CloudPassage

WHITE PAPER

WHY SECURITY SHOULD CARE ABOUT “THE APPLE EFFECT”– HOW CLOUD COMPUTING UNLOCKS CONTINUOUS INNOVATION

Summary

Apple has been an industry leader in consumer technology products for at least two reasons: One, it effectively aligned and streamlined business processes to create and maintain a culture of continuous innovation, and two, coupled that with brilliant product vision and design, and excellence in execution.

The result of this has been delivery of new products on such a regular basis until consumers' brains essentially got re-wired to expect that something new from Apple was coming. This phenomenon is called "the Apple Effect". This culture of continuous innovation forever altered the company's trajectory and literally changed the way we think about product development and how we now do business.

Apple has been an industry leader in consumer technology products for at least two reasons: One, it effectively aligned and streamlined business processes to create and maintain a culture of continuous innovation, and two, coupled that with brilliant product vision and design, and excellence in execution.

In the B2B world companies now expect each other to deliver on Apple's promise and deliver innovative products and services on a regular basis. To meet customer expectations, creative B2B companies are taking note of Apple's success and beginning to use internal automation processes such as continuous integration/continuous delivery (CI/CD) to enable rapid innovation.

Of course, enabling a culture of continuous innovation requires a dynamic information technology (IT) environment with scale, and speed, and a way to quickly and effectively maintain security visibility on a much broader scale than has been the norm across traditional IT environments.

Enterprises are leveraging Infrastructure-as-a-Service (IaaS) to improve operational agility, increase efficiency, and support the modern application infrastructure. While these faster computing environments are revolutionizing application development and enabling continuous innovation, they are not without security challenges.

As a virtual hosting solution, public cloud computing is somewhat more abstract than a traditional IT environment, so security teams struggle to maintain security and compliance visibility due to decentralization of IT, the expanding cloud attack surface, and pervasive cloud service misconfigurations that create risk.

Nevertheless, hoping to reap its benefits, application owners are pushing security practitioners to figure out how they can still accomplish security and compliance. This is the fundamental challenge that we address at CloudPassage.

In this white paper, we'll examine these security and compliance challenges and demonstrate a way to improve security visibility, eliminate blind spots, and harness the power of IaaS to develop a culture of continuous innovation without compromising on security.

Why Security Should Care About the Apple Effect

Any doubt about cloud as a disruptive trend in IT evaporated long ago. Any shadow of doubt is now surely gone, perhaps with the exception of a very few technology dullards who, by virtue of failing to adapt, are likely to go the way of the dinosaur.

To date, Amazon has been the leading enabler of cloud adoption with Amazon Web Services (AWS), and has revolutionized the way that enterprises develop and execute technology.

According to Amazon, the number of active AWS users exceeds 1,000,000. While small and mid-size companies make up the majority of that user base, recent polls by private consulting firms suggest that enterprise-scale users contribute at least 10% of that total.[1]

By 2020, cloud leader Amazon is expected to have revenue of $44B and to still be winning twice the combined cloud revenue of its two biggest rivals.[2] But as so often happens with any massively disruptive trend, the other major players are racing to catch up. Microsoft and Google are gaining momentum with their cloud platforms.

Based on revenue projections for 2020, Microsoft Azure will be at $19B and Google Cloud at $17B. In 2018 alone, AWS grew 49% in the first quarter, while Google and Microsoft grew their cloud business at close to 100%, although at smaller volumes. A near-50% quarterly growth rate for Amazon means it added almost as much revenue as Microsoft earned: $1.8B.[3]

In 2018, 50% of the global enterprises surveyed confirmed they would rely on public cloud infrastructure, or IaaS, to enable digital business transformation.[4]

As a security practitioner, you've likely heard the buzz around public IaaS – you may even have encountered early deployments in your own enterprise which in turn are driving other changes to your IT and development environments. And for good reason. To enable rapid innovation, public cloud adoption is driven by the need for infrastructure automation and the incorporation of DevOps.

There's a lot of chatter and momentum around these trends for a good reason. The central purpose underlying all of them? The need for speed. And that may leave you wondering, "Why is this new need for speed so important to my company?"

The short answer is that any technology-centric company now has to meet buyer expectations of continuous innovation. It all comes back to "the Apple Effect".

How Apple Changed the Way We Do Business

Apple remains a leading innovator, though it wasn't always so. From 1985-1997, Apple struggled to achieve market success, especially after the departure of Steve Jobs (1985) and increased competition from other giants, such as IBM, that decided to enter the personal computer market.

