451 Research

S&P Global
Market Intelligence **Business Impact Brief**

Securing the Evolved Hybrid

The 451 Take

The realities of the modern enterprise ecosystem drive an ever-greater push to reach customers wherever they are and to support employees from wherever they work. This has meant that IT infrastructure has had to blend resources from various sources, and in most cases, that means hybrid. The challenge is that many organizations have arrived at hybrid without a formal plan, which creates security gaps that increase business risk.

The architectural building blocks that make up their hybrid environments were added independently based on needs at the time: a partner had a key function or dataset in one provider; machine learning capabilities of another provider were key to a new service; the front end to an application needed to be placed in a new region to improve customer experience. All of these made sense independently. The problem lies in the complexity that has been created in cramming them all together, making it much more difficult to secure. While 57% of respondents to a 451 Research study indicated they were operating hybrid infrastructure, only 43% said that they had a formal plan for hybrid operation that includes addressing security.

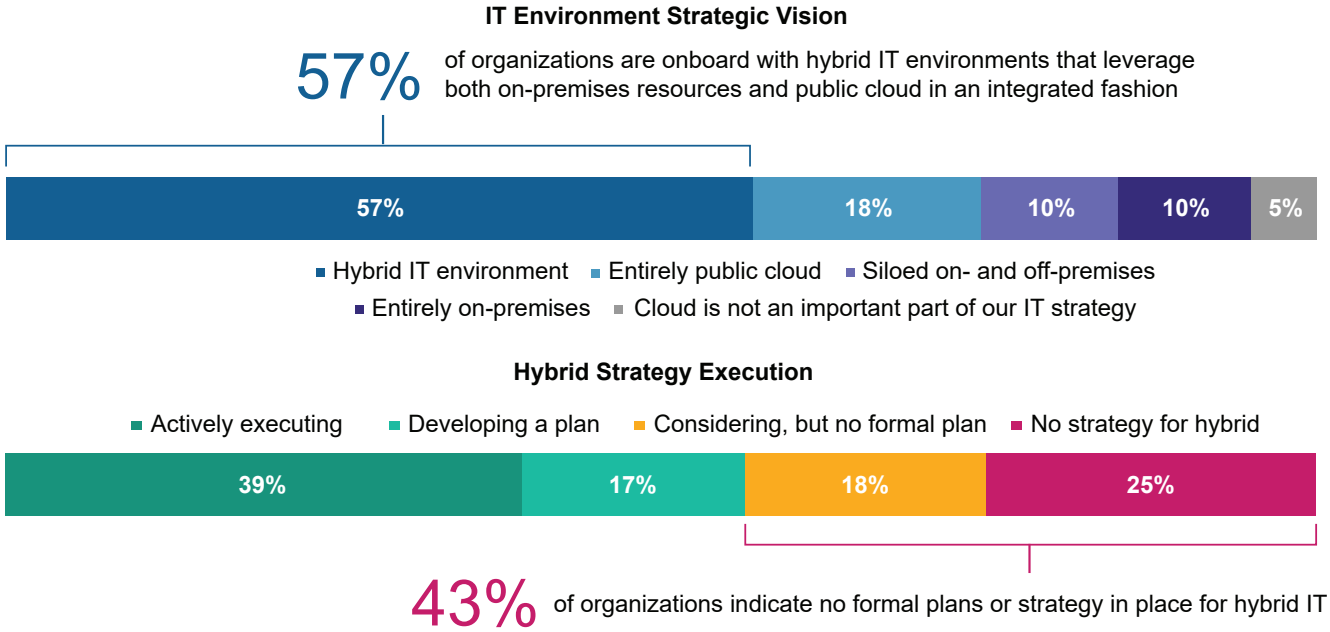
IT Environment Strategic Vision; Hybrid Strategy Execution

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Organizational Dynamics 2020

Q: Which of the following best describes your organization's existing or planned IT operating environment? (n=434)

Q: Which of the following best describes the state of your organization's strategy regarding hybrid IT? (n=457)

Base: All respondents



Complexity widens security gaps created by the differences in the environments that make up the hybrid infrastructure. If those differences aren't addressed, security protections can be compromised. Enterprises face many challenges in securing hybrid environments – cloud skills gaps, insufficient automation, organizational silos – and any one of them can be the weak link in their chains of defense. Hybrid creates the additional challenge of integrating third-party service providers into enterprise operations while still achieving compliance goals. Hybrid hampers security policy management by requiring security teams to translate policy directives into controls that can be different in each environment. Controls that are available on-premises aren't the same in a cloud provider, and the various providers have differences, as well. This raises the risk of configuration errors creating security exposures.

The 451 Take (continued)

It can seem daunting to untangle the complexities of hybrid infrastructure security, but it's a problem that is critically important to address. There are important considerations that can make hybrid security work efficiently and effectively. Addressing visibility problems needs to be a first priority, and enterprises can tackle this with systems that understand and integrate the telemetry options from clouds and containers, as well as traditional infrastructure.

To fully understand and act on that integrated telemetry, enterprises need to have established a source of truth, an anchor for correlating information about assets, devices and users. Being able to reliably identify and tie together events that span a hybrid environment offers greater levels of situational awareness. It also allows security policies to operate with a higher level of abstraction because they can be built with a global, rather than local, perspective. Security management systems that can operate at this level can also address another hybrid security challenge by normalizing controls across an infrastructure. That can allow security policies to be built at a high level and then translated into the native controls at the local level.

It's important to consider the value of data-centric security protections alongside the infrastructure security capabilities that they rely on. Establishing protections that can move with data from edge to cloud to core, or wherever it's being created or put to work, can reduce risk while increasing usability. This is particularly important in hybrid environments, where native protections can vary.

Effective hybrid security can be achieved with effective and early planning, and an expectation that visibility and common control capabilities have to extend across the full infrastructure. Organizations need to step beyond legacy approaches and evaluate points of risk, building in security early in the transformation process. It's an investment that will yield benefits in efficiency and effectiveness and give enterprises the infrastructure agility to be at their competitive best.

Business Impact

EFFECTIVE SECURITY POLICY. Increased visibility can improve security awareness and increase the effectiveness of security policies by giving security teams a deeper understanding across hybrid infrastructure.

OPERATIONAL EFFICIENCY. Normalizing controls across hybrid environments can simplify policy management and reduce configuration errors. The automation required to operate at hybrid scale can be a force multiplier for security teams.

SECURITY CONSISTENCY. An improved approach to hybrid security operations can deliver more consistent security outcomes. Having capabilities that can be depended on in differing environments reduces IT workloads while improving developer productivity. Wrapping protections around data – so that the protections travel with the data to ensure its proper use – can deliver consistent protections.

Looking Ahead

Mastering hybrid security gives enterprises the ability to keep pace with their business needs. It's the foundation of establishing infrastructure agility and a key to staying competitive in a dynamic market. It's also a foundation for greater innovation, allowing developers and applications to thrive and expand while security teams can rise from operational toil to address more strategic security initiatives. As organizations plan the next steps in their infrastructure, they need to make it a priority to build in security considerations at the start and ensure that they'll be able to deliver resources securely across their hybrid landscape.