See It, Fix It, Manage It

Ensuring Hybrid and Multicloud Applications Are Reliable and Secure

Pathfinder Report

February 2022

Commissioned by

FORWARD NETWORKS

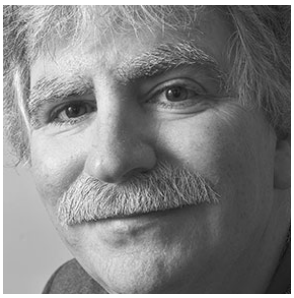
451 Research

S&P Global
Market Intelligence

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About the Author



Mike Fratto

Senior Research Analyst, Applied Infrastructure & DevOps

Mike Fratto is a Senior Research Analyst on the Applied Infrastructure & DevOps team at 451 Research, a part of S&P Global Market Intelligence. He covers enterprise networking, including campus and datacenter networking, SDN, SD-WAN, SD-Branch, cloud networking, container networking, networking as a service, network performance monitoring, and network automation and orchestration. He has extensive experience reviewing and writing about enterprise remote access, security and network infrastructure products, as well as consulting with enterprise IT, equipment and software vendors, and service providers.

Prior to joining 451 Research, he was with GlobalData as Research Director with the Global IT Technology & Software team covering the enterprise networking and datacenter technology markets. Mike was with TechWeb for more than 15 years, most recently as Editor of Network Computing. He was Lead Analyst with InformationWeek Analytics, Senior Technology Editor with Network Computing and Executive Editor for Secure Enterprise. He has spoken at several conferences including Interop, SD-WAN Summit, MPLS + SDN + NFV World Congress and SDN NFV World Congress, as well as to local groups, and he served as the chair for Interop's Datacenter and Storage tracks. Prior to Network Computing, Mike was an independent consultant.

Mike teaches a graduate course in network security for Syracuse University's Information Science and Technology program. The course presents a technical and theoretical overview of network security strategies and technologies and how network security can fit into an organization's overall IT architecture.

Mike graduated from Syracuse University with a bachelor's degree in Information Science and Technology.

Executive Summary

The last few years have seen a rapid shift in how applications are architected, deployed and managed throughout their lifecycle. The shift has happened at all levels of IT; organizational changes have pushed developers and operations staff into collaborative DevOps teams, into launching new roles and titles, such as site reliability engineers, and adopting new and adapting existing technologies and products to support the diverse, agile world of hybrid and multicloud computing.

That paradigm shift has made IT teams more agile and responsive to business demands but brings with it difficulties in ensuring these diverse cloud environments – along with the features and capabilities each offers – are used in a way that complies with regulatory, industry and company requirements and policies. Maintaining visibility and ensuring applications are compliant are difficult IT tasks in one type of environment; the multitude of environments with their various features and capabilities greatly complicates the ongoing management and monitoring of cloud services and applications.

Enterprise IT, security and governance teams can improve their network performance and compliance monitoring by using visibility software that consistently collects and rationalizes data from cloud services, as well as builds monitoring and auditing processes and workflows to ensure that applications remain in compliance and are operated in accordance with company policy and expectations across the application's lifecycle. The operative word is 'consistent,' which forms the basis for end-to-end performance and security visibility.