Apple's success fully drove its culture of innovation by adopting design thinking to drive its culture of continuous innovation. Design thinking is a solution-oriented process that places the consumer at the heart of all development stages to achieve innovation.

By focusing on a holistic user experience, Apple created a culture that enabled continuous innovation at all levels, just as CI/CD enables software engineering teams to rapidly develop and improve business applications. And that in turn enabled excellence in execution, the result of which was new product rolling out on a regular basis. Apple's culture of continuous innovation would forever alter the company's trajectory and literally change the way we think about product development, as well as how we now do business.[5]

Apple's product journey started with the launch of the Apple I computer in 1976, followed by its dot matrix printer in 1982. It's true culture of continuous innovation appeared with the release of the iMac in 1998, continued improving with the launch of the iPod and iTunes, and matured with the release of the iPhone in 2007, an event that transformed the company into what it is today.[6]

From the time of the iMac, Apple has focused intently on continuous innovation to deliver a constant stream of new capabilities and improvements, whether minor updates, or major upgrades. Apple customers don't just buy Apple products, they also buy or buy into a non-stop stream of "something new," the effect of which is both, intoxicating and addictive.

The positive impact of constant improvements and enhancements to existing products was not lost on Apple. They targeted this pattern, repeating it over the years with essentially every Apple product in the market to continue expanding the positive impact. And it worked. Consumers came to anticipate something new from Apple every year or so.

And Apple has delivered on that promise again and again, with the iPad, Siri, Cloud, with bigger and better iPhones and the Apple Watch. Apple has proved, it can successfully deliver products that consumers neither know they want, yet discover they can't live without.

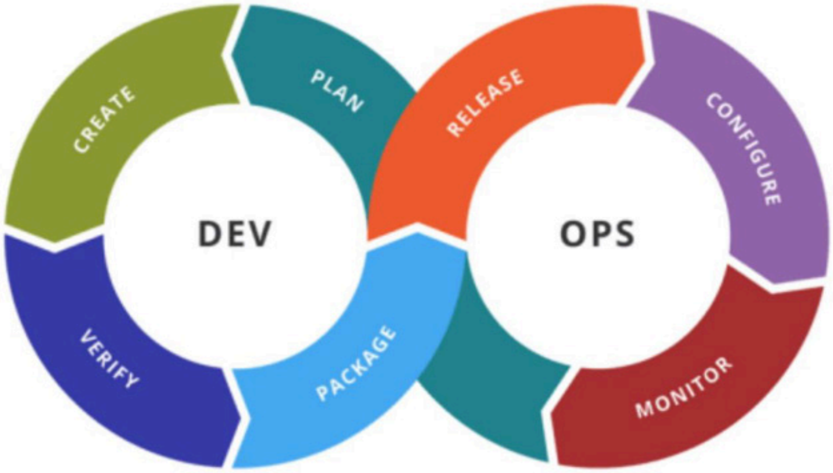
The Apple Effect has sparked more than just a new approach to product development. It denotes a major change in what we've understood about brand engagement and marketing brought about by the creation of a movement that literally altered the mindset of buyers. Buyers who were at first only end-consumers, now engage with expectation derived from continuous innovation and continuous rapid delivery. This in turn has bled over into the thinking and expectations of B2B buyers and decision-makers. So much so, in fact, that businesses now expect CI/CD of new products from other businesses. This has inspired B2B companies to study Apple's playbook and begin to utilize CI/CD tools and processes to enable their own continuous innovation.

Achieving Continuous Innovation

Compared to continuous innovation in devices or manufacturing which would take major capital investment and time to change, software is the most obvious area of a business where continuous innovation can have immediate impact.

Achieving continuous innovation in software often leads to rapid adoption of cloud, particularly public IaaS. It's the fastest route to cloud infrastructure, as well as the one with the lowest risk and best economics compared to building your own within your own cloud data center. Adopting cloud infrastructure complements the implementation of CI/CD technologies, as well as DevOps application development and management models, etc. as continuous delivery is a software approach that helps you release products reliably, at any time you choose.

Achieving continuous innovation in software often leads to rapid adoption of cloud, particularly public IaaS. It's the fastest route to cloud infrastructure, as well as the one with the lowest risk and best economics compared to building your own within your own cloud data center. Adopting cloud infrastructure complements the implementation of CI/CD technologies, as well as DevOps application development and management models, etc. as continuous delivery is a software approach that helps you release products reliably, at any time you choose.



