InformationWeek CONNECTING THE BUSINESS TECHNOLOGY COMMUNITY

JUNE 2021

Monitoring Critical Cloud Workloads

With the proliferation of cloud computing in the IT enterprise and companies moving more mission-critical applications to the cloud, the IT organization needs to provide a level of trust to the business that those workloads are being adequately monitored for security threats. And while many companies understand that need and are making strides, there are still too many situations where the inability to monitor in real-time opens up the enterprise to damaging business results. In this special report, we will discuss how to advance your ability to monitor critical workloads as they move about the various cloud platforms in your company.

informa tech

INSIDE

ALL IMAGERY PROVIDED BY GETTY IMAGES

NEXT

Monitoring Critical Cloud Workloads: A Guide to Modernize your Cloud and Application Approach

By Bill Kleyman, EVP of Digital Solutions at Switch; Contributing Editor, InformationWeek

The concept of a "digital footprint" is a part of our everyday lives as users leverage more devices to consume productivity applications as well as those for entertainment. New requirements continue to push organizations of all shapes and sizes to invest in their capabilities to support a digital market through it all.

"Direct digital transformation investment was growing at 17.5% CAGR and expected to approach $7.4 trillion over the years 2020 to 2023 as companies build on existing strategies and investments," states Shawn Fitzgerald, IDC Analyst. "Organizations with new digital business models at their core are well-positioned to compete in the digital platform economy successfully."

Here's another interesting stat from the IDC report: Sixty five percent of organizations will aggressively modernize legacy systems with extensive new technology platform investments through 2023. This means that leaders in the business and technology space are already looking at ways to optimize their cloud workloads.

A significant part of this investment will revolve around applications, cloud computing, and ensuring the best possible performance for those resources. However, in the world of cloud computing and applications, there is a misconception related to monitoring cloud workloads and services. It's not just about performance. Security is a critical concern as well.

"Protection requirements for cloud-native applications are evolving and span virtual machines, containers, and serverless workloads in public and private clouds. Security and risk management leaders must address the unique and dynamic security requirements of hybrid cloud workloads." — Gartner

Sixty five percent of organizations will aggressively modernize legacy systems with extensive new technology platform investments through 2023. This means that leaders in the business and technology space are already looking at ways to optimize their cloud workloads.

This report will dive into some of the significant changes in our industry related to cloud computing and what you can do to ensure you have the right cloud monitoring practices in place to support your most critical workloads.

Understanding the Drivers of Change

The kinds of applications and services we are deploying into the cloud have fundamentally changed. These services are the lifeblood of our businesses and allow users to operate efficiently. In 2020, we learned just how vital cloud computing alongside the applications we deploy are to business longevity and effectiveness. More than ever before, it's these workloads that we must both monitor and secure.

According to IDC, cybersecurity has become highly complex as IT architecture rapidly evolves beyond the old paradigm of data centers, secure perimeters, and on-premises employees. The new architecture is hugely decentralized with geographically dispersed data centers, colocation facilities, multiple public clouds, edge computing, remote employees, and various endpoint devices. Thus, while enterprises now benefit from greater agility, scalability, and productivity, they are also more vulnerable to malicious actors due to an increased attack surface. To overcome this daunting challenge, executives need to understand how to secure their core, edge, and the cloud using newer security paradigms.

"New insights have shown that there is a tectonic shift of data and applications from on-premises to a multi-cloud environment, and this shift has rendered many traditional security tools ineffective," said Chris Kanthan, research manager of the Infrastructure Systems, Platforms and Technologies Group at IDC. "There is no single product to resolve this cybersecurity challenge. Instead, enterprises need a holistic strategy that comprises next-generation applications, pertinent frameworks, robust policies, cloud-specific security architecture, and comprehensive processes to secure their data."

To that extent, security best practices must evolve as well. Security for the data and applications created in the cloud, sent to the cloud, and downloaded from the cloud are almost always the responsibility of the cloud customer. Today's cloud workloads often have a shared responsibility model where some security burdens fall on you, the application's consumer, and the cloud. Protecting your cloud data and critical workloads requires visibility, control, and often a broader approach to security architecture.

