NETWORKComputing

SPECIAL REPORT: JANUARY 2023

Sponsored by

Infoblox

Future of Cloud: What's Up in 2023

The use of public cloud services will continue its growth into 2023 and beyond. Beyond cloud computing, many organizations are looking to use Infrastructure-as-a-Service, Network-as-a-Service, Platform-as-a-Service, and other offerings to simplify infrastructure requirements and management challenges. So, what's in the plans for the cloud in the new year?

INSIDE:

Brought to you by

informa tech

👋 Hi Christopher, welcome back! Want to connect with an expert and learn more about our solutions?

Next

FEATURE

Cloud Options Abound: Trends for 2023

In the year to come, some of the biggest trends that will dictate cloud success are the continued use of hybrid and multi-cloud implementations, the use of newer as-a-Service offerings designed specifically for cloud-first enterprises, and the adoption of modern monitoring and observability solutions that make use of AI.

Lacking a crystal ball, the easiest way to make predictions for what's going to happen next in any field is to spot the current emerging trends and extrapolate. Using this approach, it is clear that there are several dominant areas to focus on with respect to cloud in the new year. They include the growing adoption of hybrid and multi-cloud strategies, the embracement of different and newer as-a-Service offerings, and the complexity that makes security, performance monitoring, and troubleshooting harder.

The Age of Hybrid and Multi-Cloud

Hybrid and multi-cloud are mainstream for enterprises, according to two vastly different, large industry surveys. In one, a 451 Research survey of 2,500 IT decision makers and cloud, DevOps, and networking professionals around the world (commissioned by Cisco), 82 percent of those surveyed said that they had adopted a hybrid cloud strategy with at least one public cloud service to run their internal and customer-facing applications. Of this number, almost half have a multi-cloud strategy where they are using two or more public cloud services.

In another study, a Harris poll (conducted on behalf of IBM) of 3,014 business and IT professionals across 12 counties and 15 industries with deep knowledge of their organization's cloud and digital transformation investments, strategies, and desired business outcomes, 77 percent of the respondents are already using hybrid cloud services.

A common theme among these and other studies is that individual clouds cannot address all of an enterprise's requirements, so enterprises must use a hybrid or multi-cloud approach. That is particularly the case as enterprises seek to modernize operations. "The key value of cloud for businesses is rapid access to innovative technologies, data sources, and applications required to navigate current disruptions and transform businesses," said Rick Villars, Group Vice President of Worldwide Research at IDC.

How does a hybrid or multi-cloud strategy help in this area? The greatest pressure on IT and network managers today is meeting the modern business expectations for availability, performance, responsiveness, and more. All of these factors are driven by an ever-more demanding user population. For example, many enterprises now operate with an always-on approach, which places a burden on keeping applications, sites, and services running all the time.

In hybrid and multi-cloud environments, cloud providers have built-in capabilities to help ensure availability and performance. They can route around an outage and easily scale to deliver consistent performance.

Quite interestingly, such benefits and resiliency capabilities of cloud are placing new demands on the data center part of a hybrid environment. The Uptime Institute's 12th Annual Global Data Center Survey found that more organizations are investing in bolstering data center resiliency. Specifically, data center owners and operators are making significant investments in the resiliency of their physical infrastructure, with about 40 percent of respondents reporting increased redundancy levels at their primary data centers in the past three to five years.

New 'As-a-Service' Options Gain Favor

Cloud service use is rampant in businesses today. Many have moved to Software-as-a-Service offerings for everything, including email, collaboration, ERP, and more. Still more use scalable cloud services for compute and storage.

For IT and networking professionals, especially those responsible for hybrid and multi-cloud efforts, the attention is on infrastructure and networking offerings. For years, many enterprises have routinely used Infrastructure-as-a-Service (IaaS) for raw facilities (servers, instances, storage, interconnectivity, etc.) to run production and development environments.

