Secure by Design:

The New Blueprint for Cloud Migration

A research report in conjunction with Cloud Bridge, SentinelOne and AWS

Foreword from Bytes Software Services

Today, cloud migration has become a defining catalyst for innovation, agility, and long-term competitiveness. The insights uncovered in this research—conducted by Cloud Bridge in collaboration with SentinelOne and AWS—reflect the real challenges customers experience across complex, multi-cloud environments. At Bytes, our role is to help organisations turn these insights into action, enabling secure-by-design cloud transformation across every stage of the journey

Executive Summary

Cloud migration has become a strategic cornerstone of digital transformation, enabling organisations to modernise infrastructure, improve agility and scale securely to meet changing business demands. It is also a critical foundation for AI and AI-driven agents, providing the flexibility organisations need to experiment, innovate, and realise value from emerging technologies.
For many organisations, cloud is no longer a future ambition but an operational necessity.

As adoption accelerates, organisations are moving larger volumes of data and increasingly critical workloads and applications into public cloud environments. At the same time, heightened regulatory scrutiny and a more active threat landscape are placing demands on IT and security teams to ensure a smooth and secure transition. This shift introduces new considerations around security, compliance and operational control – particularly when teams are under pressure to deliver transformation at speed.

Importantly, these challenges do not reflect a limitation of public cloud itself. When security and compliance are designed in from the outset – supported by the right tooling, frameworks, and partners – cloud migration becomes faster and more resilient, strengthening an organisation's overall security posture.

This report explores the realities of modern cloud migration, based on research of 300 IT and security practitioners and leaders in UK organisations. It examines the key hurdles organisations encounter – from embedding security too late in the migration process to maintaining visibility and control across expanding cloud environments. Finally, it highlights how a secure-bydesign approach, combined with strong cloud and security partnerships, enables organisations to migrate with confidence and fully realise the benefits of cloud.

Key Findings

Bytes Perspective: What These Findings Mean for UK Organisations

These findings align with what we see across our customer base: security must shift left, skills gaps remain, visibility is now foundational, and regulation increasingly shapes cloud strategy. Bytes helps organisations operationalise these insights with cloud strategy, migration expertise, identity and security architecture, and continuous compliance support.

By the end of 2026,

respondents predict almost half **(46%) of all data, workloads, and applications** will be hosted in public cloud

Yet 73% of IT leaders

say cloud migration projects have taken longer than planned and **almost half say IT teams lack knowledge** to ensure cloud is securely configured

83% experienced

security issues while migrating data, workloads, and applications to public cloud, **while 90% say regulations were a 'major source of complexity'**

As a result, the total estimated **cost of underestimating security requirements** for public cloud migrations is

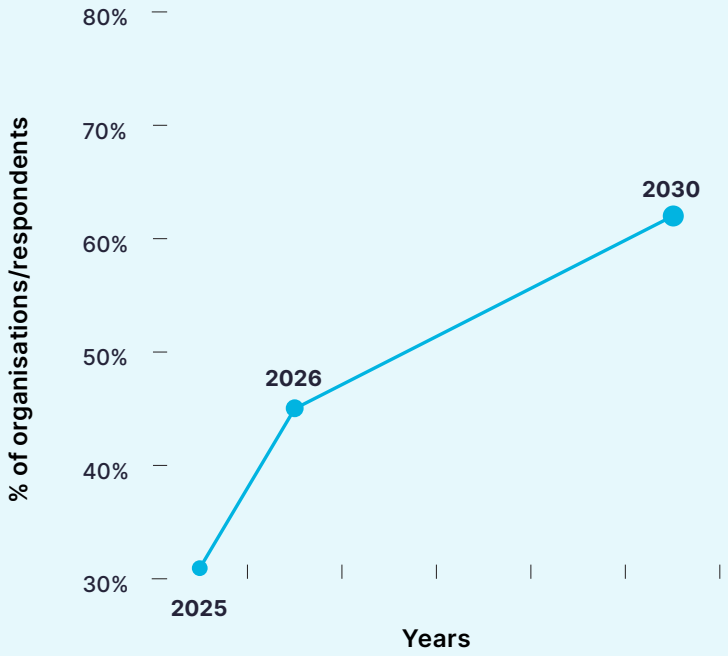
£625,000+ per organisation

"Bytes focuses on secure cloud transformation. We don't just migrate workloads, we help customers re-architect with security at the centre," said Philip Reeve, Cloud Solutions Director at Bytes. "We bring deep cloud expertise, proven governance models and a track record of delivering scalable, secure cloud environments. Our key differentiator is that we lead with security, embedding it into every stage of the transformation journey – from cloud strategy and platform engineering to automation and AI integration. That's why our partnerships with AWS and SentinelOne are so critical – together we give customers the confidence to modernise quickly, operate securely and deliver real business outcomes in the cloud."