Guide to Critical Workload Monitoring: A Phased Approach

The vast majority of organizations continue to invest in their cloud strategies. The beauty of the cloud is that it allows for true application and service versatility. That said,

many leaders in the space don't adopt just one type of cloud solution. According to Gartner, by 2022, about 75% of enterprise customers using cloud infrastructure as a service (IaaS) will adopt a deliberate multi-cloud strategy, up from 49% in 2017. However, this evolution won't be without its challenges.

"Multicloud; mixtures of virtual machine (VM), container, and serverless approaches; and vulnerabilities resulting from mistakes in configurations create a complexity dilemma that inhibits the market and weakens the integrity of applications," explains Frank Dickson, IDC program vice president, security and trust. "Hybrid cloud workload security vendors need to ameliorate the resulting complexity, creating multi-cloud solutions that deliver simplicity for users."

To make life easier, let's explore a core set of best practices for cloud application monitoring and security best practices that can help guide enterprises toward a more secure cloud model.

Phase 1: Creating a Critical Cloud Workload Monitoring Baseline

During the first phase, you'll establish a baseline that will help you understand the current state of your critical cloud workloads, how you're monitoring them, and where you're assuming risk. Once that's accomplished, you can build on your baseline to deliver real critical cloud workload monitoring and security solutions. Consider these steps in phase 1:

Step 1: Each workload is unique – Identify your sensitive and regulated data. The first thing you'll need to do is understand, at its core, how your workload framework will look. This means classifying data, services, and workloads based on their classification of risk. You might also need to classify critical cloud workloads based on regulations and compliance. In a data-driven world, a large area of risk revolves around data theft or data leakage. If this happens, it can result in serious regulatory penalties or loss of intellectual property. Data classification will help you categorize your data to fully assess this risk and apply proper monitoring and security solutions.

Step 2: How are your critical cloud workloads and respective data being accessed? How is it being shared? With advancements in cloud security, the good news is that sensitive and even regulated data can effectively be held securely within the cloud. However, to ensure the security of your critical workloads, you have to monitor accesses, privileges, and rights of those workloads. It's recommended that you actively assess permissions on files and folders in your cloud ecosystem. You can also use automated tools to see if any changes are being made to those workloads or data sets. Further, you can define access contexts like user roles, user location, device type, access time, and more.

Step 3: Know where shadow IT or shadow cloud is being used. Many leading organizations still suffer from cloud sprawl. This can lead to not only increased cloud costs, but it can also impact critical cloud workload security. Be sure to use your alert systems, firewalls, log management, or SIEM to uncover what cloud services are being used in your organization that you may not know about. These types of tools can help you further understand your risk profile.

Step 4: Always test and always audit configurations for infrastructure-as-a-service (IaaS) partners. Understand that cloud computing can be complicated. Your cloud and IaaS environments may contain numerous critical settings for your cloud workloads. Some of these settings, when not configured properly, can create an exploitable weakness. Be sure to constantly audit your configurations for identity and access management weaknesses. You can also audit respective network configurations, encryption standards, and access methodologies.

Step 5: Uncover malicious user behavior. Risky user behavior is a constant challenge. Ransomware and phishing

attacks are becoming more prevalent, and inadequate risk-based training for end-users can have severe consequences for your critical cloud workloads. You can leverage tools that analyze user behavior analytics (UBA). These tools look for anomalies in behavior and will help you mitigate both internal and external data loss.

Phase 2: Protect Your Critical Cloud Workloads

Working with critical cloud workloads involves understanding your cloud security and workload risk posture. Once you establish a baseline, you'll be able to apply protection services, tools, and best practices to your applications and workloads based on their respective levels of risk. Consider the following steps to get started with your baseline:

Step 1: Apply data and critical workload protection policies. In phase 1, we recommended you classify your essential workloads of cloud and data sets. Once that's been accomplished, you're able to assign governing policies controlling what data can be stored in the cloud and how it traverses multi-cloud ecosystems. From there, based on classification, your tools should also be able to quarantine or remove sensitive data found in repositories that shouldn't contain either that data or workload. User training can also help your organization ensure that wrong application or data sets don't end up outside of where it's supposed to reside.