Some make use of Platform-as-a-Service (PaaS) offerings, which add development tools, applications, and databases. By offering all of these things as one service, enterprises can focus on their applications. An additional benefit is that an enterprise can ensure all business units are using the same tools and applications, and things like databases are made available in such a way as to protect data and meet compliance requirements.

More recently, cloud providers have started offering what is called **Everything-as-a-Service** (EaaS). EaaS, which is often referred to as IaaS Plus, extends the traditional infrastructure into the application development space. EaaS includes all code and settings along with infrastructure and software to run an application. Both the application and its environment run together. EaaS can be used in production environments as well as for development, testing, and QA.

EaaS is well suited to today's cloud-native development

environments. An EaaS can use automation to configure servers for a specific application. And a solution might be a self-service offering that integrates with normal DevOps workflows, tools, and methodologies. That last capability is particularly important today, given the way applications are developed and maintained so rapidly and by distributed teams. Many EaaS offerings also integrate into existing DevOps ecosystems. With such capabilities, an EaaS is well-suited in meeting the needs of modern application development that is driven by fast-changing business requirements.

New Business Models Need New Networking Options

The world is transforming into a service-based economy. In fact, two-thirds of the global GDP (and 77% of the US GDP) is now service-based. Much of this growth comes from a shift from selling products to selling products-as-a-service. Things that were purchased from traditional manufacturers (lighting fixtures, hospital beds, jet engines, etc.) are now sold as services. A customer pays a monthly service charge, and the "as-a-service" enterprise installs and maintains the equipment.

In the old economy, the enterprise network only had to extend to where product sales were made. In an as-a-Service model, however, the network now has to extend all the way to where equipment is in use – the customer's site.

One service gaining interest is Network-as-a-Service (NaaS), which provides networking hardware, software, and maintenance services as an operational expense instead of the traditional upfront expense. Like other cloud services, NaaS is managed by the service provider and delivered for a fixed fee.

NaaS has emerged as a critical offering due to the embracement of hybrid and multi-cloud strategies. NaaS is the logical outcome of many business processes moving to the cloud. For the vast majority of enterprises, no other model really makes sense. Most enterprises do not have the specialized skillset needed to build and operate their own private networks to connect data centers, private clouds, and multiple public clouds.

Bring everything together

Along similar lines, there is integration Platform-as-a-Service (iPaas). iPaaS is a cloud-based solution that simplifies application integration across on-premises and cloud environments. It is used by enterprises to accelerate innovation and lower integration and operations costs.

With these benefits, it is no surprise that iPaaS offerings have become and will remain very popular. The iPaaS market is estimated to be worth $23.7 billion by 2028, increasing at a CAGR of 37.2% from 2022 to 2028, according to Verified Market Research. And according to Gartner, iPaaS has been one of the fastest-growing

enterprise software market segments since they began tracking it years ago.

Why the great interest and booming future market? As enterprises deepen their cloud dependency, iPaaS becomes integral to nearly every business model. It acts as a conduit for communication between multiple systems, allowing for integration and data sharing. Thus, an iPaaS service connects otherwise disjointed systems to deliver a unified solution.

Marrying Networking and Security

Businesses today face new security challenges that were not imaginable a few years ago. More applications and services are accessed via cloud offerings. Workers and applications are widely distributed, meaning there is no hard edge to the enterprise network. And there is a need to integrate a large number of devices (smart sensors, wearables, IoT devices, and more) that the business has no control over.

So, cybersecurity is a growing concern. In the Network Computing The 2022 State of the Network Management Report, security was the top concern of the 300 information technology professionals surveyed. In fact, 81 percent of those surveyed were concerned or very concerned about cyberattacks. And half of the respondents rated network security as one of their most pressing network management priorities for the next 12 to 24 months, making it the top priority.

As attacks evolve and use cases change, many enterprises are looking for alternatives to traditional security approaches. In particular, there is increasing demand for modern security approaches that converge networking and security. This is driving great interest in technologies, including SD-WAN and Secure Access Service Edge (SASE).

