ALERT LOGIC™

KEY STEPS IN

Defining a Shared Responsibility Model for Public Cloud Environments

Understanding the crucial role organizations play in securing their “cloud-first” business initiatives from cybercriminal activity.

Executive Summary

Cyberattacks are on the rise, and organizations of all sizes are being targeted daily with more sophisticated threats. With the explosion of public cloud adoption in recent years, cybercriminals are catching up and have found ways to broaden their attack scope that now includes both traditional infrastructure and cloud environments. It's imperative that all organizations understand the strategic role they play in defending their cloud-based infrastructure from the breadth of vulnerabilities being exploited by cybercriminals. An important element of that defense is knowing which parts of the cloud they and their service providers are responsible for and, based on that, building plans for how they'll protect their business and their users in the months and years to come.

INTRODUCTION

Determining "Responsibility" for Cloud Security

Every day, more organizations are adopting "cloud-first" strategies, shifting core business processes to public cloud systems and services. And though security concerns have been a barrier to digital transformation and cloud adoption in the past[1] , it's clear from the latest market projections—which see worldwide spending on public cloud services and infrastructure reaching US$210 billion in 2019 (up 23.8% over 2018)[2] —that the industry now prioritizes the benefits of the shared cloud model over potential security risks to businesses and their customers.[3]

As more organizations of all sizes and types take their businesses to the cloud, they're able to take advantage of the latest cloud security tools and services to augment their existing system safeguards.[4] Yet, these tools and services can lend a false sense of security if they have not also reconfigured their security strategy for a cloud model, because ultimately, the responsibility still rests on the customer to understand the evolving attack surface, determine how best to leverage the tools offered by cloud providers, and augment with third-party security services to alleviate the burden on internal delivery and operational teams.

61%

of U.K. and U.S. based CISOs

Many businesses—especially SMBs—continue to struggle with misconfigurations, which can lead to costly security vulnerabilities.

Survey commissioned by Nominet

With Public Cloud Environments, Security is a Shared—But Separate—Responsibility. Based on the Shared Security Responsibility Model (see Diagram 1), public cloud providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform take responsibility for the physical security of their infrastructure, networks, and foundational services. Meanwhile, the onus is on customers to correctly deploy and maintain the security of everything within their respective cloud(s). This includes configurations, installations, administration, and ongoing upkeep, not to mention their own intra-organizational protection and privacy protocols.

Anything the customer loads or does via shared cloud platforms is the customer's responsibility. As such, it stands to reason that when customers use public platforms for their data-driven business activities, their protection protocols shouldn't look and feel too different from security processes used for securing data hosted on-prem or in secure data centers.

However, because the common, overarching assumption is that public cloud providers are protecting their platforms as well as all of the activities and customer data hosted there, it's easy to lose sight of the fact that customers are equally, if not even more accountable, for protecting their cloud-based business. And when customers neglect to keep up their side of the SSRM, they're unwittingly putting their businesses at risk from potential vulnerabilities that come with the cloud's larger attack surface.

62%

identify misconfiguration of the Cloud as their biggest risk.

2019 Cybersecurity Insider AWS Cloud Security Report.

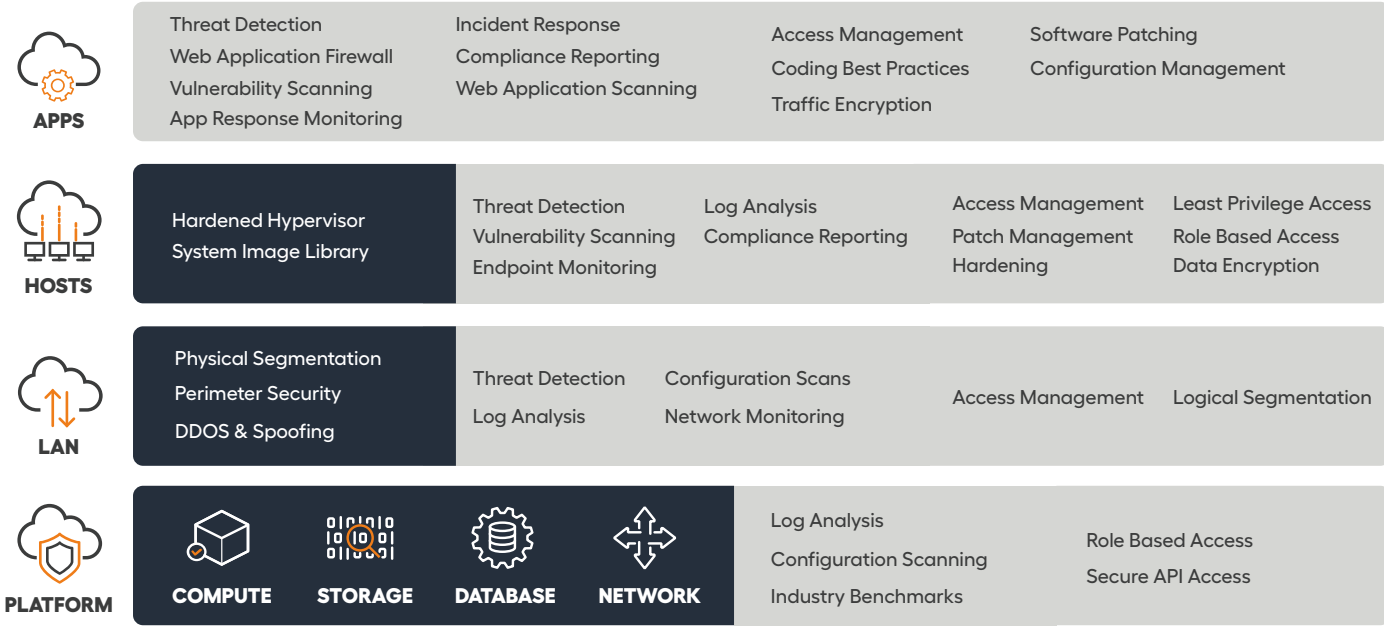


Diagram 1.Shared Security Responsibility Model (SSRM)

When Cybercriminals Strike Customer Vulnerabilities.

In July 2019, Capital One banking firm announced that a massive breach had exposed the personal and financial data of 106 million users. Paige Thompson was later indicted in connection with the crime, as well as for breaching thirty other organizations.[5] Thompson reportedly used a Server-Side Request Forgery (SSRF) attack to access the data through a customer-side misconfiguration of the customer's open-source Web Application Firewall (WAF).

Following the announcement, Amazon confirmed that "AWS was not compromised in any way and functioned as designed."[6]

Meanwhile, Capital One's shares fell 10%, while steps taken to notify victims and offer free credit monitoring and identity protection were expected to cost US$100–150 million.[7]

What You Don't Know About Your Cloud Security Can Definitely Hurt Your Business and Your Users

While the cloud itself is not inherently risky, it's the areas that customers often overlook from a security perspective that open them up to potential exploitation from cybercriminals.

Just as Cloud Technology Continues To Evolve, So Too Do Cybercriminals' Techniques. Today's cybercriminals are using increasingly sophisticated methods to find and infiltrate vulnerable systems. Customer SaaS applications are especially vulnerable to attacks. At the same time, the containers used to host cloud-based servers, databases, and the like are also highly susceptible to potential vector attacks[8], including OS exploits, container breakouts, denial of service, embedded malware, and credential theft[9] that are made possible when customer-side configurations, access management, and settings aren't updated on a regular and frequent basis.

Cyberattacks Hit All Sizes and Types of Organizations. Nearly half of all cyberattacks are committed against small businesses, according to Verizon's annual Data Breach Investigations Report.[10] Yet, our Alert Logic 2019 Critical Watch® Threatscape Report uncovered alarming evidence that small- and medium-sized businesses (SMB) are not adequately protecting their cloud-based initiatives. Encryption-related misconfigurations remain the largest group of SMB security issues; among the top workload configuration issues, 66% were related to weak encryption, including SSL ciphers, MAC algorithms, and TLS 1.0 encryption protocol.

of unpatched vulnerabilities in the SMB space are more than a year old.

Many businesses—especially SMBs—continue to struggle with misconfigurations, which can lead to costly security vulnerabilities.

Alert Logic Critical Watch Report

These and other results indicate that encryption is not yet an instinctive behavior, despite being a best practice and a requirement of many current regulations and legislation.

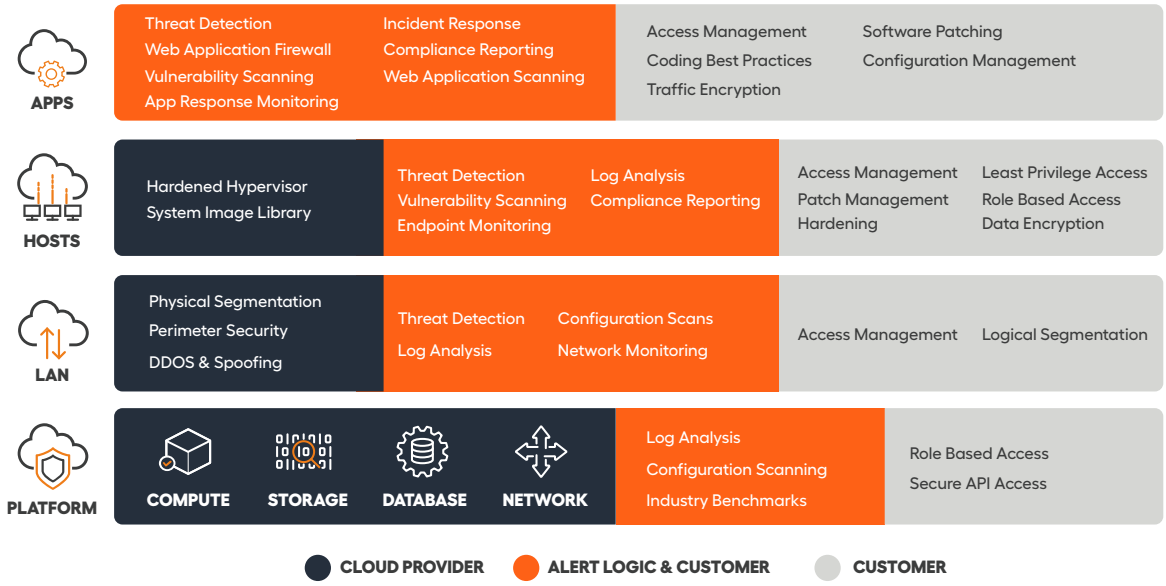
What's at Stake When Organizations Maintain Weak Encryption and Leaky Bucket Configurations? Ultimately, cybercriminals don't have to work very hard to infiltrate poorly secured systems, even if they're hosted in the cloud. The result: business and user data, security credentials, and other sensitive information become easy pickings on GitHub and the dark web.

SOLUTION

Use the SSRM to Build a Cybersecurity Defense Plan to Future-Proof Your Evolving Cloud-Based Business Initiatives

Given the increasing frequency of cyberattacks on businesses in all industries, we recommend that "cloud-first" businesses take these five steps to build their cybersecurity defense plans, in order to future-proof the security of their current and future public cloud-based initiatives:

1. **Assess your current security maturity level.** Using the SSRM as a foundation (Diagram 2), conduct an in-depth review of each layer of public cloud engagement, confirming the layers that you're responsible for—especially, focusing on the top three layers (i.e., apps, hosts, and networks) where customer involvement in security upkeep is most crucial.

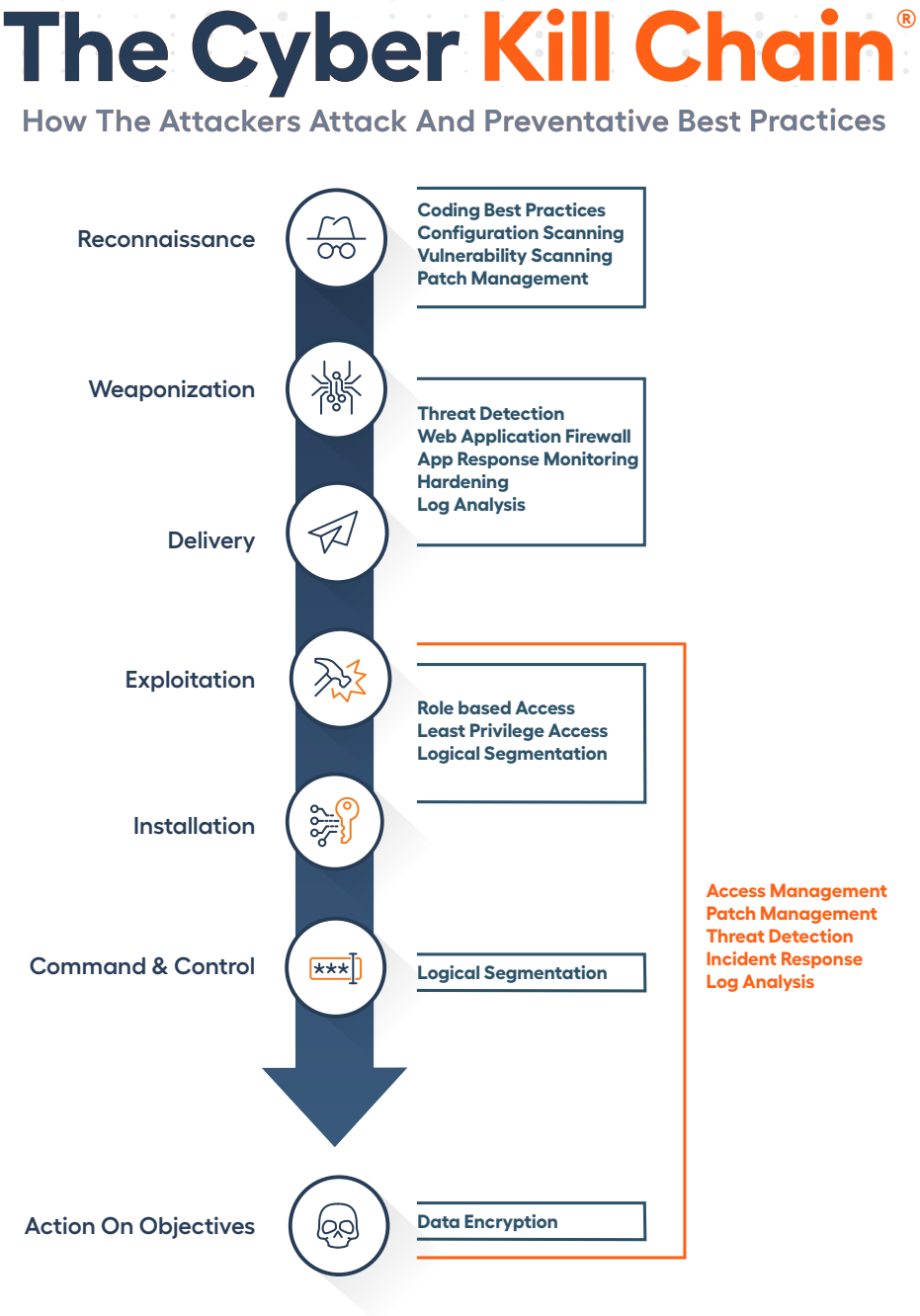


2. **Determine action steps to fill in security gaps.** Based on your findings in Step 1, go through the four layers of the SSRM and identify the steps you'll need to take to bolster your security protocols at each level, using the cyber kill chain (see Diagram 3) as a guide to prioritize increased protection measures where you need them most.

A NOTE ABOUT FILLING GAPS IN YOUR SECURITY COVERAGE: Depending on the extent of your in-house IT and operations capabilities, you may find it beneficial to work with a threat management provider, like Alert Logic, that combines industry-leading technology, cutting-edge intelligence, and expert people-power to future-proof every area of your evolving business, without having to take on the work and cost of building out your own security solutions.

3. **Prioritize security in all future development work.** Once you've established an action plan to mitigate vulnerabilities, we recommend that you take a page from the Privacy by Design playbook[11] (the foundation upon which GDPR was developed[12]), and integrate security into the delivery pipeline at every stage of the development process, rather than it being left as a module that's added on at the end of projects.

4. **Fortify your environments against future threats.** Consider integrating the following areas into your defense strategy for added protection of your cloud security attack surface:
   a. Access Management:
      i. Maintain the principle of least privilege (POLP), limiting access rights for users to the minimum permissions they need to perform their work.



   ii. Identify integrations, ensuring access is locked.
   iii. Enable multi-factor authentication (MFA) for added security.

b. Logical Segmentation:
   i. Segment cloud accounts according to data sensitivity, developing a variety of models, including multi-account, by app and business units.
   ii. Build logical network boundaries to boost performance and limit unauthorized traffic.

c. Monitoring:
   i. Early detection of exposures is key to mitigating risk from insecure configurations or new vulnerabilities that may crop up in the cloud.
   ii. Continuous assessment of your environments is vital, as new vulnerabilities are uncovered every day, and not just after cloud provider-pushed system updates.
   iii. Mitigate the impact of attacks with proactive monitoring of networks and applications for known and unknown threats (especially zero-day attacks) that can expose critical business data.

5. **Socialize security across your organization.** Build a security-conscious culture, socializing the idea of "security in cloud-first" with all employees:
   a. Institute awareness training on an annual basis and after major incidents or business changes (e.g., system compromise, merger/acquisition, ERP implementation, new hires or fires).
   b. Train public-facing staff to recognize, handle, and report internal security infiltration attempts.
   c. Develop clear processes that employees can follow if they think they've detected security threats.

CONCLUSION AND NEXT STEPS

Expanding the Shared Security Responsibility Model

As more companies transform their business practices to meet the evolving needs of their consumers, organizations are moving to the cloud at an unprecedented rate. But, with the move to the cloud comes additional responsibilities on the part of customers—to keep their configurations, installations, and intra-organizational protection and privacy protocols safe from crafty criminals who are waging ever more aggressive attempts to breach cloud-based infrastructure, systems, platforms, and applications.

Organizations of all sizes and types have the power to protect themselves and their users from cybersecurity threats by taking a proactive approach that keeps shared security responsibility of cloud platforms top of mind, now and in the future.

Public cloud platforms provide the elasticity and agility your business needs to meet consumers demand at scale. Yet, customer tenancy comes with certain responsibilities—including staying up to date on the latest privacy and protection protocols that can keep your business-critical applications safe from cyberattacks.

If you're struggling to keep up, we can help! Learn more about our integrated security approach for public and multi-cloud workloads here.

About Alert Logic

Alert Logic is the industry's first SaaS-enabled managed detection and response (MDR) provider, delivering unrivaled security value. Since no level of investment prevents or blocks 100% of attacks, you need to continuously identify and address breaches or gaps before they cause real damage. With limited budget and expertise, this level of security can seem out of reach. Our purpose-built technology and team of MDR security experts protect your organization and empower you to resolve whatever threats may come. Founded in 2002, Alert Logic is headquartered in Houston, Texas, with offices in Austin, Cardiff, London, and Cali, Colombia, and online at alertlogic.com. **Alert Logic – our knowledge is your advantage.**

ALERT LOGIC™

SOURCES:

[1]*As suggested by studies cited in https://www.techrepublic.com/article/security-is-the-no-1-it-barrier-to-cloud-and-saas-adoption/*

https://assets.kpmg/content/dam/kpmg/ca/pdf/2018/03/cloud-computing-risks-canada.pdf

https://www.isc2.org/-/media/ISC2/Landing-Pages/2019-Cloud-Security-Report-ISC2.ashx?

[2]*https://www.idc.com/getdoc.jsp?containerId=prUS44891519*

[3]*https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/cloud-adoption-to-accelerate-it-modernization*

[4]*https://www.computerweekly.com/news/252470022/CISOs-think-cloud-safer-but-security-fears-remain*

[5]*https://www.wired.com/story/capital-one-paige-thompson-case-hacking-spree/*

[6]*https://www.newsweek.com/amazon-capital-one-hack-data-leak-breach-paige-thompson-cybercrime-1451665*

[7]*https://www.bloomberg.com/news/articles/2019-07-29/capital-one-data-systems-breached-by-seattle-woman-u-s-says*

https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/

https://appleinsider.com/articles/19/08/15/capital-one-hacker-investigated-for-30-more-data-breaches

https://www.forbes.com/sites/petercohan/2019/07/30/will-capital-ones-106m-name-data-breach-cut-into-awss-growth/#25b9b20e49d5

https://www.wsj.com/articles/capital-one-reports-data-breach-11564443355?

[8]*https://containerjournal.com/topics/container-security/the-4-most-vulnerable-areas-of-container-security-in-2019/*

[9]*https://www.oreilly.com/ideas/five-security-concerns-when-using-docker*

[10]*https://enterprise.verizon.com/resources/reports/dbir/*

[11]*See https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf for an outline of the seven foundational principles of the Privacy by Design framework.*

[12]*https://martechtoday.com/privacy-design-deeper-dive-gdpr-requirement-212463?*

ALERT LOGIC™