7 Essentials for Public Cloud Security Optimization

CloudBolt software

CloudBolt software

Where are you in your public cloud security journey?

Public cloud adoption is exploding. Gartner forecasts worldwide public cloud end-user spending to grow 18% in 2021 to $304.9 billion. Organizations are taking hybrid and multi-cloud approaches to digitally innovate, modernize processes, build efficiencies, and collaborate among teams. With the right public cloud approach, your development team can get the resources they need fast to move your enterprise forward.

But with any technology, there is risk. Security breaches happen, and the proliferation of public cloud has given rise to shadow IT and other threats to your critical data and infrastructure. A recent market report indicated that **83% of organizations believe security is a huge challenge**. There are numerous points of potential failure in your enterprise and understanding them early can be the difference between averting disaster and not.

Here, we cover the seven essential tips every enterprise needs to consider to keep their public cloud environments secure.

Tip 1: Avoid Getting Run Over by a Cloud Shared Security Model

CHALLENGE

In the world of public cloud, it's important to remember that security is a two-way street. The security onus does not fall solely on the platform vendor, nor does it fall solely on the end customer. This is why the Cloud Shared Security Model exists. However, there are obligations you must meet in order to keep your data safe and in the right hands. The key is knowing what parts you are responsible for as a user and what parts the cloud platform provider must do. And, you can't forget about app security either.

SOLUTION

Know your responsibility as a customer. For your public cloud, have you turned on important features such as multi-factor authentication or set up all of your root account capabilities? Don't underestimate the fundamentals of good security on your side of the equation. Are you cloud services configured correctly? And what about that relationship with your applications in your environment?

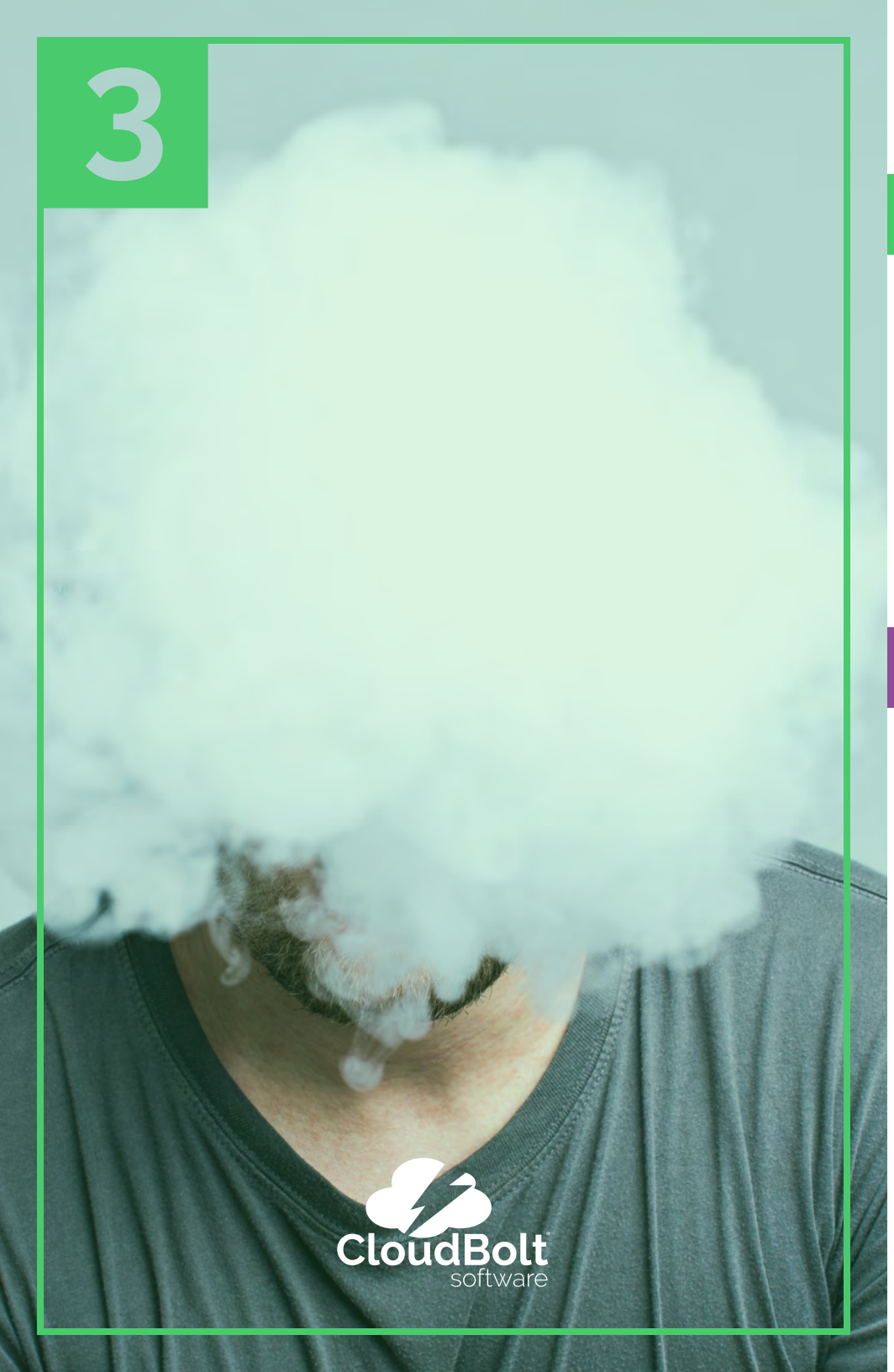
Tip 2: Don't Let Your Public Cloud Setup Set You Up for Failure

CHALLENGE

Public cloud services connect to many different aspects of your enterprise. These interconnected tools can pose numerous risks if they aren't configured correctly. One incorrect configuration could snowball into a much bigger threat if it isn't identified and corrected. The numbers in the market bear this out: 66% of organizations leave back doors open to attackers through misconfigured cloud services and 22% of breaches are through cloud resource misconfiguration, according to the 2020 Sophos State of Public Cloud Security Report.

SOLUTION

Establish best practices for your configuration process to ensure what you've done is correct. Mistakes can always still happen, so use solutions that identify potential misconfigurations proactively. For example, make your resource provisioning leverage blueprints that can be made robust enough to avoid misconfigurations through right input fields.



Tip 3: Make Visibility the Priority

CHALLENGE

Sure, cloud implementations are supposed to make life easier for your entire organization, from IT through developers on down. But, sprawl can be a headache for people managing cloud environments. For example, you could have 750 S3 buckets spread across 30 different AWS accounts. Do you have a view into how many of those buckets are publicly accessible? Do you know who has access to them?

SOLUTION

Take all the necessary steps to ensure visibility into your entire public cloud infrastructure is in place. You need every detail of your cloud configuration, from VPC CIDR, ELB Security Groups, DB encryption and more, at your fingertips at a moment's notice. This way you'll mitigate the issues that could arise from the unintended consequence of factors such as shadow IT. This will also help you drive more accountability in the environment.

Tip 4: Nail Down Access Management or Risk Getting Hammered

CHALLENGE

Whenever there's something new in technology, whether it's new in public cloud or some other area, it's a common pitfall to sit in awe of how cool it is and forget about the fundamentals of good security posture. One of those fundamentals is about access management. According to the Sophos report, 33% of organizations reported that cybercriminals gained access by stealing cloud provider account credentials. In fact, 91% of users had overprivileged Identity and Access Management roles.

SOLUTION

Having a robust access management system can't be a "nice to have" in the current public cloud climate. Always know exactly who has access to what, with full auditing and logging capabilities in the backend. Ensure your policies around privilege escalation are constantly being reviewed and updated so everyone has least privilege at all times. Use role-based access control to stop bad actors from accessing your sensitive workloads and data. You can further automate this by establishing approval workflows for sensitive/expensive data or resources and making that part of your provisioning process.

5

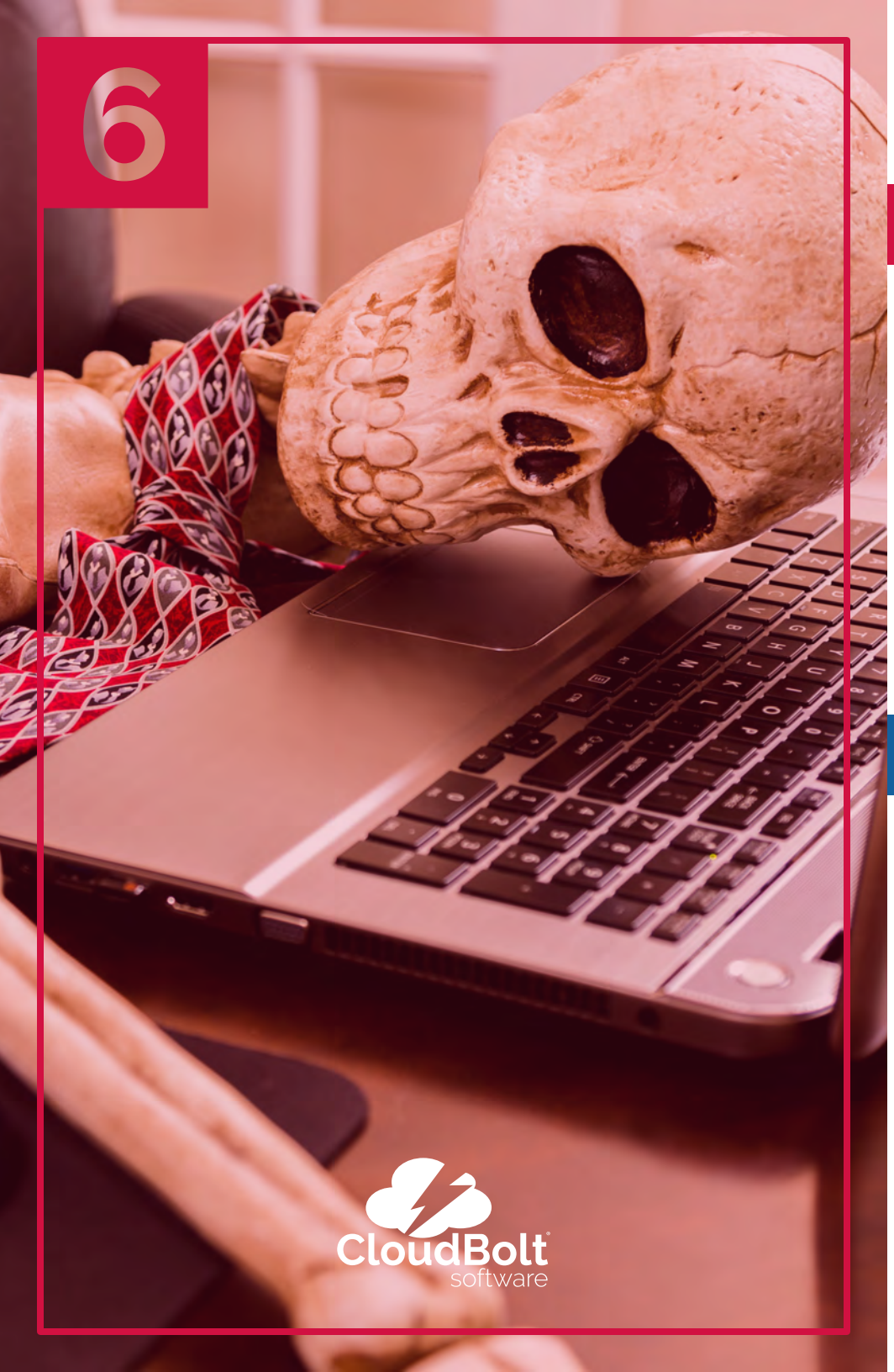
Tip 5: Build Security into Your Development Process on the Front-End or Prepare to Look Like a Back-End

CHALLENGE

You've probably heard of, or been directly involved in, a scenario like this: A dev team builds an app that needs to be in production but gets held up because the security team realizes there are lots of gaps. This can lead to delays or a push to get the app into production and fix the security issues later, which doesn't always end in the best result.

SOLUTION

A surefire way to avoid the mess: build security into all processes around development. Much is made in the public cloud world about a "shift left" mentality for DevSecOps, or building security into every part of the development process, and in the long run it's the best method for keeping your offerings secure and all of your stakeholders happy. This way when there's an issue at any level—development, staging or production—the right alerts and sent and the right actions are taken to resolve security red flags.



