



**censornet.**

---

Protect your Business

# **Your Guide to Vendor Consolidation**

November 2022

# The growing momentum for consolidation



## How many specialised security products does your organisation use?

Statistically, the number is likely to be high. In an attempt to handle attacks from all sides, the average small or medium firm uses 24 point-products to protect themselves. However, more security tools, doesn't translate to stronger security. Each point-product has a narrow focus and this approach has inadvertently created gaps between individual point-products. Gaps that can be exploited by hackers and widen the attack surface.

Too many mid-market businesses are managing disparate point products and incompatible dashboards, while struggling to integrate new systems with existing defences. The substantial operations overhead that comes with managing this number of products is cumbersome and unnecessary. The list includes increased training requirements, poor visibility of the whole security ecosystem, and the manpower to respond to the alerts that pour in from each product.

However, a fragmented security stack isn't the only thing causing a headache for IT security teams. An unmanageable number of products, difficulty getting a holistic picture of security and challenges attracting or retaining team members are combining to create the perfect storm. All while budgets are being stretched thinner and thinner.

In this guide, we will investigate how mid-market organisations can navigate these challenges and address the complexity, costs and inefficiencies in their security posture. We'll drill down into how security vendor consolidation can provide a solution for strained IT teams and why it's particularly relevant for the growing mid-market.

It's a journey that can take many years so we explore the questions security leaders should ask as they embark on the process, and highlight the difference between consolidation and integration.

Finally, we'll outline the positive impact consolidation can have. We'll look at the benefits that come from an integrated and seamless approach - everything from reducing complexity, to overcoming operational burdens and strengthening the security posture to support the needs of a digital business.

# Contents

**01**  
Security vendor consolidation:  
Why should the mid-market care?



→

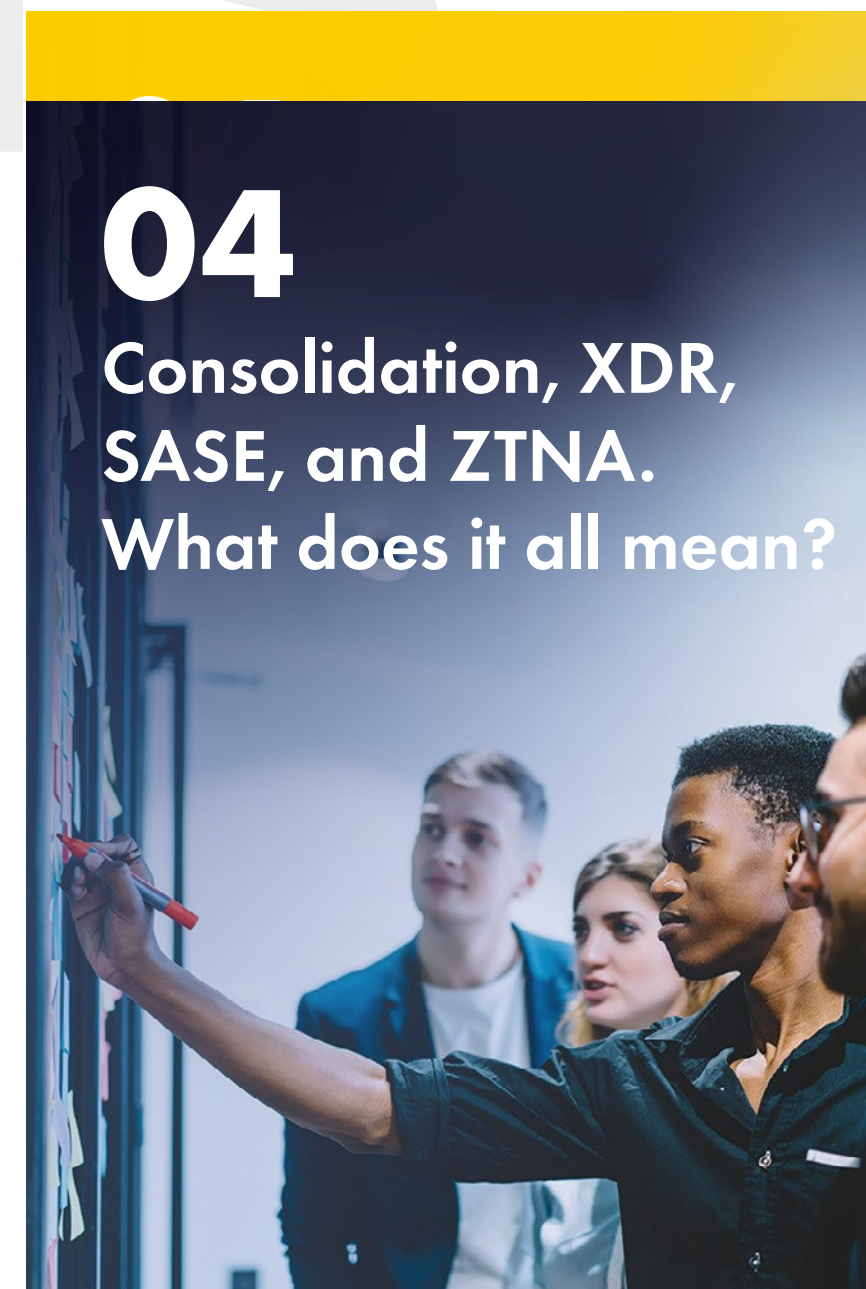
**02**  
Seven key questions  
for successful vendor  
consolidation



