

UPDATED 14:48 EST / NOVEMBER 10 2019



As cloud security improves, a weak link emerges: people



CYBERSECURITY SPECIAL REPORT BY PAUL GILLIN
([HTTPS://SILICONANGLE.COM/AUTHOR/PAULGILLIN/](https://siliconangle.com/author/paulgillin/))

Last summer Capital One Financial Corp. was the victim of a massive data breach (<https://siliconangle.com/2019/07/29/huge-breach-100m-customer-records-stolen-capital-one/>) encompassing more than 100 million credit card applications and revealing 140,000 Social Security numbers. The cause: a misconfigured web application firewall, which is an appliance or software application that protects applications that run on the web.

The misconfiguration enabled the attacker, a former Amazon Web Services Inc. employee, to launch a server-side request forgery or SSRF, an attack that tricks a server into connecting to a server it wasn't supposed to connect to.

If those terms sound unfamiliar, it's because they had barely been heard of a few years ago. They're a new kind of cybersecurity vulnerability that was born in the cloud.

"SSRF has become the most serious vulnerability facing organizations that use public clouds," Evan J. Sharn, a product security manager at Cloudflare Inc., wrote in a detailed description of the breach posted on his personal blog (<https://ejj.io/blog/capital-one/>). In an interview with Brian Krebs

(<https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/>), Johnson elaborated that the potential damage of SSRF attacks are “being worsened by the offering of public clouds.”

Although the servers and data that were breached were on AWS infrastructure, Capital One assumed full responsibility (<https://www.capitalone.com/facts2019/>) for the incident. It had to. Under AWS’ Shared Responsibility Model (<https://aws.amazon.com/compliance/shared-responsibility-model/>), customers are responsible for configuring their own guest operating systems, databases and applications.

That may surprise some people. Cloud infrastructure providers make their services so simple to set up and administer that it’s tempting to assume that they also protect whatever customers run on them. But in most cases, everything above the infrastructure layer is the customer’s responsibility, including patches, data encryption, access control and malware prevention.

“A huge misconception is that the infrastructure-as-a-service model extends security to the customer’s systems when the providers are only securing the systems they are hosting,” said Jesse Emerson, vice president of Americas managed security services at managed security services firm Trustwave Holdings Inc.

“Simply put, when you use cloud services, the providers are responsible for securing the underlying infrastructure – customers are responsible for securing their data and applications,” said Robert Sadowski, trust and security marketing lead for Google LLC’s Cloud Platform.

And that misperception appears to be widespread. A recent survey (<https://static.helpsystems.com/powertech-x/pdfs/guides/ema-helpsystems-security-megatrends.pdf>) of an undisclosed number of information technology and security professionals by Enterprise Management Associates Inc. found that 53% believed IaaS providers are accountable for most or all public cloud security.

To err is human

The issue isn’t with the cloud itself. Most security professionals now agree that cloud infrastructure is at least as secure as the best enterprise data centers. Instead, the problem is with the free-wheeling and sometimes haphazard ways it’s adopted.

Cloud servers are basically no different than boxes in an on-premises data center. However, the ease with which cloud instances can be provisioned has led many organizations to delegate authority for using them in ways they would never do with their own infrastructure.



Many IT organizations have embraced the cloud as an expedient way to satisfy demands from their developers and end users for faster provisioning and greater control over their applications. Cloud providers have made it easy for people with only modest technical skills to install applications and

upload data.

But ease of use can also create a sense of false security. “The objective of making cloud management user-friendly can have unintended side effects, such as making it easier to make serious mistakes — one-click disasters, if you will,” said Kon Leong, chief executive officer of ZL Technologies Inc., a maker of records management and governance software.

“The speed with which organizations are adopting cloud is ahead of their ability to secure that usage,” said Doug Cahill, a senior analyst at The Enterprise Strategy Group Inc (<http://www.esg-global.com>). “The security operations team isn’t always involved. You’ve got line-of-business people who are clouding on their own and they may not be clouding properly.”

