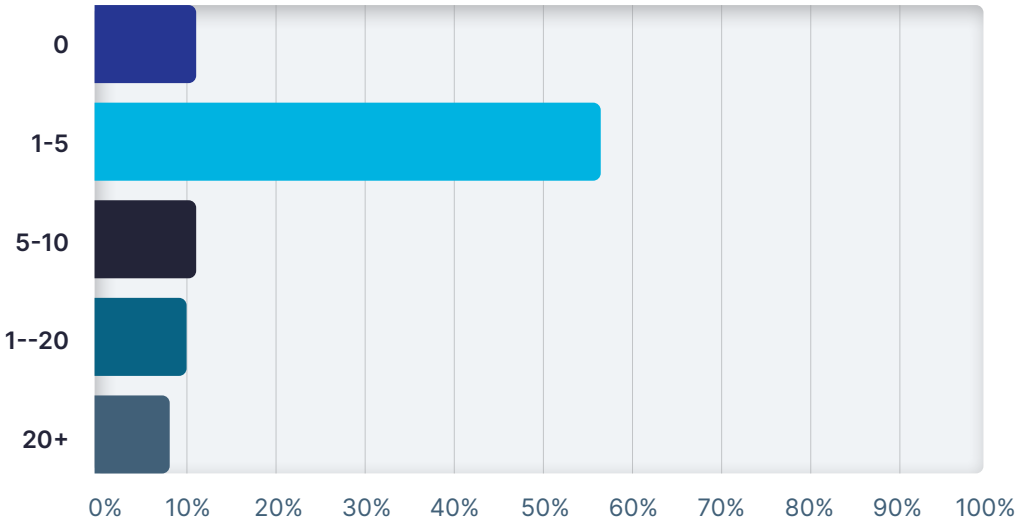
It is surprising to see that as many as 58% of respondents have less than 5 security vendors in their organisation, particularly when you consider that it is best practice to have security solutions in place that cover: Email, Web, Identity, Data, Cloud, Network monitoring and Endpoints.

The high percentage could however be explained by the fact that these organisations have other technologies in place that are delivering some of the necessary functions but are not considered to be security vendors. We know, for example, that Microsoft has many in-built security capabilities, but few organisations will categorise them as a security vendor.

Often, when we start an engagement with an organisation and we audit their security posture, it is not uncommon to discover up to 20 different security vendors in situ. While this number is a little high, it is best practice to have a layered approach to security, so it is about striking the right balance between having sufficient depth on each area of security, and the number of vendors required to provide it.

Q2.

How many people in your organisation are directly aligned to security?



Summary

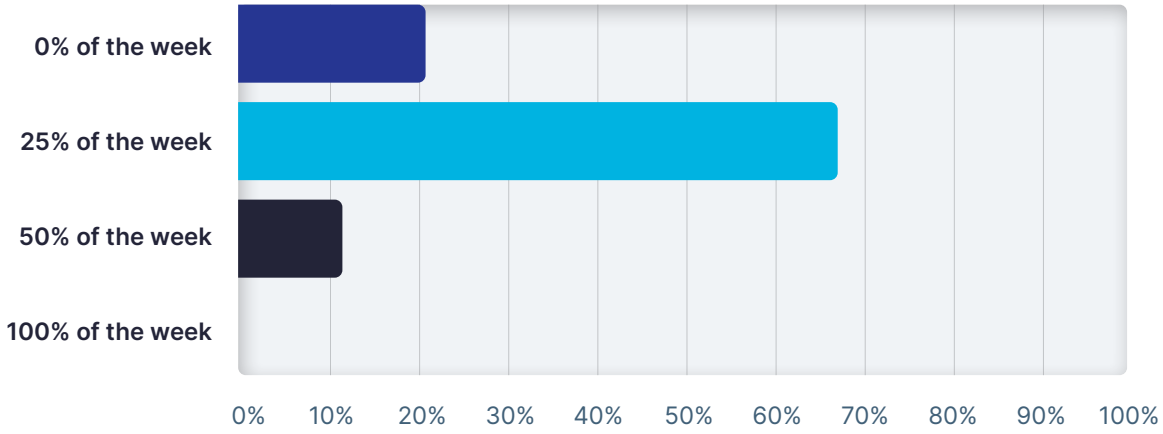
While it is encouraging that 88% of organisations that responded have at least 1-5 dedicated security personnel, it is concerning that 12% of organisations have no one directly aligned to security. This is probably because finding affordable and experienced security professionals remains challenging and is still not seen as a high priority in some Boardrooms.