**03**  
Consolidation isn't just  
about saving money,  
it's about reputational  
protection



**04**  
Consolidation, XDR,  
SASE, and ZTNA.  
What does it all mean?



**05**  
Integration and consolidation  
What's the difference  
and why are both  
important for the  
mid-market?

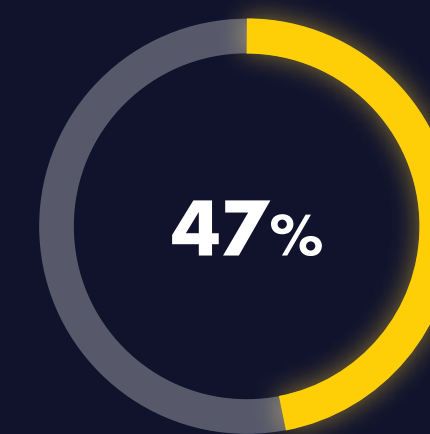


→

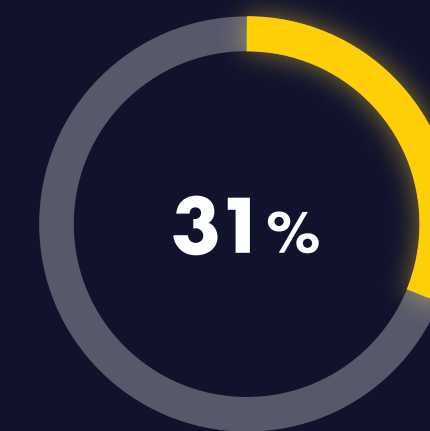
# 01

## Security vendor consolidation: Why should the mid-market care?

According to our [UK Mid-Market On Code Red report](#), the round-the-clock threat of attack and the stress it causes means that the average amount of sleep someone responsible for cybersecurity gets is 5.7 hours, significantly less than the seven hours or more recommended by the NHS<sup>1</sup>.



of security personnel admit to feeling overwhelmed when faced with too many cyber security alerts



of security personnel are unable to cope following prolonged periods of work-related stress and burn-out

It's no wonder then that our research shows nearly half (46%) of organisations in the mid-market want to see security vendors open up traditionally closed point products to enable an automated response to cyberattacks.

### Consolidation a priority already

Across all sized businesses, consolidation is accelerating. According to Gartner, [75% of organisations are pursuing a vendor consolidation strategy, up from 29% in 2020](#). It's becoming clear that consolidation, when done correctly, is an effective strategy to help navigate the ever-evolving threat landscape, product overload and the uncertain economic climate. In fact, Gartner states that already, [57% of organisations are now working with fewer than ten vendors for their security needs](#).

So, what does consolidation look like for small-medium organisations? It means taking a more coordinated approach. Email, web, identity, and cloud application security systems working in tandem, identifying and tracking attacks before they proliferate across an organisation. By implementing a consolidated approach, security teams can gain a holistic view of their security systems and achieve tighter integration between previously disconnected security products, ultimately improving their threat detection and response efficiency.