Ninety percent of the 1,000 respondents to a recent McAfee LLC report (<https://www.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/rp-cloud-adoption-risk-report-iaas.pdf>), in fact, said they had experienced some security issues with IaaS. “It’s possible the speed of cloud adoption is putting some practitioners behind,” the report stated.



ESG's Cahill: "Line-of-business people are clouding on their own and they may not be clouding properly." Photo: ESG

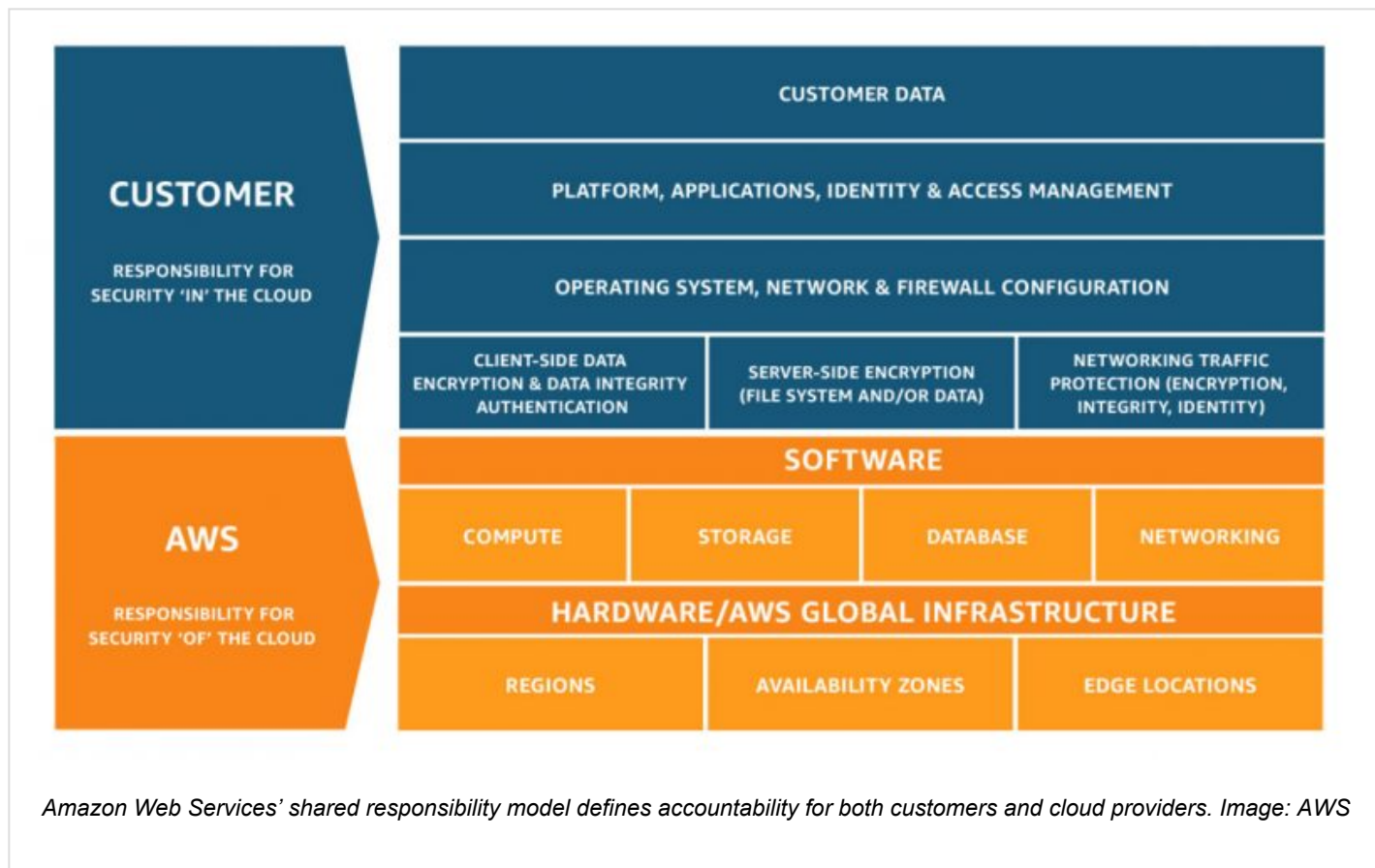
Lack of security procedures or simple carelessness can blindside even the most web-savvy organizations. In September, thieves swiped more than 24 million account records (<https://www.bankinfosecurity.com/luminpdf-leaked-exposed-data-for-243m-users-a-13100>) for users of Lumin, a cloud-native PDF reader produced by New Zealand-based Nitrolabs Ltd., after the data was left in the open for months on a public-facing MongoDB database on a cloud server.

