Cloud Application Security

The Amazon Web Services Shared Responsibility Model

Scott Fletcher
Solutions Architect
RedShield Security, LTD

The Preconceived Cloud Security Problem

Businesses are overwhelming realizing the benefits of adopting cloud infrastructure strategies. Software, Platform and Infrastructure "As A Service" options are supporting wholesale Digital Transformation for small to medium businesses and large enterprises alike. Eight out of ten organizations depend on cloud services for critical business functions including web application publishing, communication, productivity, application development, business intelligence, and disaster recovery and storage solutions[1]. With nine out of ten organizations significantly concerned about cloud security and the inherent risks to their data[2], an alarming number of organizations lack an effective strategy to manage vulnerabilities and risk within their cloud computing environments, mistakenly assuming that "my cloud provider takes care of security for me".

SaaS vs PaaS vs IaaS - As A What?

Software as a Service has revolutionized how organizations consume commodity services like email with industry leaders like Microsoft and Google now providing fully managed services, instead of simply supplying the software which you'd install and operate yourself. The majority of security professionals will agree that for most businesses operating a commodity service like email yourself introduces unnecessary risk, given the knowledge and ongoing time required to regularly upgrade, patch, to ensure it meets security industry guidelines. In this case outsourcing to an industry leader with significant resources and mature security processes not only reduces cost, but is an effective strategy to mitigate the risk of the system and data being compromised.

Infrastructure as a Service such as Amazon EC2 is the most commonly used cloud service. It allows companies to leverage a wide range of resources, also gaining full control over critical security aspects such as the underlying operating system which many bespoke enterprise level application ecosystems require. Infrastructure as a Service is just that, Infrastructure. Cloud providers offer a number of tools to secure and support Infrastructure as a Service environments however it's incumbent on the tenant to implement them. Secure cloud hosting requires new strategies and technologies however many organizations do not have, or are unable to find the resources to implement or maintain the security controls to achieve this outcome.

[1] LinkedIn Cyber Security Survey 2017

[2] LinkedIn Cyber Security Survey 2017

The IaaS AWS Cloud Security Shared Responsibility Model

Cloud service providers like Amazon Web Services invest significant resources placing the utmost importance on the security of their environments. Fundamentally this includes the availability and security of their global physical data center infrastructure, the virtualization hypervisor, and software defined networking components.