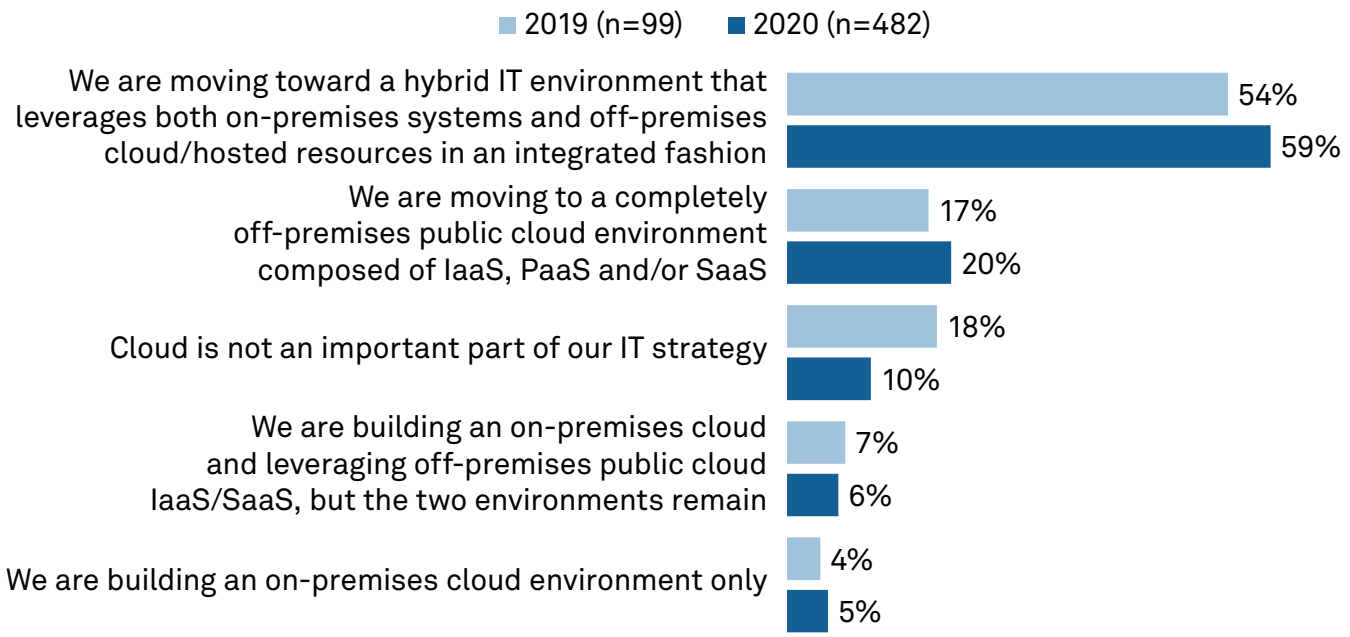
Key Findings

- The large majority of enterprises are moving to hybrid or multicloud architectures that comprise multiple cloud services and on-premises datacenters. Operating in multiple environments requires enterprise IT to rethink their approach to governance, monitoring and reporting on applications and environments continually throughout the application lifecycle.
- A growing number of enterprises are placing mission-critical applications in cloud services. This suggests they are confident in their ability to properly configure, secure and operate cloud services in ways that meet the demands of highly sensitive data and access requirements.
- Data residency, compliance and auditing are three of the top issues enterprise IT teams face with cloud computing. Hybrid and multicloud computing complicate these issues further due to the variance in visibility and monitoring capabilities within the environments and the difficulties in aligning service features with policy and regulatory requirements.
- The majority of enterprises use the infrastructure management, monitoring and security services available from cloud providers, but a significant portion plan to replace those with third-party products. Doing so reduces some of the variability in feature capabilities across clouds, but there still may be significant differences in how those third-party products are deployed and managed.
- Continually monitoring and auditing hybrid and multicloud environments is a burden that IT teams will have to bear to ensure their cloud applications are secure throughout their entire dynamic lifecycle. The number of functions that differ among cloud services makes achieving and maintaining a consistent configuration difficult but not impossible.

Cloud Usage for Mission-Critical Applications Is Commonplace

The majority of enterprises are moving to a multicloud strategy that not only uses multiple cloud services, but also multiple types of cloud service, such as IaaS, PaaS and SaaS, as well as on-premises clouds. According to recent 451 Research survey data, 59% of enterprises said they are moving toward an integrated multicloud IT architecture, while another 20% are moving entirely to the cloud (see Figure 1). Some enterprises will also continue building their own clouds on-premises and in colocated datacenters for those workloads they prefer to run on their own infrastructure. The benefits of cloud services are evident: lower-cost application environments for short- and long-term projects; a more agile environment that scales on demand, balancing cost against performance and availability; and a wide range of services common to IT without the associated overhead and licensing that occurs with similar on-premises products. Enterprises of all sizes are using clouds effectively and reliably for both mission-critical and non-mission-critical applications, but the complexity of these environments is posing a challenge in establishing effective visibility.