CI/CD Pipeline

The continuous delivery approach generally goes hand in hand with CI, which is also a software engineering technique. Together they comprise a system enabling you to continuously merge the work of developers with a mainline at any given time in the product life cycle. Both CI and continuous delivery are useful to both big teams, as well as teams and companies of all sizes, as delivery is unavoidable to every application developer. Here's where DevOps enters the picture to enable the invaluable need for speed.

DevOps is basically the automation of agile methodology with the goal of empowering developers to respond to the needs of the business in near real-time. In other words, DevOps should ultimately remove much of the latency that has existed for years around software development by giving you automation with a standard and centralized platform for testing, deployment, and production.

In a nutshell, well-implemented DevOps initiatives will deliver rewards in terms of IT efficiency and quality that enable developers to move away from the "waterfall" model, where a new software deployment is given a long timeframe. Rather than allowing a lot of time for preparation and planning before it goes live, it takes on an agile approach, whose core elements are collaboration across teams, deploying quickly, and improving continuously.

Perhaps, one of the best things about applying CI/CD tools and processes is that they give you the ability to create a repeatable and dependable way to deploy your applications. That way how you deploy your application becomes a scripted, repeatable process working the same way each time.

Many enterprises are already finding that app modernization driven by CI/CD goals is truly helpful because it reduces the time required to integrate new capabilities into applications, and thus improves IT support for business operations.

Why Cloud Computing Should Matter

Cloud computing, delivered through services like AWS and Azure, is extremely beneficial for your company because it allows you to create the modern, agile application environment your developers and IT departments need to innovate faster and more continuously. All of which is critical to staying competitive. *How does IaaS enable this?*

In today's digital economy, you're likely constantly looking for ways to be more agile, to differentiate your offerings and outpace the competition. With the power of IaaS, your organization can get instant access to products and services at the forefront of digital innovation, such as serverless computing.

With easily accessible revolutionary services from AWS and Azure, you can set up cloud computing infrastructure in minutes, without having to incur any major capital expenses. This means your IT team can develop new products, rethink business models, and reach customers in new ways in a fraction of the time it currently takes you.

Equally important, coupling these services with security best practices can help you stay secure and compliant without compromising agility.

The alternative to not taking advantage of the new IaaS environment is, that you end up a dinosaur and potentially disappear, as half the companies on the Fortune 500 have disappeared since 2000, many of them due to digital disruption.[7] You could become another dinosaur among them.

How You, as a Security Leader, Can Enable Continuous Innovation

As a security leader, you have the ability to enable all the benefits of the cloud so that your enterprise can reap the rewards of using public cloud, without creating undue risk. By making security an integral part of the development process from the beginning, you are able to address any vulnerabilities that arise as soon as they are detected at any point in the process.

More importantly, by protecting your company's assets and avoiding a misconfigured cloud, you can prevent a potential security nightmare.

Misconfiguration of cloud platforms jumped to number one as the single biggest threat to cloud security (62%).[8] To avert this kind of threat, you have to cover your company's assets. Which means, you need security visibility to know:

- What assets you have
- What needs to be protected, and
- What potential issues exist in and around those assets.

Armed with that information, you can facilitate resolution.

Two big categories of risk exist within IaaS environments:

- Risks associated with actual security exposures, meaning you can get hacked, and
- Risks that you fail an audit, or regulatory compliance risk that leads to fines.

If you're not secure, you will get hacked. And then fined, making the management of your compliance role a lot more complex and difficult.

So why is security challenging in AWS and Azure, or any IaaS environment?

First of all, the scale and speed of IaaS environments are bigger and much faster compared to traditional IT environments, and as a virtual hosting, solution public cloud computing is somewhat more abstract. Instead of being accessible through physical hardware, all servers, software and networks are hosted in the cloud, off premise. It's a real-time virtual environment hosted between several different servers simultaneously.

The good news is that even though it's slightly more complex, IaaS gives you the scale and speed you need to enable CI/CD.

While scale and speed are friends of CI/CD, they can be the enemy of security if not handled correctly. In a nutshell, the challenge is that there are simply more things in more places that need to be monitored and protected. Additionally, the rate of change, both for code and infrastructure, or the latter, now essentially being more code, is orders of magnitude higher.