SD-WANs are widely used for enterprise connectivity. They offer cost savings, performance, and safety by giving users easily manageable links to branch offices and other remote groups for data, voice, or video communication. Unfortunately, without the assistance of third-party applications, SD-WANs often lack important security attributes, such as VPN protection and web gateways. With enterprises wanting networking and security bundled together, many SD-WAN providers are now partnering with security solutions providers.

In contrast, SASE is a framework that brings together networking and security services into a unified solution. It is designed to provide strong security from edge-to-edge, delivered as a service to the data center, remote offices, roaming users, and more.

SASE, as originally framed by Gartner, brings together two elements, one related to connectivity and one related to security. From the connectivity side, a SASE service might offer features to help people and sites connect and do so efficiently. Specifically, an offering might include a

software-defined WAN (SD-WAN), content delivery network, WAN optimization, and more features, all delivered in the form of a network-as-a-service offering.

From the security side of an offering, a SASE service might offer network security features such as a cloud access security broker (CASB), web application and API protection as a service (WAAPaaS), domain name system (DNS) services, cloud secure web gateway (SWG) elements, and support for zero-touch network access (ZTNA) and virtual private networking (VPN).

SASE revamps network security in somewhat the same way that software-defined networking (SDN) is impacting network infrastructures. Both take advantage of virtualization networking, powerful low-cost cloud resources, and a new generation of network services. SASE adoption is also being fueled by the arrival of increasingly complex security challenges (e.g., the ever-evolving cyber threat landscape), as well as the general increased use of managed services.

More Clouds, More Complexity

As hybrid and multi-cloud infrastructures become more common, networking infrastructures are becoming more complex. They typically are comprised of on-premises and multiple cloud elements. IT managers and security teams use many disparate tools to monitor conditions. Many of the tools are siloed and generate vast amounts of logs, traces, and alerts.

Unfortunately, businesses are often overwhelmed by this flood of data. Making matters worse, much of the data is hard to assimilate, making it harder to analyze the information and spot performance or security problems in the making or ones underway.

The challenge is that IT managers, networking professionals, and security teams must correlate and unify data across multiple products from different vendors, many of which use proprietary formats. So, instead of focusing primarily on detecting and responding to performance, availability, or security events, a staff spends most of its time normalizing this data as a prerequisite to understanding and responding to threats and incidents.

What it comes down to is that traditional approaches that rely solely on logs or metrics do not tell a company why something happened or when it might happen again. They do not provide logical steps to fix an issue or prevent it in the first place.

Enter modern monitoring and observability solutions. Modern monitoring and observability solutions give enterprises a chance to react more quickly to threats, bottlenecks, and disruptions. They provide context for events.

Advanced monitoring and observability are even more important in enterprises where distributed systems can make collaboration truly monstrous to attain.

They provide vital clues to the health of the entire system, continuously alerting and documenting "unknown unknowns" or problems that arise because of the system's complexity.

The use of cloud-based resources (applications, compute power, infrastructure, and more) makes network management more challenging. Visibility gaps in network monitoring and alerting tools arise with networks now stretching into third-party managed infrastructure-as-a-service (IaaS) clouds and apps/data moving into platform-as-a-service (PaaS) and SaaS environments.

So, even more monitoring and observability capabilities are needed. That is why the industry is undergoing a shift away from separate network, application, and device monitoring and observability tools to a more inclusive approach that makes use of artificial intelligence (AI) for IT operations (AIOps).

AIOps platforms combine traditional monitoring and observability tools with streaming telemetry. They analyze all of the data to spot anomalies, derive insights, and make predictive assessments of the state of the systems. They analyze each data source and correlate multiple anomalies to automate the identification of problems while also providing detailed information about the potential source of any problem. Thus, if a modern monitoring and observability platform, enabled by AI, is properly implemented, it provides more visibility into potential problems and eliminates many manual troubleshooting and remediation tasks.

A final word

A successful cloud strategy can deliver important benefits to an enterprise. It can enable IT to provide self-service access to infrastructure, the ability to leverage innovations readily available in public clouds, and lower operating costs by paying for resources and services only as they are consumed.