Figure 1: The Use of Hybrid Multicloud IT Architectures Will Continue to Grow

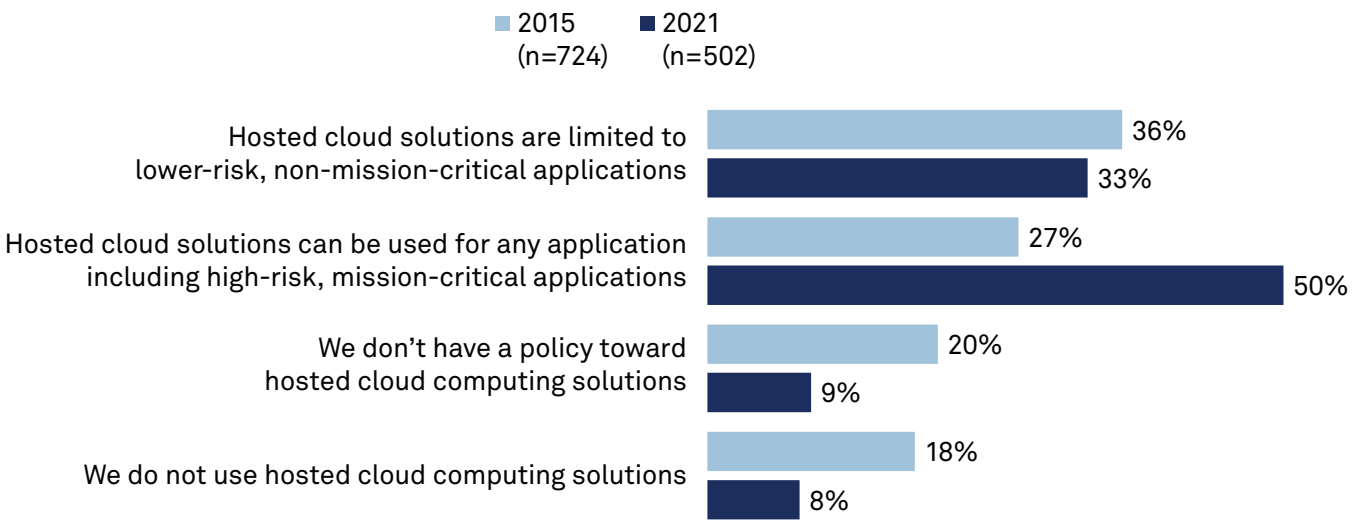


Q: Which of the following best describes your organization's overall IT approach and strategy?
Base: All respondents (2019 had abbreviated fielding)
Source: 451 Research's Voice of the Enterprise: Digital Pulse, Budgets & Outlook 2021

Hybrid and multicloud bring their own issues. Prior to hybrid and multicloud computing, enterprises strived to build computing environments that were consistent so that IT could leverage experience and education on the IT systems over the long term. The new cloud paradigm involves diverse environments (each with its own set of features and capabilities) that IT has to learn, manage and govern. The decision regarding which cloud to use for enterprise applications is most often driven by business units, developers and application architects, or company policy. The result is that teams must manage a variety of environments that need to be consistently secured and protected. Historically, most applications have been contained entirely within a single on- or off-premises cloud environment – the cloud as a replication of the datacenter – and this is still the case for many enterprises. However, cloud-native applications are being developed and deployed using more than one cloud service, which makes securing, monitoring and auditing cloud and application deployments difficult to accomplish using current tools and processes.

The Importance of Cloud Governance

Figure 2: Clouds Are Used to Host Mission-Critical Applications



Q: How would you best describe your organization's policy toward usage of hosted cloud computing solutions (hosted private cloud, IaaS or PaaS) today?