The evolving state of cloud adoption

Cloud migration continues to accelerate, reshaping how organisations manage data, workloads, and applications. **Today, organisations no longer debate whether to move to the cloud, but how to do so efficiently, securely, and at scale.** What was once a bold digital strategy has become a standard operating model, as businesses shift an increasing share of their core operations into public cloud environments.

Chart:
Percentage of data, workloads, applications currently or predicted to be hosted in public cloud



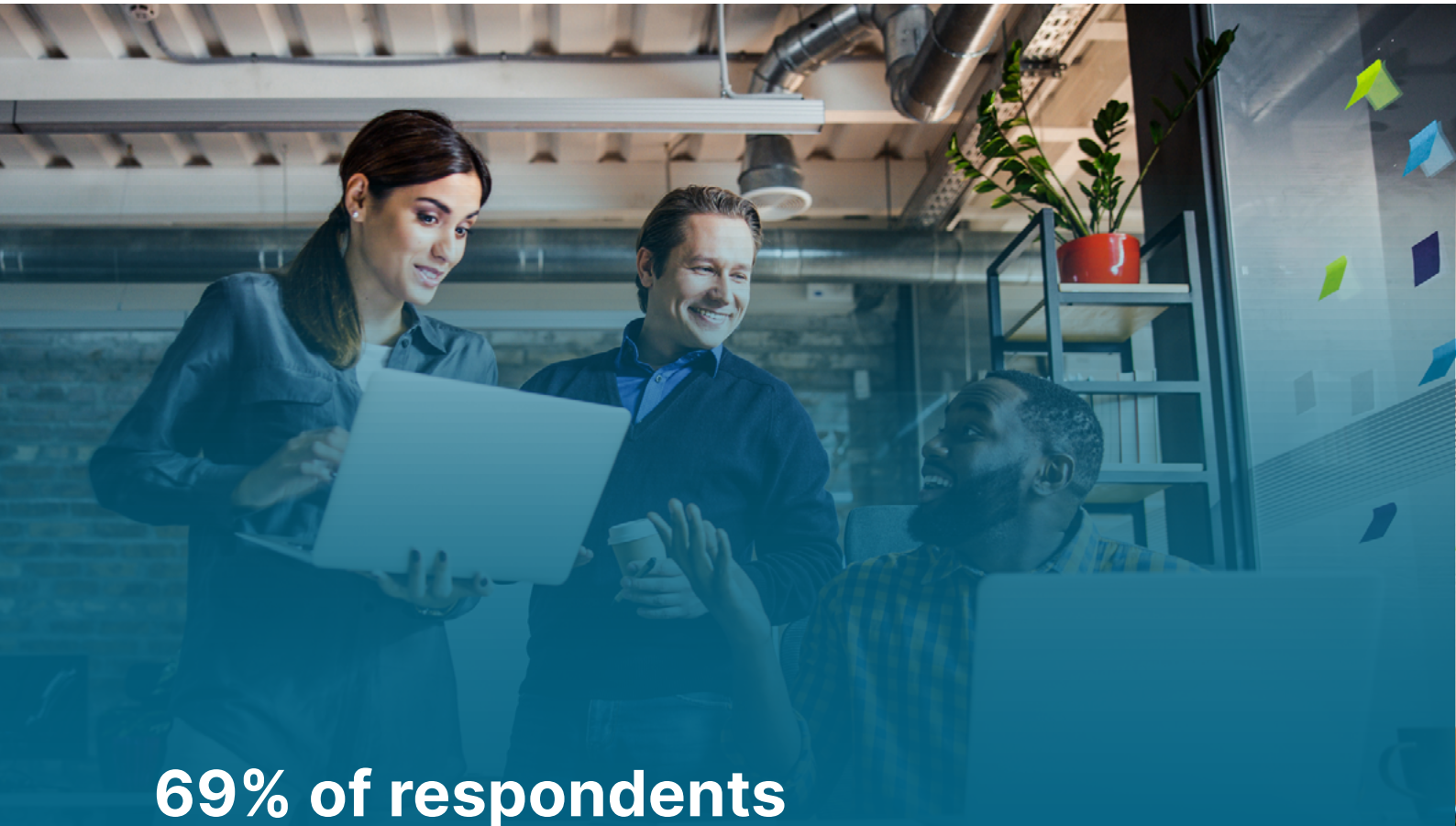
Most organisations now rely heavily on hyperscale providers such as AWS, with many engaging multiple cloud platforms. As a result, organisations are not just moving to the cloud, but also operating within and across cloud environments – optimising for cost, performance, and regulatory alignment. This signals a growing maturity in how organisations view cloud: not as a single destination but as a dynamic, evolving ecosystem.