The suggestion to organisations that are struggling to provide minimum viable levels of security, is to look to partner with specialist managed security providers. These partnerships can deliver many benefits, such as constant cover, up to date skills and experience on tap, and measurable service levels.

Of the findings, it is encouraging that almost a third of respondents have over 5 security personnel in situ. It is likely that many respondents that fall into this bracket have their own SOC and that security is treated as a priority at the Board level. It is also likely however that many of the respondents in this category may be having to increase resources to support a sprawling number of different security vendors. In this instance, our advice is to review your vendor portfolio and see if there are consolidation opportunities as these will almost certainly help optimise resourcing levels.

Q3.

In an average working week, what percentage of time would teams not directly associated with security engage in hands-on management of security tools and tasks?



Summary

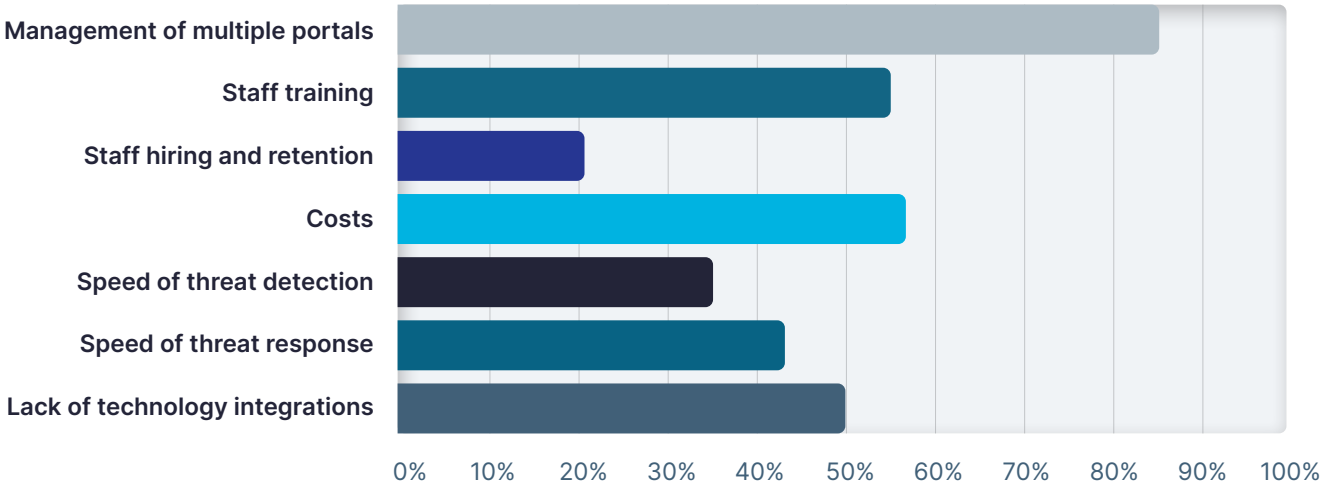
Most organisations we see still have a sizeable number of people involved in security management but not exclusively aligned to security tasks. For example, infrastructure managers, network managers and those involved with end user computing all perform security-related tasks as part of their business-as-usual activities, but don't necessarily consider themselves as security specialists.