Early last year FedEx Corp. was embarrassed (<https://siliconangle.com/2018/02/15/fedex-exposes-confidential-customer-data-via-misconfigured-aws-storage/>) when nearly 119,000 documents, many containing highly sensitive customer information, were left unprotected on an Amazon S3 storage instance.

None of these incidents was the fault of the big cloud providers, all of which offer world-class security controls. However, each defines its offerings a bit differently and many services are extra-cost options. Controls also aren't necessarily simple to understand. Amazon overhauled security controls (<https://siliconangle.com/2017/11/07/aws-ramps-security-encryption-s3-storage-service/>) on its S3 cloud storage service two years ago after numerous customers accidentally left confidential data publicly exposed because of confusion about nested and overlapping permissions.

Incidents such as these highlight the need for organizations to understand their responsibilities before using cloud infrastructure and to develop procedures that protect users from themselves. Gartner Inc. estimates (<https://www.gartner.com/smarterwithgartner/is-the-cloud->





secure/) that over the next six years, 99% of cloud security failures will be caused by human error and “90% of the organizations that fail to control public cloud use will inappropriately share sensitive data,” wrote Gartner Brand Content Manager Kasey Panetta. “CIOs must change their line of questioning from ‘Is the cloud secure?’ to ‘Am I using the cloud securely?’”

Perception shift

Perceptions about cloud security have shifted markedly in recent years. No long ago, the issue consistently ranked within the top two reservations chief information officers expressed about moving to the cloud, but those fears have largely subsided. A recent study (<https://nominetcyber.com/cyber-security-and-the-cloud/>) of U.S. and U.K. security professionals by British domain registrar and cybersecurity firm Nominet UK found that 61% say cloud environments are at least as secure as on-premises infrastructure. CIOs recognize that cloud infrastructure providers can commit resources to cybersecurity that dwarf that of all but the largest institutions.

“In general, cloud is more secure than an enterprise data center,” said John Veizades, vice president of engineering and product at Megaport Ltd., a provider of cloud connectivity services. For example, he noted, cloud providers are better able to respond to “zero-day” or heretofore undiscovered threats because they monitor so many attack points. “Cloud vendors are aware of these things much sooner than you are as an IT administrator,” he said.

SHARE

The quality of cloud security is now so high that it's easy to become lulled into thinking that the platform provider takes care of everything. But as AWS' Shared Responsibility Model illustrates, there are clear lines of demarcation.

In an essay (<https://www.redhat.com/en/topics/security/cloud-security>) about the distinctions between on-premises and cloud security, Red Hat Inc. draws the analogy to an apartment building. Landlords secure the building perimeter but leave the security of individual apartments to their tenants. In a similar way, cloud providers defend the infrastructure that customers rent from them but leave control of the systems software, applications and data to the customer.

The most common cloud security risks are the same as those inside the walls of a company. Cloud can magnify their impact, however. Take password security. Weak passwords (<https://siliconangle.com/2017/08/09/study-finds-major-companies-fail-basic-password-security/>) have long been one of the most stubbornly difficult problems for enterprises to solve, but when the asset being protected is a cloud administration account, the risk to the business can be severe.

"If I can get into the console, I may have unfettered access to all servers on the account," Cahill said. "The best practices we use for securing customer-managed environments still apply." Multifactor authentication (<https://siliconangle.com/2017/11/20/its-time-for-multifactor-authentication-everywhere-says-centrify-executive-cyberconnect/>) is a relatively simple remedy that all cloud providers offer, but none imposes it by default.

An even bigger problem in recent years has been misconfigured cloud services like the one that was at the root of the Capital One breach.