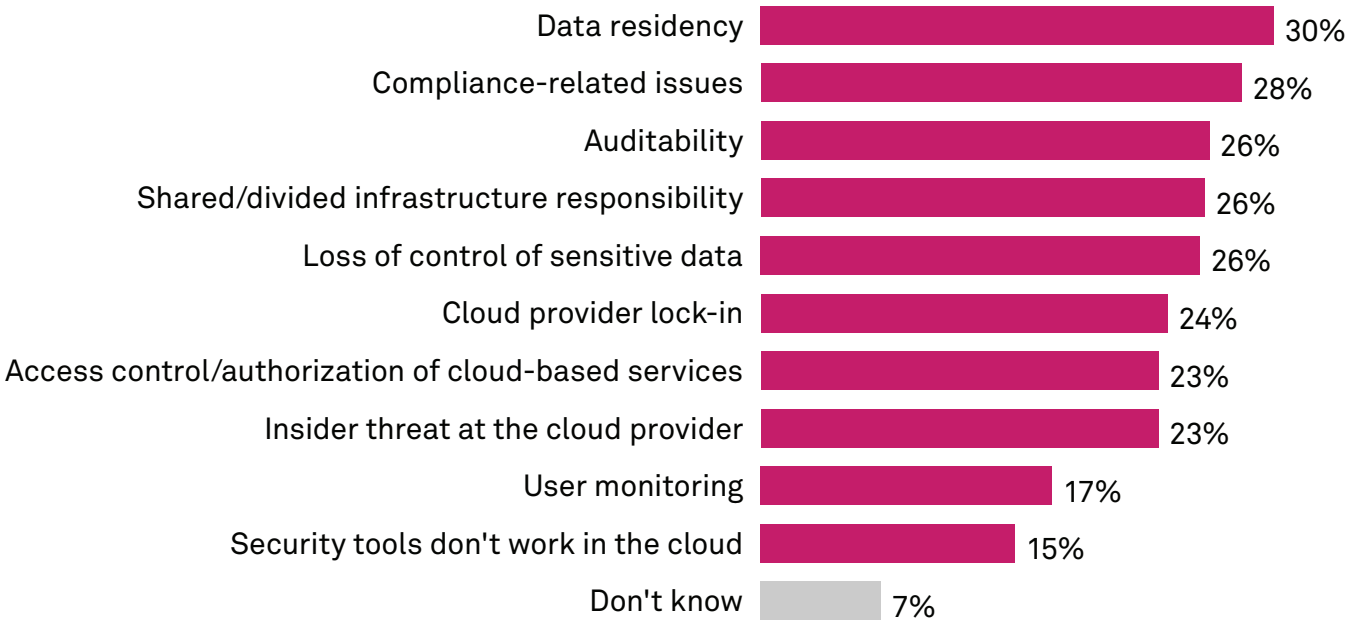
Base: All respondents

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

Effective governance is necessary for hybrid and multicloud environments. There is a common belief that clouds are used for non-critical workloads and applications, but our data shows the opposite is true: 50% of enterprises are using clouds for mission-critical applications (see Figure 2), which is a significant increase since 2015, when only 27% of respondents said cloud could be used for any application, including high-risk applications. Enterprises will continue to use clouds for mission-critical applications, and they will need tools and processes to ensure the cloud services are properly configured, reliable and resilient against outages.

Complicating matters is that each cloud service and on-premises environment is different. Cloud services offer a suite of security and visibility tools – from network security, such as firewalls and VPN, to identity and access management, access controls for applications and data stores, anti-denial of service, and monitoring tools. Third-party security products can be deployed as virtual machines in the customer's instances, but how those products are integrated into the cloud service and how they are managed varies from service to service. Business units and application owners have staff who are skilled and trained in the cloud services they use, but centralized business functions like security and governance require staff who are appropriately skilled on *all the cloud services* the enterprise uses in order to properly secure, audit and monitor cloud applications. The entire process of securing and auditing cloud applications will get more demanding as enterprise applications become more horizontally integrated across application components in different cloud services.