The same is true for DevOps, as most development is based on the security-by-design principle so, by the very nature of this, they are also engaged in security-related duties.

Q4.

What are the main challenges or pain points of using multiple security vendors?

(Select all that applies)



Summary

Many of these challenges are the by-product of having an overly complex security environment that consists of many different security vendors.

- **Many vendors = more management of multiple portals**
- **Many vendors = more costs, as there are less economies of scale opportunities**
- **Many vendors = more staff training needed (which increases the overall cost burden)**

And so on.

Investment in training is always an interesting conversation to have.

CFO: What if we train them and they leave?

CEO: What if we don't and they stay?

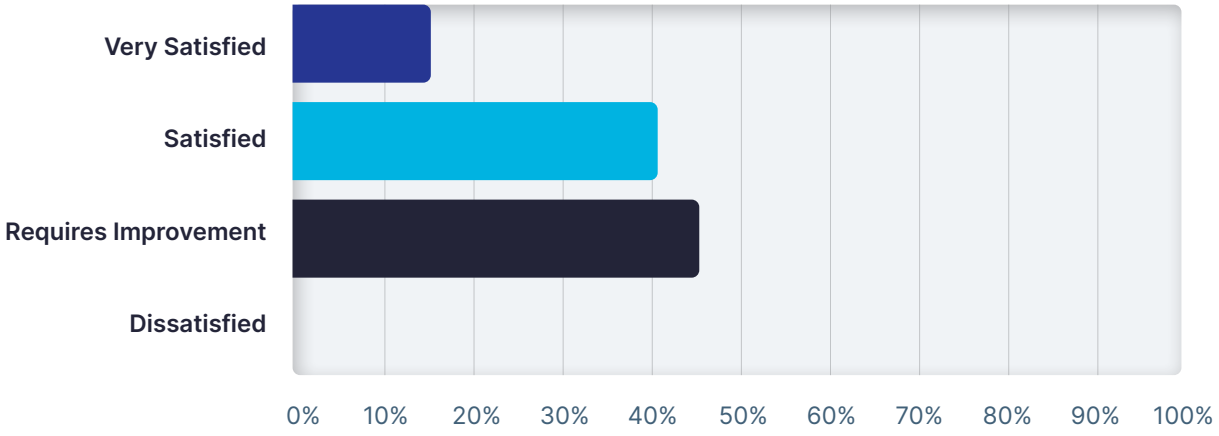
When it comes to security, you simply can't take the risk. Security professionals must be able to expertly use the tools they are being asked to use, else the investment in the tool is largely wasted – and this comes down to regular and high-quality formal training.

Vendor consolidation helps addressing most of the challenges listed and entails benefits such as: fewer vendor portals to manage, less staff training (which has the added benefit of reducing the need to take staff away from their day job during training), less need to hire people, reduced costs through economy-buying, and a better all-round security posture as threats are typically responded to more quickly and more efficiently.

Like most things, it is a balance between minimising your vendor stack to unlock the above benefits and needing enough technologies to provide the security layering mentioned earlier.

Q5.

How satisfied are you with the current performance, reliability, and integration of your security tools?