Step 2: Own the keys to your kingdom and encrypt your data. You'll have a few options here. When working with critical cloud workloads, it's essential to know where your encryption keys are being held and who has access. Remember, the cloud service provider will still have access to your encryption keys if you use their services. If this is a concern, encrypt your critical workloads and data using your keys. The significance here is that users can still work with the data without interruption, and you can still have the critical workloads reside in the cloud.

Step 3: Limit how data is being shared. When data hits the cloud, it's essential to enforce access control policies across all of your services and critical workloads. You can start with easy tasks like setting users or groups to viewer- or editor-access only. You can also granularly manage what information can be shared externally.

Step 4: Unmanaged devices should have limited (if any) access to data and critical cloud workloads. The beauty of the cloud is that it gives users access to critical workloads from almost anywhere they can be productive. However, this does not mean that unmanaged devices like a personal phone should be creating a blind spot for security. Manage critical cloud workloads by controlling downloads to unmanaged devices. Further, you can require device security verification before any data or workload is accessed.

Step 5: If you're working with the cloud, be sure to apply advanced malware protection to infrastructure-as-a-service (IaaS) models. We discussed shared-responsibility cloud models earlier. When working with IaaS cloud models, you will share the security responsibility of your operating systems, applications, services, development platforms, network traffic, and more. Numerous critical cloud workload solutions can be applied to ensure that your slice of security remains persistent. For example, monitoring for anomalous behavior, data leaks, and even malware can improve your security postures. Further, new critical cloud workload monitoring and security solutions allow you to deploy machine-learning-based protection for general-purpose workloads and even data repositories.

Phase 3: Responding to Critical Cloud Workload Issues

No critical cloud workload monitoring will ever be 100% effective. As the workloads in your cloud are accessed, there may be incidents that require a review or that trigger an automated response. If this happens, consider these steps:

Step 1: Higher-risk workloads may require additional verification. Even though a user might have elevated privileges, they might be accessing a high-risk critical cloud workload from a new device. If this happens, leverage tools that will, for example, automatically require two-factor authentication to prove the identity and the validity of the device.

Step 2: Cloud architectures are not set in stone. Adjust cloud access as new data and services are delivered. Although it can be challenging to predict every single cloud service being accessed, you can automatically update web access policies. For example, you can leverage intelligent services like web gateways or gateway monitoring tools to better understand a cloud service profile. From there, these services can block access or present a warning message. This can be accomplished by integrating a cloud risk database and critical workload monitoring tools with your physical security architecture (e.g., firewalls and web gateways).

Step 3: Removing malicious content, like malware, from your cloud services. Scanning your storage repositories – both onsite and in the cloud – is an absolute must. Malware may compromise a shared folder that syncs automatically with a cloud storage service. This can allow for the replication of malware in the cloud without user action. Be sure to scan your files and cloud data repositories with anti-malware solutions to avoid ransomware or data leakage.

When it comes to critical cloud workloads and security, nothing should be set in stone. This means that you need to evolve and adapt with your services constantly. Challenge your cloud providers and application developers to stay on top of security and adjust your policies accordingly.

What Happens When You Get It Right?

First, there will be significant business benefits to ensuring that your critical workloads are secure and properly monitored. Second, you'll see that good cloud monitoring and security architecture will help your people as well. "When an organization adopts true cloud, development, and application security practices, you'll start to see noticeable change within the code, production, and even performance of applications," stated Adam Auerbach, vice president and co-head of DevTestSecOps Practice at EPAM. "Operations teams will move from service providers to real enablers. This means spending more time on critical things like automation to enable developers to have more control over standing up new environments and promoting code."

As a final note, it's also essential to train your people to improve their security posture. You could have the best tools

in place and still have manual access with critical workload management. Worse yet is when organizations focus too much on tools and not at all on culture. “Implementing tools and some level of automation is the easy part,” said Auerbach. “Getting the company culture changed to support a new way of working, blending of roles, and having time for innovation, on the other hand, is going to take a lot of time and effort. But it’s worth it. It’s key to figure out what those issues are and how to solve them; this needs to be flushed out first. This way, you unify culture to use your development, cloud, monitoring, and security tools properly.”

Final Thoughts

Working with cloud computing has been an eye-opening experience for many organizations. For many, cloud technologies have improved time to market, lowered operational and capital expenditures, and provided organizations with the ability to adjust provisioning to dynamically meet changing needs globally.