1. <https://www.nhs.uk/live-well/sleep-and-tiredness/how-to-get-to-sleep/>

# 02

## Seven key questions for successful vendor consolidation

**Vendor consolidation promises a great deal for stretched mid-market IT teams. Fewer licenses to manage, fewer updates to oversee, and fewer integrations to build and maintain all mean more time available for strategically valuable work.**

Above all, though, vendor consolidation promises to reduce the number of vulnerabilities 'in between' different vendors' systems – and so improve the resilience of companies' overall protection. Indeed, according to Gartner, 65% of organisations who are currently pursuing or plan to pursue vendor consolidation expect to improve their overall risk posture.

That's the goal. However, for those organisations who have begun pursuing vendor consolidation, the biggest drawback according to Gartner (for 24% of respondents) was actually a reduction of the quality of their risk posture.

### So what's causing that negative impact?

The reality is that many mid-market firms are facing short-term financial pressures that might impact their decision making. That's not to say that quality vendor consolidation has to mean massive expense – but it is to say that if you grab the cheapest thing quickly, you're unlikely to build a resilient consolidated security system.

Equally, every vendor does things differently. If you don't assess your choices carefully, you're likely to reintroduce those risky gaps between products. And as soon as they're there, attackers will know how to target them. Suddenly you're wide open to threats again.

So – how do you avoid falling into that 24% that fails to benefit from consolidation? Here are seven key questions to consider when you're setting out on the journey.

### 01

#### Come up with a plan - what are you trying to achieve?

It might sound obvious, but it's always wise to put first things first. What is the goal of your consolidation programme? Being driven purely by cost savings or an arbitrary vendor cap isn't going to yield the best results. What security goals do you need to achieve, and where are you seeing poor performance that needs to be improved? Shoot for those points, and let the end benefit guide purchase choices.

### 02

#### Have you developed a security framework aligned with your objectives?

In 99 cases out of 100, getting down to a single vendor is impossible and inadvisable. Instead, you need to consolidate the tools that make sense at the right time, with an eye to the future. You might start with a web security deployment and then add on application security and data loss prevention over time, ensuring the platform you're using enables that journey. Again, ensure your business needs drive the process.

Seven questions continued on next page →

## 03

### Have you mapped out if you're going to have security gaps?

Consolidating frontline defences with fewer vendors can expose weak spots in your security. When you plan out your transitions, give particular attention to areas where two vendor systems will need to talk to each other for the first time. How are you going to bridge that gap and ensure the two systems work well together? Have you planned in a review process to identify further gaps that may have been missed?

## 04

### What's your total cost of ownership with a smaller number of vendors?

Cost may not be the best consideration to lead your consolidation strategy, but it is a significant area of benefit when done right. Keep track of the savings you're likely to reap from the process, and ensure that the cost of ownership is moving in the right direction. If you're seeing overall cost heading far northwards, there may be more procurement conversations to be had.

## 05

### What's your projected ROI?

This question takes the previous point a step further. Don't just consider the cost of licences and maintenance – what savings will you see in terms of staff time and resource? What cost benefits are you going to see in the wider business? You may well see less disruption to other teams as a result of smoother security processes, and of course there's the projected benefit of reduced time neutralising threats that penetrate your first line of defence. Overall, ROI may be more significant than immediate bottom-line savings.

## 06

### Are you working with the right partners?

Sometimes, the work of a consolidation programme could be massively reduced by the right VAR or MSP – someone who understands your business and needs, has a shrewd knowledge of the vendor market, and can help you get up and running fast. If the legwork or research required feel out-facing, consider finding a trusted partner that can help thin the field and identify the best solutions for you.

## 07

### Are you heading into any technological dead ends?

Don't make the mistake of seeing consolidation as a simple retrenching of what you've already got. As you move forward with new vendors, you will need to make choices about which technologies and approaches to invest in. As you do, make sure you're not pursuing dead ends. VPN technology, for example, is a dying art, and for good reason – as we move towards a world where zero-trust approaches deliver more flexible, granular, resilient security, VPNs are not only outdated – they actively stand in the way of your organisations' evolution.