Summary

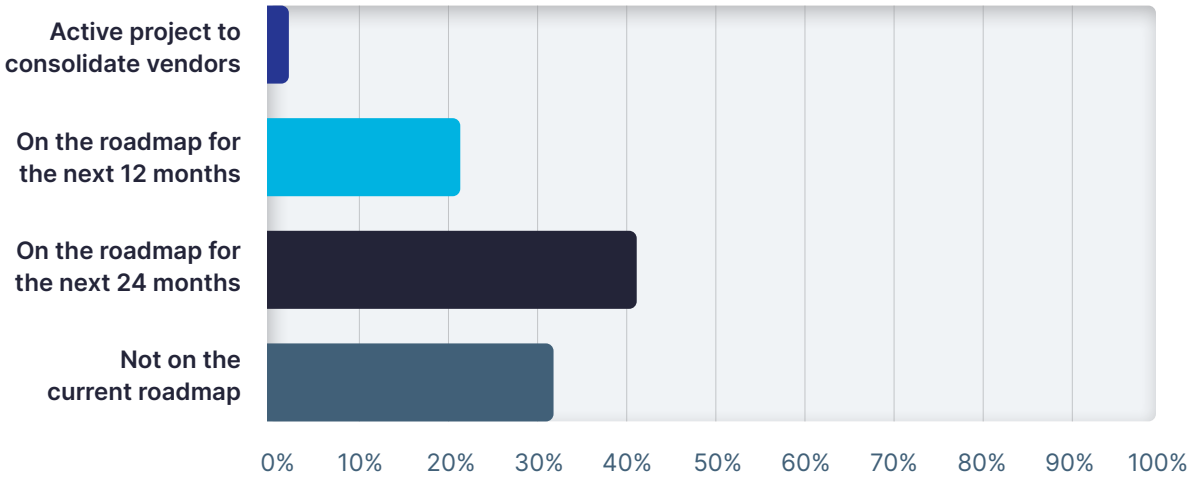
This is a matter of whether you see the glass half-empty or half-full. On the one hand it can be argued that almost 55% of respondents are either satisfied or very satisfied with the current performance, reliability, and integration of their security tools. However, on the other, you have 45% of respondents saying their environment needs improvement, which is a common theme in the industry.

The findings from the last question are part of the problem, and vendor-consolidation is certainly part of the solution, particularly when it comes to integration satisfaction. As detailed, consolidation can deliver demonstrable cost savings and better performance which can directly impact the overall satisfaction levels.

One of the other factors however that feeds into the over satisfaction of Security professionals is Board support and budget – or lack of it. This is one of the main challenges our customers tell us about and is an area we are often asked to help them with. We have successfully assisted several Security teams to better position the need for more investment and the returns it will deliver to their Management Teams.

Q6.

How likely will you consolidate your security vendors in the next 12/ 24 months?



Summary

This is line with what we are seeing in the market. These results however can be a little misleading as many of the organisations that state consolidation is "Not on the current roadmap" have already consolidated to a greater or lesser degree. When this is considered alongside the other findings, it is very encouraging that virtually every respondent is, or is likely to consolidate over the next 2 years.

The challenge many organisations face with consolidation is the sequencing of it as most organisations already have contracts and renewals in place that need to be respected.