In the year to come, some of the biggest trends that will dictate cloud success are the continued use of hybrid and multi-cloud implementations, the use of newer as-a-Service offerings designed specifically for cloud-first enterprises, and the adoption of modern monitoring and observability solutions that make use of AI.

About the Author: Salvatore Salamone is the managing editor of Network Computing. He has worked as a writer and editor covering business, technology, and science. He has written three business technology books and served as an editor at IT industry publications including Network World, Byte, Bio-IT World, Data Communications, LAN Times, and InternetWeek.

INFOBLOX PERSPECTIVE

The Future of Cloud

Modernizing core network services is a necessary and vital part of cloud migration. DNS, DHCP, and IPAM, collectively known as DDI, offer foundational network services providing visibility, automation, and control to NetOps and SecOps professionals. They allow organizations to accelerate cloud adoption and improve business agility more easily.

Businesses looking to modernize IT and possibly gain a competitive edge are adopting new trends and technologies at a scale never seen before. Adopting public cloud is among the most accepted technology transitions for organizations looking to ensure growth. It is also accepted that this transition can be complex and comes with a fair amount of risk. This is because adopting public cloud services forces organizations to evolve from a centralized business model to a distributed one. With this distributed model, IT operations teams often lack visibility into assets deployed on-premise and cloud, want more complete process automation between data center and cloud, and seek consistent policy controls across hybrid deployments. On-premises to cloud migration complexities and lack of skilled personnel further compound the problem. Modernizing IT infrastructure becomes crucial in addressing these challenges.

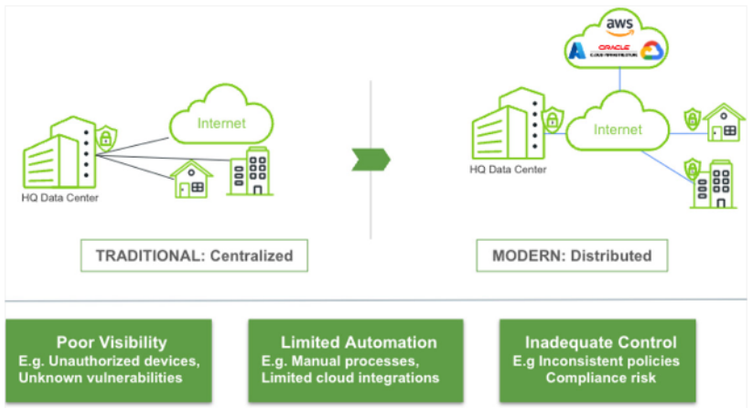

Figure 1: Public cloud services forces organizations to implement a distributed model

A Rock-Solid Foundation Addresses These Challenges

Public cloud adoption needs to be grounded on a solid foundation, a solid foundation of core network services that provide comprehensive visibility across networked resources. One that simplifies adoption through pervasive automation in your distributed environment. And last but not least, one that helps you enforce consistent policy controls and mitigate risks.

Core Network Services Provide This Foundation

Core network services, which include DNS, DHCP, and IP address management, also known as DDI, make all network and cloud interactions possible. DNS is a naming system for resources and services on the Internet. DHCP automatically assigns IP addresses and other communication parameters to devices connected to the network. IPAM is a methodology for planning and managing the assignment and use of IP addresses and related resources of a computer network.

Why Infoblox

Your core network services have to be reliable and provide a broad swath of integrations with the public cloud

ecosystem. Infoblox is the market leader in DNS, DHCP, and IPAM. With Infoblox's fully-featured flagship NIOS, rock-solid reliability comes from 20 years of leadership and innovation. Infoblox has the broadest ecosystem integrations in the industry across cloud providers and cloud orchestration tools, and an array of virtual appliances, all secure and hardened to address your high availability and resiliency requirements.

As the leader in core network services, Infoblox has innovated further and introduced a cloud-native platform that puts your digital transformation on a firm footing. Our BloxOne platform makes it possible for organizations to consume a broad range of DDI capabilities in the form of modular, scalable cloud-managed services and applications.