As cloud environments scale and diversify, organisations are increasingly looking beyond infrastructure alone to business value and innovation driven by cloud native services, which power AI and Agents. As a result, many are pairing cloud platforms with structured governance, automation, and security tooling that provides consistent visibility across environments.

84% of respondents
have migrated data, workloads or applications from one public cloud provider to another.

79% of organisations
either use, or plan to use AWS.

Overall confidence in cloud migration is high. Teams report feeling well-equipped to manage the transition of complex systems, workloads and data. But some caution remains, particularly around workloads with strict data residency or regulatory requirements, reflecting the need for careful planning. Notably, confidence is strongest among security teams, while IT and DevOps teams tend to take a more measured view (see Appendix I for full dataset).

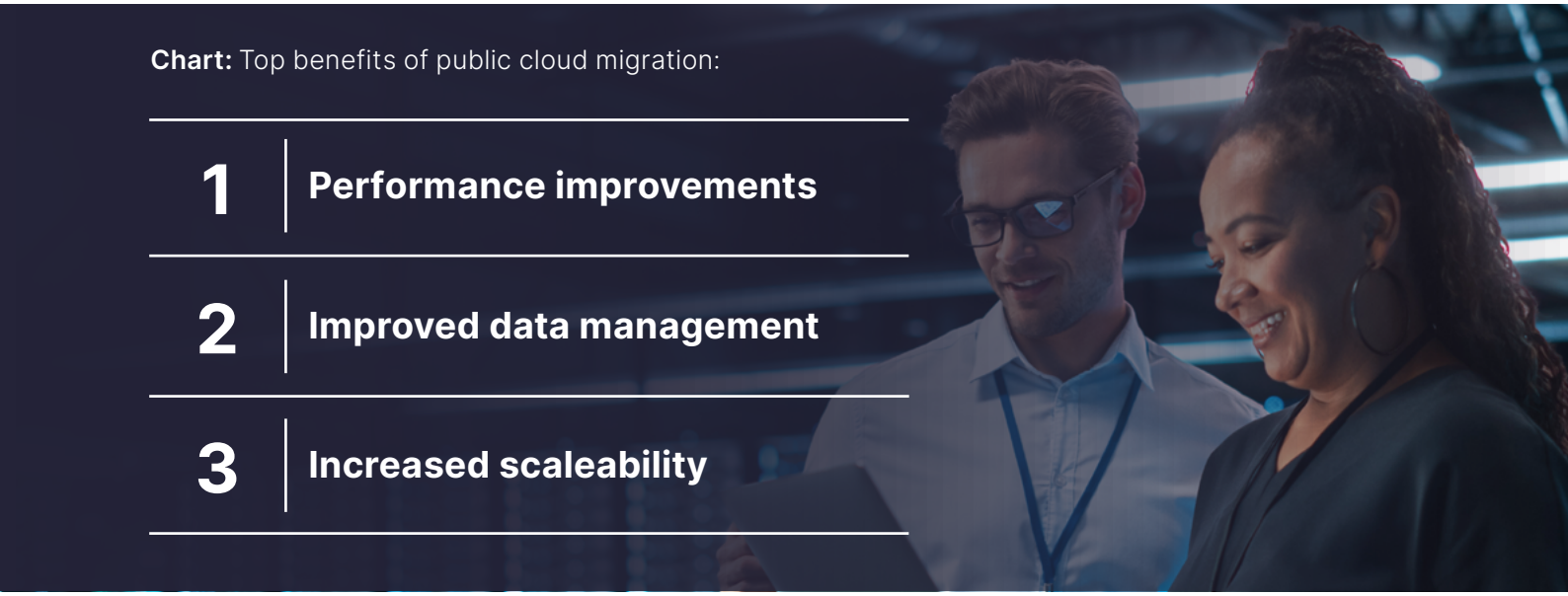


69% of respondents
rate their confidence in migrating to public cloud at four or five out of five, yet fewer than one in three feel “extremely confident”

Despite the complexities involved, the benefits of public cloud migration are already being realised. **Organisations that have migrated report tangible improvements that continue to reinforce the business case for cloud investment.** Increasingly, cloud is not just an enabler, but a foundation for long-term competitiveness and innovation.