The volume of cloud security incidents attributed to misconfiguration rose 20% in 2018, making misconfiguration "the single-biggest risk to cloud security, with 62% of surveyed IT and security professionals noting it as a problem," said IBM Corp.'s 2019 X-Force Threat Intelligence Report (<https://www.ibm.com/account/reg/signup?formid=urx-36763>).

Risk Based Security Inc.'s 2019 mid-year report (<https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report>) documented 149 incidents in which misconfigured cloud databases and services collectively exposed over 3.2 billion records, up 54% from the previous year.

McAfee's survey found that users identify, on average, 37 misconfiguration incidents per month. But researchers also estimated that about 99% of misconfigurations go unnoticed. "Our real-world data shows that companies actually experience closer to 3,500 such incidents" per month, they wrote.

Cloud providers are aware of the risks and responding. "We encourage customers to turn on additional layers of protection from across our threat protection stack, not just address misconfigurations we help identify through Azure security services," said Scott Woodgate, senior director of Microsoft Azure.



The “sheer complexities of navigating cloud infrastructure” can lead to configuration errors, said Trustwave’s Emerson. “Seemingly minute mistakes can easily lead to a catastrophic compromise if they aren’t caught.”

Eager coders

Software developers have embraced the cloud with fervor because of the speed with which they can spin up servers that match the target destinations for their applications. And many IT organizations oblige by giving their development teams the means to provision their own cloud infrastructure. The increasingly popular agile programming technique called DevOps encourages this by giving developers control of both the application and the environments they run upon. DevOps also promotes continuous integration and delivery or CI/CD, with changes pushed daily or even more frequently.



BMC's Srinivasan: “Automation is not a luxury, but a necessity.” Photo: Twitter

Developers aren’t known for their attention to security, however. “With each update comes the risk of a single mistake, misconfiguring a cloud IaaS or platform-as-a-service resource and rendering it vulnerable,” said Vidhya Srinivasan, vice president of marketing, digital service and operations management at BMC Software Inc.

ESG’s Cahill was even more blunt. “To the security team, DevOps is like running with scissors,” he said. “There’s a huge cultural dynamic. Development teams are empowered to get applications built quickly and they fear the security team will slow them down.” A variation of DevOps called DevSecOps bundles security into the development process and is a good discipline for enterprises to adopt, experts recommend.

Some of the most notorious cloud breaches have been the result of sensitive data being left in the open on cloud servers. Human error is again to blame. Amazon’s S3 storage is configured to notify users when data is exposed on the public internet but people sometimes either don’t understand the warnings or ignore them, said Leigh-Anne Galloway, cybersecurity resilience lead at PT Global Solutions Ltd., which does business as Positive Technologies. “The default stores are created with a secure configuration, so all leaks are associated with user actions,” she said.

Cloud service providers aren’t entirely blameless. The frequency with which they roll out new services can be dizzying for administrators who are accustomed to the relatively static nature of their own environments. The EMA study reported that 73% of enterprise security teams said lack of visibility within cloud infrastructure limits their effectiveness.



“Cloud service providers are constantly releasing new services, and while they may be similar, they are not identical,” said Srinivasan. “Each instance must be configured appropriately.”

Many of those new services are meant to strengthen security. At Microsoft Corp.’s Ignite conference this past week, for example, the company introduced (<https://www.microsoft.com/security/blog/2019/11/04/microsoft-announces-new-innovations-in-security-compliance-and-identity-at-ignite/>) a broad range of new and enhanced services addressing everything from authentication to insider risk management. Amazon and Google maintain a similar innovation pace.

That can challenge the ability of a security team to keep up. “Manual or ad-hoc security cannot keep pace with a growing or large-scale cloud footprint that is inherently dynamic,” Srinivasan said. “Automation is not a luxury, but a necessity.”

The task gets harder in a multicloud environment, which is fast becoming the norm for organizations that want to pick and choose the best platforms for each workload. Gartner says (<https://www.gartner.com/smarterwithgartner/why-organizations-choose-a-multicloud-strategy/>) 81% of public cloud adopters are already working with two or more service providers, but multicloud complexity (<https://siliconangle.com/2019/01/25/complexity-concerns-rain-multicloud-parade/>) is a daunting challenge. While the services cloud providers offer are similar, they aren’t identical. Each must be mastered and configured individually.