BloxOne DDI ensures easy deployment in distributed locations so remote users can access their cloud-based applications from the closest entry point in the cloud, reducing latency and improving application performance.

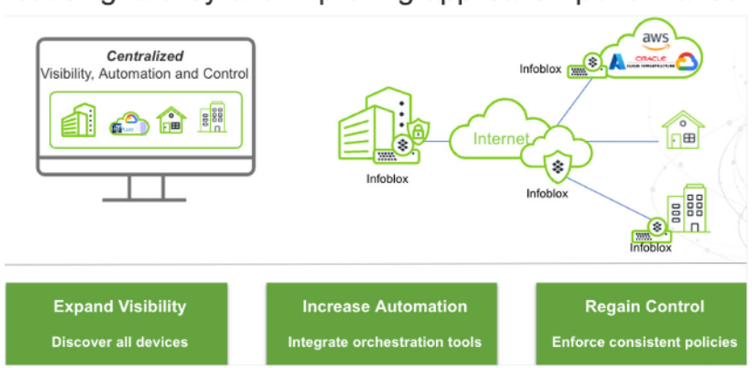

Figure 2: Benefits of modernizing your core network services

Your DDI infrastructure is no longer constrained by factory-delivered hardware or by the need to add new appliances for new functionality. Instead, you can quickly expand services as your needs dictate. BloxOne solutions rapidly scale to thousands of virtual appliances, all centrally managed through the cloud. In addition, updates and grades are automatic providing administrative efficiency and ease of use that comes with cloud-managed solutions.

Conclusion

Modernizing core network services is a necessary and vital part of cloud migration. DNS, DHCP, and IPAM, collectively known as DDI, offer foundational network services providing visibility, automation, and control to NetOps and SecOps professionals. It is a single source of truth for automating asset management and establishing common access policies. Simply put, it allows organizations to accelerate cloud adoption and improve business agility more easily.

About the Author: PG Menon is Senior Director of Product Marketing at Infoblox. He was most recently Senior Director, at Aruba Networks, A Hewlett Packard Company where he was product marketing lead for its campus switching product line. Before Aruba, PG was senior director of technology strategy at Brocade Communications where he led several initiatives such as SDN and DevOps for cloud and datacenter markets. Prior to Brocade, PG was a founding executive in a number of startups. PG Menon has an MS EE from Rensselaer Polytechnic Institute and BS in EE from IIT, Varanasi, India.

Just in Time Infrastructure: Infrastructure at the Speed of Business

IT must deliver infrastructure in a timely, just in time, manner these days to keep pace with the speed of modern business. To achieve this, enterprises are turning to a variety of infrastructure-focused as-a-Service offerings.

Enterprises are under increased pressure to deliver new digital products and services faster than ever before to meet internal user and customer demands and expectations. Much recent attention has focused on accelerating development and deployment cycles, but those efforts are in vain if the infrastructure is not ready or available to support those efforts.

Gartner cited this issue as one of its top trends impacting infrastructure and operations this year. It noted: "the increasing speed of technology change has created tremendous opportunities (and pressure) for IT leaders to align with business priorities."

The expected shorter timelines for development and deployment are feeding into a trend Gartner calls just-in-time infrastructure, which emphasizes deploying infrastructure as quickly as possible. Gartner and others are starting to see SOWs (statements of work) and purchase agreements for infrastructure and services that list expected delivery time next to each line item.

This aligns with the demands on IT of increasing responsiveness to business needs. The issue has become more pronounced due to pandemic-related disruptions.

A recently released "2022 technology industry outlook" from Deloitte noted the lingering impact of the pandemic in accelerating the pace of business. When the pandemic began two years ago, it forced many organizations into the future, rapidly accelerating digital transformation. Supporting such transformation and the speed at which it needs to be undertaken requires what Deloitte says is a need to take cloud to the next level.

"As more companies embrace cloud and service-based IT to drive innovation and transformation, everything-as-a-service will be critical to digital transformation, particularly for new solutions and business models," according to the report.