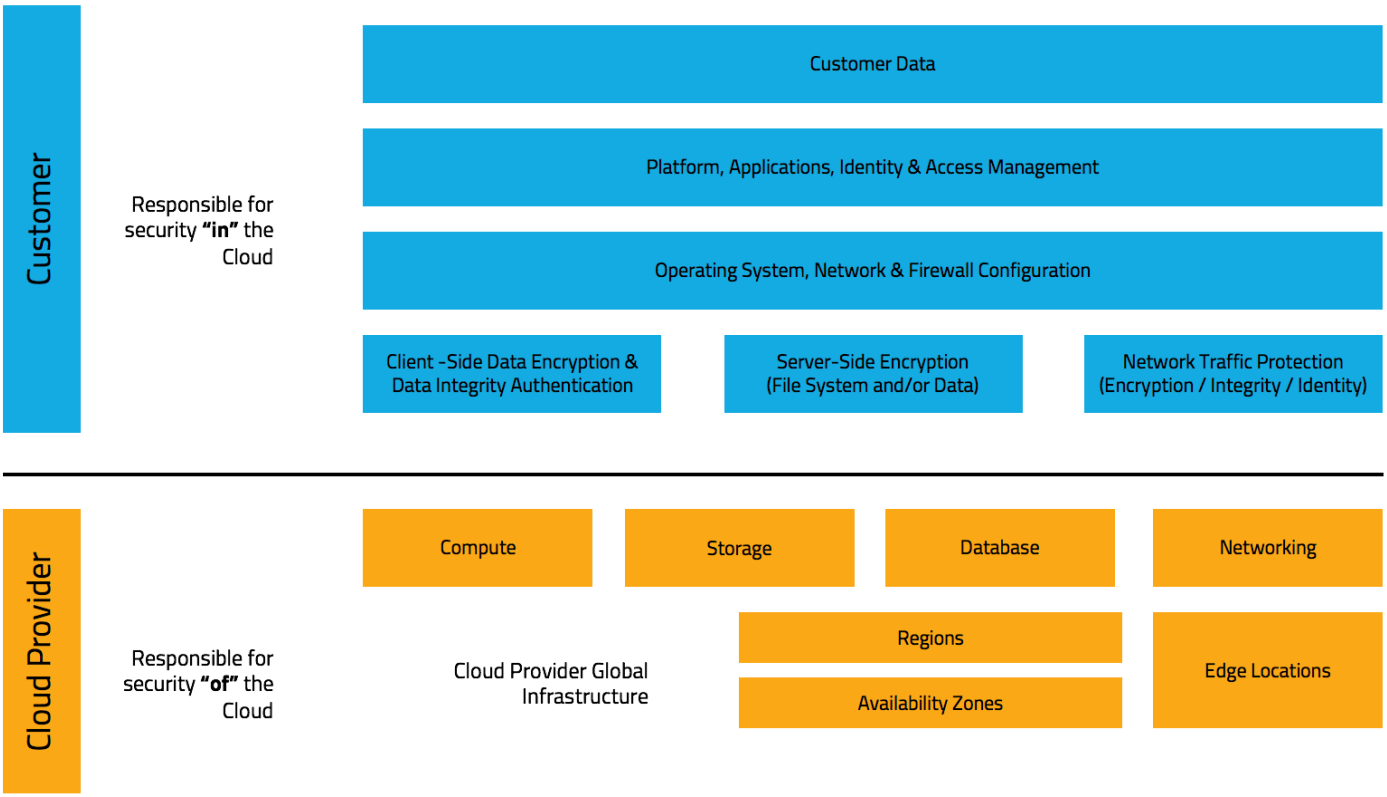

Figure 1: Amazon Web Services Infrastructure as a Service Shared Responsibility Model

The delineation for organizations using the most common Infrastructure as a Service is clear, everything you place in the cloud is your responsibility, including client and server side encryption, operating system, network and firewall configurations, vulnerability management and patching, identity and access management, the software you install, and your customers' data. Gartner cited the lack of assumed responsibility to be the primary factor when predicting that through 2020, 95% of cloud security incidents will be the fault of the tenant not the provider.

Managing security asymmetry has been a key challenge for cloud providers who have introduced additional platform, container, and abstract services to allow a cloud consumer to move some, or all of the security responsibilities to the provider themselves. Unfortunately, the benefits of such offerings are marred by the requirement of the cloud provider to restrict access to features and functionality that pose a security risk. Many of today's applications were not designed or built for cloud compatibility and rely on functionality that is only available as part of Infrastructure as a Service, leaving YOU, the cloud tenant squarely responsible for the security of the environment.

RedShield - Managed Application & Cloud Perimeter Security

Effective cloud security requires secure infrastructure, secure applications, and robust security operations. RedShield secures your network perimeter and hosting infrastructure following application agnostic industry best practices. Our core service mitigates DDoS attacks, enforces adherence to web protocols and standards, ensures behavioral compliance and fair use, while reliably blocking attacks and providing comprehensive protection for high-security environments.

With 84% of attacks occurring at the application layer and half of these involving business logic, the continued security of your cloud environment is dependent on an effective vulnerability management programme capable of addressing these complex issues. As experienced penetration testers, application specialists, network engineers, and technologists we've built an award-winning managed application and perimeter security service that redefines the AWS Cloud Shared Responsibility Model.