However, the needs and goals of each organization and industry differ, making it impossible to adopt a one-size-fits-all cloud strategy—or even to adopt the same strategy for each critical cloud workload within an organization. Understanding your workload attributes (performance, security, integration, and data volume) is vital in making cloud deployment, monitoring, and security decisions. It is essential to consider the cumulative impact of these attributes on your critical workloads and how you utilize cloud computing.

Moving forward, cloud proliferation will only continue to expand. Leaders in the technology space will need to take a reflective approach to deploying, managing, monitoring, and securing their most critical cloud workloads. What are you doing well? Where can you improve? Critical cloud workload management is never a “set it and forget it” model. To stay ahead of the malicious actors that threaten your critical cloud workloads, it’ll be essential to think differently and apply best practices, contextually, to your cloud workloads.

About the Author: *Bill Kleyman brings more than 15 years of experience to his role as Executive Vice President of Digital Solutions at Switch. Using the latest innovations, such as AI, machine learning, data center design, DevOps, cloud and advanced technologies, he delivers solutions to customers that help them achieve their business goals and remain competitive in their market. He was ranked #16 globally in the Onalytica study that reviewed the top 100 most influential individuals in the cloud landscape; and #4 in another Onalytica study that reviewed the industry’s top Data Security Experts.*

Ways to Put a Lid on Cloud Waste

It's easy to underuse and overspend on cloud assets. The good news is that there are tools and practices that IT can apply to better manage cloud assets and tamp down the waste.

By Mary E. Shacklett, Technology Commentator and President of Transworld Data

In 2020, annual company cloud waste was estimated at $17 billion, largely lost on idle and excess resources. This was according to Jay Chapel, CEO and co-founder of ParkMyCloud. Chapel should know. His company makes a business out of helping corporate IT departments identify wasted cloud assets and excess spend. "For example, one healthcare IT provider was found to be wasting up to $5.24 million annually on their cloud spend — an average of more than $1,000 per resource per year," he said.

Cloud waste is also why it might be a good time to bring in a cloud auditor to evaluate usage and spend. In this way, overages in cloud spend can be identified and eliminated. Alternately, IT could perform its own internal audit.

Cloud Sprawl

There are many places to look for cloud waste. The first is over-deployment of cloud resources that can result in "cloud sprawl."

Cloud sprawl is most likely to occur when cloud resources get provisioned from multiple points within an enterprise without centralized coordination. This results in departmental "cloud silos" of activity since there is no central control point for cloud budgeting, tracking or usage.

Many companies attempt to tackle this problem of cloud silos by placing IT in the role of a centralized cloud management agent. Companies might even invest in an IT asset management system that is supposed to track and monitor every IT asset in the enterprise, so the enterprise knows how much it has — and also how much it is spending on that IT.

Unfortunately, even IT asset tracking systems have their limits. For instance, there might be a standalone cloud-based application that users access through an internet portal, but that doesn't present itself on the networks that IT tracks. HR payroll, benefits and insurance systems that are signed into through internet portals are examples of this. In these cases, the cloud usage may not be visible — although the costs associated with them certainly will be

A detailed audit of all enterprise cloud resources can uncover situations like this, because the auditor not only looks at assets tracked by an asset management system — he or she also interviews individual user departments about the applications and systems they use. This is how the hidden cloud use gets uncovered.

Poor Cloud Utilization

A second source of cloud waste occurs when cloud resources aren't optimally put to work. IT application testing in the cloud is a prime example.

The virtual operating systems that are deployed in the cloud for application testing are paid for by the hour, minute or second. This is beneficial for developers during testing because the spend is less than if they had to deploy virtual OSs in their own data centers, where hardware and software is capitalized and expended for over years. However, cloud

testing becomes a significant cost drain when the application developer completes testing and forgets to de-allocate the test OS that is now idle, and that continues to be charged for. When this happens, the test OS becomes a wasting asset.

Cloud resource waste can also occur when processing and storage are over-allocated. In an on-premises data center, over-allocation is a common practice, because you already own (or lease) the resource and are paying for it no matter what you use. Therefore, you have the luxury of provisioning more processing in case there are spikes or provisioning more storage because you may need it. When this practice of overestimation spills over onto the cloud, the risk is that you might be allocating (and paying for) more storage or processing than you use since there is no absolute "fixed pricing" for the cloud in most cases.