Chart: Top benefits of public cloud migration:

1	**Performance improvements**
2	**Improved data management**
3	**Increased scaleability**



“As public cloud adoption continues to accelerate, the question for business and technology leaders is no longer whether to migrate, but how to maximise its impact,” says Rob Hale, EMEA Security Partner Leader, AWS. “Organisations are realising clear gains in performance, scalability, and data management, which are transforming how they operate and compete. Cloud has become a catalyst for innovation and modernisation – giving businesses the agility to adapt faster and drive growth in an increasingly digital world.”

Navigating the complexity of cloud migration

Chart: Top three challenges respondents have encountered when migrating data, workloads or applications to public cloud:

1. **Data exposure during transfer**
2. **Cost predictability or management**
3. **Integration issues**

Chart: Top five security concerns relating to migrating data, workloads and applications to public cloud:

1. **Data security and privacy risks**
2. **Identity challenges**
3. **Expanded attack surface**
4. **Securing AI models**
5. **Limited visibility or monitoring during or after migration**

Public cloud migration has become central to digital transformation strategies, giving organisations the flexibility, scalability, and innovation potential to modernise faster. As adoption grows, organisations are discovering that successful migration requires more than technical execution alone. **Secure, seamless transformation depends on thoughtful planning, clear visibility and close collaboration.**

Security sits at the centre of this process. **Data exposure remains one of the most common and potentially damaging challenges encountered during and after migration,** reflecting how quickly sensitive information can be put at risk when visibility or control is lost. **However, these risks are not inherent to cloud and can be avoided**. When organisations embed strong identity controls, encryption, and continuous monitoring early in the project, they can significantly reduce exposure while gaining deeper insight into how workloads behave in cloud environments.

Public cloud platforms provide powerful native security capabilities. The differentiator lies in how effectively organisations apply these capabilities – supported by experienced partners – to ensure controls are implemented early, consistently and at scale.

Security and compliance considerations can also influence migration timelines if they are addressed too late, often resulting in delays or rework. When handled proactively, however, these same disciplines create a stronger, more predictable foundation for migration. **Aligning teams early around security and compliance enables organisations to move faster, reduce risk, and build environments that are secure by default.**

In fact, **all** respondents who experienced migration delays cited security and/or compliance as significant contributing factors – reinforcing the importance of addressing these areas upfront.

73% of respondents
say their cloud migration projects have taken longer than planned, with a third reporting delays of more than three months.

To navigate these complexities successfully, **organisations are increasingly taking a more structured approach to cloud migration** – one that embeds good practice from the outset. Success consistently depends on four key principles:

Build security in early

Treat protection and governance as foundational elements of migration planning, not post-migration additions

Protect investment value

Recognise that security is a cost-control mechanism as much as a risk-control measure, reducing rework and financial exposure later in the migration lifecycle

Make compliance continuous

Address regulatory requirements from the start and validate them throughout the migration process

Clarify cloud ownership & control

Improve collaboration and visibility so teams take responsibility for securing and operating cloud environments once live

Let's take a closer look ↘

Building in security early

Many of the security challenges organisations encounter during cloud migrations stem not from the cloud itself, but from when security is introduced into the process. When controls are designed alongside migration plans – rather than retrofitted after workloads are already deployed – organisations are able to move faster and with greater confidence.

Embedding security early allows visibility, monitoring, and governance to evolve in step with migration. This reduces the likelihood of data exposure, misconfiguration and rework, while giving teams greater assurance as environments scale. Organisations that lead with security often adopt a platform-led approach, prioritising unified visibility across endpoints, workloads, and cloud services. This reduces reliance on fragmented tools and allows security to scale automatically as cloud environments grow.

Yet the research highlights that security is still too often introduced later than intended:

57%

of respondents say security teams are consulted too late in public cloud migration planning to have a meaningful impact

52%

have been part of a migration where security requirements were overlooked, underestimated, or addressed late

85%

say post-migration audits often reveal preventable security mistakes

76%

believe the broader IT team underestimates the security impact of quick fixes made during cloud migration

Public cloud platforms themselves provide many of the capabilities need to address these issues.

Native services – such as automated compliance checks, identity frameworks, and AI-driven detection – make it possible to design security that scales with workloads.

The differentiation lies in how effectively organisations apply these capabilities, supported by the right partners and security platforms, to ensure controls are implemented consistently and early enough to deliver real value.

Financial impact of **underestimating cloud security**

When security is introduced late, the impact is often felt beyond risk alone. Although organisations allocate around 14% of their migration budgets to security, late-stage implementation can drive significantly higher costs due to remediation, downtime and redesign. On average, organisations report **spending more than £625,000 as a result of underestimated security requirements**. Furthermore, **one in ten organisations have suffered a breach linked to late-stage security implementation** – a reminder that security is not a barrier to agility, but a foundation for sustainable transformation.

By embedding security from the start – using automation, governance frameworks, and clear collaboration between IT and security teams – organisations can unlock the full potential of the cloud safely. Security by design not only prevents costly issues later on; it enables organisations to move faster, innovate with confidence, and maintain trust as they scale.

Consequences of late-stage security implementation

Making compliance continuous

Compliance continues to play a defining role in public cloud migration. When addressed early, it can act as a powerful enabler – providing clear guardrails that help protect data, strengthen governance and build trust with customers.

While 90% of respondents say regulations are a major source of complexity when migrating to public cloud, these frameworks are not a barrier. The real challenge lies in ensuring teams have the processes and support to apply requirements consistently as cloud environments evolve.

80% of repondents
say compliance requirements often delay or derail cloud migration projects

Each regulation introduces its own technical and procedural considerations, shaping how public cloud environments are designed and operated. Most organisations find meeting these expectations challenging, particularly as environments scale. However, when compliance is embedded from the outset – supported by automated checks and expert guidance – it can streamline decision-making and reduce risk throughout the migration journey.

Specialist partners play a critical role here, helping organisations operationalise compliance by translating regulatory intent into technical controls, automating validation, and embedding assurance into day-to-day workflows.

For many organisations, compliance gaps only surface once systems are live, when remediation is slower and more costly. Early validation, automated assurance, and the right partnerships allow teams to address requirements as they build, rather than retrofitting controls later. Regulations are not just legal obligations; they're design parameters that should guide how organisations build, secure, and govern their cloud environments from day one.

83%
of respondents say compliance violations are often discovered after data, workloads, and applications go live in public cloud

76%
of respondents say mistakes made during migration are a direct cause of failed audits, dropping to 60% for security practitioners

Clarifying cloud ownership and control

Clear ownership is essential to building secure and resilient cloud environments. **Yet the shared responsibility model is still widely misunderstood.** Some teams assume cloud providers manage all aspects of security – an assumption that is surprisingly more common among security professionals than IT teams.

77% of respondents
believe their public cloud provider is responsible for securing all aspects of their environment

In reality, the shared responsibility model is designed to strengthen security outcomes. While cloud providers secure the underlying infrastructure, customers retain control over their data, identities, and configurations. When these roles are clearly defined and understood, the model becomes a powerful way to layer security and reduce risk across environments.

48%

of respondents said IT teams often lack the knowledge to ensure environments are configured securely, **rising to 60% for IT practitioners,** but only **29% of cybersecurity practitioners**

Partners and security platforms can support this by reinforcing shared ownership, improving visibility, and helping teams put the right guardrails in place from day one. For many organisations responsibility for cloud security is distributed across IT, security and platform teams. Differences in cloud experience and tooling can create uncertainty around ownership of specific controls, leading to misalignment when making configuration or governance decisions.

Trusted partners can help bridge this gap by providing clarity, best practices, and shared processes that align teams around common goals. This alignment becomes increasingly important as cloud services evolve rapidly and new capabilities are introduced.

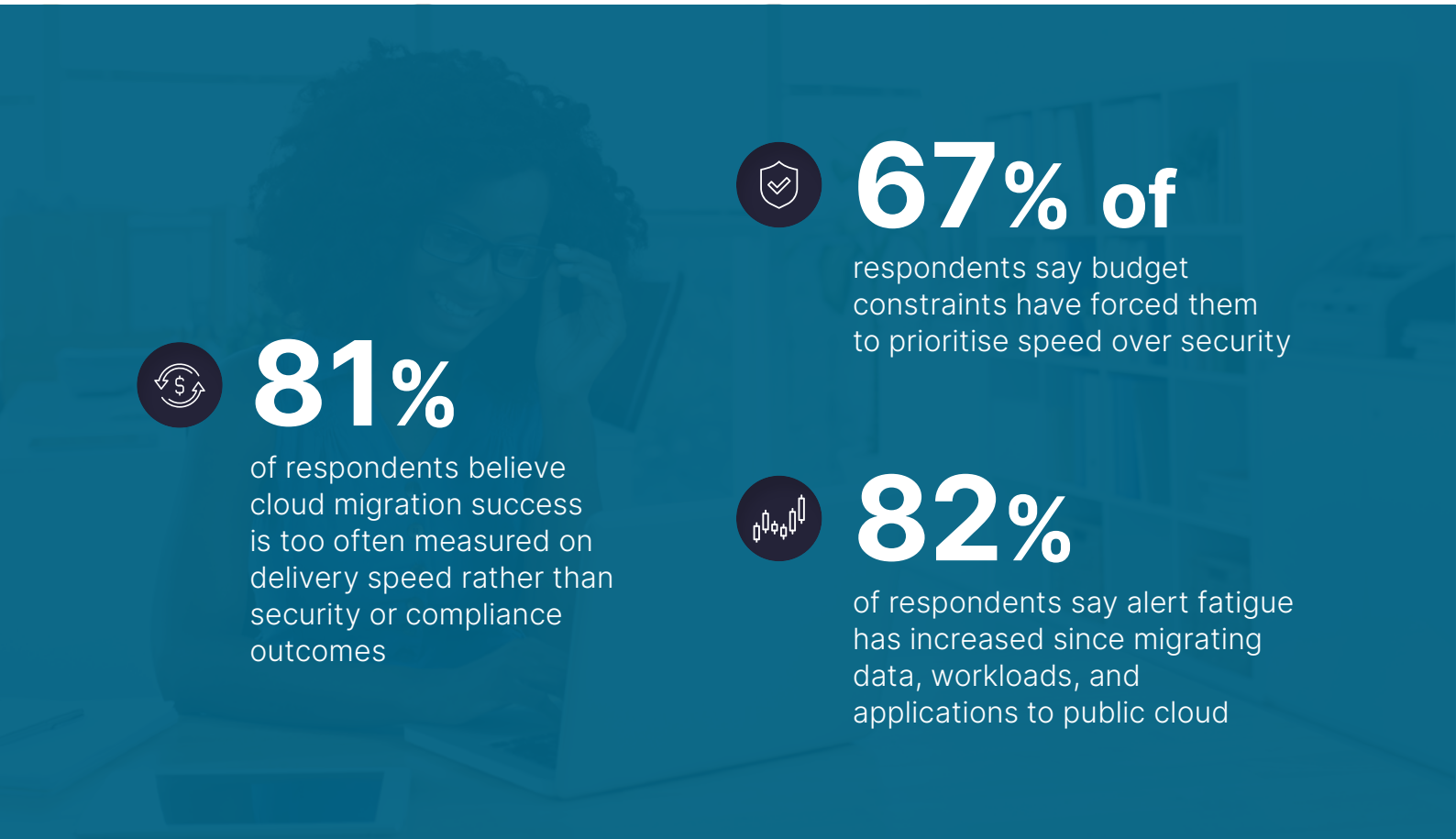
Maintaining consistent visibility and control across expanding environments can be challenging without a coordinated approach. As services proliferate, organisations risk developing blindspots that limit their ability to manage risk effectively.

64% of respondents
say inconsistent security configuration and tooling has created blind spots (rising to 77% among IT practitioners)

69% say evolving
requirements make it difficult to choose the right public cloud security approach

Platform-based security approaches are increasingly valuable here, helping organisations reduce tool sprawl and achieve unified visibility across cloud, identity and endpoint environments. Combined with expert guidance, this enables security to scale in line with the business.

Despite growing maturity, many organisations still measure migration success by delivery speed rather than long-term resilience. While speed remains important, prioritising the right security posture helps reduce misconfigurations, minimise alert fatigue, and deliver outcomes that stand up over time.



81%
of respondents believe cloud migration success is too often measured on delivery speed rather than security or compliance outcomes

67% of
respondents say budget constraints have forced them to prioritise speed over security

82%
of respondents say alert fatigue has increased since migrating data, workloads, and applications to public cloud

"Cloud has transformed how organisations operate, but it has also expanded the surface that needs protecting," said Chris Hosking, AI & Cloud Security Evangelist at SentinelOne. "Security teams can't rely on traditional methods to manage such dynamic environments. They need visibility and intelligent automation that keep pace with constant change.
By combining strong security foundations with smarter, AI-powered, integrated tools, organisations can move beyond simply managing cloud risk to actively strengthening their resilience. This will turn cloud from a potential vulnerability into a core enabler of business progress."

The complexity of cloud migration means that even well-prepared teams can encounter challenges. Misconfigurations, identity gaps, and limited visibility remain the most common causes of incidents during and after migration. These issues rarely stem from negligence – they're the byproduct of rushed timelines and stretched internal resources.

83% of organisations
have experienced security issues during or after migrating data, workloads, and applications to public cloud

80% of respondents
think time pressures during migration have led to security flaws or compliance risks

Chart: The most common security issues during or after migrating data, workloads, and applications to public cloud

1. **Identity challenges**
2. **Misconfigured cloud storage or services**
3. **Challenges securing AI models**

The right partnerships can make all the difference. Experienced cloud and security partners bring structure, insight and independent oversight, helping organisations reduce the likelihood of error and apply best practices consistently. **Successful migrations typically combine three elements: scalable cloud platforms, unified security platforms, and specialist partners that orchestrate secure design, execution, and governance.**

Only 12% of organisations
manage cloud migration security entirely in-house,
with most relying on third-party tools and consultants

Embedding security early is the most effective route to long-term resilience. Taking a secure-by-design approach allows teams to bake in compliance and deploy faster without sacrificing control. Programmes like AWS Migration Acceleration Program (MAP) can also help offset initial migration costs, enabling organisations to adopt best practices and mature their cloud posture sooner. MAP is a comprehensive, proven framework developed from AWS's experience migrating hundreds of enterprise customers. It provides funding, tooling, and partner support to help identify migration opportunities, reduce cost and risk, and execute migrations efficiently. It's a key part of how AWS helps both customers and partners move faster and smarter in the cloud.

“Many organisations invest in powerful cloud and security technologies but only unlock a fraction of their potential,” **said Philip Reeve, Cloud Solutions Director at Bytes.** “When security, identity, and runtime protection are treated as architectural foundations rather than bolt-ons, teams move faster and get far more value from their technology investments. The role of the right partner is to turn capability into outcomes – not just deploy tools.”

91% of respondents

that strong security is best achieved through incorporating it by design rather than relying on post-migration assessments or tools

77%

of respondents have used or plan to use AWS MAP to support migration

A real-world example of how partnerships enable secure cloud migration

A large UK-based enterprise undergoing a complex AWS cloud migration was struggling with limited visibility across its endpoint, identity, and cloud environments.

Disjointed legacy tooling and accumulated technical debt made it difficult to secure workloads consistently as they moved to the cloud.

By working with Bytes, a specialist cloud migration partner, and adopting SentinelOne's unified, platform-based security approach, the organisation was able to embed security earlier in the migration process.

This delivered consistent visibility from endpoint to cloud, reduced operational complexity, and enabled teams to detect and respond to risks in real time.

As a result the organisation reduced risk during and after migration, accelerated its data centre exit, and moved to the cloud with greater confidence and control.

Conclusion: Turning cloud ambition into secure, lasting success

How Bytes Helps You Deliver Secure-by-Design Cloud Migrations

Bytes supports organisations across the full cloud lifecycle—from strategy and readiness to migration, modernisation, governance, and ongoing cloud security operations. Our strategic partnerships enable unified visibility, secure-by-design architectures, and accelerated, resilient delivery

Cloud migration is no longer a question of if, but how well. As organisations move more critical data, workloads and applications into public cloud, success increasingly depends on getting the foundations right from the outset. **Security, compliance and operational control are not obstacles to progress – they are the enablers that allow organisations to modernise faster, scale confidently and realise lasting business value from the cloud.**

Working together, Bytes, AWS and SentinelOne provide a proven framework for secure cloud transformation. As a Premier AWS Consulting Partner, Bytes helps organisations across the full AWS journey – from migration and modernisation to ongoing optimisation – bringing deep expertise, established governance models and a secure-bydesign approach that addresses the challenges most likely to slow progress or increase risk. **Ultimately, this helps organisations to get to AWS faster – and then make it work harder**.

At the same time, **SentinelOne's Purple AI** enhances security operations by accelerating investigation and response across dynamic cloud environments. By helping teams quickly surface relevant signals, prioritise genuine threats and automate routine analysis, **Purple AI** reduces operational overhead while improving decision-making. Embedded from the outset, these capabilities support a security-by-design approach that enables organisations to migrate faster, operate with confidence, and maintain strong protection as environments grow.

Together, this combination enables organisations to move to the cloud with clarity and confidence – modernising securely, operating efficiently and building environments that are resilient by design. For organisations at any stage of their cloud journey, a secure-by-design approach, supported by the right platform and partners, is the most effective way to turn cloud ambition into long-term success.