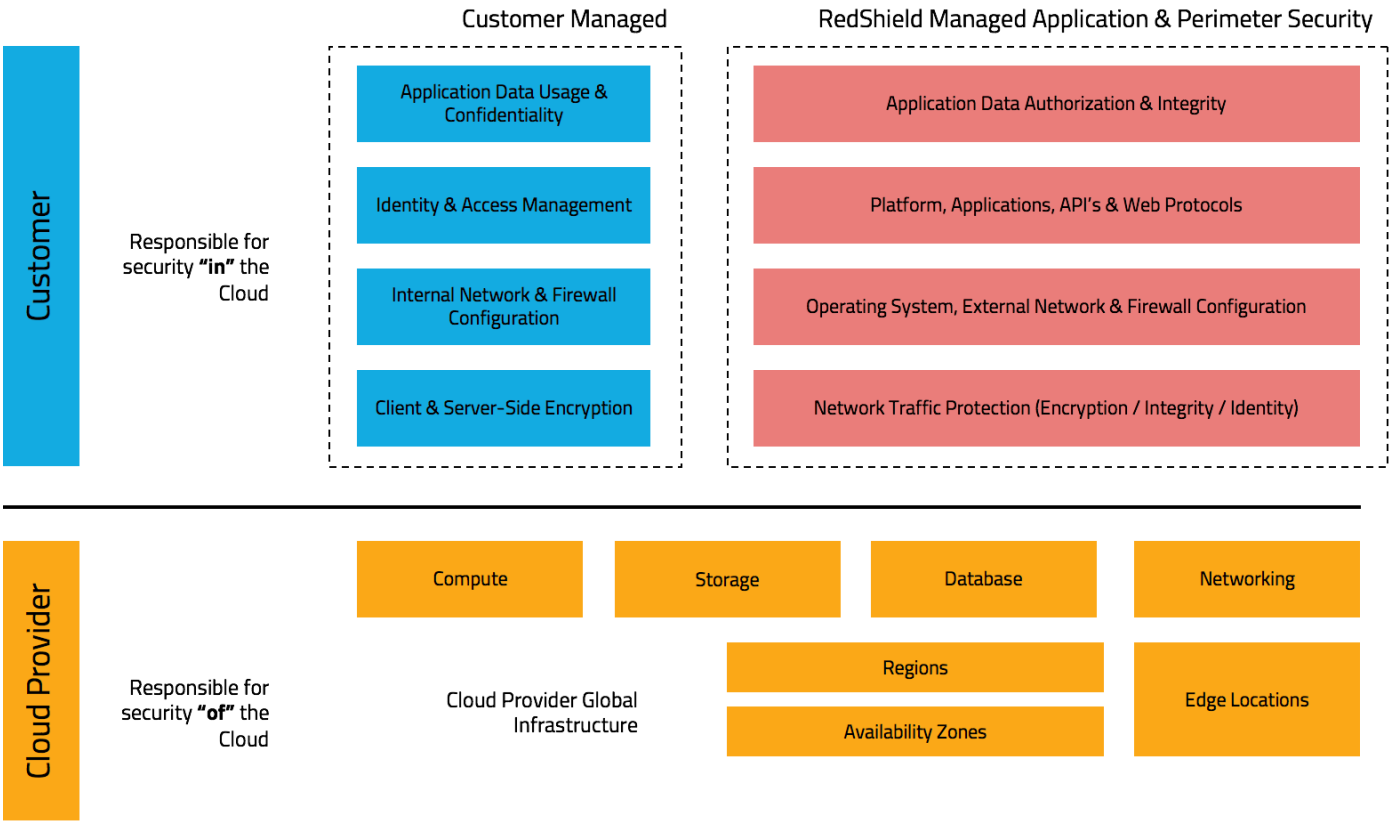

Figure 2: RedShield Infrastructure as a Service Shared Responsibility Model

RedShield simplifies cloud security. Whether you're building new or migrating an existing application, you must also secure the environment. Fundamentally maintaining a secure environment relies on an effective vulnerability manage programme and having available resources with the knowledge, experience, and tools, to provide continual assessment, analysis, and to take action when required.[3] RedShield's experts provide this comprehensive assurance and secure hosting solution for your cloud environment and applications through the use of Gartner Magic Quadrant tools, industry best practices, and mature security operations processes.

[3] https://www.sans.org/reading-room/whitepapers/application/building-application-vulnerability-management-program-35297

RedShield - Your 24/7 Cloud Security Operations Team

If cloud security was like a Formula 1 racing car needing servicing, RedShield are the pit crew; trained, well organized with the best tools, ready to deliver fast results. Conversely cloud security products including AWS WAF, Inspector, and CloudFront are tools; analogous with a torque wrench, useful in the right hands but do absolutely nothing on their own. Tools must be used by experts with the requisite knowledge and processes to deliver tangible results. Like a Formula 1 racing car, an effective cloud security program has numerous interrelated and dependent components. Using Maslow's theory, we are able to define and categorize the activities that are required to secure cloud hosted applications and environments:

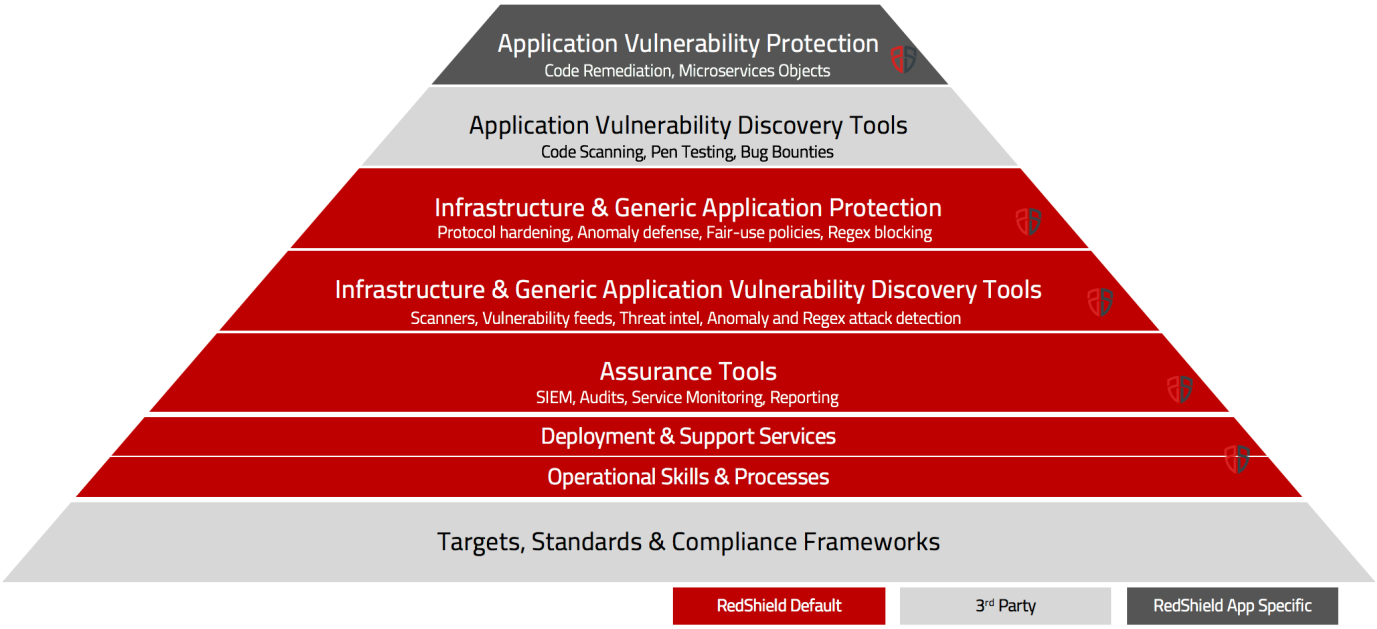

Figure 3: Web Application Defense Hierarchy of Needs

Securing Your Cloud Infrastructure

Secure applications rely on secure infrastructure. Our baseline deployment and service includes over 4700 custom shields for effective traffic hygiene and generic application protection. RedShield's integrated vulnerability management solution continuously scans your network and applications for security vulnerabilities, infrastructure misconfigurations, and verifies that deployed shields are working as expected. Results are available via our secure portal and reviewed daily by our team of security analysts who take all necessary actions to ensure your infrastructure meets security industry guidelines.

Amazon's Inspector offers limited vulnerability coverage, primarily focusing on the operating system, its configuration and required security patches. This inside out approach fails as it is not a true representation of

your Internet presence and completely omits web application layer vulnerabilities. An additional vulnerability scanning service would be required to detect infrastructure and application issues also leaving you responsible for interpreting results and patching vulnerable systems.

Securing Cloud Application Connectivity

RedShield secures connections to applications and services in your cloud environment. We provide complete SSL certificate lifecycle management, and maintain secure configurations that follow industry recommended guidelines to ensure the confidentiality and integrity of your application and users data. We can also provide solutions for legacy applications, and legacy application integrations that rely on potentially deprecated cryptographic libraries without compromising compliance requirements or the transmitted data.