Figure 3: Top Cloud Security Concerns for Enterprises



Q: What are the top potential issues with cloud solutions (e.g., hosted private cloud, IaaS or PaaS)? Please select up to three. Base: All respondents (n=367)

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

Two of the top cloud security concerns enterprises have are compliance and auditability (see Figure 3). Compliance and auditing of IT systems, two critical components of IT governance, are difficult enough in environments that are controlled by the enterprise, such as on-premises datacenters and colocated servers. Add in cloud services, and it becomes critical to clearly delineate the lines of responsibility between the enterprise and cloud provider (also a top concern among enterprises). Security departments must have solutions to ensure that applications in cloud services are continually in compliance with government and industry regulations, as well as company policy. The vast majority of noteworthy security issues involving cloud services pertain to configuration errors of the cloud service, either when the service or application was initially deployed, or errors that have crept in over time.

There are many sources of configuration errors, such as improper defaults provided by the service, staff's unfamiliarity with the features of the cloud service, lack of awareness of proper security controls, or simple expediency as developers, for example, want to focus on development and not operations. The ability to independently and automatically assess and verify that cloud configurations are implemented in accordance to preapproved policy and guidelines helps ensure that misconfigurations don't crop up, and that alerts are sent when they do, so operations can address them in a timely manner.

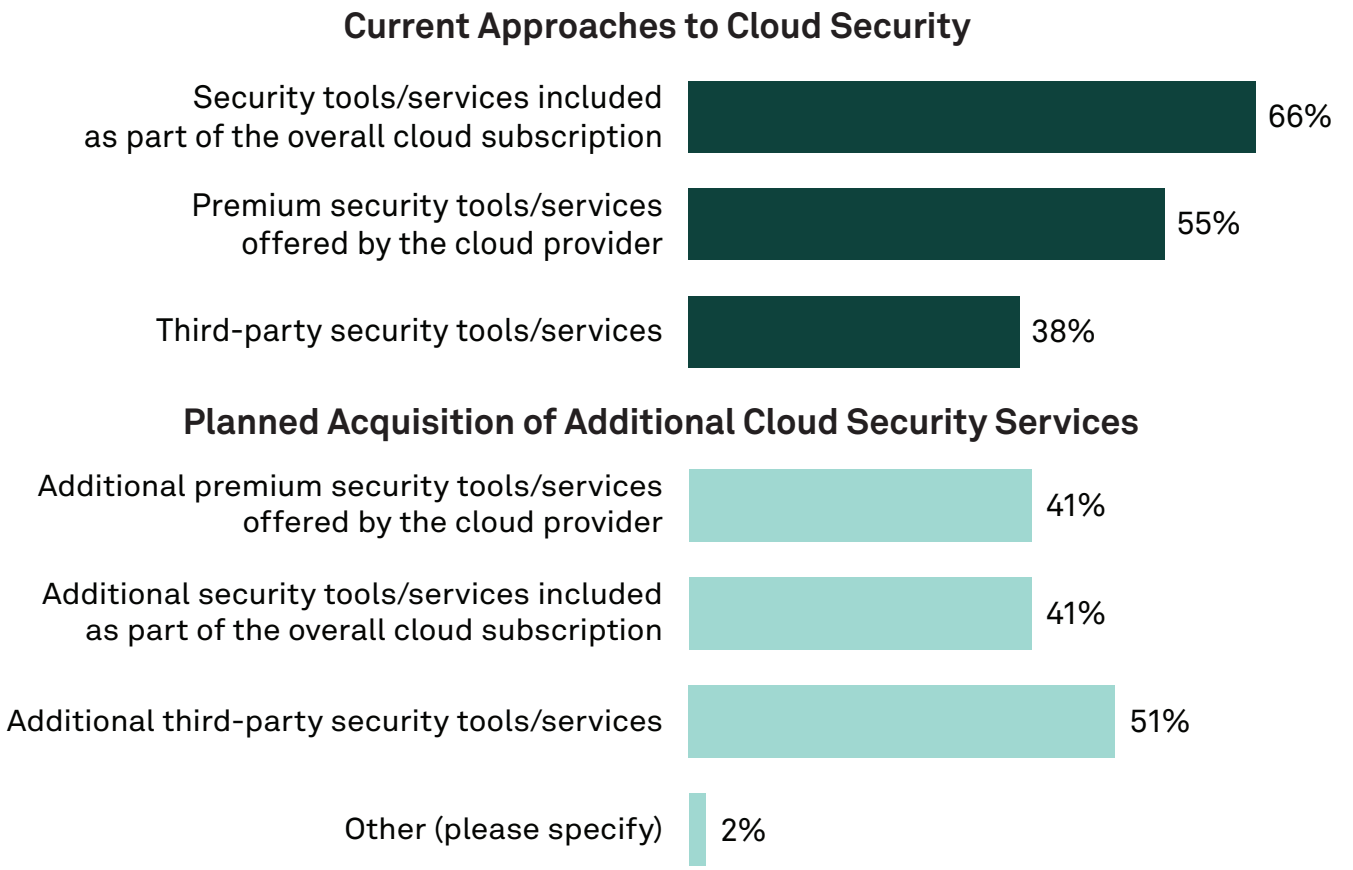
Ensuring data residency is a top concern for remaining in compliance with privacy regulations and avoiding the stiff penalties associated with non-compliance. Due to the fluidity of cloud applications, ensuring data stays within a confined region is difficult, as are monitoring and reporting requirements. In some cases, cloud services provide features to keep data within a region, but when applications are processing data, it is up to enterprise application teams to ensure that the data doesn't leave the prescribed region. Monitoring for data locality, alerting on violations, and reporting (on demand) where data has been stored and used is a critical function of departments tasked with data governance.