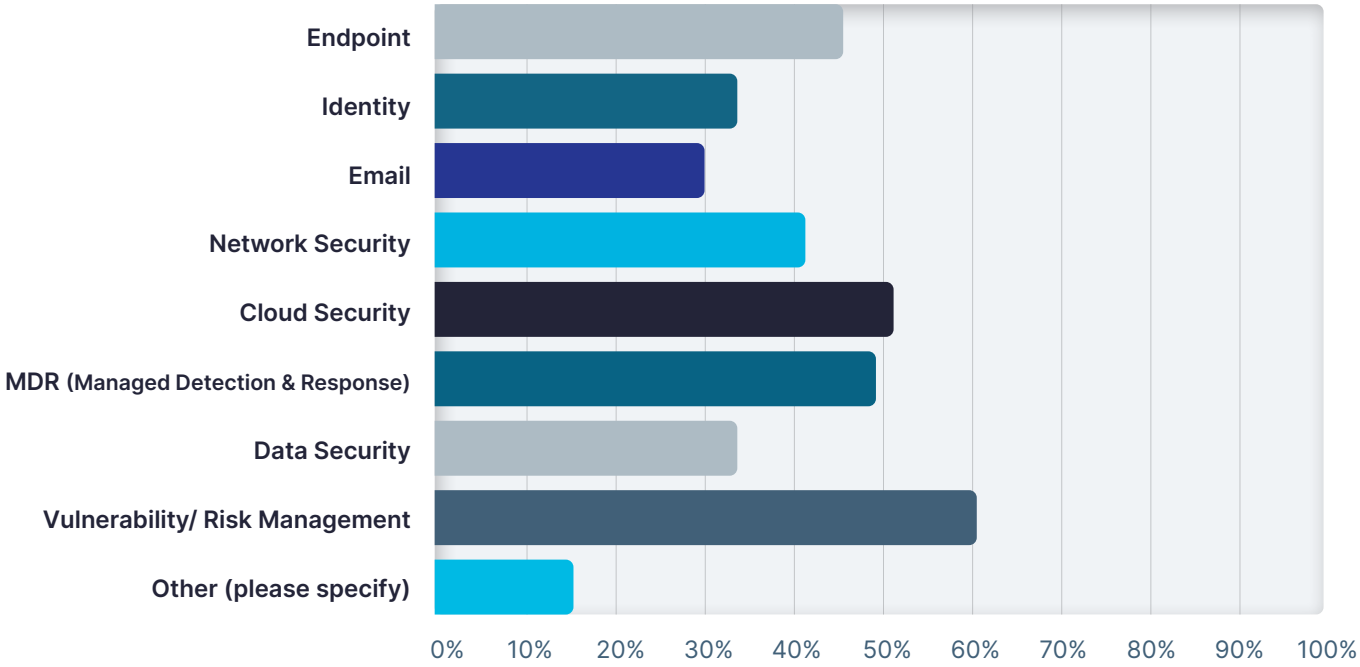
Depending on the contractual landscape, it is often advised to choose a consolidation vendor then start small and ramp up over a 1-2 year period. Over this time, most third-party technologies will have been cost effectively replaced at their renewal time. This "budget harvesting" approach frees up budget to be re-invested elsewhere and so brings broader benefits.

Bytes can offer expert consolidation advice and point out some of the pitfalls to avoid.

Q7.

What security functions are you most interested in consolidating?

(Select all that applies)



Summary

It is not a great surprise that every respondent has highlighted multiple security functions that they would like to consolidate, and equally not a surprise that certain functions have scored highly. As an example, cloud security makes sense as security teams are moving away from relying on native cloud tools and turning instead to solutions that can provide a multi-cloud view. This new approach is allowing teams to act faster and provider a better level of protection to their organisation.

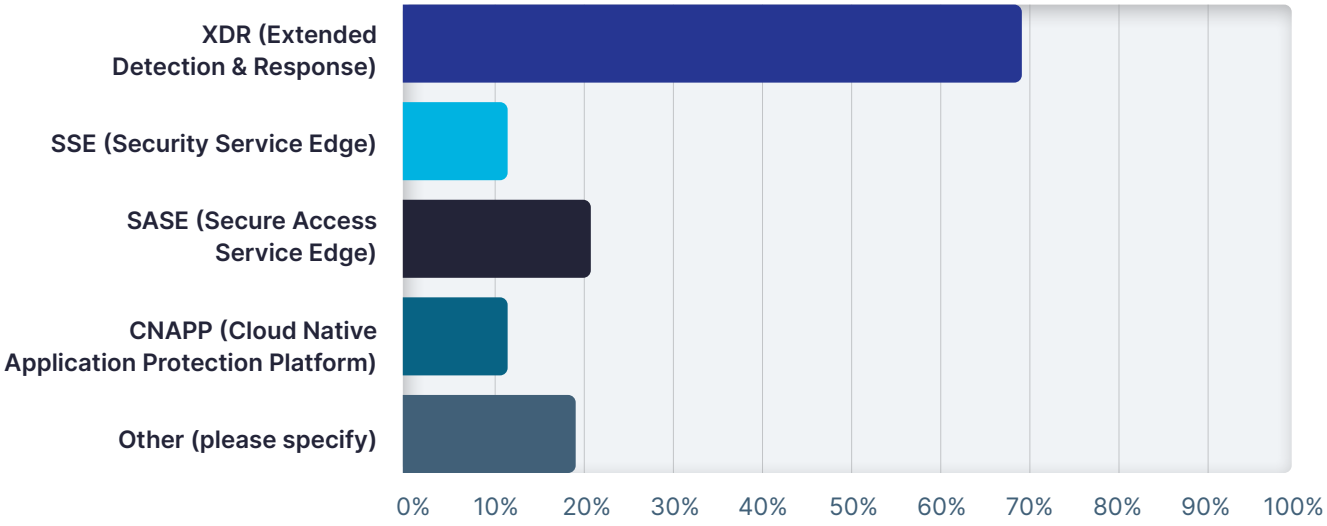
Another example is the ever-decreasing number of organisations that are investing in Endpoint security, as they are instead choosing to invest in Managed Detection and Response. This is because of evermore sophisticated malware and the need to have skilled personnel who can connect the dots when it comes to cyber incidents. Sometimes this level of skill is available internally, and sometimes it is provided externally via specialist security organisations such as Bytes.

It is not surprising that Email security is relatively low down the list as it remains the most targeted vector so is good practice to have a layered approach for it.

Q8.

What security solutions are you most interested in consolidating to?

(Select all that applies)



Summary

The findings of this question largely reflect the key marketing messages of the largest vendors and also the level of complexity involved in the consolidation exercise.

XDR is relatively easy to do, doesn't rely on expensive hardware or constant updates, and offers many immediate benefits. SASE on the other hand is quite complex and requires a greater degree of planning and expertise. Some organisations, for example don't fully understand the difference between SSE and SASE and don't necessarily appreciate that SSE is infact a component of SASE.

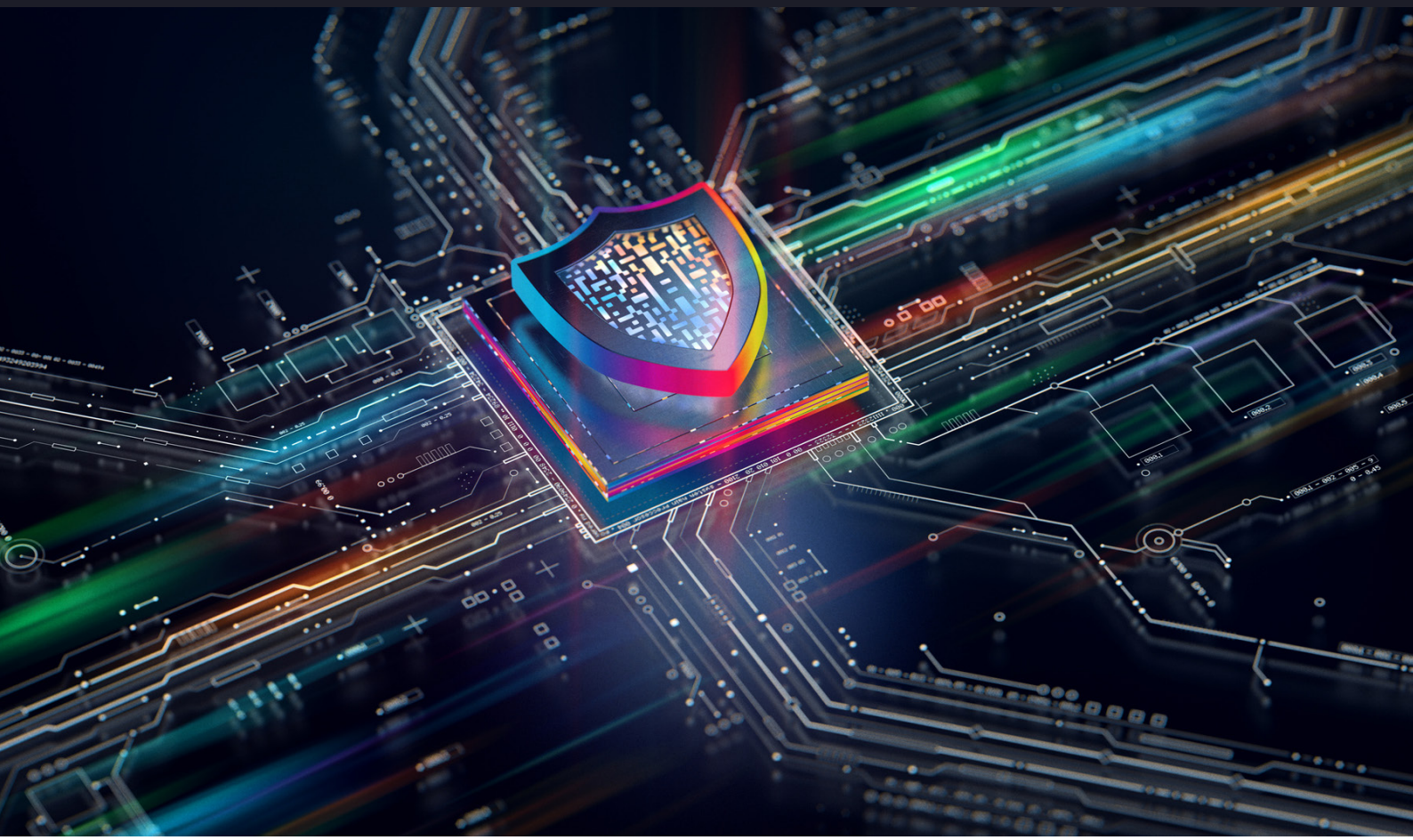
BYTES | Smarter together

Summary

The findings from this survey suggest that there is an increasing number of organisations that see the benefits in vendor consolidation. To fast-track this transition, the following 4-phase approach is recommended:

- ✔ **Gap analysis with Bytes to understand the security posture within the organisation.**
- ✔ **Functional analysis by vendor to understand where there is cross-over between the various in-situ solutions and the potential target areas of consolidation.**
- ✔ **Contractual and renewal analysis of the existing vendors to understand the optimal timeframes to consolidate.**
- ✔ **Commercial modelling to detail the expected savings and return on investment.**

More info about phase 1, “The Gap analysis” can be found on the next pages.
