S&P Global
Market Intelligence
451 Research
Business Impact Brief

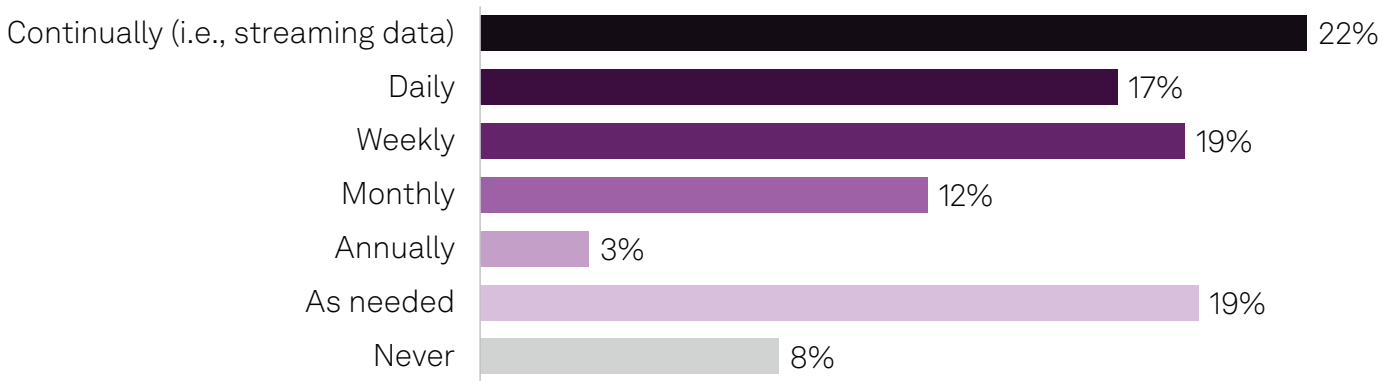
Cyber resilience and data migration challenges present opportunities for trusted partners

The Take

Enterprise demand for enhanced cyber resilience and data migration capabilities presents significant business opportunities for resellers, service providers and other consulting partners. Cybersecurity incidents, especially ransomware and malware, have become the primary cause of outages for most organizations. Nearly a third of organizations have experienced an outage in the last two years, and the average reported cost of an outage increased from $2.15 million in 2023 to $2.33 million in 2024, an 8% rise, according to 451 Research's Voice of the Enterprise (VotE): Storage, Disaster Recovery study. These factors are driving additional investment in cyber resilience. By helping customers mitigate risks, avoid outages and minimize financial impacts, resellers can strengthen their status as trusted advisors.

Data migration is a key service that partners provide to facilitate infrastructure updates and hybrid cloud modernization, and the importance of these services has risen in recent years. Resellers and consultants should view data migrations not as tedious, time-consuming chores, but as opportunities to deliver greater value to customers. Migration complicates security efforts by introducing vulnerabilities that can disrupt operations. About 44% of organizations have experienced unplanned downtime due to migration issues, according to 451 Research's VotE: Storage, Data Migration 2024 study, and 38% report data loss or corruption. Nearly three-fourths (73%) of organizations express concerns about security threats during the migration process. A partner with secure, consistent data migration practices can alleviate fears of security incidents and failed migrations.

Data migrations occur frequently at most organizations



Q. How often does your organization transfer on-premises data to or from public cloud environments?
Base: Respondents whose organizations have migrated data to a cloud service provider (n=276).
Source: 451 Research's Voice of the Enterprise: Storage, Data Migration 2024.

Hypervisor migrations also pose risks that can result in outages or data loss. Transitioning between hypervisors can expose systems to threats such as unauthorized access, misconfigurations and increased downtime. Without effective security protocols, organizations are more vulnerable to cyber threats, highlighting the need for comprehensive security strategies to safeguard virtualized environments during migration.

A key challenge in both data and hypervisor migrations is disparity in tools and skills between the original and new platforms. The complexity of hypervisor migrations allows partners to differentiate themselves by using their expertise to recommend processes and tools that ease the transition and minimize disruption while maintaining security and reliability. Partners that lack this expertise should invest in new tools and work with vendors that offer training and certification programs to equip their teams.

S&P Global
Market Intelligence

451 Research
Business Impact Brief

Business Impact

Security teams are overwhelmed. Only 5% of respondents to the VotE: Information Security, SecOps 2024 study say they can respond to all security alerts in a typical day, while 43% miss over half of their daily security alerts, and 19% respond to less than a quarter of alerts. Organizations need tools and services to prioritize and deliver actionable alerts. Comprehensive cyber resiliency requires additional collaboration between security and infrastructure operations professionals. Resellers, service providers and consultants can bridge the gap for organizations that lack current skill sets or adequate staffing.

Migrations are getting larger. Two in five respondents (40%) have conducted a migration of more than 1 petabyte of data between on-premises and public cloud environments. With large payloads becoming more common, companies must consider the risk of extended unplanned downtime, experienced by 44% of respondents, and data loss or corruption, reported by nearly 40%.

Migrations are common. According to our Voice of the Enterprise: Storage, Data Migration 2024 study, nearly 40% of respondents transfer data between on-premises and public cloud storage environments on a continual or daily basis. Only 8% of respondents say their organization has never performed a data migration. Data migration is necessary when operating in hybrid and multicloud environments, especially for customers seeking flexibility in workload venues. And with many organizations considering new virtualization platforms, data and hypervisor migrations present additional opportunities for resellers to offer migration services.

Looking ahead

As organizations prioritize cyber resiliency in their IT strategies, many recognize the need for support from trusted partners to enhance their ability to withstand and recover from cyber threats. Proactive prevention and protection are crucial. Despite the many threat-detection tools available, internal teams struggle to handle the volume of daily alerts. Skilled service providers can help sort false positives from legitimate threats, reducing the security burden and ensuring the top threats receive proper attention. Resellers and consultants can also implement intelligent tools to analyze suspicious usage patterns and help organizations detect potentially compromised accounts and data.

To safeguard recovery operations, service providers should ensure that backup repositories use immutable storage to prevent deletion or corruption by bad actors or accidental customer actions. Partners should also provide secure lab environments for customers to quarantine data and run tests to ensure all traces of virus or ransomware are eliminated before recovery. By protecting the backup safety net, partners can provide reliable safeguards against data loss.

Our research indicates that 24% of organizations use a service provider to manage their migrations, while 9% hire a consultant, and most backup and security software is recommended and transacted through reseller channels. This trend highlights the reliance on external expertise to facilitate smooth transitions and bolster cyber resiliency. As migrations grow, both in size and complexity, organizations increasingly turn to trusted partners for assistance. By adopting proactive cyber resiliency measures and strategically partnering with resellers, providers and consultants, organizations can enhance their security frameworks and better prepare for potential cyber threats.