AWS provides the secure, scalable cloud foundation that underpins this transformation. Through its shared responsibility model, native security services and established frameworks such as the Well Architected Framework and Migration Acceleration Program (MAP), AWS enables organisations to design resilient architectures, reduce risk and accelerate delivery – supported by funding, tooling and partner expertise.

Bytes helps customers access AWS funding programmes – including MAP – to reduce costs and accelerate delivery. Whether you're starting out or scaling up, Bytes brings clarity, pace, and long-term value to every stage of an AWS journey – including a complimentary AWS Migration assessment to help organisations benchmark their current state and plan what's next – with speed, security, and confidence.

SentinelOne complements this foundation with its unified, AI-powered Singularity Platform, which delivers continuous visibility and protection across endpoints, cloud workloads and identities. By embedding detection and response into cloud environments as they evolve, the Singularity Platform helps teams identify misconfigurations, identity misuse and emerging threats early – before they escalate into incidents. This unified approach ensures security scales in line with cloud adoption, rather than becoming a bottleneck.

About Bytes Software Services

Bytes Software Services is one of the UK's leading providers of cloud, security, and digital transformation solutions. **As an AWS Premier Tier Services Partner**, we help organisations modernise securely, accelerate cloud adoption, and maximise long-term value from their technology investments.

Our team brings deep expertise across cloud architecture, migration, identity, cybersecurity, FinOps, governance, and ongoing cloud operations—supporting customers at every stage of their transformation journey.

Through strong partnerships with industry leaders such as AWS and SentinelOne, we deliver secure-by-design cloud platforms, unified visibility and protection, and scalable solutions that empower organisations to innovate with confidence.

Whether you're migrating critical workloads, strengthening cloud security, or modernising applications, Bytes provides the strategic guidance, technical capability, and proven frameworks needed to turn cloud ambition into real business outcomes.

About Cloud Bridge

Cloud Bridge is a globally recognised AWS Premier Partner and three-time AWS award winner: Rising Star Partner of the Year (2023 EMEA, 2022 UK&I) and SMB Partner of the Year (2025 UK&I). We help organisations make sense of AWS – turning complexity into clarity and transformation into measurable traction.

We deliver end-to-end AWS lifecycle support at global scale, from migration and modernisation to long-term managed services, solving hard IT challenges across cost, architecture, operations, and governance. By weaving automation, data intelligence, and agentic AI through every engagement, we accelerate delivery, strengthen control, and unlock smarter outcomes.

At Cloud Bridge, we don't just get you to the cloud – we make sure you get lasting value from it.

About SentinelOne

SentinelOne (NYSE:S) is the world's most advanced, autonomous AI-powered cybersecurity platform. Built on the first unified Data Lake, SentinelOne empowers the world to run securely by creating intelligent, data-driven systems that think for themselves, stay ahead of complexity and risk, and evolve on their own.

The SentinelOne Singularity™ Platform enables global enterprises to automatically prevent, detect, and respond to cyberattacks with machine speed and pinpoint accuracy. Leading organizations—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow™.

Learn more at sentinelone.com

About AWS

Amazon Web Services (AWS), the world's most comprehensive and broadly adopted cloud, enables customers to build anything they can imagine – by offering the greatest choice of innovative cloud capabilities and expertise, on the most extensive global infrastructure with industry-leading security, reliability, and performance.

Security is our top priority at Amazon Web Services (AWS). Our infrastructure and services are architected to provide customers with the most secure cloud computing environment available today. AWS helps meet the unique security requirements of even the most sensitive workloads including government, financial services, and healthcare.

Methodology

This research was conducted by SAPIO Research as an online survey of practitioners and decision makers responsible for IT or cybersecurity. SAPIO Research surveyed 300 respondents in the UK from a cross-section of organisations with more than 500 employees.

Appendix

Table showing on a scale of 1-5 (1 being not at all confident, 5 being extremely confident), how confident respondents feel migrating the following data, workloads or applications to a public cloud environment..

	Total % confident (4 or 5 out of 5)	% confidence in security teams	% confidence in IT teams
Business critical internal systems	71%	63%	79%
Workloads dependent on specialised or legacy hardware	71%	80%	62%
Large-scale data warehousing	70%	76%	65%
Financial or sensitive customer data	70%	60%	81%
Applications with latency requirements	69%	81%	52%
Intellectual property repositories	68%	62%	73%
Highly regulated applications/workloads	66%	51%	80%
Data requiring strict data residency	65%	53%	77%