### Consolidation is rarely a simple process or a straightforward journey.

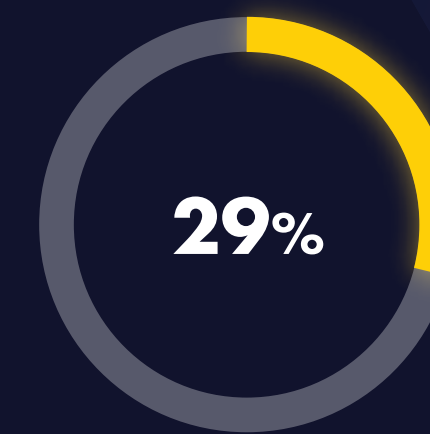
It takes time and Gartner recommends that security and IT leaders plan for at least two years to consolidate effectively. With a clear focus and plan, you can achieve a unified security environment and ensure your risk posture improves as you consolidate.



# 03

## Consolidation isn't just about saving money, it's about reputational protection

Consolidating your cybersecurity vendors comes with a whole host of benefits, from reduced workload to improved threat intelligence. But it's not a magic solution to every business challenge – particularly when it comes to cost.



In recent Gartner research, only 29% of organisations said they consider reduced spending on licensing to be the primary benefit of vendor consolidation.

It was the lowest ranked benefit. At the same time, 15% felt that increased spending could be a drawback of consolidation – a significant number (although this was not the leading drawback). In other words, if you're looking to save a quick buck, consolidation may not be the shortcut you're looking for.

→ Companies don't have to rip and replace – just slowly move to consolidation to make the change cost effective.

However, mid-market firms are facing more financial pressures than ever – which means there's a need to stay focused on reducing complexity and increasing efficiency across the board – something consolidation does very well. Cost savings may not come directly off the license budget, but when the team is working better, faster, and the organisation is achieving better security with less back-end management and admin workload, then savings come in other ways.

And although consolidation may not always equate to immediate savings, it also doesn't have to break the bank or come with a price hike.

### The risks of a patchy defence

The monthly bill is important, but it also can't be the sole deciding factor in whether or not to pursue consolidation. Put simply, the more siloed point products you deploy, the greater the chance you'll end up with blind spots and gaps that attackers can exploit. Consolidation allows for more tightly joined-up defences, with multiple products operating from the same unified platform.

That kind of joined-up protection is more important now than ever. The threat level for the mid-market is increasing, both in volume and the complexity of the attacks. As many as two in three (65%) mid-market organisations suffered an outage in 2021, with half (33%) seeing systems knocked offline for more than a day. This rate of attrition isn't surprising: in order to stay protected, mid-market businesses need to stop over a billion cyber threats a day.

And the risk is increasing. According to Accenture's Cost of Cybercrime report, malware is the most expensive type of cybercrime in the UK, and is now costing firms 15% more than in previous years. The evolution of cybercrime means that costs stack up quickly for businesses – whether that's through upfront ransom, recovery costs, or managing the aftermath of a breach.

The reputational impact of not being fully protected is also huge: this isn't about consolidating for consolidation's sake.

According to the Journal of CyberSecurity firms experience a 5-9% decrease in reputational intangible capital following a major data breach.

Put together, the bottom line is that licensing costs are far from the only cost to be considered for mid-market businesses. A consolidated defence could end up saving a great deal both financially and reputationally.

### Reducing the cost of cyber threats

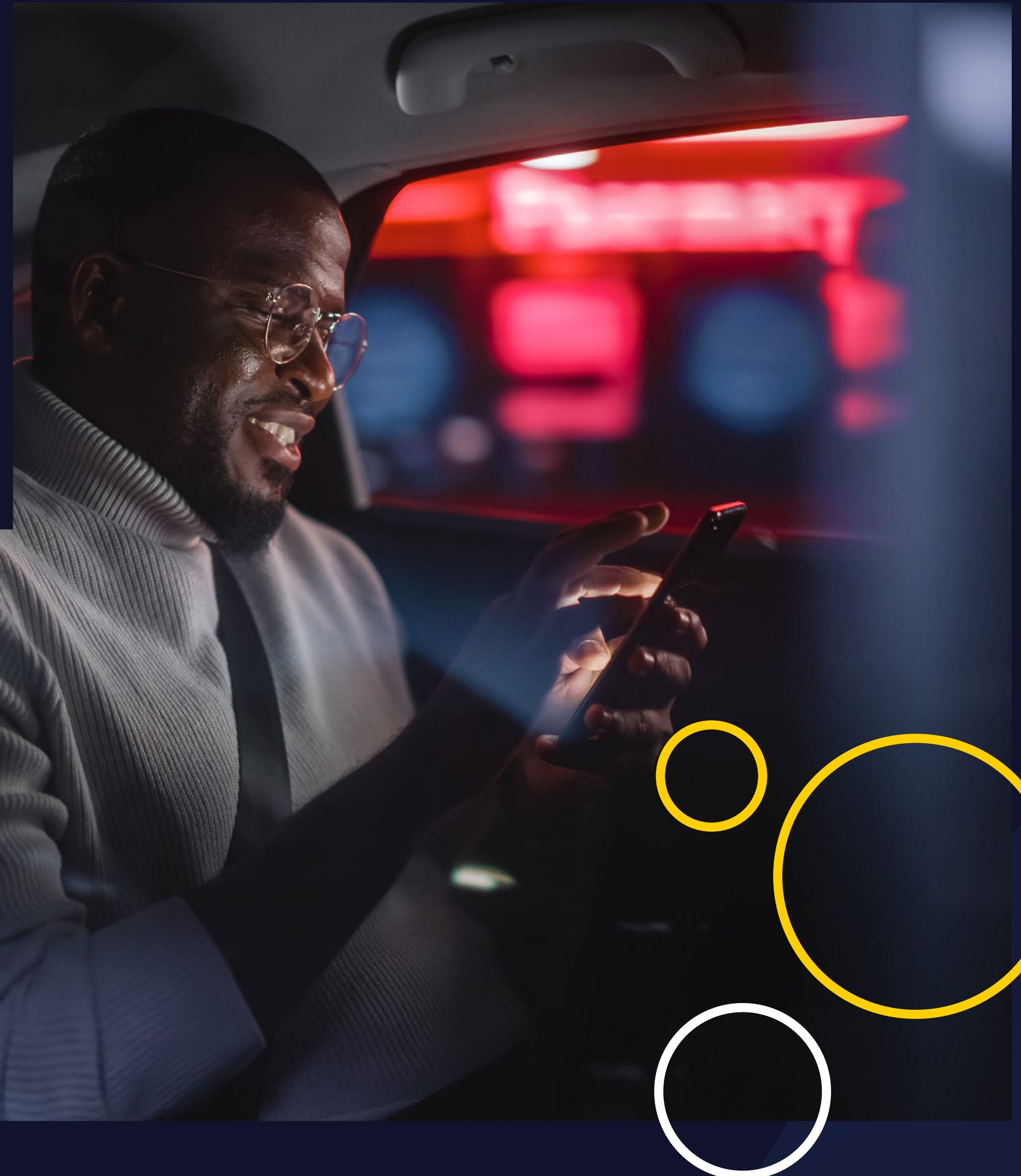
So what does that look like in practice? What benefits does consolidation bring that will help achieve those savings?

First off, a consolidated approach means teams can move away from the more expensive and time-consuming approach of running separate solutions in silos. Rather than overseeing a portfolio with all the various update schedules, integrations, after-sales services, and management requirements that entails, IT teams can hand the majority of the back-end work to a single vendor. Implementation of new capacities and products comes as standard, and monitoring and reporting can be handled through a single dashboard, rather than a forest of different systems. As a result, staff time is freed up, integrations run more smoothly, and the costs of keeping up with evolving threats comes down.

Consolidation also enables the running of truly digital business, giving users the freedom to access the applications and data they need regardless of device or location, whilst providing visibility for IT and adequate protection. Rather than having to consider new contracts or providers to protect evolving tech requirements and an ever-more mobile workforce, the relevant capacities can be added to the platform as required. Joined up security also ensures that dispersed staff pose less of a risk: threats can be tracked across devices and apps, ensuring that cross-channel attacks are stopped early.