What to do

All those factors don’t add up to a case against using the public cloud. Service providers have made huge strides in hardening their services and their pace of innovation will continue to outstrip that of most of their customers. Microsoft alone employs 3,500 cybersecurity professionals and has invested more than \$1 billion in Azure security, Woodgate said.

Cloud security services are typically tightly integrated with the underlying infrastructure, unlike the patchwork of point products that are common in enterprise security operations centers. “Our tools can actually help save employees’ time so they can focus on doing more innovative work instead of plumbing,” said Google’s Sadowski, who claims that cloud security services are far less complicated than people think.

Cloud providers can also apply best practices that may be overlooked in a data center, he added. “For example, we encrypt customer data at rest and in transit to our cloud by default,” Sadowski said. “Data automatically defaults to HTTPS between the customer and Google and we never give any government entity backdoor access.”



SHARE

Microsoft recently added automatic malware detection that alerts customers if they inadvertently upload malware, Woodgate said. The service encrypts data at rest by default with a Microsoft- or customer-managed key and offers a fully audited troubleshooting process that grants limited access to a support technician to fix a problem. For security professionals, there are machine learning-based filters in Azure Sentinel that cut down on noise and enable them to pinpoint problems more precisely.

“These tools exist; the key is turning them on and using them,” Woodgate said.

Experts say the fundamentals of securing the cloud are the same as securing the data center. Multifactor authentication is mandatory, Woodgate said. “It helps eliminate a lot of vulnerabilities,” he said.

Cloud providers also suggest imposing strict access controls, always encrypting data and knowing what infrastructure the organization controls: Any that uses public cloud should also become familiar with the shared responsibility model. “It’s important to highlight that security in the cloud is a shared responsibility between the customer and their cloud provider,” said Sadowski.

The complexity of administering multicloud and hybrid cloud environments raises the bar on asset management, said BMC’s Srinivasan. “It is mandatory to know what hardware, services and applications you have, where they are running and how they are configured,” she said. “Having an automated way to map and catalog systems, services and relationships is now crucial.”

All major cloud providers offer security hubs that provide comprehensive views of a customer’s services, but they’re only useful for instances the customer knows about. All services should be provisioned under the watchful eye of the IT department.

ESG’s Cahill recommends adopting the practice of “least privilege access,” which restricts access rights to only those resources a user absolutely needs. Network segmentation, which is commonly used on-premises to split networks into multiple subnetworks for performance and security purposes, can be applied at a finer-grained level in the cloud, said Megaport’s Veizades.

“You can think of a network as supporting one application whereas in a data center is supports many applications,” he said. “You can now think about micro-segmentation of network access.”

Automating asset discovery using automated tools from cloud providers is also important because the process is impractical to manage manually, Srinivasan said. “Integrating an automated cloud security process with the service desk for closed-loop change management is also critically important,” she said. “This provides documentation and an audit trail of security problems found and changes made.”



SHARE

Organizations should make regular scanning and continuous monitoring of all databases routine as well, taking advantage of the rich logging and event management tools cloud providers offer, said Trustwave's Emerson. "If a vulnerability is caught early, it can be stopped from evolving into a major security incident," he said.

But even the most meticulous precautions are no match for a careless or poorly trained user. For all the firepower cloud giants have brought to protecting their customers, the greatest threat is at the keyboard.

Photo: Brian Smithson/Flickr (<https://www.flickr.com/photos/smithser/3870653508/>)

Since you're here ...

Show your support for our mission by our 1-click subscribe to our YouTube Channel (below) — The more subscribers we have the more then YouTube's algorithm promotes our content to users interested in #EnterpriseTech. Thank you.