Many cloud vendors have tried to address this problem of over-allocation because they don't want their clients unpleasantly surprised with unexpected costs. Vendors do it by offering on-demand processing and storage that increments and decrements based upon demand. In this way, IT only pays for what it consumes.

Understanding What Cloud Costs

Cloud purchase agreements and bills can be extremely complex, and the challenge of deciphering them is compounded when multiple cloud providers are involved. For example, a virtual operating system might be called an "instance" or a "virtual machine," depending upon which cloud you're using. Another issue for companies is exceeding the processing and usage thresholds they signed up for. At certain thresholds, new (and more expensive) pricing kicks in. Pricing can also vary depending on what geographies you are operating in. All of these issues are explained in the fine print of cloud vendor contracts, but when the fine print isn't read and higher-than-expected bills come in, companies get surprised.

To help, cloud providers have tried to assist clients in understanding how cloud costs are computed so the element of unpleasant surprise can be eliminated. They have done this by providing tools that can project budget costs based upon forecasts that IT provides — but the tools are only as good as the data that is plugged into them.

Final Remarks

For its 2021 State of the Cloud Report, Flexera, which sells computer management software, conducted a survey of 750 IT professionals. Survey respondents said that they were wasting an average of 30% of their cloud spend. Thirty-six percent of respondents said their companies were spending more than $12 million annually on the cloud, and another 32% said that their cloud spend was running between $2.4 and $12 million annually.

The "spend wasters" were idle or underutilized resources that remained deployed in the cloud and were not shut down after use; an inability of companies to understand how cloud providers were charging for services and resources; and internal problems in companies because cloud services were being subscribed to from every corner of the organization with little centralized coordination.

The good news is that there are tools and practices available that IT can use to better manage cloud assets and tamp down waste. If these tools and practices are implemented, there is opportunity to eliminate what many believe is a 30% cloud overspend. Think about the other IT projects and initiatives that could be funded!

About the Author: *Mary E. Shacklett is an internationally recognized technology commentator and President of Transworld Data, a marketing and technology services firm. Prior to founding her own company, she was Vice President of Product Research and Software Development for Summit Information Systems, a computer software company; and Vice President of Strategic Planning and Technology at FSI International, a multinational manufacturer in the semiconductor industry.*

What Will Be the Next New Normal in Cloud Software Security?

Accelerated moves to the cloud made sense at the height of the pandemic — organizations may face different concerns in the future.

By Joao-Pierre S. Ruth, Senior Writer, InformationWeek

Organizations that accelerated their adoption of cloud native apps, SaaS, and other cloud-driven resources to cope with the pandemic may have to weigh other security matters as potential "new normal" operations take shape. Though many enterprises continue to make the most of remote operations, hybrid workplaces might be on the horizon for some. Experts from cybersecurity company Snyk and SaaS management platform BetterCloud see new scenarios in security emerging for cloud resources in a post-pandemic world.

The swift move to remote operations and work-from-home situations naturally led to fresh concerns about endpoint and network security, says Guy Podjarny, CEO and co-founder of Snyk. His company recently issued a report on the State of Cloud Native Application Security, exploring how cloud-native adoption affects defenses against threats. As more operations were pushed remote and to the cloud, security had to discern between authorized personnel who needed access from outside the office versus actual threats from bad actors.

Decentralization was already underway at many enterprises before COVID-19, though that trend may have been further catalyzed by the response to the pandemic. "Organizations are becoming more agile and the thinking that you can know everything that's going on hasn't been true for a long while," Podjarny says. "The pandemic has forced us to look in the mirror and see that we don't have line of sight into everything that's going on."

This led to distribution of security controls, he says, to allow for more autonomous usage by independent teams who are governed in an asynchronous manner. “That means investing more in security training and education,” Podjarny says.

A need for a security-based version of digital transformation surfaced, he says, with more automated tools that work at scale, offering insight on distributed activities. Podjarny says he expects most security needs that emerged amid the pandemic will remain after businesses can reopen more fully. “The return to the office will be partial,” he says, expecting some members of teams to not be onsite. This may be for personal, work-life needs, or organizations want to take advantage of less office space, Podjarny says.

That could lead to some issues, however, with the governance of decentralized activities and related security controls. “People don’t feel they have the tools to understand what’s going on,” he says. The net changes that organizations continue to make in response to the pandemic, and what may come after, have been largely positive, Podjarny says. “It moves us towards security models that scale better and adapted the SaaS, remote working reality.”

The rush to cloud-based applications such as SaaS and platform-as-a-service at the onset of the pandemic brought on some recognition of the necessity to offer ways to maintain operations under quarantine guidelines. “Employees were just trying to get the job done,” says Jim Brennan, chief product officer with BetterCloud. Spinning up such technologies, he says, enabled staff to meet those goals. That compares with the past where such “shadow IT” actions might have been regarded as a threat to the business. “We heard from a lot of CIOs where it really changed their thinking,” Brennan says, which led to efforts to facilitate the availability of such resources to support employees.

Meeting those needs at scale, however, created a new challenge. “How do I successfully onboard a new application for 100 employees? One thousand employees? How do I do that for 50 new applications? One hundred new applications?” Brennan says many CIOs and chief security officers have sought greater visibility into the cloud applications that have been spun up within their organizations and how they are being used. BetterCloud produced a brief recently on the State of SaaS, which looks at SaaS file security exposure.

Automation is being put to work, Brennan says, to improve visibility into those applications. This is part of the emerging landscape that even sees some organizations decide that the concept of shadow IT — the use of technology without direct approval — is a misnomer. “A CIO told me they don’t believe in ‘shadow IT,’” he says. In effect, the CIO regarded all IT, authorized or not, as a means to get work done.

Demand for high usability and flexibility in technology in the new landscape will also present new challenges for chief security officers, Brennan says, as they are called upon to facilitate that. “They’re still going to be held accountable for protecting the business,” he says. “I would suspect there’s going to be a focus on different type of security control.” This might include a move toward awareness and remediation to how and what technology employees deploy versus blocking or stopping approaches to security, Brennan says. “We may see more trends move towards that because that’s the only way you can accommodate this increased demand for usability.”

About the Author: ***Joao-Pierre S. Ruth has spent his career immersed in business and technology journalism first covering local industries in New Jersey, later as the New York editor for Xconomy delving into the city’s tech startup community, and then as a freelancer for such outlets as TheStreet, Investopedia, and Street Fight. Joao-Pierre earned his bachelor’s in English from Rutgers University.***

The Cloud Comes of Age Amid Unprecedented Change

The cloud is set to help businesses lead by outmaneuvering uncertainty. It's now imperative that they lean into the cloud and catch up with leaders before the gap becomes too large.

By Karthik Narain, Global Lead, Accenture Cloud First

During the pandemic, the cloud has emerged as the fastest and most resilient method to keep businesses and communities running. From working and attending school remotely, to shopping online and interacting with our health provider, cloud services have enabled it all.

As a result of COVID-19, cloud adoption has increased dramatically. Accenture research found that cloud spending in the first quarter of 2020 was nearly triple that of the previous year. According to Gartner, by November 2020, 70% of companies using cloud had plans to increase spending due to the disruption. Cloud spending as a percentage of the global enterprise IT market will increase from 9.1% in 2020 to 14.2% in 2024. As the cloud becomes an essential part of the enterprise IT estate, we're seeing the long-promised transformational benefits start to materialize. It now seems that even the most optimistic of the cloud advocate's predictions are coming true. The cloud isn't simply making business processes cheaper or more efficient — it's changing how we work, live, and interact with the society.

In fact, cloud was a pervasive theme across Accenture's Technology Vision 2021 report, serving as a key enabler for each of the five trends that we think businesses will need to address over the next three years.

1. Tapping Into the Cloud To Differentiate

Just look at how businesses compete. The influx of cloud technologies during the pandemic has underlined that the technology stack is a core mode of differentiation. Industry competition is now frequently a battle between technology stacks, and the decisions leaders make around their cloud foundation, cloud services and cloud-based AI and edge applications will define their success.

Look at manufacturing, where companies are using predictive analytics and robotics to inch ever closer to delivering highly customized on-demand products. The pandemic has forced even the most complex supply chain operations from manufacturers to operate at the whim of changing government requirements, consumer needs and other uncontrollable factors, such as daily pandemic fluctuations. Pivot quickly, and you'll not only emerge as leaders of your industry, you may even gain immeasurable consumer intimacy.