Making Infrastructure Available at the Speed of Business

There are several ways IT deliver infrastructure in a timely manner to meet modern business speed requirements.

Traditionally, enterprises have turned to cloud services, including **Infrastructure-as-a-Service (IaaS)** and **Platform-as-a-Service (PaaS)**. IaaS provides the raw facilities (servers, instances, storage, interconnectivity, etc.) to run development and operations environments. But a PaaS adds tools, applications, and databases. By offering all of these things as one service, an enterprise can focus on its applications.

Increasingly, other options are being explored. One is **Network-as-a-Service (NaaS)**. NaaS is the logical outcome of many business processes moving to the cloud. It offers a turnkey solution that typically includes equipment, software, orchestration, and management at a fixed recurring cost, with services tailored to meet the user's specific business requirements.

Another relatively new entrant to the market is **Everything-as-a-Service (EaaS)**. In contrast to PaaS. EaaS, which is often referred to as IaaS Plus, extends the traditional infrastructure into the application development space. EaaS includes all code and settings along with infrastructure and software to run an application. Both the application and its environment run together. EaaS can be used in production environments as well as for development.

One of the appealing aspects of EaaS is that such services typically let a business give developers and ops teams a choice in how they access the services. That might include access via a web portal, command-line interface, or directly through a developer's CI/CD tools. That capability is particularly important today, given the way applications are developed and maintained.

And along the lines of what's old is new again, some enterprises are re-discovering composable infrastructure. Composable infrastructure makes use of a pool of physical or virtual infrastructure that can be provisioned on demand as required. A defined pool of infrastructure can contain compute, network, and storage resources.

Composable infrastructure was typically considered for on-premises environments. But now, there is interest in extending its benefits to cloud and hybrid environments. To do that requires a high degree of process and automation maturity, coupled with a firm understanding of resource requirements.

The common theme across all of these approaches is that they are designed to help enterprises move quickly when opportunities arise, or new applications or services are needed.

About the Author: Salvatore Salamone is the managing editor of Network Computing. He has worked as a writer and editor covering business, technology, and science. He has written three business technology books and served as an editor at IT industry publications including Network World, Byte, Bio-IT World, Data Communications, LAN Times, and InternetWeek.

What to Expect from Network-as-a-Service (NaaS) Technology

Network-as-a-Service (NaaS) is gaining momentum. Since NaaS is easily accessible from anywhere on any device, it's expected to become indispensable in remote/hybrid work models in the years ahead. Is your organization going to jump onboard?

Network as a Service (NaaS) technology provides networking hardware, software, and operational/maintenance services as an operational expense instead of the traditional upfront expense. Like other cloud services, NaaS is managed by the service provider and delivered for a fixed fee.

NaaS is the logical outcome of many business processes moving to the cloud, observed Jacob Martin, a software engineer at IT infrastructure automation company Spacelift. NaaS replaces VPNs, MLPS connections, legacy network configurations, and several types of on-premises hardware, such as load balancers and firewall devices. "It has had a significant influence on enterprise networking architecture," he noted.

In essence, NaaS is a network subscription service. "Enterprise customers often think of NaaS as being similar to other cloud-based services, but in reality, NaaS is far less standardized than SaaS, and the decisions on how to use NaaS are far more complex," explained Nick Nagy, principal consultant with global technology research and advisory firm ISG. The added complexity is largely driven by the need for on-premises equipment. "Enterprises have to decide how to employ various elements of NaaS to meet their business objectives, and this often comes down to an OpEx versus CapEx decision, influenced by tax implications."

Multiple Benefits

For organizations that find a subscription approach to enterprise networking appealing, NaaS offers a turnkey solution that typically includes equipment, software, orchestration, and management at a fixed recurring cost, with services tailored to meet the adopter's specific business requirements. "This enables the enterprise customer to smooth out the financial and operating lumps that come with ongoing technology refreshes," Nagy said.