Support Our Mission: >>>>> **SUBSCRIBE NOW** >>>>> (https://www.youtube.com/user/siliconangle?sub_confirmation=1) to our Youtube Channel

... We'd like to tell you about our mission and how you can help us fulfill it. SiliconANGLE Media Inc.'s business model is based on the intrinsic value of the content, not advertising. Unlike many online publications, we don't have a paywall or run banner advertising, because we want to keep our journalism open, without influence or the need to chase traffic. The journalism, reporting and commentary on SiliconANGLE (<http://www.siliconangle.com>) — along with live, unscripted video from our Silicon Valley studio and globe-trotting video teams at **theCUBE** (<http://www.thecube.net>) — take a lot of hard work, time and money. Keeping the quality high requires the support of sponsors who are aligned with our vision of ad-free journalism content.

If you like the reporting, video interviews and other ad-free content here, please take a moment to check out a sample of the video content supported by our sponsors, **tweet your support** ([https://twitter.com/intent/tweet?text=I am really loving the @SiliconANGLE business model for free quality journalism and reporting](https://twitter.com/intent/tweet?text=I+am+really+loving+the+%40SiliconANGLE+business+model+for+free+quality+journalism+and+reporting)), and keep coming back to **SiliconANGLE** (<http://www.siliconangle.com>).

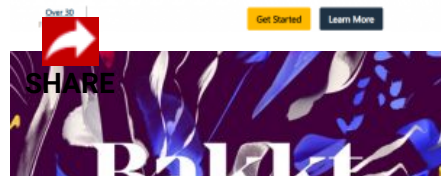
LATEST STORIES



Large ASP.NET hosting provider crippled in ransomware attack

(<https://siliconangle.com/2019/11/11/large-asp-net-hosting-provider-crippled-ransomware-attack/>)

SECURITY - BY DUNCAN RILEY (<https://siliconangle.com/author/duncanriley/>) . 55 MINS AGO



Bakkt bitcoin custodial service now available after gaining regulatory approval

By Matt ... 11/11/2019 ...



As cloud security improves, a weak link emerges: people - SiliconANGLE

(<https://siliconangle.com/2019/11/11/bakkt-bitcoin-custodial-service-now-available-gaining-regulatory-approval/>)

BLOCKCHAIN - BY DUNCAN RILEY (<https://siliconangle.com/author/duncanriley/>) . 1 HOUR AGO



Twitter releases draft policy on how it will handle deepfakes

(<https://siliconangle.com/2019/11/11/twitter-releases-draft-policy-will-handle-deepfakes/>)

POLICY - BY DUNCAN RILEY (<https://siliconangle.com/author/duncanriley/>) . 2 HOURS AGO



SpaceX's first 60 operational Starlink satellites deploy in orbit

(<https://siliconangle.com/2019/11/11/spacexs-first-60-operational-starlink-satellites-deploy-orbit/>)

EMERGING TECH - BY MARIA DEUTSCHER (<https://siliconangle.com/author/chi22/>) . 8 HOURS AGO



Google updates Chrome browser with a focus on easier content distribution

(<https://siliconangle.com/2019/11/11/google-updates-chrome-browser-focus-easier-content-distribution/>)

APPS - BY MIKE WHEATLEY (<https://siliconangle.com/author/mikewheatley/>) . 9 HOURS AGO



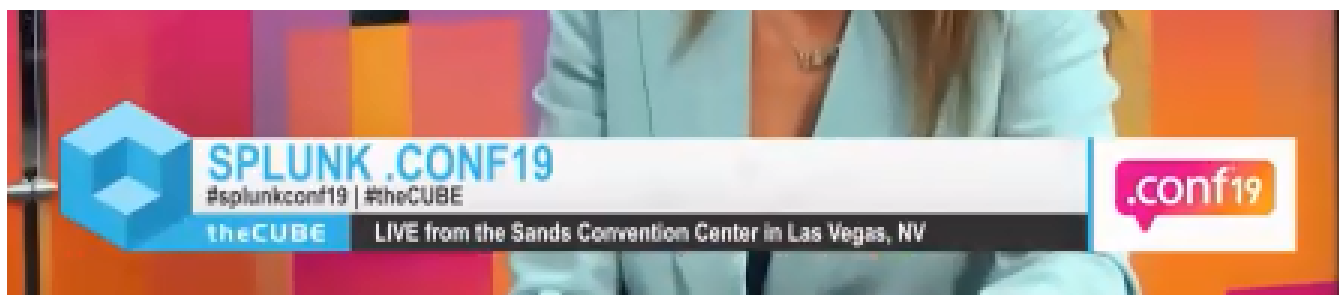
UPS and HerdX team up on blockchain-tracked beef delivery from US to Japan