Cloud Provider Security Tools Today, Third-Party Tools Tomorrow

Enterprises have a variety of ways to secure cloud environments, and those choices are impacted by factors such as cost, the security products and services already in use in the enterprise, the preferences made by application and business owners, and the capabilities needed to ensure security, reliability and monitoring. Currently, the majority of enterprises rely on the security tools and services provided by the cloud provider (see Figure 4). Those services are marketed as easy to use, readily available, scalable and reliable. They are designed to be used by knowledgeable cloud users who are not necessarily security experts. The simplicity of management features reduces the operational overhead needed to configure and manage them compared to stand-alone security products, but often, insecure default settings are left unchanged, or security features are misconfigured by unknowledgeable staff, which exposes enterprise data and takes the application or cloud service configuration out of compliance.

In many cases, the cloud services' security products are integrated with other cloud service functions, making for near seamless adoption. A large minority of enterprises, 38%, currently use third-party tools and services. This is likely driven by IT departments that have standardized on specific security products and services that are supported in the cloud service. As we have noted, having a virtualized instance of a security product still requires service-specific configuration, operation and monitoring because of how the cloud services interconnect virtual machines.

Figure 4: Approaches to Cloud Security and Plans for Acquiring Cloud Security Services



Q: Which vendor-based security tools does your organization currently use for its off-premises cloud architectures? Please select all that apply. Base: Respondents who use hosted cloud architectures (n=274)

Q: During 2021, does your organization plan to acquire additional security services for its off-premises cloud architectures? Please select all that apply. Base: Spends on securing hosted cloud architectures via vendor base security tools, abbreviated sample (n=86)

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

For cloud users operating in a single cloud, the included and premium security services are an easy option to adopt. But when an application is distributed across two or more cloud services, as we have noted will be the case, the ability to properly ensure that there are consistent security controls and cloud configurations in place will become very complex because of the differences in service features and options among the various services. IT teams will have to thoroughly evaluate each service and function, ensure that each provides the necessary capabilities, map those functions to policy-driven requirements, and continually ensure the services remain in compliance and don't creep into insecure and non-compliant configurations.