So why is security challenging in AWS and Azure, or any IaaS environment?

First of all, the scale and speed of IaaS environments are bigger and much faster compared to traditional IT environments, and as a virtual hosting solution, public cloud computing is somewhat more abstract. Instead of being accessible through physical hardware, all servers, software and networks are hosted in the cloud, off premise. It's a real-time virtual environment hosted between several different servers simultaneously.

Also, because, as a security professional, you likely have a million things to address and may not have a big enough team tackling all your organization's security challenges.

While anyone can inventory assets, how fast can you actually do that if you're doing it manually? And if you're doing it manually, by the time you finish the environment has likely changed. Again.

So how do you keep up with growing inventory of 10s of 1000s of assets and potential issues to resolve? And how do you get the necessary high scale and high speed necessary to keep up?

The answer: Automation.

So how do you keep up with growing inventory of 10s of 1000s of assets and potential issues to resolve? And how do you get the necessary high scale and high speed necessary to keep up?

The answer: Automation.

Automation Is Key to Effective IaaS Security and Compliance Visibility

In order for you, as a security practitioner, to enable all the benefits of the cloud, you have to figure out how to maintain awareness of your assets and the issues that threaten those assets, and be able to resolve those at high scale, and high speed. That's only possible with automation.

CloudPassage makes this process very fast, and very easy by utilizing automation within Halo Cloud Secure.

For decades, security and automation has been like a gym membership for security professionals. We all knew we needed to do it. So, we bought automation tools and took one or two steps in the right direction, but we'd never actually complete the task.

Adoption of IaaS is like a forcing function because now we have to do a better job of security or we're risking a data breach.

Amazon and Microsoft do a stellar job of securing the cloud as part of the Shared Responsibility Model with an army of people focussing just on security issues. The good thing is that even if you're a two-person company, you're still getting all the benefits that Amazon provides a major company like Netflix. You still get the high-water mark for cloud security.

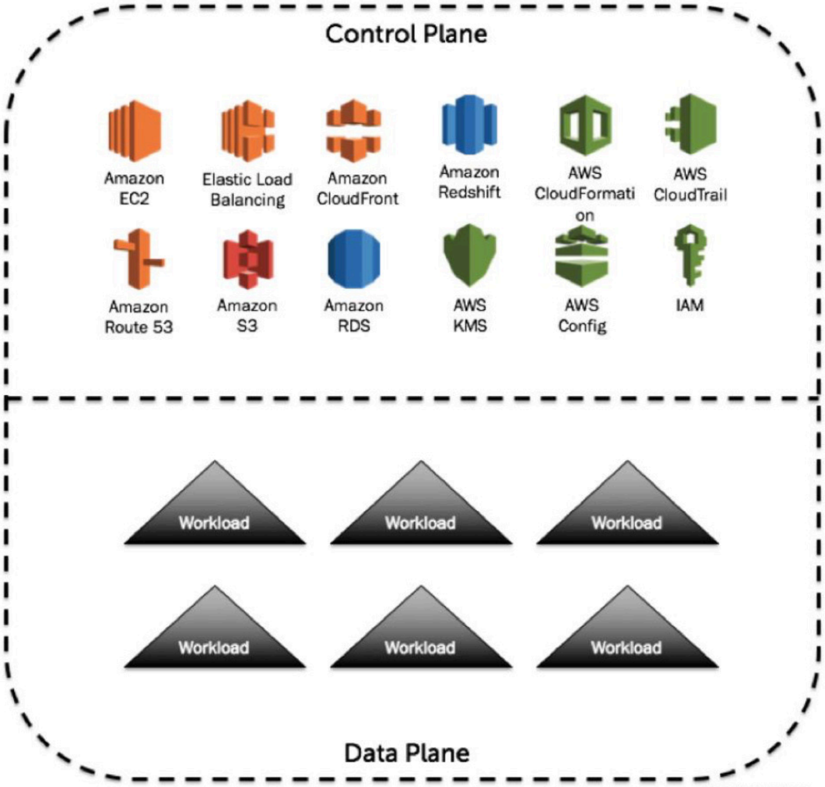
Now all you have to do is meet your part of the Shared Responsibility Model by securing your assets "in the cloud."

While this may sound like an overwhelming challenge, it's also an opportunity for you to enable your company to make the most of the cloud and in turn, to take on new technology, so you can innovate and deliver products continuously and, ultimately, stay competitive.

Enabling you to effectively maintain your part of the Shared Responsibility Model is where Halo Cloud Secure can help.

Gain Complete Security Visibility of Your Public Cloud Faster and Easier

According to Gartner, the strategy for securing IaaS environments occurs within two layers: the data plane and the control plane.



Credit: Gartner

The data plane is where your workloads reside, including data and applications, and the control plane provides services to provision, deprovision, and manage your workloads. A vulnerability in either plane can expose your organization to the risk of a breach or noncompliance.

To have a complete view of your public cloud security posture, you need visibility of both the data and control plane.

Unfortunately, most public cloud security solutions only focus on protecting one but not both planes. This means you are faced with the operational overhead of running and managing multiple security tools to obtain complete visibility, or by accepting the hidden risks that accompany partial security coverage.

According to Gartner, the strategy for securing IaaS environments occurs within two layers: the data plane and the control plane.

Halo Cloud Secure is an automated public cloud security solution that delivers comprehensive visibility, protection, and continuous compliance monitoring to reduce cyber risk.

Unlike point solutions that provide limited coverage, Halo Cloud Secure finds critical risks other tools miss by protecting your public cloud control plane and data plane.

- Automatically Discover Public Cloud Assets: Quickly discover and inventory assets in use across any number of public cloud accounts in use in your organization to better manage cyber risk.
- Reduce Your Attack Surface: Reduce the attackable surface area of your public cloud deployments by instantly and continuously identifying your greatest risks and most vulnerable services.
- Find Critical Risks Other Tools Miss: CloudPassage offers the best security visibility coverage for AWS and Azure with a broad set of over 20,000 policy checks and deep coverage that monitors both the control plane and data plane of your public cloud environment--including virtual machines, containers, and serverless workloads.

Harness the Power of IaaS

Cloud offers an enhanced level of flexibility and scalability with its on-demand unlimited virtual space and abundant server resources. In terms of agility, application owners are able to get to market faster, while not having to put giant investments upfront.

For the IT organization that’s responsible typically for managing costs across all application hosting, the ability to use the entire hosting environment to host many applications allows it to optimize its budgets, time and resources using a single approach.

At the same time, the new IaaS environment presents new issues to solve. You can no longer use hardware devices, nor gain access to the physical network, nor assume that your application will be hosted in a dedicated environment that you own and you control.

Nevertheless, application owners, hoping to reap its benefits, are driving security practitioners to figure out how they can still accomplish security and compliance. This is the fundamental challenge that we at CloudPassage address.

Learn more about how Halo Cloud Secure can help you gain the critical comprehensive security and compliance visibility you need to effectively monitor and protect your IaaS environment. *Download our product brief.*

FOOTNOTES

[1] *https://www.forbes.com/sites/johnkoetsier/2018/04/30/cloud-revenue-2020-amazons-aws-44b-microsoft-azures-19b-google-cloud-platform-17b/#46e731187ee5*

[2] *Ibid*

[3] *Ibid*

[4] *https://www.logicmonitor.com/wp-content/uploads/2017/12/LogicMonitor-Cloud-2020-The-Future-of-the-Cloud.pdf*

[5] *https://www.designorate.com/design-thinking-case-study-innovation-at-apple/*

[6] *https://www.nydailynews.com/news/national/apple-turns-40-timeline-tech-giant-evolution-article-1.2581048*

[7] *https://www.weforum.org/agenda/2016/01/digital-disruption-has-only-just-begun/*

[8] *https://pages.cloudpassage.com/cyberthreat-defense-report.html*

ABOUT CLOUDPASSAGE

Founded in 2010, CloudPassage® is a security pioneer awarded the first-ever patents for universal cloud infrastructure security and is a leading innovator in cloud asset visibility. CloudPassage Halo® is an award-winning security solution purpose-built for the cloud that helps customers automatically discover cloud assets, reduce their attack surface, and find and respond to critical risks other tools miss. It provides unrivaled visibility and continuous compliance for the cloud deployments of some of the world's most demanding IT shops in technology, finance, security, media, e-commerce, and hospitality. CloudPassage is backed by leading Silicon Valley firms Benchmark, Four Rivers Group, Lightspeed Venture Partners, Meritech Capital, Musea Ventures, Shasta Ventures, Sozo Ventures, and Tenaya Capital.

CloudPassage

www.cloudpassage.com | 800.215.7404