If, however you would like to discuss this service, or any aspect of the findings detailed in this report, please contact your Bytes Account Manager, or visit www.bytes.co.uk



CAF Gap Analysis

Bytes CAF Gap Analysis provides organisations with a security focused gap analysis based on the National Cyber Security Centre Cyber Assessment Framework (NCSC CAF).

The NCSC CAF outlines 14 cyber security & resilience principles, which are recognised to have a material impact on your ability to prevent cyber attacks and to reduce the overall risk associated to your IT infrastructure.

The **Bytes CAF Gap Analysis** provides expert analysis of your security solutions, processes, and procedures to provide tangible recommendations on how best to improve your organisation's security posture.

Why Bytes Offer This

The CAF Gap Analysis session allows Bytes to deliver value to the customer by assisting in the alignment of their security infrastructure to industry recognised frameworks.

- Collate information on your current security solutions, their functionality & utilisation.
- Compare your current security provision across multiple areas to the 14 cyber security & resilience principles.
- Deliver a session outlining the results, identifying key focus areas & outlining improvement recommendations.
- Provide a detailed report with RAG Matrix, tangible next steps, improvement areas & impact of gap analysis.

Key Features & Benefits

- **Simplicity:** No tools or scripts
- **Bespoke:** Tailored to each individual company
- **Detailed:** Encompasses all areas of security best practice
- **Industry Recognised:** Internationally approved, continually updated framework
- **Zero Cost:** Our expert-led service is completely free
- **Independent advice:** Vendor agnostic approach focused on best practices

What To Expect?