Cloud providers adhere to strict guidelines and regularly change services, deprecating SSL protocols and cipher suites they deem to be insecure potentially causing connection failures for legacy applications. Content Distribution Network services like CloudFront also have strict SSL certificate requirements leaving you responsible for ensuring the correct certificate configuration and also certificate lifecycle management.

Cloud Application Acceleration & Monitoring

RedShield employs a number of strategies to accelerate your application, reduce latency, page load times and improve usability. We constantly monitor your application, its performance, uptime, and response metrics. We support all acceleration technologies including SPDY and HTTP/2 and configure these and deploy our proprietary acceleration shields as required. Application performance statistics, bandwidth utilization, and user metrics are available in real-time via our secure portal. Our 24/7 Security Operations Centre actively monitors all available performance indicators and will notify you whenever your application behaves abnormally.

Most cloud providers suggest using Content Distribution Networks like Amazon's CloudFront to accelerate applications. In all cases you are responsible for configuration and testing. In many cases acceleration is either "on" or "off" and unable to be customized. Often applications migrated to the cloud are not acceleration compatible leaving no cost-effective options to address performance issues.

Advanced Application Specific Shielding

Penetration Tests, Code Reviews, and incidents often reveal easily exploitable logic flaws. By maintaining application state and rewriting requests and responses RedShield can rapidly patch any application security issue. We have had exceptional success in mitigating issues that other security tools such as Web Application Firewall (WAF) and Next Generation WAF cannot solve.

Most cloud providers including Amazon offer an add-on WAF tool. These request admission filters do not provide a solution for business logic, authentication or authorization vulnerabilities often found by manual security testing. You are also responsible for preventing business disruption, your team must both optimize the rules to ensure that customers or developers are not frustrated by the WAF mistakenly blocking legitimate traffic and whilst also not permitting attackers to bypass or evade the WAF controls. Hansen et al[4] prove that with regex based input validation, like a WAF, is a very difficult task.

Managing Distributed Denial of Service & Anomalous Events

RedShield's 24/7 Security Operations Centre monitors all connections to your application, its performance, and response times to detect BOTS, anomalous and malicious traffic patterns. Our cloud platform responds to DDoS attacks from the first malicious request before it reaches your environment, securing and accelerating your application by offloading inspection of requests, detection and response of attacks to our high-performance platform.

Amazon recommends using CloudFront, their Content Distribution Network solution (CDN) as a means to combat DDoS attacks by routing application traffic via an edge location closest to the user. This hyper connectivity also benefits attackers who can now send even larger volumes of attack traffic to your application. Without adopting and thoroughly testing auto-scaling policies your environment would quickly become overwhelmed and fail. CDN's like CloudFront are also unable to automatically respond to DDoS attacks as they do not understand your applications ability to manage load. You are responsible for detecting application performance degradation and taking action by writing rules to block attacks using coarse controls E.g. deny all from an IP range, or rate limiting the number of requests per IP.

Detecting Attacks & Managing Security Incidents

RedShield monitors all aspects of the web dataplane including TCP, SSL/TLS, HTTP, Firewall, and Application. As an application aware service, we inspect and respond to every request before it reaches your environment. Our unique ability to detect and block attacks across a series of requests provides complete protection for complex issues like authentication, authorization and workflow exploits. Our 24/7 Security Operations Centre SIEM solution analyses all available logs providing real-time protection for your applications and environment.

Cloud providers do grant access to usage, debug, and security logs for services in use by a cloud tenant. It is your responsibility to consolidate logs for any additional systems and applications that you run in your

[4] https://www.blackhat.com/presentations/bh-usa-05/bh-us-05-hansen.pdf

environment. You are solely responsible for log consolidation, analysis, alert configuration, attack detection, and incident response.

Let Us Secure Your Cloud Environment

RedShield succeeds where Do-It-Yourself cloud tools and 3rd parties fail. Many cloud security tools are ineffective due to lack of skills and resources leading to poor configuration, lack of ongoing maintenance, or were simply never designed to solve today's cloud or application security challenges.

RedShield allows you to run your applications in a cloud environment without having to become a cloud or application security expert. With base security policies in place often in hours you can confidently migrate your application to the cloud knowing it's protected from day one. Contact RedShield for a no-obligation assessment today.

Contact: Sales@RedShield.co