For the vast majority of enterprises, no other model really makes sense, stated Robert Blumofe, executive vice president and CTO of the content delivery network, cybersecurity, and cloud service firm Akamai Technologies. "How many enterprises really have the specialized skillset needed to build and operate their own networks?" he asked. For many organizations, NaaS is by far the better option, Blumofe added. "The scope for traditional private networking services is shrinking, and the scope for a new access-based model is growing."

Blumofe observed that enterprises have traditionally used private networks to interconnect their offices and data centers. "Going forward, this type of private network really only makes sense on the backend as a way to connect private and public clouds," he said. "For this use case, NaaS is really a great solution."

Office buildings, on the other hand, should be treated like private coffee shops with high-quality Wi-Fi connecting "customers" directly to the Internet, Blumofe noted. "After all, what really is the difference between working from home, or on the road, or in the office?" he asked. Workers, wherever they are, need access to their necessary applications. "This new form [of technology] is essentially an overlay network that provides zero-trust application access as a service."

NaaS's flexibility and scalability are unmatched, Martin said. "It tailors to your needs because changes are made in the software instead of the hardware, and such customizations are actioned on demand," he explained.

Potential Pitfalls

NaaS disadvantages include a lack of vendor flexibility in terms of both portability and long-term commitments. "Additionally, there can be issues with legacy systems, such as software or hardware that isn't compatible with the solution," Nagy warned.

Martin agreed, noting that most NaaS compatibility issues are related to infrastructure, such as old hardware or on-premises applications still in use. "Coincidentally, some essential processes or applications operate on on-premise data centers instead of the cloud in many enterprises," he said. "Thus, it could be a bit challenging to migrate to the NaaS model, although there are services that can certainly make it easier."

Because a NaaS connection is typically established using "best effort" public broadband, the service is only available in places where broadband Internet connections are available, cautioned Ajay Pandya, director of product management at cloud networking platform provider Masergy. "Performance can be limited to the speed of the last-mile connectivity," he said.

Potential loss of control is an issue for some potential adopters. "When outsourcing their network services, some clients have concerns regarding service responsiveness and their ability to control their network resources," Pandya said. "In response, co-managed NaaS solutions have arrived, allowing clients to share the work of managing their network, bandwidth, and firewall policies, for instance."

Nagy added that some large multinational enterprises may find NaaS to be a poor fit due to tax and accounting issues.

Previous Next

Future Outlook

Since NAAS is easily accessible from anywhere on any device, it's expected to become indispensable in remote/hybrid work models in the years ahead. "You may work from anywhere as long as you have Internet access and log-in credentials," Martin noted. "The provider offers both network and security services, which further strengthens the integration between the network and network security."

The best way to get started with NaaS, Nagy said, is to define the service portfolio scope and business objectives. "Then determine the preferred financial model, meaning CAPEX versus OPEX."

About the Author: A veteran technology journalist, John Edwards has written for a wide range of publications, including the New York Times, Washington Post, CFO Magazine, CIO Magazine, InformationWeek, Defense Systems, Defense News/C4ISR&N, IEEE Signal Processing Magazine, IEEE Computer, The Economist Intelligence Unit, Law Technology News, Network World, Computerworld and Robotics Business Review. He is also the author of several books on business-technology topics. A New York native, John now lives and works in Gilbert, Arizona.

How to Address Cloud Misconfiguration-Caused Breaches

Complexity is on the rise in most enterprise cloud environments. While eliminating misconfigurations may be nigh impossible, IT must try to limit them and the potential damage they may cause.

When preparing large-scale hacks and exploits, bad actors often rely upon human error, naivety, and carelessness - more than they do their own skill and cunning. The truth is that most companies have all the right security tools and resources to address most vulnerabilities in their security.

However, we've found that the unpredictable human element is the most difficult to manage. For instance, user misconfigurations remain the greatest threat to cloud security. However, there are ways you can deal with this threat. This guide will show you how to remediate and potentially mitigate cloud misconfiguration-based breaches as efficiently as possible.