Tip 6: Comply or Die

CHALLENGE

A decade ago, compliance management was extremely expensive. It took considerable investment to ensure your systems were compliant along important frameworks. Today, in the public cloud world, much of compliance management is automatable. With more awareness, especially at the corporate board level, about breaches and security vulnerabilities, knowing where you stand on compliance and having a good answer for it is key. Plus, it might be driven by industry standards depending on your industry.

SOLUTION

Understand the needs of your business when it comes to compliance, both from a regulatory and a non-regulatory standpoint. Whether it's CIS, or the AWS Well-Architected Framework, or something else, it's a smart practice to align what you're doing to a framework for solid compliance. Otherwise, what you're doing could be considered subjective and won't stand up to scrutiny. If possible, establish automated policies to track and alert about any deviations in compliance frameworks. You can then send these alerts directly to users or to various groups through emails, Slack or other means.

Tip 7: Create the Right Plan for When Things Go Wrong

CHALLENGE

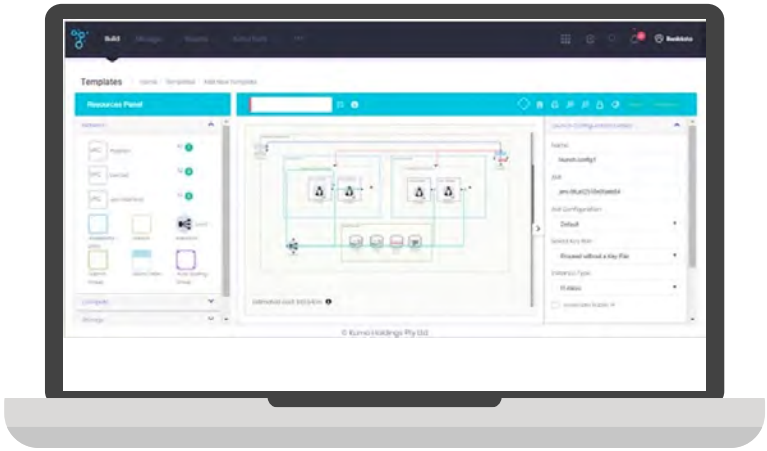
Now that you know about all the measures you need to have in place to make public cloud computing secure, it's important to know nothing is ever 100% foolproof or truly fully secure. You can only do your level best, and that includes planning for when things do in fact go wrong. Almost three-quarters of organizations hosting data or workloads in the public cloud experienced a security incident in the last year, according to the Sophos report.

SOLUTION

Develop a formal crisis response plan for what you'll do in the event of a security incident. Test your response on a regular basis. Ensure every important stakeholder in your enterprise is involved, has input, and understands their role. Run simulations. Make necessary updates to improve your processes for when a breach or other bad episode takes place. The last thing you want is to get caught flat-footed. Simple things such as recorded certified trainings for your employees on a bi-annual basis can keep everyone alert and make security everyone's priority.

Get proactive about your public cloud security posture.

Now that you've discovered the key essentials for improving your public cloud security posture, it's time to partner with a leader in the cloud management space to get the most out of your public/private/multi-cloud investment.



CloudBolt's Cloud Security Optimization features are vital to your public cloud success. Providing robust toolsets for multi-clouds and hybrid cloud environments, you can visualize and manage your security health with strong monitoring and real-time, actionable insight. Shake off the old way of securing your cloud and get the dynamic security solution you actually need to protect your multi-cloud environment.

Learn more here about how CloudBolt provides enterprise-grade cloud security optimization for your organization.

Visit www.cloudbolt.io to learn more or contact us now at sales@cloudbolt.io. Our team is ready to help you on your journey. Your path to better public cloud security awaits.

CloudBolt software

Join the conversation

CloudBolt Software is the enterprise cloud management leader. Our comprehensive solutions for IT automation, orchestration, self-service IT, cost optimization, and security help enterprises simplify complexity and achieve rapid time-to-value anywhere on their hybrid cloud, multicloud journey. Our award-winning cloud management platform and infrastructure integration services are deployed and loved by enterprises worldwide. Backed by Insight Partners, CloudBolt Software has been named one of the fastest-growing private companies on the Deloitte Fast 500 and Inc. 5000 lists. In addition, CloudBolt is 2020 CODiE award winner for best cloud management and featured in Gartner's Magic Quadrant for Cloud Management Platforms.

WWW.CLOUDBOLT.IO INFO@CLOUDBOLT.IO 703.665.1060