The CAF Gap Analysis is delivered through the following stages:

Discovery: We collect and collate information on your current security solutions, processes and procedures.

Analysis: We reference your answers against the 14 principles of the NCSC CAF.

Consultation: We host a session to discuss and clarify the information collected and to gather any additional information needed to create your report.

Outcome: A bespoke and detailed report is produced and will include a high-level score against each of the 14 principles, as well as detailed explanations to justify the score and recommendations for next steps to improve the overall result.

CIS Gap Analysis

The Center for Internet Security (CIS) Top 18 Critical Security Controls is a prioritised set of best practices created to stop the most pervasive and dangerous threats of today. Developed by leading security experts from around the world, the set is refined and validated every year.

While there is no silver bullet for security, organisations can significantly reduce their risk of compromise by implementing the CIS top 18 critical security controls, as they move from a compliance-driven approach to a risk management one.

Bytes are here to help you along that journey, starting with **a free-of-charge analysis** of how your current security provision aligns to the CIS Top 18 Controls.

Bytes CIS Gap Analysis Session gives businesses a Security Posture Gap Analysis based on the CIS Top 18 Controls. Those 18 security best practices are most likely to have a material impact on your business' ability in preventing breaches and reducing risk.

Key Features & Benefits

- **Simplicity:** No tools or scripts
- **Bespoke:** Tailored to each individual company
- **Detailed:** Encompasses all areas of security best practice
- **Industry Recognised:** Internationally approved, continually updated framework
- **Zero Cost:** Our expert-led service is completely free
- **Independent advice:** Vendor agnostic approach focused on best practices

An expert analysis of security solution details by our engineers will provide tangible recommendations on improving/refining your security provision to maximise risk-reduction and compliance while keeping expenditure under control.

We have created this engagement to better work with our customers in **building a first-class cyber security strategy** which complies to established best practices.

What To Expect?

The CIS Gap Analysis is delivered through the following stages:

Discovery: We collect and collate information on your current security solutions, processes and procedures.

Analysis: We compare your current security provision across multiple areas to the top 18 CIS Controls.

Consultation: We deliver a session outlining the results, identifying key focus areas & outlining improvement recommendations.

Reporting: We provide a detailed report with RAG Matrix, tangible next steps, improvement areas & impact of gap analysis.

About Bytes

Bytes provides leading insights, expertise and practical help to over 3,600 organisations nationwide. We enable effective and cost-efficient technology sourcing, adoption, security and management of software, hardware and cloud services.

Our UK business began in 1982 and has grown profitably each year to reach a turnover in excess of £1bn, making us one of the largest software services and solutions businesses in the country.

The most important aspect of our business is our people. We value initiative, teamwork and achievement. Together, we focus on providing the highest levels of service so we can deliver our ultimate goal – customer satisfaction and success.

Our customers include leading brands, such as Marks & Spencer, BBC, NHS, Clifford Chance, BUPA, Thames Water, Hiscox, Allen & Overy LLP and thousands more across retail, media, finance, manufacturing, legal, healthcare and the public sector.

We work closely with the majority of IT vendors and are delighted to regularly receive honours from them in addition to being named a Sunday Times Best Company to Work For 2020.

About Bytes Cyber Security

By acting as an independent, trusted advisor, our customers benefit from a wealth of knowledge that aids the delivery of an end-to-end and integrated methodology to cyber security. Our consultancy led approach enables our team to fully understand our customers challenges and business goals, ensuring we deliver innovative and relevant security solutions.

Bytes uniquely brings together cyber consultancy, solution specialists, pro-services and managed services under one roof.

UK Head Office
Bytes House
Randalls Way
Leatherhead
Surrey
KT22 7TW

01372 418 500
tellmemore@bytes.co.uk
bytes.co.uk

BYTES | Smarter together