Finally, consolidation helps organisations move to a zero trust posture, the next step in the evolution of cyber security – where every user and every request is granted the least amount of privilege. Under zero trust, authentication is based on rich contextual data – the more the security system knows about a user’s behaviour, the more accurately it can identify them and grant access when appropriate. A consolidated system enables deeper insight, allowing for a user-friendly, high-security zero trust approach.

In the end, the long-term benefits of consolidation heavily outweigh any questions about immediate cost-savings, or the lack thereof. With the financial and reputational costs of cybercrime higher than ever, it’s an opportunity businesses can’t afford to miss.





# 04

## Consolidation, XDR, SASE, and ZTNA. What does it all mean?

According to Gartner, by the end of 2023 more than 80% of organisations will have completed extended detection and response (XDR) projects and nearly 70% will have completed secure access service edge (SASE) projects. For many, these projects aren't an end in themselves – they're compelling first steps in the journey towards consolidated security<sup>2</sup>.

Why is that the case? In essence, SASE provides secure enterprise access, while XDR focuses on detecting and responding to threats through increased visibility on networks, cloud, endpoints, and other components. Together, they provide a framework for more integrated, seamless cybersecurity – rather than relying on a siloed portfolio of point products.

But with so many terms and technologies in the mix, it can be hard to see the wood from the trees. So let's take a step back.

### What is XDR – and why does the mid-market need it?

The term 'extended detection and response' originally comes from Palo Alto. At its heart, XDR is all about analytics – collecting and analysing a huge amount of data about potential threats to an organisation's extended landscape and rapidly moving to counter them.

It's also about controlling the flow of data across the organisation, performing a data loss prevention (DLP) function by stopping sensitive information from proliferating across cloud apps or via email.

It could, for example, refer to projects which free companies' users from being tied to a single corporate device. Working autonomously, it provides a more intelligent, case-by-case way to determine access and safe behaviour, rather than simply authenticating one set of devices or protecting a perimeter. What does all this have to do with consolidation?



When companies are operating on a consolidated, platform-based model, one single system can process threat intelligence, device telemetry, and web, email, and cloud app activity to generate a wide view of the environment and any threats it faces.

And if that sounds like the kind of high-cost deployment that only major enterprises need to invest in, think again – this technology is increasingly accessible to the mid-market. And the need for autonomous, integrated security and DLP is every bit as acute in medium-sized organisations as in their larger counterparts.

<sup>2</sup> Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022, September 2020

### SASE: what and how?

What about SASE? This term has become something of a buzzphrase in recent years, and includes both network and security elements. Essentially, it means shifting access management to the edge of the network, authenticating at the point of access rather than trying to operate a centrally-managed pseudo-perimeter. Many organisations consider this approach when replacing complex legacy firewall hardware appliances or VPN infrastructure, particularly given many no longer have a LAN.

But SASE is very much a long-term journey. The goal for mid-market organisations is not a single purchase or transition, but rather getting set up to finish there as a final destination. What's the first step on that journey? Adopting a zero-trust network access (ZTNA) approach.

Under the Zero Trust framework, no-one is trusted. Users must prove their identity before being granted access. Importantly, this trust must be continually assessed and re-evaluated. For example, if the same user logged in from two different cities just minutes apart, a red flag would be raised and access instantly withdrawn.

Most large organisations are already adopting ZTNA. However, for companies in the mid-market with lean security teams, zero-trust can seem like a challenging policy to enforce. But it doesn't have to be. The key is to adopt a platform that automatically reviews access requests 24/7 and deploys intelligent data analysis to determine context-based approvals at lightning speed. This is hugely powerful for lean security teams.

### Putting it all together

So with all that said, why are XDR and ZTNA (with SASE on the horizon) the first steps in the consolidation journey? And why are they so relevant to the mid-market?

Most XDR solutions are focused on integrating and simplifying multiple security solutions used by large global enterprises. But mid-market firms struggle with a very different reality. They may not have sufficient controls in the first place. They often have limited budgets rather than huge, complex teams, and are facing an increasingly complex threat landscape.