A true cloud transformation should start with a plan to shift significant capabilities to cloud. It is more than just migrating a few enterprise applications. Implementing a "cloud first" strategy requires companies to completely reinvent their business for cloud by reimagining their products or services, workforce, and customer experiences.

2. Digital Twins Unleashed

Cloud stacks enable businesses to do new things with old ideas. Take digital twins, a technology that's been around for decades, but which is now being reimagined thanks to the cloud. The cloud allows digital twin models — essentially digital representations of physical objects and processes — to be hyper-scaled and enriched with artificial intelligence.

That changes everything. Leaders are starting to connect massive networks of intelligent twins, linking many twins together to create living models of whole factories, product life cycles, supply chains, ports, and cities. These unbroken threads of data will soon be essential to every enterprise. Data and intelligence can now serve as the primary orchestrators of the business, increasing real-time agility at scale, overhauling their innovation processes, and forming entirely new mirrored-world ecosystems and partnerships.

As a result of COVID-19, cloud adoption has increased dramatically. Accenture research found that cloud spending in the first quarter of 2020 was nearly triple that of the previous year.

3. Democratized Technology

But it's not just systems that the cloud is helping to improve, cloud tools are also helping to unlock the full potential of people. This was clear during the pandemic where cloud collaboration tools have been critical to productivity. We can now see that they're capable of much more. Thanks to the cloud, once complex enterprise tools are being democratized. Cloud-enabled technologies like natural language processing and low-code/no-code platforms are allowing people to take control without having to continually call on IT for support.

That means IT can focus on higher value tasks, but it also means that all people are empowered to use technology more freely to unlock productivity and spark innovation.

The approach is powerful. G&J Pepsi, for example, armed a group of workers with little or no software development skills with Microsoft's cloud-based Power Apps tool, which simplifies app development. The group created eight applications without a professional developer on staff and saved $500,000 in the first year alone.

4. Bring Your Own Environment to Work Anywhere

The pandemic has not only changed how we work; it's also changed where we work — once again enabled by cloud-based remote working tools. After the pandemic, it's unlikely we will return to how things were. We expect to see a hybrid model where people work from offices for some of the time, and home for some of the time, depending on need.

Where once Bring Your Own Device was a trend, we are moving to a model of Bring Your Own Environment (BYOE). Leaders can rethink the purpose of working at each location, and when it makes sense to be at certain sites or with certain people. But the level of virtual working, collaboration and connectivity is not possible without the cloud and with related enabling technologies like cloud-based cybersecurity tools.

5. Richer, Stronger Ecosystems

And it's not just people that the cloud is helping to connect. Cloud-based technologies like blockchain, distributed ledger, distributed database and tokenization are underpinning a new generation of multiparty systems that share data between individuals and organizations in a way that drives efficiency and builds new business and revenue models.

During the pandemic, technologies that were once considered too complicated, far from maturity or niche suddenly took center stage, from contact tracing to frictionless payments. Businesses are hoping to build on this start. Our Technology Vision 2021 research found that 90% of executives believe that multiparty systems will enable their ecosystems to forge a more resilient and adaptable foundation to create new value with their organization's partners.

A New World in the Clouds

The pandemic changed the world. Leading in the uncertain future will require businesses to be masters of change, able to navigate industry convergence, localized supply chains, mass virtualization, and rapidly and continuously changing customer expectations.

With their accelerated digital transformations, cloud-centric enterprises will attack some of the deepest-set challenges the world faces. Technology will help expand the definition of "value" to include how businesses can have a positive impact on the environment and how people live.

The cloud is set to help businesses lead by outmaneuvering uncertainty. It's now imperative that they lean into the cloud and catch up with leaders before the gap becomes too large.

About the Author: Karthik Narain is Global Lead of Accenture Cloud First. Follow him at @KarthikSNarain.

CYBERCRIMINALS HAVE THE ADVANTAGE.

TAKE IT BACK.

You shouldn't have to choose between protecting your business and propelling it forward. Stop breaches 84% faster with SaaS-delivered Network Detection & Response.

See for yourself.
extrahop.com/demo

ExtraHop

PREVIOUS