More enterprises plan to use third-party security tools and services and rely less on those provided by cloud services. The migration may be due to maturity within IT, and teams trying to bring consistency and control to cloud usage, as well as an increase of cloud-native security products and services. The use of third-party tools provides feature and management consistency across cloud services and environments while simplifying some aspects of reporting and governance.

However, security departments will still have the complicated, time-consuming and expensive task of reporting on and ensuring cloud applications and services remain compliant. Cloud providers and their individual services deliver varying degrees of visibility into the configuration and operation of the service, and none report on third-party applications. IT will have to collect the operational data – such as configuration and when changes occurred across a variety of products and services – merge that data with on-premises environments, and then process the collected data into actionable reports of compliant and non-compliant components. A failure to do so can result in vulnerable data, services exposed to attack and fines due to regulatory violations.

Use Cases

Hybrid and multicloud management and governance will be top of mind for enterprise IT as the reality of operating within dynamic and diverse environments sets in. Enterprises already spend time and money on monitoring and governance that could be used elsewhere, and those costs will only increase – not only the personnel costs to collect, process and analyze the data, but any costs to move the data out of the cloud service. These costs may be high, depending on the volume of data exported.

Visibility. The first step for enterprise IT will be gaining visibility into the use of cloud services – the functions that are used – whether from the cloud service or from a third party, and how applications are configured and deployed. With application architectures like microservices, containers and multicloud applications, understanding the application topology – including the application dependency and communication chain – will be critical. Some of this data will come from application architects, but it also must be collected from live environments to independently ensure that the application is configured and operating as intended.

Rationalizing. Next, IT will have to rationalize the security, monitoring and availability controls across each service and product to ensure that the applications and clouds are conformant to IT and the business goals. Conformance in multiple environments is not new to IT and security teams; what is new is the diversity of users operating their own clouds, which will have to be brought under IT's umbrella without stifling innovation. With DevOps driving the speed and frequency of how applications are developed, deployed and managed, the data collection will have to be automated and real-time in order to keep up with changes to applications and infrastructure and ensure that cloud applications remain compliant.

Auditing. Once cloud and application configuration data is collected and processed, it can be used to monitor changes and flag potential issues as they arise across all environments. This is the point where configuration errors can be caught before landing the enterprise in the news for a data breach or inadvertent exposure. Auditing also allows IT to quickly and efficiently respond to legal requests, regulatory demands and third-party auditors with a current report that can be used to prove its operational compliance. The cost savings of automating report generation can be significant.

Verifying data flow. Modern applications built using cloud-native and microservices architectures use the network as the communication bus compared to passing data through a monolithic application. The network-based applications should be operated with strict access controls applied so that only authorized application components can use them. The challenge is that the application components can scale dynamically and even move from location to location automatically, and the access controls and other security functions must move with them. The dynamism of cloud-native applications brings a whole new layer of complication for IT to face, and active, real-time monitoring will be the key to proper management.

Integrate with DevOps. DevOps strategies are changing how applications are managed throughout their entire lifecycle. The mantra from security professionals is to build security into the application from the start, and this applies to monitoring and auditing capabilities as well. With DevOps, lots of small changes occur over the application's lifecycle that could impact visibility. This drives the requirement for monitoring and auditing capabilities to be embedded into the DevOps workflows so that changes to the application can be tested and validated during pre-deployment and later verified independently by company or external auditors.

Conclusions

Hybrid and multicloud architectures bring benefits to the enterprise, and the trend is toward continued growth in the use of these architectures. This means that new demands will be placed on IT to ensure that hybrid and multicloud applications are compliant with regulatory and company policies and are configured and operating in the way IT intends. Collecting, rationalizing and analyzing data from a diverse set of similar environments like cloud services will place unique demands on IT to monitor and report on the applications and application environments. Enterprises will have to adopt new processes to meet their reporting and monitoring goals.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence