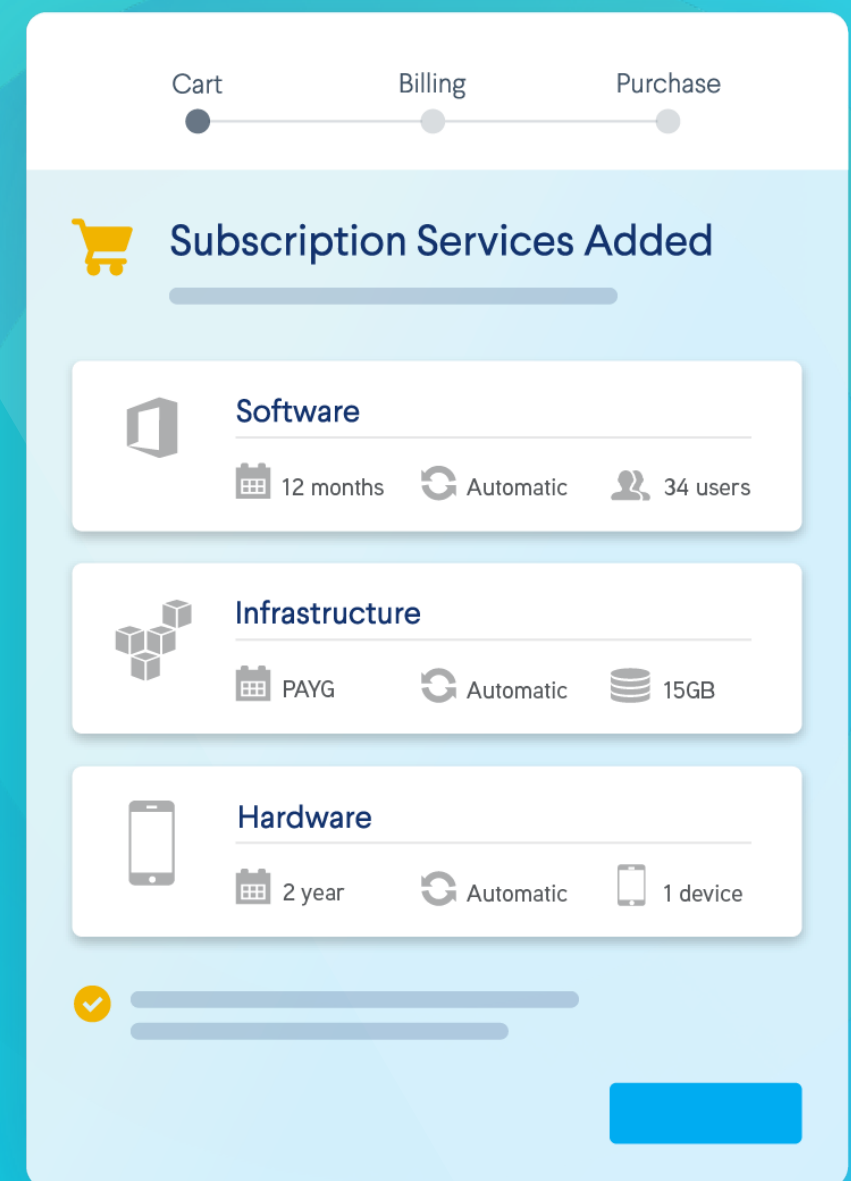


NEW GUIDE

7 Best Practices to Secure IaaS Sales on Your Digital Marketplace

Consumers of IaaS look to the reseller community to help them avoid the near limitless risk of IaaS overconsumption



GUIDE

In 2018, Tesla suffered one of the first high-profile crypto-jacking incidents in an attack that also compromised sensitive data. Worse, they didn't even discover the breach themselves. Redlock, a cybersecurity firm, discovered that hackers had infiltrated Tesla's systems through an unsecured Kubernetes administration console and from there compromised their Kubernetes pods. Redlock reported the breach immediately to Tesla, ending an embarrassing and potentially dangerous incident for the world's most valuable automaker.

Since then, the hacking community has only intensified its targeting of IaaS. Last summer, Ermetic announced the results of a study done in partnership with global intelligence firm IDC¹, which found that of the 300 companies they surveyed, 79 percent experienced a cloud breach in the past 18 months, while 43 percent reported 10 or more breaches in that timeframe. The problem will continue to grow as IaaS expands, because it offers a wealth of data that can be stolen or held for ransom and nearly limitless computing resources that can be exploited for gain.

A lot of companies understandably have reservations about moving to the cloud, even as they realize that it must be one of their top strategic priorities to remain competitive. These reservations are what lead them to consider purchasing IaaS from a reseller, rather than directly from a hyper scaler like Microsoft, Amazon, or Google. Those resellers offer value-added services that can ease that transition to cloud infrastructure by helping companies avoid configuration missteps that can lead to inadvertent overconsumption or security breaches.

"In most cases the Cloud-Native-Breach is an opportunistic attack on data left open by errors in how the cloud environment was configured. About 99% of misconfigurations go unnoticed by companies using IaaS"

MCAFEE
CLOUD-NATIVE. THE INFRASTRUCTURE-AS-A-SERVICE (IAAS) ADOPTION AND RISK REPORT. 2019



Those missteps can be costly if they're detected too late. Consumers of IaaS need to be especially vigilant, since most IaaS bills are post-paid and only available at the end of a billing period. Thankfully best practices can be established that mitigate the two main challenges in reselling IaaS: helping customers build secure IaaS environments and creating secure customer-focused marketplaces.

Successful IaaS Practices

At the core of a successful cloud-based marketplace must be sound operational practices that secure transactions and allow trusted relationships to be built between the marketplace, its vendors, channel partners, and the companies that purchase and consume their services. When fraudulent transactions take place, companies scramble for their commercial agreements to determine who bears fiscal responsibility, as relationships and reputations get put at risk. The post-paid billing relationship between the IaaS provider, the reseller, and the end customer makes IaaS an attractive target for bad actors, since it offers the possibility of avoiding early detection.

Bad actors will follow familiar tactics, such as posing as legitimate customers, using real company information, stolen credit cards, or phishing tactics to fraudulently obtain credentials that will grant them access to IaaS resources. Fraud and phishing are popular techniques because they're comparatively low effort techniques when compared to the effort necessary to compromise the sophistication of modern security systems. Sound knowledge about those security systems and the infrastructure into which they are embedded is required for those systems to be successful. Compared to phishing, gaining access to a misconfigured system is next to effortless.

Consider that Redlock reported² that gaining access to Tesla's systems was uncomplicated, the administration console wasn't password protected. Yet, the exploitation of the breach after they gained access was sophisticated and novel in its approach. The hackers used multiple evasion techniques to allow the breach to remain undetected.

These efforts included hiding the mining pool server address to avoid IP/domain based threat detection efforts, as well as configuring the mining software to not elevate the CPU usage to avoid consumption-based detection. Proper configuration could have prevented the initial breach. A refined approach would have been needed in their detection systems to discover that their systems were compromised after the fact.

Beyond bad actors looking for digital or human vulnerabilities, well-intentioned employees can inadvertently cause overconsumption of IaaS resources through infrastructure misconfiguration or missteps in architecture or solution design. With software cycles having accelerated to weekly or even daily deployments, companies can introduce security vulnerabilities in deployments, make mistakes in automated testing that strain resources, create logical errors that consume more storage or processing resources than anticipated, and other issues that can drive unexpected IaaS costs. Throw into the mix the power of auto-scaling or serverless function as a service (FaaS) computing (for example, AWS Lambda, Azure, and GCP FaaS offerings) that can consume resources seemingly without limit, and costs can rapidly balloon out of budget. As part of a risk management strategy for IaaS, monitoring practices that can detect engineering errors must form part of the core security of the platform.

In sum, cloud security for IaaS means guarding employees against fraud and phishing attacks, configuring the IaaS environments correctly, and operating those platforms over time with a sound security framework and well-developed practices. Companies looking to move their solutions onto cloud infrastructure need to consider IaaS security as a prerequisite to healthy commerce in the cloud.

Addressing the IaaS Skills Gap

Accessing those skill sets that will allow them to secure their environments can pose a significant barrier to entry for many companies. In the same study referenced above, Ermetic announced that the top operational challenge faced by companies is finding personnel with the expertise to secure their solutions





According to McAfee's risk report³ on IaaS adoption, lack of staff with the skills to secure cloud infrastructure was the leading cause of IaaS security issues from the companies they surveyed. The results can be catastrophic, as Capital One found out in the highly publicized breach of their AWS environment in 2019 that saw the theft of 106 million credit cards and other confidential customer information. The cause? A misconfigured Web-Application-Firewall (WAF) that was assigned too many permissions. The example is an echo of Tesla's experience. Even large companies can lack the appropriate skills sets to protect their cloud infrastructure and make missteps in their rush to adopt cloud services.

It's abundantly clear that companies need assistance in securing and managing their cloud infrastructure and that they are aware of it. SMBs specifically are aware of this skill gap and it is at the top of the reasons why they look to buy IaaS from resellers instead of directly from hyper scalers like Microsoft, Google, and Amazon. A recent AppDirect [study](#) found that SMBs prefer to buy from resellers because they understand the SMB's business needs (66 percent), because resellers are seen as trusted consultants (60 percent), and for the support resellers can offer them (63 percent). For IaaS resellers, there is a clear benefit in providing value-added services. Those services allow them to help their customers keep their core business in focus during their move to the cloud without the distraction of building expertise in new areas first.

IaaS resellers who can become a trusted partner for their customers through their value-added services are also setting themselves up for success by dodging a potential security pitfall of their own. Customers whose IaaS environments have been compromised through a security or a misconfiguration breach pose a liability risk to resellers that will still have to compensate the cloud provider. In helping to secure their customer's infrastructure, cloud service providers de-risk their own operations. This will allow consumers of IaaS to accelerate their strategic cloud ambitions worry-free the reseller, as a trusted advisor, scales out complementary services without worrying about their customers' inexperience.

"Often consumers accelerate the journey to the cloud without proper planning... leading to an overconsumption of IaaS, PaaS, SaaS services across their CSPs."

VIKRAM KUNCHALA, PRINCIPAL
DELOITTE RISK & FINANCIAL ADVISORY



GUIDE



Best Practices for Securing IaaS Sales

Building secure IaaS experiences for your customers must begin before, be embedded during, and live on after your sales process. Tailoring your catalogue to your customers' needs, managing their experience in your pre-sales process, and offering them services to manage their post-sale security will be key to getting them successfully and securely launched in the cloud.

Best Practice #1: Prioritize an Assisted Sales Model

Because lower friction transactions typically drive more sales, it can be tempting to reduce the checks and balances in digital marketplaces in exchange for a better user experience. Because self-service e-commerce models are very familiar today, it may also seem natural to offer self-service for IaaS purchases.

However, an assisted sales model is the quickest way to bring your marketplace online for both you and your customers. It will allow you to avoid early threats from bad actors looking to compromise your sales process by requiring more validation at the outset. It will also offer your customers a high-touch customer experience as you introduce a new marketplace and give them time to appreciate the benefits. That high-touch experience will be essential in helping you and your customers understand how you can help them cover any IaaS skill gaps they may have in their business.

In short, focusing on assisted sales instead of self-service will get you to market more quickly while allowing you to secure your marketplace and help your customers secure their environments. From that starting point, you can iteratively improve the experience for your customers as you learn to engage in these new ways together.

Best Practice #2: Demonstrate The True Value of an IaaS Reseller

Using that assisted sales model, get to know your customer's business so that you can add value by rounding out the gaps in their team with your own expertise. In offering your own or reselling a partner's managed service or security consulting offering, you can lower their barrier of entry to the cloud. With them relying on you to manage their infrastructure, they can focus on their core business instead of focusing on building out new technical expertise.

In addition to managed services and security offerings, consider how you can best guide your customers to the top IaaS and SaaS security practices, whether that's through training, professional services, or support.

Here is a shortlist of areas of where they may need you to lend them your expertise:

- Adopting a security framework
- Training and tools for their staff
- IaaS configuration/setup
- Securing credentials
- Monitoring tools, processes, and alerts for their:
 - IaaS usage
 - Network
 - End-point
 - Applications & services
 - Active processes
 - Message queues
- Access Control, including
 - Identity access management
 - Firewalls
 - Web Application Firewalls
 - Whitelisting/blacklisting sites, IPs, or geographies
- Data protection
 - Disaster recovery processes
 - Data backups
 - Data encryption (in transit / at rest)
- Incorporating regular security audits as a best practice
- Building IaaS security audits into their CI/CD pipeline



GUIDE



Best Practice #3: Simplify IAAS Offering for The Customer

Your customers have a lot to navigate as they begin their journey into IaaS, and lack of skills and expertise is likely at the top of their list of challenges. They may already have an idea of what cloud provider they'd like to start with, or they may be looking for a reseller that has a multi-cloud offering that can help them make a decision. If they're approaching the problem on their own, they'll need to work through the offerings of the different cloud providers to determine which suits their business best. Coming to a trusted advisor will help them get there more quickly.

They'll also need help understanding the complex commercial arrangements between the different cloud providers. What are their responsibilities, your responsibilities, and the cloud provider's responsibilities?



GUIDE

Consider how your team can simplify and explain the shared responsibility model and how it differs between providers in a multi-cloud environment. Lending them your expertise will help them make an informed decision from the outset. Demonstrating the complexity of these relationships may also help them make a decision about which responsibilities they want to take on and which they might want to have a managed service provider take on for them.

Best Practice #4: Use The Partner's Tools

Each IaaS provider offers a host of tools that can help you and your customers manage your IaaS offering. For the reseller community, you will find tools that allow you or your customers to set spend thresholds and configure alerts. Having the right alerts in place can help you advise your customers that there may be an issue with their consumption before they get to the end of the month. One best practice is to review monitoring and consumption reporting as often as daily or ensuring there is adequate automation to raise alerts as immediately as the information is available from the cloud provider. With the speed at which resources can be consumed, potential issues cannot be identified early enough. Leveraging your partner's tools or offering supplementary value-added monitoring tools or services can help fill the gap for your customers.

In addition to the software tools that they provide, hyper scalers also provide rich documentation resources, as well as first- and third-party tools that can be used to secure IaaS environments.

Best Practice #5: Vet Your Customers & Your Channel Partners

If you are selling IaaS today and have established customer and partner vetting practices, keep those best practices in place on your digital platform. Vetting practices like credit checks, references, address validation, and others offer tried and tested means of identifying potential fraudsters looking to get access to your resources. With the post-paid nature of IaaS, these practices are essential to securing your selling process and your marketplace.

These practices don't just help weed out criminals. They also help you better understand and engage with your legitimate customers, as you understand their buying power and their tolerance for fiscal risk. When you understand these aspects of your customers, you'll be able to better understand how to engage with them digitally and answer important questions, such as whether or not you should accept payment by credit card or by invoice only.

Best Practice #6: Control Access

Just as you need to know who is buying from you, you have to know who is connecting to your products, services, and marketplaces. The technical way to achieve this is by federating identity and access management (IAM) across all platforms using your corporate identity provider (IDP). Providing a federated IAM solution not only increases your solutions' security by simplifying your security processes, it also can improve the user experience if you implement single sign on (SSO), and allow you to more easily introduce additional security measures, like multi-factor authentication in a standardized way across all touchpoints.

Federated identity control will allow you to more easily extend existing employee, customer, or partner on-boarding and off-boarding procedures. As you stand-up your first marketplace or are auditing your existing one, revisit your current access control security policies. Are they sufficient for your new digital marketplace? Maybe you'll want to introduce a new policy, like disallowing the use of non-corporate email addresses.



Best Practice #7: Educate Your Staff

If there's a common thread between every article, book, or consultation on cloud security practices on the market today, it's this: train and educate your staff. They are your frontline security. Whether it's recognizing a phishy email or a phony invoice, mistakenly clicking on a link to malware, giving the wrong information over email, or applying these best or worst practices to their daily interactions with your systems, your employees are the ones who will compromise your systems or save them. Keep them up to date on the external threats your business is facing. Make sure they're getting refresher training. And, most importantly, make sure they understand the new unique challenges that might be introduced by IaaS and other sales on your digital marketplace.

Conclusion

If they were driven by price alone, two-thirds of the SMBs would choose a cloud provider over the cloud reseller. Your customers are coming to you for your expertise. Lending them that expertise re-affirms why they selected you in the first place.

The best practices described here will allow you to establish a set of standards that will allow you to protect the integrity of your marketplace and your customers' IaaS investments. And in building that trusted system, you are establishing a foundation for an ecosystem where your customers, partners, and your business can thrive and scale without worry.

About AppDirect

AppDirect offers a subscription commerce platform that removes the complexity of building a recurring business model. Sell any product, through any channel, on any device—as a service. Our platform opens up endless opportunities for commerce innovation, giving businesses the freedom to grow. We power millions of subscriptions worldwide for organizations like Jaguar Land Rover, Comcast, Sage, Keller Williams, ADP, and Deutsche Telekom.

For more information visit www.appdirect.com



GUIDE