(<https://siliconangle.com/2019/11/11/ups-herdx-team-blockchain-tracked-beef-delivery-us-japan/>)

BLOCKCHAIN - BY KYT DOTSON (<https://siliconangle.com/author/kitdotson/>) . 12 HOURS AGO

CUBE EVENT COVERAGE (<https://siliconangle.com/category/cube-event-coverage/>)





Explore more videos at theCUBE
 (<https://www.thecube.net>)

LATEST FROM THECUBE (<https://siliconangle.com/category/cube-event-coverage/>)

Mitigating failure in microservices remains a cloud-native challenge for developers

(<https://siliconangle.com/2019/11/11/detecting-and-mitigating-failure-in-microservices-remains-a-cloud-native-challenge-for-developers-cubeconversations/>)

Viewers speak, Comcast listens, and cable TV rides its own wave of digital transformation

(<https://siliconangle.com/2019/11/11/viewers-speak-comcast-listens-and-cable-tv-rides-its-own-wave-of-digital-transformation-comcastinnovation-guestoftheweek/>)

Q&A: Inside Microsoft's embrace of GitHub's strong open-source community

(<https://siliconangle.com/2019/11/11/qa-inside-microsofts-embrace-githubs-strong-open-source-community-msignite/>)

Analyst Q&A: Microsoft's ecosystem 'trust factor' gets a big boost (<https://siliconangle.com/2019/11/08/qa-microsofts-ecosystem-trust-factor-gets-big-boost-says-analyst-msignite/>)

An OS for people: How a simple word-processing program grew to planetary scale

(<https://siliconangle.com/2019/11/08/os-people-simple-word-processing-program-grew-planetary-scale/>)

Discover Kubernetes Special Report


Many throats to choke: For better or worse, multiple clouds are here to stay

(<https://siliconangle.com/2019/08/25/many-throats-choke-better-worse-multiple-clouds-stay/>)

Google releases its Scaffold tool for automating Kubernetes into general availability

(<https://siliconangle.com/2019/11/07/google-releases-scaffold-tool-automating-kubernetes-general-availability/>)

Kubernetes infrastructure company Diamanti raises \$35M (<https://siliconangle.com/2019/11/07/kubernetes-infrastructure-company-diamanti-raises-35m-series-c-round/>)

 nite, Microsoft convincingly addresses the multicloud imperative (<https://siliconangle.com/2019/11/06/ignite-microsoft-convincingly-addresses-multicloud-imperative/>)

At Ignite, Microsoft pitches its new role embracing the wider tech ecosystem

(<https://siliconangle.com/2019/11/05/analysts-see-latest-releases-as-evidence-of-evolving-new-role-for-microsoft-msignite/>)

View full report coverage (<https://siliconangle.com/tag/kubernetes/>)

UPCOMING CUBE EVENTS (<https://www.thecube.net/upcomingevents/>)



KubeCon + CloudNativeCon 2019

(<https://www.thecube.net/kubecon-19>) Nov 18-21

(<https://www.thecube.net/kubecon-19>)



Qualys Security Conference

(<https://www.thecube.net/qualys-security-conference-2019>) Nov 19-19

(<https://www.thecube.net/qualys-security-conference-2019>)



Accenture Executive Summit 2019

(<https://www.thecube.net/accenture-executive-summit-2019>) Dec 02-03

(<https://www.thecube.net/accenture-executive-summit-2019>)



AWS re:Invent 2019

(<https://www.thecube.net/aws-ri-2019>) Dec 02-04

(<https://www.thecube.net/aws-ri-2019>)

Join our community



our personalized daily newsletter.

SHARE

I AM INTERESTED IN



Please enter your email ID

SUBSCRIBE NOW



(<https://siliconangle.com>)



SHARE