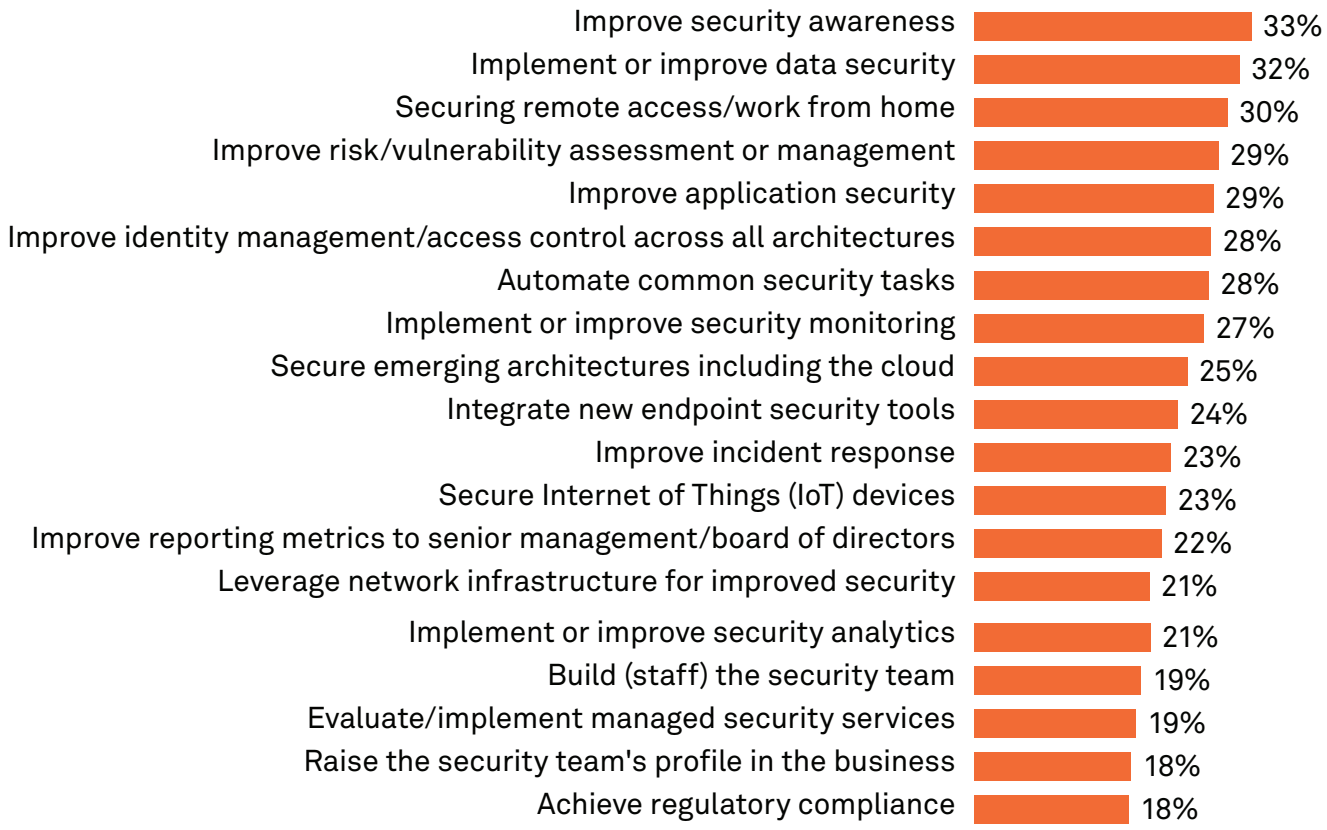
Securing Data Democratization in the Cloud

The 451 Take

Organizations are democratizing their data, combining analytic and transactional datasets to drive transformation and better customer, user and stakeholder experiences and outcomes. As data coalesces in cloud environments, it becomes available for a variety of processes and tools, for developers and users alike. Governance, risk and compliance frameworks to support privacy and trust have pushed data security toward the top of the priority list. For example, respondents to a recent 451 Research survey cited implementing or improving data security as a top strategic objective (see figure below), second to improving security awareness.

Top Information Security Strategic Objectives



Q: What are your top strategic security objectives for 2021? Please select all that apply.

Base: All respondents (n=354)

Source: 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2021

Underlying this strategic objective has been a confluence of technology and development trends, disproportionately creating both more data and more data security risk. Data democratization is the combination of all transactional and analytic datasets to achieve better user experience and product/service enhancement for data-driven enterprises. Because it's built on ever more rapid and dynamic release cycles, there is less time to consider, audit or remediate gaps in data security. Downtime risk aversion means that data is seldom deleted or removed. Because developers have more access to ever increasing cloud services, the pace of change will only pick up. Any non-integrated or non-automated security will be left behind.

As these datasets are gathered, accessed, processed and transmitted by many rapidly changing automation workflows, they are increasingly difficult to manually discover, categorize, classify and protect. Control frameworks and risk management frameworks are increasingly measured continuously, rather than reflecting a single point-in-time audit or remediation. As such, the sooner an enterprise can show continuous understanding and protection of data, the sooner it can fulfill its data security objective.

Given that the 'shared fate' or 'shared responsibility' security models still place the task of securing the data itself in the hands of the tenant organization, not the public cloud service provider, a new data security approach that controls and governs data democratization over the entire data lifecycle is needed.

Business Impact

Data discovery and access monitoring are essential. The initial challenge is to find all data sources scattered throughout the cloud and classify them. With continuous monitoring, developers can identify data owners and dynamically map ingress and egress channels to mitigate risks. Dynamic monitoring forms the basis of dynamic policy creation and enforcement.

Data risk management should be as dynamic as the data itself. Given the fluid and rapid nature of data growth, static and one-time controls do not provide any lasting value because they immediately become obsolete. Outdated data visibility and control only creates problems for both security controls and data democratization. Outdated controls give a false sense of security at best; at worst they further isolate or impede the datasets from being analyzed. Data security that provides automated monitoring of the data lifecycle over time offers assurance of both data safety and utility.

Watch out for data sprawl. As data coalesces, it is shared by more stakeholders and used in more processes. At the same time, portions of that data may be duplicated and modified for individual purposes. For example, rapid promotions and relegations of development or test environments may result in production data being accessed by test workloads with additional risk and little or no functional benefit.

Traditional perimeters are increasingly ephemeral. Cloud workloads, network edges and boundaries may have short life spans, while the underlying shared data persists. While it is important to have controls for those workloads and edges, it is also important to plan for dynamic and persistent data security controls in addition to the ephemeral controls.

Leverage cloud-native constructs. With so much of the cloud environment – compute, network, storage and identity – being dynamically defined, any holistic data security must leverage the native interfaces of the cloud environment. Leveraging common automation approaches ensures that data security does not become a separate programming step when new data is provisioned or shared in new ways.

Looking Ahead

Data democratization will continue to drive initiatives in artificial intelligence (AI), customer experience (CX) and user experience (UX) for enterprises. This also means a significant increase in collection and curation of datasets for these initiatives. Rapid development driven by these AI, UX and CX initiatives will mean more frequent releases of software, products and services. DevSecOps cycles, in turn, are expected to further accelerate. The frequency of these releases will change, moving from weekly or monthly to hourly or daily.

Risk management will be incorporated into product lifecycles, with the frameworks that cover the start and finish of every release over time. Many traditional security, audit and remediation initiatives have been applied retroactively to understand and fix security risks at a single point in time. These backward-looking audits have significantly slowed down or disallowed key business initiatives. With data security inherently being part of the data democratization process, cloud service stakeholders – and especially developers – will be enabled to use cloud-native constructs and continuous automation tools whenever possible. In this scenario, developer experience, where the concepts and capabilities for data security are understood and implemented quickly, becomes essential.