Understanding Cloud Misconfigurations

According to Neil MacDonald (analyst and vice president of Gartner): "Nearly all successful attacks on cloud services result from customer misconfiguration, mismanagement, and mistakes." While it may sound accusatory, it's accurate. There are not very many instances of breaches caused by vendor negligence.

A cloud misconfiguration describes any improper implementation of cloud services that may undermine performance, security, or general reliability. Malicious actors can use these vulnerabilities to exploit misconfigured infrastructure and use it to leverage and launch multi-company cyberattacks.

Causes and examples of misconfigurations include:

- Inexperienced users
- Erroneous storage access settings
- Lack of proper validation of credentials
- Lax access restriction to workloads
- Disabled logging and monitoring

Providing Ample Training and Education for Users

According to the AWS shared responsibility model, compliance and security are not the sole responsibility of the vendor or cloud security provider. Essentially, the customer plays a role as important as the provider's in protecting their data and other digital assets. However, the AWS model of share responsibility is only one example. Typically, most cloud vendors subscribe to their own protocols and ethos regarding shared responsibility.

Thus, customers must be well-trained and security conscious. Again, unlike website vulnerabilities, most (if not all) breaches in cloud security are caused by errors on the client/customer side.

We've seen how mobile workforce infrastructure migration has increased network security risks for companies. Users/workers must be informed of the latest protocols and practices.

This process may mean altering their habits and having a basic understanding of how to operate cloud, network, and/or website monitoring tools. This knowledge will help them validate configurations. Furthermore, it will allow them to detect any faults or breaches that may result from misconfigurations.

Storage Access Misconfiguration

Leaving access to cloud objects used for data storage (such as S3) and exposing them to external actors is one of the most common mistakes. Alarming, some companies have been observed to leave some of these objects open to the public.

Cybercriminals will actively scan for exposed S3 buckets or public GitHub repositories to find company secrets and credentials. Thus, ensuring that your passwords, API Keys, and admin credentials are secure and encrypted has become increasingly crucial.

Address Any Monitoring Blind Spots

Cloud is essentially the foundation of remote work. Whether you're accessing software-as-a-service products for programming or accounting, the benefits have been well documented. However, As companies and people integrate more cloud-provided services into their software stack, their security and configuration requirements change. There are a lot more moving parts to track.

Thus, it's important to ensure that monitoring and logging are turned on and applied to the correct security group configuration. It would help if you kept a track

Previous Next

record of when changes to your cloud settings were made and by whom. It will allow you to address any mistakes and refine your training for workers.

Upgrading Your Security

Another reason these misconfigurations occur is that companies fail to move from outdated security models and lack unified cloud visibility. Rapid changes to security and infrastructure may also leave users even more susceptible to making. For instance, multi-cloud environments may increase the likelihood of cloud misconfigurations occurring.

Cloud adoption is still relatively new. As such, finding security resources or programs that can keep up with the ever-evolving landscape of modern cloud services is challenging. Most traditional on-premise security controls have been translated to the cloud infrastructure.

However, they can be insufficient because certain aspects of on-premises physical security simply don't apply to cloud service security. For instance, gaining visibility across all accounts and all regions can be more difficult.

This is especially true if you have a large environment with multiple security tools for risk and compliance in different regions or departments. We suggest implementing a security service that combines artificial intelligence with network and file analysis. This solution should also provide you with dynamic logging and monitoring.

Limiting Misconfigurations

While eliminating misconfigurations may be nigh impossible (especially for large corporations with complex cloud assets), we can limit them and the potential damage they may cause. Nevertheless, ingraining a culture of security in your company is key. You can start by implementing a zero-trust environment where only the right actors can access your important cloud assets and their configuration data.

Many cloud service providers have built-in tools to address misconfigurations. They include features for logging, monitoring, access restriction, etc. Essentially, you can address some of the most common misconfiguration mistakes and prevent breaches by simply choosing a secure cloud vendor.

About the Author: Sam Bocetta is a freelance journalist specializing in U.S. diplomacy and national security, with emphases on technology trends in cyberwarfare, cyber defense, and cryptography.