But XDR and ZTNA can solve these problems. By autonomously consolidating data streams from across the organisation and generating a comprehensive picture of what's happening, they can give mid-market organisations a 360-degree view of their security in one place.

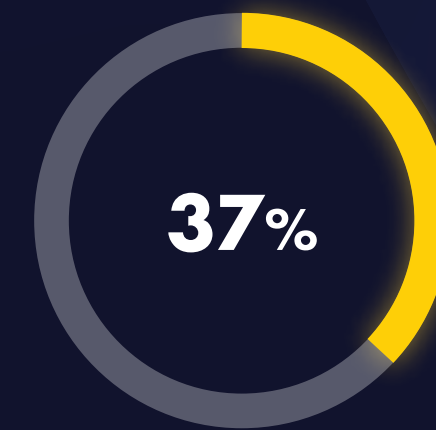
Not only does this dramatically reduce the burden on stretched security teams, it enhances protection – providing an effective defence for a more diffuse workforce and responding with agility to evolving threats.



# 05

## Integration and consolidation: What's the difference and why are both important for the mid-market?

The death of the traditional perimeter and the ubiquity of cloud-first systems mean that cyber threats are no longer confined to one particular attack vector.



Yet only 37% of the mid-market can protect themselves from these cross-channel attacks.

If a threat gets past or between one point products, the majority of companies are at serious risk of a more costly breach. If your endpoint solutions are siloed from each other, once an attack evades one defence – whether it's email, cloud, web, or identity – it's highly unlikely to be stopped by others.

This is the backdrop to the growing trend for joined-up security models. The more closely connected your security systems are, the fewer gaps you present for cyberattacks to exploit. One way to achieve this joined-up state is to attempt to integrate your point products – manually plumbing them together so they can share data and work in concert. The other is to consolidate those products in a single platform – so they're connected as standard, share data, act autonomously and are part of the same platform from the same vendor.

### Integrate or consolidate?

→ A consolidated approach comes with plenty of benefits. By delivering email, web and cloud application security with identity and context all within the same package, organisations can reduce the vulnerabilities that sit between and across major attack surfaces.

However, consolidation isn't foolproof: though you may have consolidated to one or several vendors, each may provide tools that might not be as tightly integrated as you need. As a result, choice of provider is important – otherwise, you may end up with multiple different identity stores and consoles that you've got to log into to manage the individual point products, even though you've undertaken a huge consolidation.

In short, whilst consolidating to a single vendor is obviously important, that only works if that vendor's products are very tightly integrated and talk to one another autonomously. Otherwise, you're still going to have gaps, which attackers will find – and target.

Integration means that the products you have consolidated seamlessly share data across your security infrastructure. The various security products should be simpler to use and manage (all from one platform), and reduce the need for manual intervention. That's not to mention the ease of reporting, transparency on all incoming threats, and the ability to have a holistic view of your entire security posture in one place. An integrated approach also means threat intelligence can be shared faster, so new threats are spotted more quickly.

## The way to the future: SASE and XDR

A more integrated approach to security also paves the way for emerging models like SASE and XDR. SASE allows for rapid, flexible security at the edge of the network, with authentication following the user, based on contextual data rather than weak login credentials. XDR allows for autonomous collection and correlation of data from multiple security systems, enabling faster detection of threats and improved investigation and response times through rapid analysis.

These kinds of distributed, intelligent, and autonomous abilities are essential as threats become more complex and working practices become more spread-out. According to Gartner, 89% of organizations want SASE and XDR to work together, either by consolidating into a single provider (43%) or keeping them distinct but integrated (46%). Keeping SASE and XDR distinct from one another enables a balance of best-of-breed functionality while maintaining loosely coupled integration and focus for security staff.

Whichever approach is taken, the argument for integrated security is clear. The next generation of cybersecurity is already here, and businesses are clearly stating their intent to implement SASE and XDR approaches, founded on integration. The days of point product portfolios are past: interconnection is king.



# Experience the power of integrated security

Censornet combines web, email and cloud application security with adaptive identity, so you can stop all attacks. The smart way.

See it in action now



**censornet.**

[www.censornet.com](http://www.censornet.com)